Oracle® Communications Session Director

Maintenance and Troubleshooting Guide

Release S-D7.2.0

Formerly Net-Net Session Director

October 2013

ORACLE

Contents

About this Guide

The Oracle Communications Session Director Maintenance and Troubleshooting Guide provides information extending from hardware level functionality through system level tasks to real-time application statistics. This information is applicable for the Acme Packet 9000 session border controllers.

Supported Platforms

Release Version S-D7.2.0 is supported on the Net-Net 9200.

Related Documentation

The following table lists the members that comprise the documentation set for this release:

Document Name	Document Description
ACLI Configuration Guide	Contains information about the administration and software configuration of the SBC.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.

Document Name	Document Description
Accounting Guide	Contains information about the SBC's accounting support, including details about RADIUS accounting.
Release Notes	Contains information about the current documentation set release, including new features and management changes.

Revision History

This section contains a revision history for this document.

Date	Revision Number	Description
July 12, 2013	Revision 1.00	• Initial Release

1 Log File Management

Introduction

This chapter describes the logging system implemented in Net-Net OS D6.0 and higher.

About Log Files

Log files are a critical component of system management. Log files are used to assist with debugging, system management and optimization, and identifying potential security breaches or other nonstandard activities on the system.

Each task that runs on the Net-Net 9200 is capable of outputting log file messages. Because tasks are distributed throughout the Net-Net 9200, across feature cards, CPUs, and cores, the logging system is designed to conveniently centralize the output of all logs.

Net-Net OS Log Types

The Net-Net OS creates and maintains two types of log files:

- The Acmelog—This file is used to aggregate general system events that give an overview of the health and overall operating conditions of the Net-Net 9200.
- The Process Log—The process log is a file stored on a remote Acme Process Log server, on a local (to the task) core, or both. Process logs are a compendium of task log files, which are created by every discrete task that runs on the Net-Net 9200. The process log records as much or as little information as you require based on configuration parameters. The process log, located on a local core, is also available on the Net-Net 9200, accessible via FTP.

Log File Message Levels

Log files capture messages that describe task events. A system of 10 severity codes, the Acme Packet Log Level Enumeration, is used to label events from high to low significance. Emergency represents the most critical system affecting event, while Info represents the least critical system event. In addition, three additional Acme Packet log levels are used for debugging purposes.

Task Event Severities

For a given task, different events quality for different severity levels. The Acme Packet Log Enumeration levels (event severities) are listed in the following table. *Emergency* is the highest level while *Info* is the lowest event severity level. The remaining three levels, *trace* and *debug detail* are used for highly granular trace logging.

Acme Packet Log Enumeration	syslog Severity	syslog Numerical Code
EMERGENCY	Emergency (system is unusable)	0
CRITICAL	Alert (action must be taken immediately)	1

Acme Packet Log Enumeration	syslog Severity	syslog Numerical Code
MAJOR	Critical (critical conditions)	2
MINOR	Error (error conditions)	3
WARNING	Warning (warning conditions)	4
NOTICE	Notice (normal but significant condition)	5
INFO	Informational (informational messages)	6
TRACE DEBUG	Debug (debug level messages)	7

The table above also includes the syslog severity codes and their corresponding numerical codes. When the Net-Net 9200 sends messages to an externally configured Syslog server, the event severity closely matches with the Acme Packet Log Enumeration levels, as shown above.

Logtype Facilities

A logtype facility is a second filtering criteria used when writing to log files. The facility is a tag that describes the context of the event. Facility messages are filtered by the task and then by the mechanism that writes data to task log files to limit the amount of information that gets written into a task's log file.

For example, one logtype facility is *DNS*. By configuring a task to deliver *DNS* logtypes, for a given severity level and higher, the resultant log file would only contain messages dealing with DNS activities for the specified log level range.

See the "Facility Type List" section at the end of this chapter for a complete list of logtype facilities.

Acmelog

The Acmelog is a log file located on CPU0, core 0's local file system on the active SPU. This file aggregates general system events that give an overview of the health and overall operating conditions of the Net-Net 9200.

The contents of the Acmelog are determined by the *system-log-level* parameter. This configuration dictates which event messages are written to the Acmelog. For example, if you set the *system-log-level* to **Minor**, all events Minor through Emergency are written to the Acmelog.

ACLI Configurations and Instructions

To set the Acmelog's system log level:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **system** and press <Enter> to access the system path.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **system-config** and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

   ```
   ACMEPACKET(system)# system-config
   ```

```
ACMEPACKET(system-config)#
```

4. Type **select** and press <Enter> to configure the existing system-config.

```
ACMEPACKET(system-config)# select
ACMEPACKET(system-config)#
```

5. system-log-level—Set this parameter to the minimum Acme Packet Log Message level you want the Acmelog to record.

```
ACMEPACKET(system-config)#system-log-level info
ACMEPACKET(system-config)#
```

6. Save your work using the ACLI **save** or **done** command.

File Location

The Acmelog is created by the logman process that runs on the active SPU's master core. This is Slot 0, CPU 0, Core 0, in a non-faulted state. Like all other tasks that run in this location, the Acmelog is written to the `/ramdrv/logs/` directory on Slot 0, CPU 0, Core 0's local file system.

Syslog

The term *syslog* refers to the protocol used for the network logging of system and network events. Syslog facilitates the transmission of event notification messages across networks. The syslog protocol provides a standardized means to remotely access log files. Net-Net OS's Syslog implementation conforms to the standard used for logging servers and processes as defined in RFC 3164.

The Net-Net OS's syslog message functionality lets you configure multiple syslog servers, and set the facility marker value used in the messages sent to that syslog server. The Net-Net SD can send logs to multiple syslog servers on the same host, provided they are running on unique ports.

The contents of the syslog output is identical to the Acmelog's contents.

ACLI Configurations and Instructions

This section describes how to add and remove syslog servers. You can add multiple syslog servers to your configuration.

Adding a Syslog Servers

To add a syslog server:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
ACMEPACKET#
```

2. Type **system** and press <Enter> to access the system path.

```
ACMEPACKET(configure)# system
ACMEPACKET(system)#
```

3. Type **system-config** and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

```
ACMEPACKET(system)# system-config
ACMEPACKET(system-config)#
```

4. Type **syslog-servers** and a <Space>, then **add** and a <Space>. Then enter the parameters that identify where you want to send logs: IP address, port number, and facility number.

   The facility part of your entry is an integer that identifies a user-defined facility value sent in every syslog message from the Net-Net 9200 to the syslog server. This parameter is used only for identifying the source of this syslog message as coming from the Net-Net 9200. It is not identifying an OS daemon or process. The default value for this parameter is **17**. RFC 3164 specifies valid facility values.

   Make your entry in one command-line using the syntax in the following example:

   ```
   ACMEPACKET(system-config)# syslog-servers add 10.168.192.5:514:17
   ```

   Note: You MUST enter a port number and facility number for this configuration parameter. 514 is the default syslog port number.

5. Save your work using the ACLI **done** command.

Removing a Syslog Server

To remove a syslog server:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET#
   ```

2. Type **system** and press <Enter> to access the system path.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **system-config** and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. Type **select** and press <Enter> to configure the existing system-config.

   ```
   ACMEPACKET(system-config)# select
   ACMEPACKET(system-config)#
   ```

5. Type **syslog-server** and a <Space>, then **delete** and a <Space>. Then enter the IP address, port number, and facility number that identify the syslog server you want to remove. Make your entry in one command-line using the syntax in the following example:

   system-config# **syslog-servers delete 10.168.192.5:514:17**

   The syslog server is removed from your list of syslog servers.

6. Save your work using the ACLI **done** command.

Process Log Files

Each task may generate task logs to maintain a record of events for data collection and debugging purposes. Because task logs are more data-inclusive than the Acmelog, their contents usually encompass the Acmelog contents. All tasks write their log files initially to their local file system, associated with the slot, CPU, and core where they reside.

Task Log Output

Tasks write their log file to the file system local to the CPU/core where they run. The local destination of a task's log file is `/ramdrv/logs/` local to that CPU/core.

Process Log Server

The process log server application resides on a remote server. It lets you store task logs remotely. This application is available from your Acme Packet customer support representative in either a binary program or as a perl-script.

Log File Output Locations

A task's log file output locations are determined by user configuration. The Net-Net OS uses a system of four modes to set the output of a task's log file.

- local—Writes the log file to the specified task's local file system. (default)
- remote—Writes the specified task's log file to the configured Acme Process Log Server.
- both—Writes the specified task's log file to both the configured Acme Process Log Server and the task's local file system.
- none—Task does not write to local or remote location. Logging is only sent to Acmelog and potentially syslog, depending on system-log-level setting and syslog-server setting.

Configuring Global Task Logging Level and Process Log Server

Set the following parameters to configure the process log server:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET#
   ```

2. Type **system** and press <Enter> to access the system path.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **system-config** and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. **process-log-level**—Set the starting log level for all tasks/process. Each process running on the system has its own process log.

   The default value for this parameter is `NOTICE`. Valid values for this parameter are `EMERGENCY`, `CRITICAL`, `MAJOR`, `MINOR`, `WARNING`, `NOTICE`, `INFO`, `TRACE`, `DEBUG`.

5. **process-log-mode**—Set the process log mode that you want to use from these available choices:
   - remote—Send task logs to the Process log server only
   - local—Send task logs to the local file system only (default)
   - both—Send task logs to the Process log server and to the local file system
   - none—No task logging

6. **process-log-address**—Set the IP address of the process log server.

7. **process-log-port**—Set the port number to use for the process log server. Default: 2500.

8. Save your work using the ACLI **done** command.

Task Logging

Apart from the global task logging level, you can configure logging level and log file destination for each unique task. This is accomplished by using the task-logging sub element.

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET#
   ```

2. Type **system** and press <Enter> to access the system path.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **system-config** and press <Enter>.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. Type **task-logging** and press <Enter>.

   ```
   ACMEPACKET(system-config)# task-logging
   ACMEPACKET(task-logging)#
   ```

5. **task-name**—Set the task name and location of the task you are configuring in the form: <task>@<slot>.<CPU>.<core>

6. **level**—Set the log level at which the task will write event messages. If configured, this value supersedes the global RTP startup logging level, defined by the process log-level-parameter.

   Valid values for this parameter are `EMERGENCY`, `CRITICAL`, `MAJOR`, `MINOR`, `WARNING`, `NOTICE`, `INFO`, `TRACE`, `DEBUG`.

7. **mode**—Set the mode of outputting the task's log file that determines the file's destination. Set the process log mode for the named task from these available choices:

   - remote—Send task logs to the Process log server only
   - local—Send task logs to the local file system only (default)
   - both—Send task logs to the Process log server and to the local file system
   - none—No task logging

8. **log-address**—Set the IP address and port of the process log server this task sends its task logs to. This parameter is entered in the form:

   ```
   IP_address:port_number
   ```

9. **internal-trace**—Set this parameter to **enabled** for the Net-Net SBC to save an interprocess message log (AMP traces) for messages to and from this task. The log file will be in the format: task-name.log.

10. Save your work using the ACLI **done** command.

Facility Logging

You can configure logging behavior for events of a specific facility type from a specific task. Facility logging is configured as a sub-element of task-logging, thus you must select the task-logging configuration element for the identified task before you set the facility logging parameters.

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET#
   ```

2. Type **system** and press <Enter> to access the system path.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **system-config** and press <Enter>.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. Type **task-logging** and press <Enter>.

   ```
   ACMEPACKET(system-config)# task-logging
   ACMEPACKET(task-logging)#
   ```

5. Select the task you wish to configure facility logging for and press <Enter>.

   ```
   ACMEPACKET(task-logging)# select
   <rtp_name>:
   1: sipls level=MINOR mode=BOTH server=0.0.0.0:0: 1 exceptions
   2: sipls level=MINOR mode=-none- server=0.0.0.0:0: no exceptions
   selection:2
   ACMEPACKET(task-logging)#
   ```

   Note: The number of exceptions reflects the number of facility logging configurations

6. Type **facility-logging** to enter the facility-logging configuration element for the previously selected task.

   ```
   ACMEPACKET(task-logging)# facility-logging
   ACMEPACKET(facility-logging)#
   ```

7. **facility**—Set the facility type message you want to be logged according to the following parameters. A complete list of facility types is located in the "Facility Type List" section at the end of this chapter

8. **level**—Set the log level at which the task will write this type of facility message.

   Valid values for this parameter are `EMERGENCY`, `CRITICAL`, `MAJOR`, `MINOR`, `WARNING`, `NOTICE`, `INFO`, `TRACE`, `DEBUG`.

9. **mode**—Set the mode of outputting the task's type log file that determines the file's destination.

   - remote—Send task logs to the Process log server only
   - local—Send task logs to the local file system only (default)
   - both—Send task logs to the Process log server and to the local file system
   - none—No task logging

10. **log-address**—Set the IP address and port of the process log server this task sends its type logs to. This parameter is entered in the form:

    ```
    IP_address:port_number
    ```

11. Save your work using the ACLI **done** command.

Real-time Logging Configuration

The previously discussed logging configurations are part of the Net-Net OS's system-wide configuration. You can also change a task's logging parameters in real-time, without reloading the full system configuration. These real-time commands are executed from the Superuser prompt and are as follows:

set log level

The **set log level** command lets you change the log level of a task from the command line without reloading the full system configuration. Wildcards are allowed in the task/location argument. You can enter an optional facility argument for the task(s) to only output messages of the supplied facility. Not supplying a facility argument sets the level for all facility types.

```
ACMEPACKET# set log level <task@slot.CPU.core> <log-level> [<facility>
| all]
```

set log mode

The set log mode command lets you change where an task's log files are output to, without reloading the full system configuration. Wildcards are allowed in the task/location argument. You can enter an optional facility argument for the task(s) to only output messages of the supplied facility to the given output location. Not supplying a facility argument sets the log mode for all facility types.

```
ACMEPACKET# set log mode <task@slot.CPU.core> [remote | local | both |
default] [<facility> | all]
```

set log server

The set log server command lets you change the Process server where an task's log files are sent to, without reloading the full system configuration. Wildcards are allowed in the task/location argument. You can enter an optional facility argument for the task(s) to only output messages of the supplied facility to the given Process server. Not supplying a facility argument sets the server for all facility types.

```
ACMEPACKET# set log server <task@slot.CPU.core>
<server_ipaddress:port> [<facility> | all]
```

Displaying Current Logging Configuration

You can query the current state of a task's logging configuration from the Superuser command prompt with the following commands:

show log level

The show log level command lets you view the log level for a supplied task. You can also specify a facility argument. The <task@slot.CPU.core> string can be replaced with **system** to indicate the Acmelog and Syslog settings.

```
ACMEPACKET# show log level <task@slot.CPU.core> [ all | <facility> ]
```

show log mode

The show log mode command lets you view the output mode for a supplied task. You can also specify a facility argument.

```
ACMEPACKET# show log mode <task@slot.CPU.core> [ all | <facility> ]
```

show log server

The show log server command lets you view the configured Process log server for a supplied task. You can also specify a facility argument.

```
ACMEPACKET# show log server <task@slot.CPU.core> [ all | <facility> ]
```

Log File Maintenance

Log File Compression

By default, the Net-Net 9200 compresses all task log files using gzip after they are closed by the system (because they reached the 1MB file size limit). You can turn off this behavior if you choose.

To turn off log file compression:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET#
   ```

2. Type **system** and press <Enter> to access the system path.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **system-config** and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. Type **select** and press <Enter> to configure the existing system-config.

   ```
   ACMEPACKET(system-config)# select
   ACMEPACKET(system-config)#
   ```

5. **log-compression**—Set this parameter to **disabled** to disable log file compression.

6. Save your work using the ACLI **done** command.

set log compression

The previously discussed log compression configurations is part of the Net-Net OS's system-wide configuration. You can also change logging compression in real-time, without reloading the full system configuration. This real-time command is executed from the Superuser prompt and is as follows:

The **set log compression** command lets you enable or disable log compression from the command line without reloading the full system configuration.

```
ACMEPACKET# set log compression [enabled | disabled]
```

show log compression

The show log compression command lets you view if logs are compressed or not.

```
ACMEPACKET# show log compression
```

Rotating Log Files

Log files are written until they reach 1 MB. The log file is then closed and renamed with a .1 appended to the end of the original file name. For example, sipmsg.log becomes sipmsg.log.1. New logs continued to be written to the original file, sipmsg.log, until once again they reach the 1 MB limit. Again the file is closed and renamed with a .1 appended to the original file name. The existing file with .1 appended is renamed to .2, for example sipmsg.log.2. This continues until 13 of that task's log files have been created. When this limit is reached, the oldest file (the one with .12 appended to the name) is overwritten by the previous .11 file.

If flash memory is approaching capacity, less than 12 log files might saved at one time.

Manually Rotating Log Files

You can manually rotate a task's log file by using the following command from the Superuser prompt:

```
ACMEPACKET# reset log <task@slot.CPU.core>
```

To rotate a trace log, you must include its filename at the end of the reset command. To rotate the trace log and the task log, you must include the term "all" at the end of the reset command:

```
ACMEPACKET# reset log <task@slot.CPU.core> [trace-log-filename | all]
```

Manually Deleting Log Files

You can manually delete all of a task's closed log files by using the following command from the Superuser prompt:

```
ACMEPACKET# clear log <task@slot.CPU.core>
```

To delete a trace log, you must include its filename at the end of the close command. To delete a trace log and a task log, you must include the term "all" at the end of the reset command:

```
ACMEPACKET# clear log <task@slot.CPU.core> [trace-log-filename | all]
```

Inserting Text into a Log File

You can add a text message to a log file at any point. This can be useful to note a point in the debugging process. To insert text into a log file, use the following command from the Superuser prompt:

```
ACMEPACKET# set log echo <task@slot.CPU.core> <message>
```

For example:

```
ACMEPACKET# set log echo ACLI@0.0.0 BEGINNING BATCH TEST NOW
```

Note: This command only works when the task's mode is set to local, remote, or both.

Trace Log

When it is necessary to view every message that a task sends or receives, you can use trace logging. The Net-Net 9200 outputs a protocol trace to a different log file than the aforementioned task log file. The trace log file is only created when the task's log level is set to TRACE or higher.

Trace Log Configuration

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **system** and press <Enter> to access the system path.

```
ACMEPACKET(configure)# system
ACMEPACKET(system)#
```

3. Type **system-config** and press <Enter>.

```
ACMEPACKET(system)# system-config
ACMEPACKET(system-config)#
```

4. Type **task-logging** and press <Enter>.

5. **rtp-name**—Set the task name and location of the task you are configuring in the form: <task>@<slot>.<CPU>.<core>

6. **level**—Set the log level to TRACE.

7. Save your work using the ACLI **done** command.

There are two ways to enable the trace log for a task in real-time, without reloading the full system configuration. These real-time commands are executed from the Superuser prompt and are as follows:

```
ACMEPACKET# debug <task@slot.CPU.core>
ACMEPACKET# set log level <task@slot.CPU.core> trace
```

All commands are equivalent to setting a task to debug, and writing the output to a trace log file. Valid tasks for the debug command are as follows:

arpm	auth	broker	cm
displayman	dnsres	ftpdalg	hip
lcm	lem	logman	mbcd
natm	sem	sfe	sipc
sipls	sipt	sm	snmpd
sptx			

Use the nodebug command to disable trace logging for a task.

```
ACMEPACKET# nodebug <task@slot.CPU.core>
```

Trace Log Output

The Net-Net OS follows three rules to determine trace log file output location.

When trace logging is enabled:

1. If a task's logging mode is set to **remote** or **both**, and there is a configured process log server, then the trace log messages are sent only to the remote server, not to the local file system.

2. If a task's logging mode is set to **local** or **none**, then the trace log messages are written to the local file system's trace log message file.

3. If a task's logging mode is set to **both**, but no Process log server is configured, the trace log message file is written only to the local file system.

Task and Trace log Filenames

A trace log is easily identifiable by its file name. When trace logs are stored remotely, their filenames are in the format:

```
task_name.log@slot.CPU.core
```

Remotely stored task logs are in the format:

```
log.task_name@slot.CPU.core
```

When trace logs are stored locally, their filenames are in the format:

```
task_name.log
```

When task logs are stored locally, their filenames are in the format:

```
log.task_name
```

Debug Logging Timeout

Debug logging timeout disables debug-level logging if it is accidentally left enabled. This feature is a way to protect against accidentally putting an unnecessarily high load on the system. This timer applies to debug logging enabled via the `debug <task>` ACLI command only.

When a timeout occurs, the Net-Net SBC behaves as if the `nodebug sip` command has been implemented and debugging is disabled completely. A message is written to the console, syslog, and acmelog informing the user that debug logging has been disabled for all tasks. The following is an example of what a debug timout message looks like:

```
Debug logging for lcm@0.0.0 has timed out
```

ACLI Instructions and Examples

The new configuration parameter, debug-timeout, is part of the **system-config** configuration element. If this field is configured when debugging is already enabled, the timer begins immediately.

To set a debug logging timeout on the Net-Net SBC:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **system** and press <Enter>.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type system-config and press <Enter>. The prompt changes to let you know you can begin configuring individual parameters.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. **debug-timeout**—Enter the timeout, in seconds, for a debug logging to timeout. The valid range is 0-65535, with 0 (default) disabling the timeout feature.

5. Save and activate your configuration.

Panic Log Dump

The Net-Net 9200 Panic Log Dump feature ensures that under exceptional system conditions, important debugging information is saved and archived to nonvolatile flash RAM before a card reset. This information can then be used to analyze and troubleshoot intermittent issues that are often hard to reproduce.

Just before a card goes OOS, as initiated by the system, all logs in the `/ramdrv/logs` directory of all of the cores on a TCU are compressed and saved. This may include DSP core dump images (which are often quite large).

Each TCU core zips all of its logs (included rotated backups) and pushes them to the active master core's flash RAM, in a directory called `/code/dump/SCC`, where SCC stands for Slot, CPU, Core. For example: `/code/dump/411`

> **Note:** Remember to set log levels appropriately, so they maintain a reasonable size.

Archived logs remain on the filesystem until overwritten by newer archives for the same cores, or until cleared by the user. The number of archived logs that can be stored on the system is limited by the size of the flash storage system. If filespace is exceeded, some or all files will not be archived, but the TCU(s) in question will still be reset.

Panic Log Dump Configuration

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **system** and press <Enter> to access the system path.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **system-config** and press <Enter>.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. **dump-logs-on-failure**—Set this parameter to enabled to use the panic log dump feature.

5. Save your work using the ACLI **done** command.

Managing Panic Log Dumps

To manage log dumps, you can use the **show dumps** and **delete dumps** commands.

show dumps

The **show dumps** command lists all dumps present on any SPU present, for any card, cpu, or core. A slot argument is mandatory, or cpu and/or slot can be specified as **show dumps 2 0 1**. For example:

```
ACMEPACKET# show dumps 2

Log dumps stored on SPU 0 for 2.0.0:

                    log.npm.gz     Dec 10 16:19:06          1972 bytes
                    log.lcm.gz     Dec 10 16:19:06          2197 bytes
                    log.lem.gz     Dec 10 16:19:06           896 bytes
                   log.ntpd.gz     Dec 10 16:19:06          1414 bytes
                     log.cm.gz     Dec 10 16:19:06          2944 bytes
                log.broker.gz     Dec 10 16:19:06           855 bytes
                log.kernel.gz     Dec 10 16:19:06           291 bytes
                   log.rdp.gz     Dec 10 16:19:06          2121 bytes
                   log.i2c.gz     Dec 10 16:19:06           126 bytes
                  log.dx240.gz     Dec 10 16:19:08           187 bytes
                 log.npsoft.gz     Dec 10 16:19:08          3957 bytes
              log.npu_debug.gz     Dec 10 16:19:08           131 bytes
```

```
                    log.ftp.gz     Dec 10 16:19:08          125 bytes
                   log.arpm.gz     Dec 10 16:19:08         1478 bytes
                   log.natm.gz     Dec 10 16:19:08          987 bytes
                  log.npcli.gz     Dec 10 16:19:08          898 bytes
                   log.sptx.gz     Dec 10 16:19:08          640 bytes
Done.

Log dumps stored on SPU 0 for 2.0.1:

                    log.lcm.gz     Dec 10 16:19:06         2195 bytes
                    log.lem.gz     Dec 10 16:19:06          921 bytes
                   log.ntpd.gz     Dec 10 16:19:06         1409 bytes
                 log.broker.gz     Dec 10 16:19:06          858 bytes
                 log.kernel.gz     Dec 10 16:19:06          254 bytes
                    log.rdp.gz     Dec 10 16:19:06         3539 bytes
                    log.i2c.gz     Dec 10 16:19:06          126 bytes
                  log.dx240.gz     Dec 10 16:19:06          128 bytes
                    log.ftp.gz     Dec 10 16:19:06          125 bytes
                   log.mbcd.gz     Dec 10 16:19:08         3825 bytes
Done.


No log dumps stored on SPU 1 for 2.0.0

No log dumps stored on SPU 1 for 2.0.1
```

delete dumps

The **delete dumps** command requires a slot argument, but like **show dumps** it can also take a CPU, and core argument to delete only the files from that CPU or core.

```
ACMEPACKET# del dump 2
Delete all dumped files for slot 2 [y/n]?: y

removing file /code/dump/200/log.npm.gz
removing file /code/dump/200/log.lcm.gz
removing file /code/dump/200/log.lem.gz
removing file /code/dump/200/log.ntpd.gz
removing file /code/dump/200/log.cm.gz
removing file /code/dump/200/log.broker.gz
removing file /code/dump/200/log.kernel.gz
removing file /code/dump/200/log.rdp.gz
removing file /code/dump/200/log.i2c.gz
removing file /code/dump/200/log.dx240.gz
removing file /code/dump/200/log.npsoft.gz
removing file /code/dump/200/log.npu_debug.gz
removing file /code/dump/200/log.ftp.gz
removing file /code/dump/200/log.arpm.gz
removing file /code/dump/200/log.natm.gz
removing file /code/dump/200/log.npcli.gz
removing file /code/dump/200/log.sptx.gz
deleting directory /code/dump/200
removing file /code/dump/201/log.lcm.gz
removing file /code/dump/201/log.lem.gz
removing file /code/dump/201/log.ntpd.gz
removing file /code/dump/201/log.broker.gz
```

```
removing file /code/dump/201/log.kernel.gz
removing file /code/dump/201/log.rdp.gz
removing file /code/dump/201/log.i2c.gz
removing file /code/dump/201/log.dx240.gz
removing file /code/dump/201/log.ftp.gz
removing file /code/dump/201/log.mbcd.gz
deleting directory /code/dump/201

SPU 0 deleting log dump directory /code/dump/200

Done.

SPU 0 deleting log dump directory /code/dump/201

Done.


SPU 1 deleting log dump directory /code/dump/200

Done.

SPU 1 deleting log dump directory /code/dump/201

Done.
```

Viewing Logs

Task and trace log files are located in the logs directory on the root of the local file system. You can access these files in three ways.

FTP

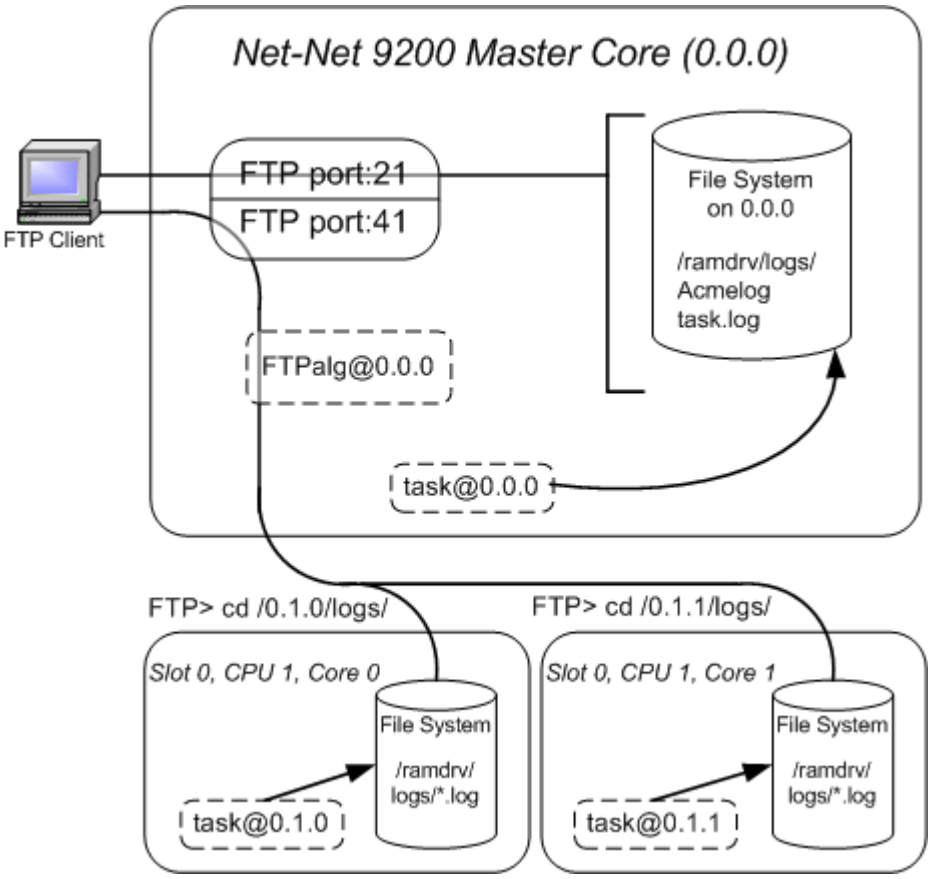
The FTPALG task can act as a proxy between the master core and all other cores on the Net-Net 9200. You can FTP directly to the master core and view and retrieve the log files located throughout the system. By FTPing to port 41, you will be redirected to view the desired log files. A system of directory names is used to navigate to the exact log file you wish to retrieve. The format of the directory names is

```
/<slot>.<CPU>.<core>/logs
```

For example, to view the logs in SPU 2's 0-CPU, core-1, you would cd to /1.0.1/logs from the root of the FTPalg.

Acmelog

To retrieve the Acmelog, you must FTP to port 21 on the active SPU. The Acmelog is located in `/ramdrv/logs/` directory, along with all other logs belonging to tasks that run on the active SPU's master core.



Note: You can also retrieve the Acmelog by FTPing to port 41 and then listing the `/0.0.0/logs` directory.

Facility Type List

- ALARM_FILTER
- ALARM_MGR
- ALG
- ANDD
- ARPMLOG
- BROKER
- CAM
- CHASSIS
- CLI
- CLIP
- HIP
- IPC (also trigger for AMP protocol tracing)
- IPFRAG
- IXF1104
- KERNEL
- LICENSE
- LOGECHO
- MEDIA
- MESSAGE
- MGCP
- REDUNDANCY
- SERVICE
- SESSION
- SFE
- SIP
- SIPNAT
- SIPREG
- SLOG_TYPE_CRITICAL
- SLOG_TYPE_EMERGENCY
- SLOG_TYPE_MAJOR
- SWINGLINE
- TAIL
- TCUHA
- TEST
- TESTMAN
- TIMER
- TM

- TRANS
- TRIP
- XC

2 Fault Management

Introduction

This chapter explains fault management on the Net-Net 9200. Topics covered include how to locate faults, communicate faults, determine their causes, and make corrections. Faults are communicated to the system administrator primarily through the following means:

- Alarms
- SNMP traps
- Graphic Display

Alarms

Overview

An alarm is triggered when a condition or event happens within either the Net-Net system's hardware or software. Alarming is the way in which the Net-Net OS alerts administrators that there are problems with the system, and that the system may or may not need attention.

The Net-Net system's alarm manager (AM) first receives an alarm message from a specific process. The AM locates the Alarm ID in the alarm table and can then proceed with the appropriate action. The alarm table is a list in the Net-Net OS that contains all of the actions required for acting on the alarm.

Alarming Process

An alarm is triggered when a condition or event happens within either the Net-Net system's hardware or software. When this event occurs, a fault is identified in a responsible task. The task sends an alarm message to the local card manager (LCM). The LCM notes the alarm and makes a determination of health impact. The alarm message is forwarded to the AM. The AM reads the following alarm message attributes:

- **Alarm ID**—A unique integer that corresponds to a specific error or failure
- **Task ID**—The task and task ID that initiated the error
- **Severity**—The severity level of the condition or system failure
- **Previous Occurrences**—The first and most recent times this alarm type happened
- **Task Location**—Slot, CPU, Core where this task is running
- **Character string**—Textual description of the event or condition
- **Count**—Number of times this alarm has occurred since the system was powered on

When the conditions that triggered the alarm have returned to normal, the AM gets a clear message from the initiating task.

Alarm Categories and Responses

Alarms can fall into one of six categories. These categories let you know where on the Net-Net 9200 a problem has been identified.

Alarm Category	Description
Hardware	This category of alarms is generated when there is a problem with the Net-Net 9200 chassis, feature or interface cards, power supplies, or cooling system. The following list provides some hardware alarm examples: • Emergency/Critical—Extreme over temperature condition • Major—Major over temperature condition • Minor—Minor over temperature condition, Fan failure, Low voltage.
System	This category of alarms accounts for problems related to the Net-Net OS. It also includes low-level system calls as well as link status alarms (e.g., insufficient memory available, no file descriptors available, link down detected).
Network	This category of alarms accounts for problems related to low level network issues. This category of alarm might occur when code is unable to communicate with the hardware. It also includes alarms related to the following: • Network processor management • NAT • CAM
Media	This category of alarm accounts for problems related to the MBCD, MBCD clients, and the functionality of ARP on the Net-Net 9200 system. It also includes alarms related to flows and bandwidth.
Application	This category of alarm accounts for problems related to applications (i.e., problems that involve protocols). The application alarm category also includes security breeches, session failures, and problems related to accounting.
Configuration	This category of alarm accounts for problems with the system, including any type of database issues that might arise.

Alarm Severity Levels

Five levels of alarm severity have been established for the Net-Net system. These levels have been designated so that the system can take action that is appropriate to the situation.

Alarm Severity	Description
Emergency	Requires immediate attention. If you do not attend to this condition immediately, there will 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.

Alarm Severity	Description
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.

Alarm Severity Health Deductions

Based on the system affected, a and the severity of alarm fired, a specified health deduction occurs.

Alarm Severity	Hardware Health Deduction	System Health Deduction	Network Health Deduction	Media Alarm Deduction	Application Alarm Deduction	Configuration Alarm Deduction
Emergency	100	100	50	0	0	0
Critical	75	75	37	0	0	0
Major	50	50	25	0	0	0
Minor	25	20	12	0	0	0
Warning	5	5	2	0	0	0

Response to Alarms

The Net-Net system is capable of taking a range of actions in response to an alarm. There are five actions the Net-Net system can take:

- Write messages to remote syslog server
- Create an SNMP trap
- Close hardware dry-contact
- Display a message on the Graphic Display
- Reboot the system

The Net-Net system maintains a table that lists the actions to take when an event of specific category and severity occurs.

Alarm Table

Based on the alarm category and severity, the following table shows the Net-Net system's response.

	Emergency	Critical	Major	Minor	Warning
Hardware	Trap Critical dry contact Graphic display Syslog	Trap Critical dry contact Graphic display Syslog	Trap Major dry contact Syslog	Trap Minor dry contact Syslog	Trap Syslog
System	Reboot* Trap Critical dry contact Graphic display Syslog	Trap Critical dry contact Graphic display Syslog	Trap Major dry contact Syslog	Trap Syslog	Trap Syslog
Network	Trap Critical dry contact Syslog	Trap Critical dry contact Graphic display Syslog	Trap Syslog	Trap Syslog	Trap Syslog
Media	Trap Critical dry contact Syslog	Trap Critical dry contact Graphic display Syslog	Trap Syslog	Trap Syslog	Trap Syslog
Application	Trap Critical dry contact Syslog	Trap Critical dry contact Syslog	Trap Syslog	Trap Syslog	Trap Syslog
Configuration	Trap Syslog	Trap Syslog	Trap Syslog	Trap Syslog	Trap Syslog

Syslog / Acmelog

The AM can write a record of the event to the syslog and Acmelog files.

SNMP Traps

The AM can send the appropriate SNMP trap to a configured trap receiver.

An SNMP trap is an automatic event notification that the Net-Net system sends to external SNMP trap receivers. See this chapter's "Supported Standard Traps"for more details.

Dry Contacts

The Net-Net system supports three relays configured as an alarm port on the MIU card on the rear of the Net-Net 9200 chassis. The alarm port has three open circuits that each close when an alarm of a given level is active on the Net-Net system. The following alarm severity levels correspond directly to an individual circuit on the alarm port:

- Critical
- Major
- Minor

Graphic Display

The Net-Net system features a four line graphic display on the front panel of the chassis. The Net-Net OS displays messages concerning current alarm conditions on the graphic display window.

During an alarm condition, the first line of the graphic display shows the number of hardware-related alarms, if any. The second line of the graphic display shows the number of link-related alarms, if any.

```
1 HW ALARM
2 LINK ALARMS
```

When an alarm condition is cleared, the base display replaces the alarm display. For more information about the alarm port and the graphic display, see the *Net-Net 9200 Hardware Installation Guide*.

Card Reset

Under certain, highly rare conditions, the Net-Net system can reset a card. The path to this happening is: failure event -> health degradation -> card switchover -> failed card reset.

Operating Status Alarms

The following system elements are periodically checked for health:

Task Status

If a task suspends or stops, it results in an EMERGENCY alarm along with a 100 point drop in the associated core's health score. When the task resumes, the EMERGENCY alarm is cleared and the core's health is restored.

CPU Core Usage

When the CPU load is greater than or equal to 95 percent, a NOTICE alarm is generated. When CPU load is greater than or equal to 99%, a WARNING alarm is generated. This degrades the core's health by 5 points. Successive high CPU usage evaluations add additional 5 point health degradations. When the processor returns to less than 95 percent usage, health is restored based upon the CPU deductions previously accumulated.

This behavior can be overridden by setting the user-defined alarm thresholds.

CPU Core Memory Usage

When a core’s memory usage is greater than or equal to 90%, a NOTICE alarm is generated. When a core's memory usage is greater than or equal to 95%, the core's health is degraded by 5 points and a MINOR alarm is generated. Successive high memory use evaluations result in continuing 5 point health degradations. When memory usage returns to < 95% usage, health is restored based upon the memory deductions previously accumulated. The SPU will reboot / reset when the memory utilization reaches 95%.

This behavior can be overridden by setting the user-defined alarm thresholds.

SPU Status

The Net-Net 9200 periodically checks the health of the 24 port Ethernet switch that interconnects the system's internal network. Port and link status are checked for each connected core including connectivity to the standby SPU.

This SPU check occurs every 5 seconds and a WARNING alarm (5 point health degradation) is issued for a downed port or link on a serviceable core.

NPU Status

The Net-Net 9200 periodically checks the health of the 24 port switch that interconnects the NPUs to the NIUs used for valid external communication. Port and and link status are assessed based upon interrupts received from the driver in

response to link state changes. Link down conditions indicate an interruption in the network path and result in the generation of a MINOR alarm (20 point deduction).

The proportion of functioning ports to those configured is used to determine an over health score for an NIU so its role (Active/Standby) may be ascertained. If a standby NIU has a higher percentage of functioning ports (configured + link active) than its redundant NIU, there will be a switchover.

User Configured Alarms

Some alarm thresholds are user-configured, overriding the default. These configurable alarms are for:

- CPU usage
- Memory usage
- Licensed session capacity

For each type of configurable alarms, you can set triggers for any combination of MINOR, MAJOR, and CRITICAL alarms severities based on the event reaching a specific level. Once triggered, the respective alarm's health deduction is removed in the affected system.

Default alarm thresholds are set to generally permissive (high) levels and degrade system health less than the amount listed for their default alarm types (link). This provides built-in warning on a system without configured thresholds, and only causes failover in extreme cases.

CPU alarms

CPU usage alarms fall into the system category. High CPU usage will generate WARNING, and NOTICE alarms by default.

Memory alarms

Memory usage alarms fall into the system category. The Net-Net 9200 generates MINOR and NOTICE alarms by default. A user-configured MINOR threshold will override the built in MINOR threshold if set lower.

License threshold

License usage alarms fall into the application category. Session usage approaching the license capacity generates a MAJOR alarm when it exceedes 98 of the maximum number of sessions. A user-configured MAJOR threshold will override the built in MAJOR threshold.

ACLI Instructions

To manually configure alarm thresholds:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **system** and press <Enter>.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **system-config** and press <Enter>.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. Type **alarm-threshold** and press <Enter>.

   ```
   ACMEPACKET(system-config)# alarm-threshold
   ```

```
ACMEPACKET(alarm-threshold)#
```

The system prompt changes to let you know that you can begin configuring individual parameters.

5. **type**—Enter the type of threshold you wish to configure. Valid types are CPU, memory, or sessions.
6. **severity**—Enter the severity level you will configure a custom health deduction for. Valid severity are MINOR, MAJOR, and CRITICAL.
7. **value**—Enter the percent of resource (type) in use that triggers the configured alarm (severity).
8. Save your work using the ACLI **done** command.

TCM2 Alarms

DSP Boot Failure

An alarm is triggered if a DSP fails to boot during system initialization. This is a health affecting critical alarm (100% health score degrade) that cannot be cleared. This condition sends the **apSysMgmtHardwareErrorTrap**. For example:

```
ID      Task    Severity        First Occurred          Last Occurred
65584  527739792     3     2011-10-11 10:11:49    2011-10-11 10:11:49
Count   Description
1       DSP#0 Boot Failure!
```

DSP Communication Timeout

An alarm is triggered if a DSP fails to reply to the host processor within 2 seconds after 3 retries. This is a health affecting critical alarm (100% health score degrade) that cannot be cleared. This condition sends the **apSysMgmtHardwareErrorTrap**.

```
ID      Task    Severity        First Occurred          Last Occurred
65586  527739792     3     2011-10-11 10:11:49    2011-10-11 10:11:49
Count   Description
1       DSP Timeout on Device #0
```

DSP Alert

An alarm is triggered if a DSP sends an asynchronous alert to the host processor indicating a DSP core halt. This is a health affecting critical alarm (100% health score degrade) that cannot be cleared. This condition sends the **apSysMgmtHardwareErrorTrap**.

```
ID      Task    Severity        First Occurred          Last Occurred
65585  527739792     3     2011-10-11 10:11:49    2011-10-11 10:11:49
Count   Description
1       DSP Core Halt on Device #0!
```

Total Transcoding Capacity Threshold Alarm

An alarm is triggered if the transcoding utilization exceeds 95% of capacity. This is a non-health affecting warning level alarm. This condition sends the **apSysMgmtGroupTrap** with the MIB OID apSysXCodeCapacity. The alarm is cleared when the transcoding utilization falls below 80% of capacity and the apSysMgmtGroupClearTrap is sent.

```
ID      Task    Severity        First Occurred          Last Occurred
131158 527739792     6     2011-10-11 10:11:49    2011-10-11 10:11:49
Count   Description
```

```
1       Transcoding capacity at  96 (over threshold of 95)
```

Licensed AMR Transcoding Capacity Threshold Alarm

An alarm is triggered if the AMR transcoding utilization exceeds 95% of licensed capacity. This is a non-health affecting warning level alarm. This condition sends the **apSysMgmtGroupTrap** with the MIB OID apSysXCodeAMRCapacity. The alarm is cleared when the AMR transcoding utilization falls below 80% of licensed capacity and the apSysMgmtGroupClearTrap is sent.

```
ID      Task    Severity        First Occurred          Last Occurred
131159  527739792     6     2011-10-11 10:11:49    2011-10-11 10:11:49
Count   Description
1       AMR Transcoding capacity at  97 (over threshold of 95)
```

Licensed AMR-WB Transcoding Capacity Threshold Alarm

An alarm is triggered if the AMR-WB transcoding utilization exceeds 95% of licensed capacity. This is a non-health affecting warning level alarm. This condition sends the **apSysMgmtGroupTrap** with the MIB OID apSysXCodeAMRWBCapacity. The alarm is cleared when the AMR-WB transcoding utilization falls below 80% of licensed capacity and the apSysMgmtGroupClearTrap is sent.

```
ID      Task    Severity        First Occurred          Last Occurred
131160  527739792     6     2011-10-11 10:11:49    2011-10-11 10:11:49
Count   Description
1       AMR-WB Transcoding capacity at 100 (over threshold of 95)
```

Displaying and Clearing Alarms

Alarms are managed using the following ACLI commands:

- show alarm

Displaying Alarms

Besides writing to various log files and sending SNMP traps, the Net-Net system can indicate the presence of an alarm in three ways:

- Commands executed on the ACLI
- On the front-panel graphic display
- Via the alarm port on an MIU

For more information about the alarm port and the graphic display, see the *Net-Net 9200 Hardware Installation Guide*.

show alarm current

The **show alarm current** command is used to display the current alarms on the screen.

To display Net-Net system alarms:

1. Enter the **show alarm current** command.

   ```
   ACMEPACKET# show alarm current
   ```

   A list of the current alarms for the system will be displayed.

```
ACMEPACKET> > show alarm current
2 alarms to show
Alarm Id    Task Id        Severity    Last Occurrence         Count   Description
--------    -------        --------    -------------           -----   -----------
22620222    tSM@2.0.0      NOTICE      2007-11-05 15:48:10.500 1       NPU0 Switchover to Active Role
22611222    tSM@1.0.0      NOTICE      2007-11-02 19:08:26.683 1       SPU1 Switchover to Active Role
```

Filtering Alarms

Some error conditions continually send alarms to the AM until the problem is fixed. To keep the alarm table from becoming overwhelmed by redundant messages from the LCM, you can set a filter. You must supply the category of alarm to filter and the time period of arrival in which redundant messages are ignored. The set command usage is as follows:

```
ACMEPACKET# set alarm filter <task@location> [hardware | system |
network | media | appl | config | all] <redundancy window in ms>
```

For example:

```
ACMEPACKET# set alarm filter lcm@0.0.0 hardware 200
```

The companion **show alarm filtered** command displays the total number of instances of redundant alarms received from a specified LCM. For example:

```
ACMEPACKET# show alarm filtered lcm@*
ACMEPACKET# show alarm filtered lcm@0.0.0
LCM Alarm Filter List on 0.0.0
Alarm Id            Process Id          Severity            Instances
--------            ----------          --------            ---------
No entries found in the Alarm Filter List.
```

Clearing Alarms

Alarms can be cleared from the Net-Net system in three ways:

- The AM clears the alarm when an indication (clear alarm message) is received from the task where the alarming condition occurred.
- The system administrator manually clears the alarm via the ACLI or EMS.
- The AM clears the alarm after receiving an indication from the display manager that the Alarm Silence button was pressed.

When a task generates an alarm, it can clear that alarm too. For the AM to clear the alarm, the event or condition that caused the alarm must revert or correct itself. For instance, if an alarm is generated because the system's temperature is high, and later the temperature returns to normal, the process that monitors these conditions sends a message to clear the alarm.

With regard to redundant architectures, if you clear an alarm using the **clear alarm** command without actually fixing the true cause of the alarm, it might have an adverse effect on the health score of the system and might, in turn, prevent future failover functionality.

Automatic Alarm Clearing

When a task automatically clears an alarm because either the event has been remedied or something else has caused the task to return to baseline operation, you do not need to perform any action to remove the alarm.

ACLI Instructions

You can clear an alarm manually, but you must first identify the alarm ID, task ID, and severity by using the show alarms command. The alarm ID is the number listed in the first column of that display.

To clear a specific Net-Net system alarm:

1. Ensure you are in Superuser Mode by noting the pound (#) sign at the end of the prompt. For example:

   ```
   ACMEPACKET#
   ```

2. Enter **show alarm current** to list the current alarms. Note the alarm ID (`ID` column) and task ID (`Task` column) of the alarm you want to clear. You will need this reference information in order to clear the alarm.

```
ACMEPACKET> > show alarm current
2 alarms to show
Alarm Id    Task Id        Severity    Last Occurrence         Count   Description
--------    -------        --------    -------------           -----   -----------
22620222    tSM@2.0.0      NOTICE      2007-11-05 15:48:10.500 1       NPU0 Switchover to Active Role
22611222    tSM@1.0.0      NOTICE      2007-11-02 19:08:26.683 1       SPU1 Switchover to Active Role
```

3. Type **clear alarm** followed by a <Space>, the alarm ID, another <Space>, the task ID, <space>, and severity of the task that generated the alarm, and press the <Enter> key.

   ```
   ACMEPACKET# clear alarm 22620222 tSM@2.0.0 NOTICE
   ```

Via the front-panel navigation buttons

You can use the Silence Alarms button located to the left of the graphic display on the front of the Net-Net 9200 chassis. Pressing this button silences the alarm port on the Net-Net 9200's MIU. This button does not clear alarms from the alarm table.

Configurable Alarm Thresholds

User-configured Alarms

Some alarm thresholds are user-configured, overriding the default thresholds at which alarms are triggered. These configurable alarms are for:

- CPU usage
- Memory usage
- Licensed session capacity

For each type of configurable alarms, you can set triggers for any combination of MINOR, MAJOR, and CRITICAL alarms severities based on the event reaching a specific level.

Default alarm thresholds are set to generally permissive (high) levels and degrade system health less than the amount listed for their default alarm types. This provides built-in warning on a system without configured thresholds, and only causes failover in extreme cases.

User-defined CPU and memory alarms are limited to degrading health by only 5 percent per health cycle, just like the higher of the two built-in alarm thresholds. This can still can reset the cards if left alone long enough, but allows enough time between resets for an administrator to remove the offending threshold and allow the system to recover. License capacity alarms do not affect system health.

CPU alarms

CPU usage alarms fall into the system category. High CPU usage will generate WARNING, and NOTICE alarms by default.

Memory alarms

Memory usage alarms fall into the system category. The Net-Net 9200 generates MINOR and NOTICE alarms by default. A user-configured MINOR threshold will override the built in MINOR threshold if set lower.

License threshold

License usage alarms fall into the application category. Session usage approaching the license capacity generates a MAJOR alarm when it exceeds 98% of the maximum number of sessions. A user-configured MAJOR threshold will override the built in MAJOR threshold.

ACLI Instructions

To manually configure alarm thresholds:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **system** and press <Enter>.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **system-config** and press <Enter>.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. Type **alarm-threshold** and press <Enter>.

   ```
   ACMEPACKET(system-config)# alarm-threshold
   ACMEPACKET(alarm-threshold)#
   ```

   The system prompt changes to let you know that you can begin configuring individual parameters.

5. **type**—Enter the type of threshold you wish to configure. Valid types are **cpu**, **memory**, or **sessions**.
6. **severity**—Enter the severity level you will configure a custom health deduction for. Valid severity are **minor**, **major**, and **critical**.
7. **value**—Enter the percent of resource (type) in use that triggers the configured alarm (severity).
8. Save your work using the ACLI **done** command.

SNMP Traps

An SNMP agent can notify an NMS of significant events by way of an unsolicited SNMP trap. SNMP traps are triggered by the AM, which decides, based on configuration, the appropriate trap to be sent. The Net-Net OS conforms to SNMPv2c.

Traps are sent according to the criteria established in the following:

- IETF RFC 1907 *Management Information Base for Version 2 of the Simple Network Management Protocol*
- IETF RFC 2233 T*he Interfaces Group MIB using SMIv2*
- or the appropriate enterprise MIB (for example the Acme Packet syslog MIB or the Acme Packet System Management MIB).

For additional information about the traps and MIBS supported by the Net-Net System, see the *Acme Packet MIB Reference Guide*.

Supported Standard Traps

The Net-Net OS supports standard traps and Acme Packet enterprise traps. See the *Acme Packet MIB Reference Guide* for specific information about each trap.

The following table identifies the standard traps that the Net-Net system supports.

Trap Name	Description
linkUp	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.
linkDown	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.
coldStart	The SNMPv2 agent is reinitializing itself and its configuration may have been altered. This trap is not associated with a Net-Net system alarm.
authenticationFailure	The SNMPv2 agent received a protocol message that was not properly authenticated. If the snmp-enabled and enable-snmp-auth-traps fields in the ACLI's system-config element are set to enabled a snmpEnableAuthenTraps object is generated.

Alarm Descriptions

This section describes the range of alarms the Net-Net 9200 uses to describe its operating conditions. Alarms are divided into six categories: hardware, system, media, network, media, application and configuration.

When alarms are displayed on the ACLI using the **show alarm current** command, the list includes the following columns:

- Alarm Id—An internally interpretted hexadecimal value.
- Task Id—The task@card.cpu.core which generated this alarm.
- Severity—The severity of the alarm created.
- Last Occurrence—The last occurrence of this alarm.
- Count—The number of times this alarm has been retriggered
- Description—A textual description of the alarm.

The alarm tables below use the ZZ notation to denote the character positions that are variable values depending on the exact location (based on slot, CPU, port, core, or location) of the alarm.

Hardware Alarms

Hardware alarms include information about fans, system power, system temperature, internal devices, MIU cards, and NIU cards on the Net-Net system.

> **Note:** If you suspect you have a hardware fault, contact Acme Packet Technical Support for assistance with running the diagnostics image loaded on the Net-Net 9200.

I2C Hardware Alarms

The following table lists the I2C hardware alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Example Log Message	Trap Generated
I2C Failure/ 11900200	MAJOR/ 50	The environmental sensor component detects a failure.	• MidPlane IDProm Write failure • PowerPlane IDProm Writer failure • I2C driver failure	apEnvMonI2CFailNotification OR apSyslogMessageGenerated (See Note 1)
I2C CARD FAILURE/ 118ZZ200	MAJOR/ 50	The environmental sensor component detects a card failure	• Unable to Read IDProm on <MODULE> x • Unable to Initialize I2C on <MODULE> x • Unable to Perform Health Scan on <MODULE> x • Unable to Switchover PHY PM 8380 Muxes to Active NPU • I2C Busy, where <MODULE> is one of the hardware modules	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)

Card Presence Alarms

The following table lists the card presence alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Trap Generated
CARD REMOVED/ 127ZZ100	NOTICE/ 0	A card has been removed.	Card in Slot XX has been Removed.	entConfigChange

I2C Alarm Types

The following table lists the I2C alarm types.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
I2C FAN FAULT/ 1186ZZ210	MAJOR/ 50	Fan fault detected.	Fan Fault on FAN Controller X - Affected fans are: Y.	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
	NORMAL/ 0	Fan fault cleared.	Clearing Fan Fault on FAN Controller X - Fan Mask Y.	
I2C COMM LOSS/ 1186ZZ211	MINOR/ 20	Communication error detected.	• Comm Error Detected on X in Slot N. • Comm Fault on FAN Controller X	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C POWER WARNING/ 118ZZ220	MAJOR/ 50 MINOR/ 20		Power Warning on X in slot N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C POWER FAULT/ 118ZZ221	MAJOR EMERGENCY/ 50	Power fault detected.	• Power Fault on X in slot N • Power not Present on Power Supply X • Voltage Input Fault detected on Power Supply X • Voltage Input Warning detected on Power Supply X • Temperature Fault detected on Power Supply X • Temperature Warning detected on Power Supply X • Fan Fault detected on Power Supply X • Voltage Output Fault detected on Power Supply X • Current Output Fault detected on Power Supply X	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C TRACKING FAULT/ 118ZZ250	MAJOR/ 50	Tracking fault detected	Tracking Fault on X in slot N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C CRC ERROR/ 118ZZ251	MAJOR/ 50	Power CRC error detected.	Power CRC Error on X in slot N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
I2C TX FAULT/ 118ZZ252	MAJOR/ 50	Power transmission error detected.	Power Transmission Error in X on slot N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C SPEED FAULT/ 118ZZ212	MINOR/ 20	Fan speed fault detected.	Inconsistent Speed Setting on FAN Controller	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)

I2C Link and Temperature Alarms

The following table lists the link and temperature alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
I2C LINK FAULT/ 118ZZ260 . . . . . . 118ZZ26F	MINOR/ 20	Link fault has been detected.	• Tx Fault on Fiber PHY X::Port N • Bandwidth differs from value set on Fiber PHY X::Port N • Tx Disable differs from value set on Fiber PHY X::Port N • SFE has been removed on Fiber PHY X::Port N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
	NORMAL/ 0	Clears the link fault alarms.	• Clearing Tx Fault on Fiber PHY X::Port N • Clearing Bandwidth Alarm on Fiber PHY X::Port N • Clearing Tx Disable Alarm on Fiber PHY X::PortN • SFE is present on Fiber PHY X::Port N	
I2C TEMP WARNING/ 128ZZ270 . . . . . . 128ZZ27F	MINOR/ 20	• Temperature fault detected. • Minor temperature fault detected on fan controller.	• Temperature Warning on X in Slot N • Setting Minor Temperature Fault on FAN Controller X. Temp is XX.	apEnvMonTempChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C TEMP HIGH/ 128ZZ280 . . . . . . 128ZZ28F	MAJOR/ 50	• Temperature fault detected. • Major temperature fault detected on fan controller.	• Over Temperature Fault on X in slot N • Setting Major Temperature Fault on FAN Controller X. Temp is XX. • HIgh Temperature Alarm on X in Slot N	apEnvMonTempChangeNotification OR apSyslogMessageGenerated (See Note 1)

Voltage Alarms

The following table lists the voltage alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
I2C VOLTAGE FAULT/ 129ZZ230	MAJOR/ 50	Voltage fault detected.	Voltage Fault on X in slot N.	apEnvMonVoltageChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C UNDER VOLTAGE/ 129ZZ231	MAJOR/ 50	Under voltage fault detected.	Under Voltage Fault on X in slot N	apEnvMonVoltageChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C OVER VOLTAGE/ 129ZZ232	MAJOR/ 50	Over voltage fault detected.	Over Voltage Fault on something in slot N	apEnvMonVoltageChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C OVER CURRENT/ 118ZZ241	MAJOR/ 50	Over current fault detected.	Over Current Fault on X in slot N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)

Specific Card Alarms

The following table lists the card specific failure alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
PHY0 UNKNOWN TYPE/ 11450401	CRITICAL/ 100	Cannot identify PHY card type.	PHY 0 Unknown Type	apSysMgmtHardwareErrorTrap
PHY1 UNKNOWN TYPE/ 11451402	CRITICAL/ 100	Cannot identify PHY card type.	PHY 1 Unknown Type	apSysMgmtHardwareErrorTrap
PHY2 UNKNOWN TYPE/ 11452403	CRITICAL/ 100	Cannot identify PHY card type.	PHY 2 Unknown Type	apSysMgmtHardwareErrorTrap
PHY3 UNKNOWN TYPE/ 11453404	CRITICAL/ 100	Cannot identify PHY card type.	PHY 3 Unknown Type	apSysMgmtHardwareErrorTrap
PARITY ERROR/ 11420402	MAJOR/ 50	Parity error detected.	• Hardware Error in HSTRL: X, HINTR: Y • Hardware Error in HRSTR: X • Hardware Error in HPER: X • Hardware Error in CPER: X • Hardware Error in MPER: X • Hardware Error in XPER: X • Testing Alarm for PE/CAM exceptions	apSysMgmtHardwareErrorTrap

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
CAM EXCEPTION/ 11420403	• MAJOR-First time alarm is posted • CRITICAL-Second time alarm is posted without a clear • EMERGENCY-Third time alarm is posted without a clear/ • 50, 100	CAM exception detected.	• Cam Search Semaphore Error, Err Code X, Err: Y • Cam Operation Failure, Err Code X, Err: Y	apSysMgmtHardwareErrorTrap
QOS ERROR/ 11420404	MAJOR/ 50	QoS error detected.	• Hardware Error in QoS_FPGA_config ( ) • Error in QoS_daemon_init ( ) • Hardware Error: QoS FPGAs initialized in failed state • Gimp HW Error, Err: X, Gimp: Y ISR_Vector: Z	apSysMgmtHardwareErrorTrap
NPM FAILURE/ 11420405	MAJOR/ 100	NPM failure detected.	Media Startup failed	apSysMgmtHardwareErrorTrap
IPT Failure/ 11420406	EMERGENCY	IPT test failure	IPT NP path Runtime Failure	
DSP FAILURE TCUX BASE/ 1003X5ZZ	MINOR CRITICAL/ 20, 100	DSP failed in TCU.	• DSP device N failed to boot • DSP device N failed to INITIALIZE • DSP DEVICE CRASHED • DSPComms Timeout • Rebooted DSP device • VAPI Request Timeout	None

Miscellaneous Hardware Alarms

The following table lists the miscellaneous hardware alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Example Log Message	Trap Generated
ETH_RATE_ERROR/ 11400408	MAJOR/ 50	Connection error between processors or processor not connected.	• Internal network eth[x] cannot achieve full line rate	None

System Alarms

System alarms include information about NIU and MIU port status, hardware threshold status, redundancy status and other system operating conditions on the Net-Net 9200.

NIU Link Alarms

The following table lists the NIU link alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
LINK DOWN ALARM GIGPORT/ 20250016-20250031	CRITICAL/ 75	Gigabit Ethernet interface goes down.	PHY X::Port N Link State is Inactive	linkDown

MIU Link Alarms

The following table lists the MIU link alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
LINK DOWN ALARM VXINTF 0/ 20240003	CRITICAL/ 75	MIU 0 goes down.	MIU X Link Is Down	linkDown
	CRITICAL/ 75	MIU 1 goes down.	MIU X Link Is Down	linkDown
	CRITICAL/ 75	MIU 2 goes down.	MIU X Link Is Down	linkDown

NPU Link Alarms

The following table lists the NPU link alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
SWING VIX ALARM/ 21420301	MINOR/ 20	Status check failed.	VIX Status Check Failed	apSysMgmtHardwareErrorTrap
SWING VIX ALARM DOWN IN PORT A/ 21420302	WARNING/ 0	Inbound port A is down.	VIX In-Port-A Down	apSysMgmtHardwareErrorTrap
SWING VIX ALARM DOWN IN PORT B/ 21420303	WARNING/ 0	Inbound port B is down	VIX In-Port-B Down	apSysMgmtHardwareErrorTrap
SWING VIX ALARM DOWN IN PORT A/ 21420304	WARNING/ 0	Outbound port B is down.	VIX Out-Port-A Down	apSysMgmtHardwareErrorTrap
SWING VIX ALARM DOWN IN PORT B/ 21420305	WARNING/ 0	Outbound port B is down.	VIX Out-Port-B Down	apSysMgmtHardwareErrorTrap
SWING PLL ALARM/ 21420306	MINOR/ 20	Status check failed.	PLL Status Check Failed	apSysMgmtHardwareErrorTrap
SWING PLL ALARM DOWN PORT A/ 21420307	WARNING/ 0	Port A is down.	PLL Port A Down	apSysMgmtHardwareErrorTrap
SWING PLL ALARM DOWN PORT B/ 21420308	WARNING/ 0	Port B is down	PLL Port B Down	apSysMgmtHardwareErrorTrap

SWING QOS ALARM DOWN PORT A/ 21420309	WARNING/ 5	Port A is down.	QoS Port A Down	apSysMgmtHardwareErrorTrap
SWING QOS ALARM DOWN PORT B/ 2142030A	WARNING/ 5	Port B is down.	QoS Port B Down	apSysMgmtHardwareErrorTrap
SWING FLAIR ALARM/ 2142030B	MINOR/ 20	FPGA link check failed.	• Flair FPGA Link Check Failed • NPU X Failed to set Swingline FPGA port selector to N • NPU X Failed to set Swingline FPGA TCU Mask to N	apSysMgmtHardwareErrorTrap
SWING FLAIR ALARM DOWN PORT 0/ 2142030C	WARNING/ 0	Port 0 is down.	Flair FPGA Port 0 Down	apSysMgmtHardwareErrorTrap
SWING FLAIR ALARM DOWN PORT 1/ 2142030D	WARNING/ 0	Port 1 is down.	Flair FPGA Port 1 Down	apSysMgmtHardwareErrorTrap
SWING FLAIR ALARM DOWN PORT 2/ 2142030E	WARNING/ 0	Port 2 is down.	Flair FPGA Port 2 Down	apSysMgmtHardwareErrorTrap

TCU Link Alarms

The following table lists the TCU link alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
FLAIR SWING ALARM/ 21430301	MINOR/ 20	FLAIR driver was not set to the active NPU.	TCU *XX* Failed to Set FLAIR Driver to Active NPU *YY*.	apSysMgmtHardwareErrorTrap

Utilization Alarms

The following table lists the system utilization alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
MEM UTIL OVER THRESHOLD/ 21E00104	MINOR WARNING NOTICE/ 5	Memory usage has changed.	Memory usage was XX percent and now is YY percent	apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)
CPU UTIL OVER THRESHOLD/ 21E00103	WARNING NOTICE/ 5	CPU usage has changed.	CPU usage was XX percent and now is YY percent	apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)

NAT UTIL OVER THRESHOLD/ 21E20105	MINOR/ 20	NAT usage has changed.	NAT table capacity XX percent is over threshold YY percent (exclude deny list).	apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)
ARP UTIL OVER THRESHOLD/ 21E20106	MINOR/ 20	ARP table usage reached 90% or greater of its capacity.	ARP table capacity XX percent is over threshold YY percent	apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)

Health Score Alarms

The following table lists the health score alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
SYS HEALTH ALERT/ 200X0201	EMERGENCY CRITICAL MINOR/ 100, 75, 20	• Boot timeout occurs • Register timeout occurs • Manifest timeout occurs • Ready timeout occurs • Becoming Active timeout occurs • Becoming Standby timeout occurs • Becoming OOS timeout occurs	• Boot Timeout on slot XX • Register Timeout on slot XX • Manifest Timeout on slot XX • Ready Timeout on slot XX • Becoming Active Timeout on slot XX • Becoming Standby Timeout on slot XX • Becoming OOS Timeout on slot XX	apSyslogMessageGenerated
SYS HEALTH UNDER THRESHOLD/ 21EX0210	NOTICE/ 0	Net-Net system's health is under threshold 50.	Health Score Dropped to XX on Card YYY	apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)
SYS HEALTH TIMEOUT/ 200X0202	MINOR/ 20	Health check timeout occurs	Health Check Timeout on Card XX	apSyslogMessageGenerated
SYS HEALTH RESET/ 200Z0203	EMERGENCY/ 100	A card has failed to boot.	Card XX has failed to boot	apSyslogMessageGenerated

Redundancy Alarms

The following table lists the redundancy alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
SYS SWITCH TO UNASSIGNED/ 226ZZ221	NOTICE/ 0	A state transition occurred to Unassigned.	<Name of HA peer> Switchover to Unassigned Role	apSysMgmtSingleUnitRedundancyTrap OR apSyslogMessageGenerated (See Note 2)
SYS SWITCH TO ACTIVE/ 226ZZ222	NOTICE/ 0	A state transition occurred from Standby/BecomingStandby to BecomingActive.	NName of HA peer> Switchover to Active Role	apSysMgmtSingleUnitRedundancyTrapOR apSyslogMessageGenerated (See Note 2)

SYS SWITCH TO STANDBY/ 226ZZ223	NOTICE/ 0	A state transition occurred from Active/BecomingActive to BecomingStandby/RelinquishingActive.	Name of HA peer> Switchover to Standby Role	apSysMgmtSingleUnitRedundancyTrap OR apSyslogMessageGenerated (See Note 2)
SYS SWITCH TO RECOVERY/ 226ZZ224	NOTICE/ 0	A state transition occurred to Recovery.	<Name of HA peer> Switchover to Recovery Role	apSysMgmtSingleUnitRedundancyTrap OR apSyslogMessageGenerated (See Note 2)
SYS SWITCH TO OUTOFSERVICE/ 226ZZ225	NOTICE/ 0	Unable to synchronize with Active HA Net-Net system peer within BecomingStandby timeout.	<Name of HA peer> Switchover to Out-of-Service Role	apSysMgmtSingleUnitRedundancyTrap OR apSyslogMessageGenerated (See Note 2)

System Task Alarms

The following table lists the system task alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
SYS TASK SUSPENDED/ 20A00101	MAJOR/ 50	A Net-Net system task (process) suspends or fails.	Task XX Failed to Spawn	apSysMgmtTaskSuspendTrap
	EMERGENCY/ 100		Task XX with PID YY is Suspended	
	EMERGENCY/ 100		Task XX with PID YY is Stopped	
	EMERGENCY/ 100		Task XX no longer Running	
	WARNING/ 5		Task XX not ready	

System State Alarms

The following table lists the system state alarm information.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
SYS SNMP AUTH FAILURE/ 20110233	MAJOR/ 0	SNMP authentication failure	• SNMP Agent got improper request from community XXX at address YYY • SNMP Agent received bad community string XXX from address YYY	authenticationFailure (See Note 3)
SYS PASSWORD RESET/ 20000236	NOTICE/ 0	Password reset to factory defaults	SA Status Change	None

System Miscellaneous Alarms

The following table lists miscellaneous system alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
NPU NONE ACTIVE/ 20020401	EMERGENCY/ 100	No NPUs are active or present.	• System Unable to Run - No NPUs Active • System Unable to Run - No NPUs present	apSyslogMessageGenerated
PHY NONE ACTIVE/ 20050402	EMERGENCY/ 100	No PHYs active or configured.	• No PHYs Active to Pass Media • No PHYs Configured to Pass Media	apSyslogMessageGenerated
RDP LINK DOWN ALARM/ 20ZZ0001	EMERGENCY NOTICE/ 0, 100	The core is non-responsive.	• Core X.X.X Link is Non-Responsive • Internal Communication Link Down (XX = => YY)	apSyslogMessageGenerated
IFSTRUCT CORRUPT ALARM/ 20000501	MAJOR/ 50	The interface structure is corrupt.	• An internal data structure is corrupt and the system may not behave properly – Error Code <X>	apSyslogMessageGenerated

Low Disk Space Alarm

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
SPACE_LOW_THRES_ ALARM_PCMIA / 24400100	User configurable/Non-health affecting	Storage space on the PCMCIA FLASH card is low; thresholds are configurable.		apSysMgmtSpaceAvailThresholdTrap

Switch Alarms

NPU Switch

The following table lists the alarms for the NPU switch.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
DX240 ERROR/ 10020300	MINOR MAJOR/ 20	NPU failed to switch over.	• NPU nn Failed to Switchover to Active Status • NPU nn Failed to Switchover to Standby Status • NPU nn Failed to Switchover to OOS Status • NPU nn Switch Failed to Perform Health Check • NPU nn Failed to initialize PHY YY • NPU nn Failed to connect to Active PHY YY • DX240 Phy Reg Read Failed • DX240 Phy Reg Write Failed • DX240 Reg Write Failed • DX240 Reg Read Failed • Fatal Dx240 Interrupt • Minor DX240 Error	apSyslogMessageGenerated
DX240 DOWN ALARM GMAC 0/ 10020302-1002030A	MAJOR/ 50	GMAC port link state is inactive.	GMAC Port nn Link State is Inactive	apSyslogMessageGenerated

SPU Switch

The following table lists the alarms for the SPU switch.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
BCM56K PCI BUS ERR/ 10010300	MAJOR/ 50	PCI Error	BROADCOM 56304 sysconf_attach PCI error on soc_unit X	apSyslogMessageGenerated

Network Alarms

The following table lists the network alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
MEDIA GATEWAY ALARM/ 310Z0ZZZ	MAJOR/ 25	Gateway is unreachable.	Gateway N.N.N.N unreachable on slot X, port Y, subport Z	apSysMgmtGatewayUnreachableTrap OR apSyslogMessageGenerated (See Note 2)
GW unreachable/ 31000000	EMERGENCY	GW heartbeat test failure	gateway x.x.x.x unreachable on slot Y port Z subport ZZ	

Media Alarms

Media alarms include events related to MBCD exception conditions. The following table lists the MBCD media alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
MBCD ALARM OUT OF MEMORY/ 40E00001	CRITICAL: for flow MAJOR: for media (if server cannot allocate a new context)/ 0	No further memory can be allocated for MBCD.	• Flow: Cannot create free port list for realm 'XXX'. • Failed to allocate new context • Media XX Timer Expired: camid=YY: unable to allocate request, context or command! dropping Flow.	apSysMgmtMediaOutOfMemory OR apSyslogMessageGenerated (See Note 2)
MBCD ALARM INTERNAL / 40000002	MAJOR MINOR/ 0	An internal software error.	Internal Error. No agent for socket <IPPort>.	apSyslogMessageGenerated
MBCD ALARM UNKNOWN REALM / 40F00003	MINOR/ 0	Media server is unable to find realm interface.	• ingress realm XXX not found • egress realm XXX not found	apSysMgmtMediaUnKnownRealm OR apSyslogMessageGenerated (See Note 2)
MBCD ALARM OUT OF BANDWIDTH / 40D00005	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50% / 0	The realm is out of bandwidth.	out of bandwidth	spSysMgmtMediaBandwidthTrap OR apSyslogMessageGenerated (See Note 2)
MBCD ALARM OUT OF PORTS / 40C00006	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%/ 0	The realm is out of steering ports.	out of steering ports	apSysMgmtMediaPortsTrap OR apSyslogMessageGenerated (See Note 2)

Application Alarms

Application alarms include events related to application exceptions on the Net-Net system.

RADIUS Connection Down Alarm

The following table lists the RADIUS connection down alarm.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
APP ALARM LOST ACCT CONN/ 51100001	CRITICAL: if all enabled and configured RADIUS accounting server connections have timed-out without response from the RADIUS server MAJOR: if some, but not all configured RADIUS accounting server connections have timed-out without response from the RADIUS server./ 1	The enabled connections to RADIUS servers have timed-out without a response from the RADIUS server.	CRITICAL: All enabled accounting connections have been lost! Check accounting status for more details. MAJOR: One or more enabled accounting connections have been lost! Check accounting status for more details.	apSysMgmtRadiusDownTrap OR apSyslogMessageGenerated (See Note 2)
APP_ALARM_EPS_RACF_CONN_FAIL	MINOR/0	Connection to External Policy Server has been lost.	Connection to External Policy Server (RACF) has been lost!!!	apSysMgmtExtPolicyServerConnDownTrap

Application Alarms

The following table lists the application alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
APP ALARM APPROACH LIC SESS CAP/ 51B00004	MAJOR/ 1	Total number of active sessions on the system (across all protocols) is within 98 to 100% of the Net-Net system's licensed capacity.	Total number of sessions (<#>) is approaching licensed capacity (<#>)	apSyslogMessageGenerated or apLicenseApproachingCapacityNotification (See Note 2)
COLLECT_ALARM_PUSH_FAIL /	MAJOR if all push receivers are unreachable MINOR if a push receiver is unreachable while other(s) are still reachable.	The push receivers are unreachable.	"Some or all of collector's push receivers are down" "All of collector's push receivers are down"	apSysMgmtPushServerUnreachableTrap apSysMgmtPushServerUnreachableClearTrap

Configuration Alarms

The following table lists the configuration alarms.

Name/ID	Severity/ Health Degradation	Cause(s)	Example Log Message	SNMP Traps Sent
CFG ALARM SAVE FAILED/ 61300001	MAJOR/ 1	The save config command execution failed on a standby Net-Net SBC peer operating as part of an HA pair.	Save Config Failed	apSysMgmtCfgSaveFailTrap

Note: 1. If the "enable-env-monitor-traps" parameter under the system-config configuration element is enabled, this trap is sent. If the parameter is disabled, the "asSyslogMessageGenerated" trap is sent instead.

Note: 2. If the "enable-snmp-monitor-traps" parameter under the system-config configuration element is enabled, this trap will be sent. If the parameter is disabled, the "apSyslogMessageGenerated" trap is sent instead if configured to enable-syslog-notify.

Note: 3. If the "enable-snmp-auth-traps" option under system-config is disabled, this trap will not be sent.

Graphic Display

The graphic display lets you view information about the system's operational status and current alarms at a glance. In addition, you can silence alarms from the front panel of the Net-Net 9200 chassis.

For a complete description of the graphic display operation, please see the *Net-Net 9200 Hardware Guide* for more information.

3 System Management

Commands discussed in this chapter are used for Net-Net OS management and system administration.

Global System Parameters

This section contains information about global system show commands.

System State

The following show commands are explained in this section:

- uptime
- state
- version
- clock
- bootparams

show uptime

The **show uptime** command displays current date and time information and the length of time the system has been running in days, hours, minutes, and seconds. For example:

```
ACMEPACKET# show uptime
  System Uptime:      5 Days, 14 Hours 23 Minutes 30 Seconds
```

show system

The **show system** command displays environmental, uptime, and memory information about the Net-Net system. For example:

```
ACMEPACKET# show system
System Uptime:      5 Days, 14 Hours 23 Minutes 52 Seconds
  Temperature Status: Normal
  Voltage Status:     Normal
  Fan Status:         Alarm
  CPU Status:         Normal
  Memory Status:      Normal
```

show version

The **show version** command displays the Net-Net OS version currently running on the hardware. This command also displays the current configuration version and the running configuration version. For example:

```
ACMEPACKET# show version
NN9200 Software Version:      5.0.0 Beta Workspace (Build 19)
NN9200 Software Build Date:   06/30/06
Built in /home/NEOBETA on acme33

Current config version:      761
Running config version:      761
```

show clock

The show clock command displays the current UTC system time and date. For example:

```
ACMEPACKET# show clock
System Time: 11:51:02  - Thu Jul 06 2006
```

show bootparams

The **show bootparams** command displays the boot parameters for both SPUs.

- boot device and unit number—describe the Net-Net 9200's management interface that is used to boot from the network
- processor number—only used for administrative purposes
- inet on ethernet—IP address of the MIU Ethernet boot interface
- host inet (h) —network TFTP server's IP address that hosts the boot image file
- gateway inet (g)—gateway IP address for the management network, where the boot image is located.
- user (u) and ftp password (pw)—user and password pair for connecting the TFTP server.
- flags (f)—only used for administrative purposes
- target name (tn)—name that appears behind the > or # at the system prompt.

The virtual management interface and gateway are also displayed. A virtual management interface IP Address is assigned to the MIU's Ethernet port on the active SPU/MIU pair. This means that you can Telnet to the configured virtual address, and you will be connected to the active SPU, regardless of which physical SPU is active.

All parameters visible in the bootparams are configurable by using the **set bootparams** command.

For example:

```
ACMEPACKET# show bootparams

 Boot parameters stored on ACTIVE SPU :

--- Slot 0 Boot Parameters ---


boot device          : eth
unit number          : 2
processor number     : 0
file name            : sd4xx.tar
inet on ethernet (e) : 172.30.92.94
host inet (h)        : 172.30.0.25
gateway inet (g)     : 172.30.0.1
user (u)             : *****
ftp password (pw)    : *****
flags (f)            : 0x0
target name (tn)     : ACMEPACKET


--- Slot 1 Boot Parameters ---
```

```
boot device          : eth
unit number          : 2
processor number     : 0
file name            : sd4xx.tar
inet on ethernet (e) : 172.30.92.92
host inet (h)        : 172.30.0.25
gateway inet (g)     : 172.30.0.1
user (u)             : *****
ftp password (pw)    : *****
flags (f)            : 0x0
target name (tn)     : ACMEPACKET


--- Virtual Management Interface Parameters ---

Interface IP Address: 172.30.92.96
Gateway IP Address:   172.30.0.1
```

Installed Features

You can audit the enabled features on the Net-Net 9200 by using the **show features** command. For example:

```
ACMEPACKET# show features
            64000 SIP sessions
            SIP, QOS, Routing, Load Balancing, Accounting
```

The same information is found by watching the boot process of the Net-Net 9200, however this command can be invoked without a system reboot.

Task Overview

Tasks run across the Net-Net system's multiple CPUs and cores. To aid in debugging, the following information is essential.

- For a given core, show the local tasks
- Show the core where each major application runs

Note: SPU2/NPU2-based systems may reflect tasks running on different CPUs/Cores than the following SPU1/NPU1-based examples.

show cpu

The **show cpu** command displays the top 15 tasks active on a specified core. Enter the **show cpu** command with the slot.cpu.core location in dotted notation. The output of this command includes the following information:

- Task Name—Name of the Net-Net system task or process.
- Task Id—Identification number for the task or process.
- Pri—Priority for the task's CPU usage.
- Status—Status of the task's CPU usage.
- Total CPU—Task's total CPU usage since last reboot.
- Avg—Displays percentage of CPU usage since the Net-Net system was last rebooted.
- Now—Task's CPU usage in the latest sample (1-2 seconds).

Note: Adding the **all** argument after the core location returns the load for all tasks on the given core.

For example:

```
ACMEPACKET# show cpu 0.0.0
CORE=0.0.0
------------------  -------- --- ---------- -------------- ----- -----
Task Name            Task Id Pri Status          Total CPU   Avg   Now
------------------  -------- --- ---------- -------------- ----- -----
iAcli               c4c7eb50 100 READY              4.198   0.0   1.2
bcmL2X.0            c477b050  50 PEND+T          27:35.258   0.3   0.4
tNetTask            c1a12010  50 PEND           26:11.257   0.3   0.3
bcmCNTR.0           c474e200  50 PEND+T          15:57.280   0.1   0.2
iCm                 c4d1f260 100 PEND+T           6:33.093   0.0   0.1
iNtpd               c4cf7c00 100 PEND+T           2:10.053   0.0   0.0
tTffsPTask          c1a15010 100 DELAY            1:43.432   0.0   0.0
iTestman            c4d9e020 100 PEND+T           1:35.513   0.0   0.0
iSm                 c4b8b6e0 100 PEND+T           1:33.421   0.0   0.0
iLogman             c4caebf0 100 PEND+T           1:25.082   0.0   0.0
tEth0CpuRx          c1a8f030  50 PEND             1:12.983   0.0   0.0
tDcacheUpd          c458d780 250 DELAY              59.307   0.0   0.0
iLcm                c4769450  60 READY              52.671   0.0   0.0
tSSH                c4c9c1b0  55 PEND+T             42.808   0.0   0.0
tIdle               c1a15350 255 READY       131:59:12.790  98.1  96.9
```

By using the optional **summary** argument, the command returns the total and current CPU load for each core. In addition, the two tasks with the current highest CPU usage per listed core are displayed. For example:

```
ACMEPACKET# show cpu summary
 Core   Cur/Total      Task: Current/Total          Task: Current/Total
------  ---------   ----------------------   -------------------------
0.0.0    2.0/20.2           bcmLSM:  0.9/0.9          tNetTask:  0.4/3.3
0.0.1    0.2/0.2          tNetTask:  0.1/0.0              tLCM:  0.0/0.0
```

- Cur (Current)—CPU usage in the latest sample (1-2 seconds)
- Total—Total CPU percentage is computed as follows:

$$\text{Total CPU \%} = (\text{Core Uptime} - \text{tIdle time}) / \text{Core Uptime}$$

show manifest

The **show manifest** command displays application tasks, their location, and internal address and socket used for communication. For example:

```
ACMEPACKET# show manifest
Location   Task       IPPort
 0.0.0     snmpd      169.254.160.0:8031
 0.0.1     dnsres     169.254.160.1:8022
 0.0.1     rasm       169.254.160.1:8030
 0.1.0     sipt       169.254.160.16:8008
 0.2.0     sipc       169.254.160.32:8010
 0.4.1     sipls      169.254.160.65:8009
 1.0.0     snmpd      169.254.161.0:8031
 1.0.1     dnsres     169.254.161.1:8022
 1.0.1     rasm       169.254.161.1:8030
 1.1.0     sipt       169.254.161.16:8008
 1.2.0     sipc       169.254.161.32:8010
 1.4.1     sipls      169.254.161.65:8009
 2.0.0     mbcd       169.254.162.0:8011
 2.0.0     sfe        169.254.162.0:8013
 3.0.0     mbcd       169.254.163.0:8011
 3.0.0     sfe        169.254.163.0:8013
```

User Sessions

Multiple Telnet, SSH, FTP, or SFTP sessions can be active on the Net-Net 9200 simultaneously. You can view the status of each session and terminate (kill) an active session from the ACLI.

show users

The **show users** command displays all active sessions on the Net-Net 9200. For example:

```
ACMEPACKET# # show users
Index      remote-address IdNum   duration      type    state redirect
-----      -------------- -----   --------      ----    ----- --------
    0                         1    2:40:01   console0   priv*
    1     10.1.20.105:2844     2    2:39:25    telnet0   user
    2                         3    2:39:17   console1  login
    3     10.1.20.105:2848     5    2:36:41       ssh0   priv C
```

The IdNum of each session is used for identifying which session to terminate. The session with an asterisk, *, trailing the state is the one you are logged in from. The session with a C trailing the state is in configuration mode. Any session with a trailing caret, ^, is dead and must be manually terminated.

Identifying Config Sessions

If you are denied from entering configuration mode because another session is in configuration mode, the ACLI will print the following warning:

```
ACMEPACKET# configure terminal


Configuration menu in use.
ACMEPACKET#
```

To identify which session is in configure mode, use the **show users** command. In the following example, the session with IdNum 5 is in config mode as noted by the C next to its state column:

```
ACMEPACKET# # show users
Index      remote-address IdNum   duration      type    state redirect
-----      -------------- -----   --------      ----    ----- --------
    0                         1    2:40:01   console0   priv*
    1     10.1.20.105:2844     2    2:39:25    telnet0   user
    2                         3    2:39:17   console1  login
    3     10.1.20.105:2848     5    2:36:41       ssh0   priv C
```


Terminating Sessions

In order to manually terminate a Telnet or SSH session on the Net-Net 9200, the **kill** command is used. The **kill** command is used in conjunction with a session IdNum, obtained from the output of the show users command. For example:

```
ACMEPACKET# kill 5
```

After executing the **kill** command, the chosen session is terminated immediately without any warning or confirmation message.

Management Applications

The Net-Net 9200 runs Telnet, FTP, and SSH applications as a means to be configured and for file retrieval. Each of these applications

show telnet

The **show telnet** command displays whether the telnet daemon is enabled or not. For example:

```
ACMEPACKET# show telnet
Telnet is enabled
```

show ftp

The **show ftp** command displays whether the FTP daemon is enabled or not. For example:

```
ACMEPACKET# show ftp
Ftp is enabled
```

show ssh

The **show ssh** command displays SSH operating parameters for each slot on the Net-Net SBC. For example:

```
ACMEPACKET# show ssh
slot 0 :
        cnum            0
        mastrFD         397
        slaveFD         398
        pipe            /pipe/ssh0
        pipeFD          396
        sesID           0
        socket          -1
        sshHdl          0
        outTID          -1
        waitTID         -1
```

Statistic Counts Explained

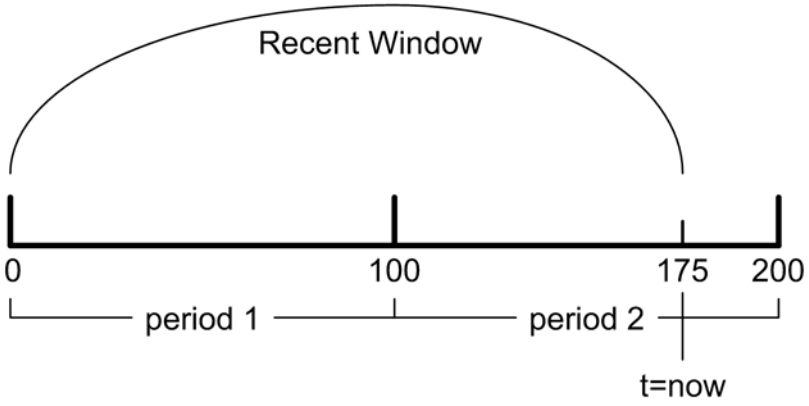
Statistical counts are based on the Net-Net OS defining a period as 100 seconds. The Recent window represents the previous complete period (100 seconds) plus the time incurred into the current period.

When you execute a **show** command, a timestamp and the period count are displayed. The period count, the number after the dash, indicates the number of seconds into the recent period. Therefore, the recent window ranges from 100 to 199 seconds. For example:

```
ACMEPACKET# show amp lcm@0.0.0
12:10:21-175 (lcm@0.0.0) ID=10000
```

In the diagram below, the Net-Net OS is 75 seconds into the current period. The Recent window includes the previous 75 seconds, plus an extra 100 seconds (1

period) before that. After period 3 is entered (not pictured below), the Recent window will begin at the 100 second mark.



For statistical displays, the columns are defined as follows:

- Active represents the current number of active counts.
- Recent High represents the highest number during the recent window.
- Recent Total represents the total accumulated count during the recent window.

The three lifetime statistics begin accumulating since the last reboot.

- Lifetime Total represents the total accumulated count.
- Lifetime PerMax represents the maximum recorded in one period.
- Lifetime High represents the highest momentary count.

Task Statistics

The commands listed in this section are used to view task statistics and related information.

Task Statistic Overviews

The following **show** commands display high-level statics for tasks based on their active or standby status.

show task active

The **show task active** command displays overview statistics for all active application tasks on all cores. For example:

```
ACMEPACKET# show task active

  Task Name    Per   Msgs   Trans   Timers   TOQs  PerCPU Total-CPU MaxCPU
--------------- --- ------- ------- ------- ------- ------ --------- --
sipt@0.0.0     118       4       0      20       1    0.0      6.10    0.0
sipc@0.0.0     118       3       0      20       1    0.0      3.77    0.0
sipls@0.0.0    118       3       0      20       1    0.0      3.74    0.0
dnsres@0.0.0   118       4       0      17       0    0.0      1.74    0.0
rasm@0.0.0     118       3       0      18       0    0.0      1.61    0.0
mbcd@2.0.0     194       4       0      20       1    0.0    108.80    0.0
sfe@2.0.0      194       4       0      21       0    0.0     20.59    0.1
natm@2.0.0     194       5       0      21       1    0.0      2.60    0.1
arpm@2.0.0     194       5       0      21       1    0.0     21.47    0.0
npm@2.0.0      194       5       0      23       1    0.0     21.05    1.5
sptx@2.0.0     194       4       0      19       0    0.0      6.42    0.0
```

show task standby

The **show task standby** command displays overview statistics for all application tasks on all standby cores. For example:

```
ACMEPACKET# show task standby

  Task Name    Per   Msgs   Trans   Timers   TOQs  PerCPU Total-CPU MaxCPU
----------- --- ------- ------- ------- ------- ------ --------- ------
logman@1.0.0    136      5       0      18       0    0.0      0.65    0.0
rasm@1.0.0      136      3       0      19       1    0.0     12.92    0.0
snmpd@1.0.0     136      3       0      18       0    0.0      0.10    0.0
sshd@1.0.0      136      3       0      18       0    0.0      0.08    0.0
auth@1.0.0      136      3       0      22       1    0.0     12.80    0.0
sfe@1.0.0       136      4       0      18       1    0.0     17.25    0.0
sfe@1.0.1       133      4       0    5018       1    0.0     15.07    0.3
dnsres@1.0.1    133      4       0      17       0    0.0      0.14    0.0
soapd@1.0.1     133      4       0      19       1    0.0      2.93    0.0
sipt@1.1.0      197      5       0      16       1    0.0      3.11    0.0
sipc@1.1.1      195      3       0      15       1    0.0      5.44    0.0
sipt@1.2.0      198      5       0      16       1    0.0      3.10    0.0
sipc@1.2.1      195      3       0      15       1    0.0      5.44    0.0
sipls@1.3.0     198      3       0      16       2    0.0      3.60    0.0
sipc@1.3.1      195      3       0      15       1    0.0      5.48    0.0
natm@2.0.0      141      5       0      19       0    0.0      0.13    0.0
arpm@2.0.0      141      5       0      19       1    0.0     11.44    0.0
npm@2.0.0       141      4       0      18       1    0.0      5.15    2.3
npcli@2.0.0     141      3       0      18       1    0.0      5.40    0.0
mbcd@2.0.1      138      4       0      25       1    0.0      6.73    0.2
xserv@6.0.0     144      3       0      24       2    0.2     97.85    0.2
```

Individual Task Statistics

The **show task command** is used to display statistics about a supplied task. This command only accepts a pre-defined set of tasks as arguments.

The **show task command** usage is as follows:

```
ACMEPACKET# show task <task>
```

where task is:

```
<name>@<card>.<cpu>.<core>
```

You may use wildcards anywhere in the task argument. For example:

```
ACMEPACKET# show task sip*@*
```

The above command returns all tasks that begin with sip at all slot/cpu/core locations on the Net-Net system.

In each task's show command output, the following statistics are displayed:

- Services—Number of times the process performs actions for different services
- Messages—Number of messages the process created and processed
- Alloc Buffers—
- Free Buffers—
- Transactions—Number of client or server transactions, both sending and receiving, for a particular process
- Timed Objects—Number of objects with timers associated with them

- TOQ Entries—Number of active timers (in the Timed Objects) placed in the timeout queue
- Operations—Number of times the process is prompted (or polled) to perform an action
- Messages Received—Number of messages received by the task
- Messages Sent—Number of messages sent by the task
- Partial Message—Number of partial messages
- Part Msg Expired—Number of times the process set a timer for a partial message and that timer expired, prompting the process to make a decision about whether to process the partial message or drop it
- Part Msg Dropped—Number of times the process set a timer for a partial message and that timer expired, prompting the process to drop the partial message
- Timed Events—Number of times a TOQ Entry timed out
- Alarms—Number of alarms the process sent
- System Logs—Number of times the process wrote to the system log
- Process Logs—Number of times the process wrote to the process log
- Remote Logs—
- Load Rate—This statistic shows an approximation (in a percentage) of time that the process has been processing

show task acli

The ACLI task statistics are displayed as follows:

```
ACMEPACKET# show task acli
09:48:56-130 (acli@0.0.0) ID=10000
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 16      16       0         16      16      16
Messages                  5       5      70       4439     241       6
Alloc Buffers            48      48       0         48      48      48
Free Buffers              0       0       0          0       0       0
Transactions              0       0       0          0       0       0
Timed Objects            17      17       0         17      17      17
TOQ Entries               0       0       0          0       0       0
CPU Slices                -       -      92       2516     110
Operations                1       1      28       2085      23       1
Messages Received         -       -      34       2219     120
Messages Sent             -       -      34       2223     123
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              0       0       0          0       0       0
Max Timed Events          0       0       0          0       0       0
Alarms                    -       -       0          0       0
System Logs               -       -       0          4       2
Process Logs              -       -       8        113      45
Remote Logs               -       -       0          0       0
Load Rate                                0.0%      4.08    0.1%
ACMESYSTEM#
```

show task arpm

The ARP Manager (ARPM) task statistics are displayed as follows:

```
ACMEPACKET# show task arpm
12:20:16-154 (arpm@2.0.0) ID=d46f4000
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   16      16       0         16      16      16
Messages                    5       5     308      62568     198       6
Alloc Buffers              48      48       0         48      48      48
Free Buffers                0       0       0          0       0       0
Transactions                0       1     153      31277      99       2
Timed Objects              19      20     153      31296      99      21
TOQ Entries                 1       1     306      62552     198       1
Operations                  -       -     308      62857     199
Messages Received           -       -     154      31284      99
Messages Sent               -       -     153      31286      99
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Timed Events                -       -     153      31274      99
Alarms                      -       -       0          0       0
System Logs                 -       -       0          1       1
Process Logs                -       -       4        709      73
Remote Logs                 -       -       0          0       0
Load Rate                                0.0%     10.93     0.0%
```

show task auth

The user authentication task statistics are displayed as follows:

```
ACMEPACKET# show task auth
12:20:49-120 (auth@0.0.0) ID=e23c11a0
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   18      18       0         18      17      18
Messages                 1175    1175     260      65250     235    1175
Alloc Buffers              48      48       0         48      48      48
Free Buffers                0       0       0          0       0       0
Transactions               32      32     119      31506     106      38
Timed Objects              54      54     119      31529     107      60
TOQ Entries                34      34     128      32609     112      40
Operations                  -       -     258      65364     212
Messages Received           -       -     130      32624     117
Messages Sent               -       -     129      32628     120
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Timed Events                -       -     128      32575     107
Alarms                      -       -       0          0       0
System Logs                 -       -       0          3       2
Process Logs                -       -       0        226      57
Remote Logs                 -       -       0          0       0
Load Rate                                0.0%     13.02     0.0%
```

show task broker

The broker daemon (broker) task statistics are displayed as follows:

```
ACMEPACKET# show task broker@0.0.0
```

```
12:21:13-144 (broker@0.0.0) ID=e1be8480
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 17      17       0         17      17      17
Messages                  3       3       2         48      33       3
Alloc Buffers            49      49       0         49      49      49
Free Buffers              0       0       0          0       0       0
Transactions              0       0       0          0       0       0
Timed Objects            18      18       0         18      18      18
TOQ Entries               0       0       0         33      33       1
Operations                -       -      77      16829     583
Messages Received         -       -       1          3       2
Messages Sent             -       -       0         64      33
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              -       -       0         32      32
Alarms                    -       -       0          0       0
System Logs               -       -       0          0       0
Process Logs              -       -      75      16630     602
Remote Logs               -       -       0          0       0
Load Rate                                0.0%      2.90    0.1%
```

show task cm

The card manager (CM) task statistics are displayed as follows:

```
ACMEPACKET# show task cm@0.0.0
12:21:34-165 (cm@0.0.0) ID=e1840610
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 16      16       0         16      16      16
Messages                  3       3     363      70275     235       3
Alloc Buffers            48      48       0         48      48      48
Free Buffers              0       0       0          0       0       0
Transactions              0       0       0          0       0       0
Timed Objects            28      28       0         28      28      28
TOQ Entries              11      11     361      70248     239      11
Operations                -       -     331      64210     216
Messages Received         -       -     330      63864     213
Messages Sent             -       -      32       6444      45
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              -       -      32       6381      20
Alarms                    -       -       0          0       0
System Logs               -       -       0          3       2
Process Logs              -       -       4        830     136
Remote Logs               -       -       0          0       0
Load Rate                                0.0%     26.03    0.0%
```

show task collect

The HDR collection task statistics are displayed as follows:

```
ACMEPACKET# show task collect
09:49:41-175 (collect@0.0.0) ID=e4e21f40
```

```
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   16      16       0         16      16      16
Messages                    3       3       2          8       5       4
Alloc Buffers              48      48       0         48      48      48
Free Buffers                0       0       0          0       0       0
Transactions                0       0       0          0       0       0
Timed Objects              19      19       0         19      19      19
TOQ Entries                 1       1      35       2088      20       1
CPU Slices                  -       -      37       2193      23
Operations                  1       1      36       2090      22       1
Messages Received           -       -       1          4       3
Messages Sent               -       -       0          4       2
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Timed Events                0       1      35       2087      20       1
Max Timed Events            0       0       0          0       0       0
Alarms                      -       -       0          0       0
System Logs                 -       -       0          1       1
Process Logs                -       -       0         85      39
Remote Logs                 -       -       0          0       0
Load Rate                                0.0%       0.24    0.0%
```

show task dnsres

The DNS Resolution Server (DNSRES) task statistics are displayed as follows:

```
ACMEPACKET# show task dnsres
12:21:56-180 (dnsres@0.0.1) ID=d431a180
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   16      16       0         16      16      16
Messages                    4       4       4         80      76       5
Alloc Buffers              48      48       0         48      48      48
Free Buffers                0       0       0          0       0       0
Transactions                0       0       0          0       0       0
Timed Objects              17      17       0         17      17      17
TOQ Entries                 0       0       0         30      30       1
Operations                  -       -       3        353      31
Messages Received           -       -       2         25      23
Messages Sent               -       -       1         54      53
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Timed Events                -       -       0         29      29
Alarms                      -       -       0          0       0
System Logs                 -       -       0          1       1
Process Logs                -       -       4        739      97
Remote Logs                 -       -       0          0       0
Load Rate                                0.0%       0.14    0.0%
```

show task ftpdalg

The FTP ALG task statistics are displayed as follows:

```
ACMEPACKET# show task ftpdalg
```

```
12:23:04-155 (ftpdalg@0.0.0) ID=e19fe510
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 17      17       0         17      17      17
Messages                  3       3       2          6       3       3
Alloc Buffers            48      48       0         48      48      48
Free Buffers              0       0       0          0       0       0
Transactions              0       0       0          0       0       0
Timed Objects            18      18       0         18      18      18
TOQ Entries               0       0       0          0       0       0
Operations                -       -       2        325       3
Messages Received         -       -       1          3       2
Messages Sent             -       -       0          5       4
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              -       -       0          0       0
Alarms                    -       -       0          0       0
System Logs               -       -       0          3       3
Process Logs              -       -       0        157      45
Remote Logs               -       -       0          0       0
Load Rate                                0.0%      0.07    0.0%
```

show task h323GkGw The H.323 Gatekeeper/Gateway task statistics are displayed as follows:

```
ACMEPACKET# show task h323GkGw
14:39:06-151 (h323GkGw@0.1.1) ID=d54af390
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 12      12       0         12      12      12
Messages                  4       4       2         34      15       5
Alloc Buffers            36      36       0         36      36      36
Free Buffers              0       0       0          0       0       0
Transactions              0       0       0          0       0       0
Timed Objects            14      14       0         14      14      14
TOQ Entries               1       1      30      69926      20       1
CPU Slices                -       -      32      73424      23
Operations                1       1      31      69932      22       1
Messages Received         -       -       1         17       8
Messages Sent             -       -       0         16       7
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Buffer Overflow           -       -       0          0       0
Timed Events              0       1      30      69925      20       1
Max Timed Events          0       0       0          0       0       0
Alarms                    -       -       0          0       0
System Logs               -       -       0          1       1
Process Logs              -       -       2       1215      27
Remote Logs               -       -       0          0       0
Load Rate                                0.0%      5.88    0.0%
```

show task h323RasGk The H.323 RAS Gatekeeper task statistics are displayed as follows:

```
ACMEPACKET# show task h323RasGk
14:39:23-168 (h323RasGk@0.4.1) ID=d54b0c90
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 13      13       0         13      13      13
Messages                 20      20      86     173784      66      24
Alloc Buffers            39      39       0         39      39      39
Free Buffers              0       0       0          0       0       0
Transactions              8       8      42      86860      25      11
Timed Objects            24      24      42      86876      25      27
TOQ Entries               9       9      75     156790      45      12
CPU Slices                -       -     113     240801      75
Operations                1       2     118     243504      77       2
Messages Received         -       -      43      86892      33
Messages Sent             -       -      42      86891      33
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Buffer Overflow           -       -       0          0       0
Timed Events              0       1      75     156781      45       2
Max Timed Events          0       0       0          0       0       0
Alarms                    -       -       0          0       0
System Logs               -       -       0          1       1
Process Logs              -       -       2       1232      36
Remote Logs               -       -       0          0       0
Load Rate                                0.0%     37.53     0.0%
```

show task lcm The local core manager (LCM) task statistics are displayed as follows:

```
ACMEPACKET# show task lcm@0.0.0
12:23:20-171 (lcm@0.0.0) ID=e0709050
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 17      17       0         17      17      17
Messages                  3       3      55       6989     345       3
Alloc Buffers            48      48       0         48      48      48
Free Buffers              0       0       0          0       0       0
Transactions              0       0       0          0       0       0
Timed Objects            34      34       0         35      35      34
TOQ Entries               1       1      34       6424      33       3
Operations                -       -      54       7291     341
Messages Received         -       -      20        575     331
Messages Sent             -       -      53       6719     103
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              -       -      34       6403      20
Alarms                    -       -       0          0       0
System Logs               -       -       0          3       2
Process Logs              -       -       4        893     159
Remote Logs               -       -       0          0       0
Load Rate                                0.0%      4.99     2.1%
```

show task lem The local element manager (LEM) task statistics are displayed as follows:

```
ACMEPACKET# show task lem@0.0.0
12:23:44-195 (lem@0.0.0) ID=e12da1b0
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 16      16       0         16      16      16
Messages                  3       3       2         42      37       3
Alloc Buffers            48      48       0         48      48      48
Free Buffers              0       0       0          0       0       0
Transactions              0       0       0          0       0       0
Timed Objects            17      17       0         17      17      17
TOQ Entries               0       0       0         38      38       1
Operations                -       -       2        361      37
Messages Received         -       -       1          3       2
Messages Sent             -       -       0         38      37
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              -       -       0         37      37
Alarms                    -       -       0          0       0
System Logs               -       -       0          0       0
Process Logs              -       -       4        702      51
Remote Logs               -       -       0          0       0
Load Rate                                0.0%      0.12    0.0%
```

show task logman The Acmelog log manager (logman) task statistics are displayed as follows:

```
ACMEPACKET# show task logman@0.0.0
12:24:08-119 (logman@0.0.0) ID=e1657e30
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 17      17       0         18      18      18
Messages                  6       6      10       2283     129       7
Alloc Buffers            48      48       0         48      48      48
Free Buffers              0       0       0          0       0       0
Transactions              0       0       0          0       0       0
Timed Objects            18      18       0         19      19      19
TOQ Entries               0       0       0          0       0       0
Operations                -       -       6       1781     237
Messages Received         -       -       5       1465     238
Messages Sent             -       -       0          8       4
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              -       -       0          0       0
Alarms                    -       -       0          0       0
System Logs               -       -       0        284     225
Process Logs              -       -       4       1239      54
Remote Logs               -       -       0          0       0
Load Rate                                0.0%      0.76    0.1%
```

show task mbcd The middlebox control daemon (MBCD) task statistics are displayed as follows:

```
ACMEPACKET# show task mbcd
12:24:22-198 (mbcd@2.0.1) ID=d3dc14c0
```

```
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   16      16       0         16      16      16
Messages                    4       4     242      38967     255       6
Alloc Buffers              48      48       0         48      48      48
Free Buffers                0       0       0          0       0       0
Transactions                0       0       0          1       1       1
Timed Objects              25      25       0         30      30      28
TOQ Entries                 1       1     192      31073     105       3
Operations                  -       -     242      39109     123
Messages Received           -       -      49       7820      77
Messages Sent               -       -     192      31135     167
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Timed Events                -       -     192      31067      99
Alarms                      -       -       0          0       0
System Logs                 -       -       0          1       1
Process Logs                -       -       4        811     171
Remote Logs                 -       -       0          0       0
Load Rate                                0.0%      6.49    0.2%
```

show task msfe

The MSFE task statistics are displayed as follows:

```
ACMEPACKET# show task msfe
12:24:37-148 (sfe@0.0.0) ID=e20a7900
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   16      16       0         16      16      16
Messages                   66      66     294      63487     207      70
Alloc Buffers              48      48       0         48      48      48
Free Buffers                0       0       0          0       0       0
Transactions               31      32     146      31722     101      34
Timed Objects              49      50     146      31740     101      52
TOQ Entries                31      32     146      31755     101      34
Operations                  -       -     295      63733     198
Messages Received           -       -     147      31727     104
Messages Sent               -       -     146      31759     103
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Timed Events                -       -     147      31723      99
Alarms                      -       -       0          0       0
System Logs                 -       -       0          1       1
Process Logs                -       -       4        720      52
Remote Logs                 -       -       0          0       0
Load Rate                                0.0%     17.46    0.0%
```

show task natm

The NAT manager (NATM) task statistics are displayed as follows:

```
ACMEPACKET# show task natm
12:24:52-131 (natm@2.0.0) ID=d53298c0
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
```

```
Services                16      16       0        16      16      16
Messages                 5       5       2        21      19       6
Alloc Buffers           48      48       0        48      48      48
Free Buffers             0       0       0         0       0       0
Transactions             0       0       0         0       0       0
Timed Objects           19      19       0        19      19      19
TOQ Entries              0       0       0         1       1       1
Operations               -       -       2       326       5
Messages Received        -       -       1        11      10
Messages Sent            -       -       0        12      12
Partial Message          -       -       0         0       0
Part Msg Expired         -       -       0         0       0
Part Msg Dropped         -       -       0         0       0
Timed Events             -       -       0         0       0
Alarms                   -       -       0         0       0
System Logs              -       -       0         1       1
Process Logs             -       -       4       704      62
Remote Logs              -       -       0         0       0
Load Rate                                0.0%     0.13    0.0%
```

Note: natm statistics are absent from SPU2/NPU2-based systems for architectural reasons.

show task npm

The NPM task statistics are displayed as follows:

```
ACMEPACKET# show task npm
14:39:40-100 (npm@2.0.0) ID=c4950010
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   16      16       0         16      16      16
Messages                    4       4       2        187      67       5
Alloc Buffers              48      48       0         48      48      48
Free Buffers                0       0       0          0       0       0
Transactions                0       0       0          0       0       0
Timed Objects              18      18       0         18      18      18
TOQ Entries                 1       1     100     348826     125       2
CPU Slices                  -       -     102     352279     105
Operations                  1       1     101     348810     105       3
Messages Received           -       -       1         71      28
Messages Sent               -       -       0        117      46
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Buffer Overflow             -       -       0          0       0
Timed Events                0       1     100     348823     125       2
Max Timed Events            0       0       0          0       0       0
Alarms                      -       -       0          0       0
System Logs                 -       -       0          3       3
Process Logs                -       -       2       1264      57
Remote Logs                 -       -       0          0       0
Load Rate                                0.0%     31.88    2.3%
```

show task ntpd

The NTP task statistics are displayed as follows:

```
ACMEPACKET# show task ntpd
09:51:14-169 (ntpd@0.0.0) ID=c767e310
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 17      17       0         18      18      18
Messages                  4       4      19       1462      48       4
Alloc Buffers            50      50       0         52      52      52
Free Buffers              2       2       0          2       2       2
Transactions              0       0       0          0       0       0
Timed Objects            19      19       0         21      21      21
TOQ Entries               1       1     169      10507     100       2
CPU Slices                -       -     186      11831     131
Operations                1       2     187      11964     143       9
Messages Received         -       -      18       1459      47
Messages Sent             -       -       0          3       2
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              0       1     169      10506     100       2
Max Timed Events          0       0       0          0       0       0
Alarms                    -       -       0          0       0
System Logs               -       -       0          0       0
Process Logs              -       -       0         82      42
Remote Logs               -       -       0          0       0
Load Rate                                0.0%      1.92    0.0%
```

show task rasm

The Radius Accounting System Manager (RASM) task statistics are displayed as follows:

```
ACMEPACKET# show task rasm
12:42:13-104 (rasm@0.0.0) ID=e2a73160
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 16      16       0         16      16      16
Messages                 65      65     206      65559     207      69
Alloc Buffers            48      48       0         48      48      48
Free Buffers              0       0       0          0       0       0
Transactions             31      32     102      32761     101      34
Timed Objects            50      51     102      32780     101      53
TOQ Entries              31      32     102      32787     101      34
Operations                -       -     207      65815     199
Messages Received         -       -     103      32767     104
Messages Sent             -       -     102      32792     103
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              -       -     103      32755      99
Alarms                    -       -       0          0       0
System Logs               -       -       0          1       1
Process Logs              -       -       4        740      51
Remote Logs               -       -       0          0       0
Load Rate                                0.0%     13.06    0.0%
```

show task secured

The Security Daemon task statistics are displayed as follows:

```
ACMEPACKET# show task secured
14:39:53-101 (secured@0.2.0) ID=d54c4910
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 12      12       0         12      12      12
Messages                 68      68     204     695014     241      72
Alloc Buffers            36      36       0         36      36      36
Free Buffers              0       0       0          0       0       0
Transactions             32      32     101     347458     100      35
Timed Objects            47      47     101     347473     100      50
TOQ Entries              33      33     202     696242     200      36
CPU Slices                -       -     269     900556     300
Operations                1       2     304    1041810     300       6
Messages Received         -       -     102     347509     121
Messages Sent             -       -     101     347503     120
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Buffer Overflow           -       -       0          0       0
Timed Events              0       1     202     696208     200       2
Max Timed Events          0       0       0          0       0       0
Alarms                    -       -       0          0       0
System Logs               -       -       0          0       0
Process Logs              -       -       2       1223      33
Remote Logs               -       -       0          0       0
Load Rate                                0.0%    139.63     0.0%
```

show task sem

The system element manager (SEM) task statistics are displayed as follows:

```
ACMEPACKET# show task sem@0.0.0
12:42:27-118 (sem@0.0.0) ID=e0cbc020
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 16      16       0         16      16      16
Messages                 23      23      66      17995    1168     913
Alloc Buffers            48      48       0         48      48      48
Free Buffers              0       0       0          0       0       0
Transactions             10      10      32       8967     560     456
Timed Objects            29      29      32       8986     579     475
TOQ Entries              11      11      32       9006     599     458
Operations                -       -      64      17706     627
Messages Received         -       -      33       8977     563
Messages Sent             -       -      32       9011     599
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              -       -      30       8994     489
Alarms                    -       -       0          0       0
System Logs               -       -       0          0       0
Process Logs              -       -       4        763      73
Remote Logs               -       -       0          0       0
Load Rate                                0.0%      3.91     0.2%
```

show task sfe

The socket front end (SFE) task statistics are displayed as follows:

```
ACMEPACKET# show task sfe
12:42:38-122 (sfe@0.0.1) ID=cb0ce030
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   16      16       0         16      16      16
Messages                   68      68     244      65630     200      76
Alloc Buffers              48      48       0         48      48      48
Free Buffers                0       0       0          0       0       0
Transactions               32      32     121      32789      99      37
Timed Objects            5050    5050     121      37807    5030    5055
TOQ Entries                32      32     121      32829      99      37
Operations                  -       -     244      65886     199
Messages Received           -       -     122      32798     100
Messages Sent               -       -     121      32833     100
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Timed Events                -       -     121      32796      99
Alarms                      -       -       0          0       0
System Logs                 -       -       0          3       3
Process Logs                -       -       0        182      72
Remote Logs                 -       -       0          0       0
Load Rate                                0.0%      16.22     0.3%
```

show task sipc

The SIP Core (SIPC) task statistics are displayed as follows:

```
ACMEPACKET# show task sipc
12:42:56-105 (sipc@0.1.1) ID=cfcff470
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   13      13       0         13      13      13
Messages                   33      33     104      32843     191      39
Alloc Buffers              39      39       0         39      39      39
Free Buffers                0       0       0          0       0       0
Transactions               15      16      51      16347      50      19
Timed Objects              31      32      51      16366      50      35
TOQ Entries                15      16      51      16369      50      19
Operations                  -       -     114      35854     109
Messages Received           -       -      52      16411      85
Messages Sent               -       -      51      16432     107
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Timed Events                -       -      52      16353      50
Alarms                      -       -       0          0       0
System Logs                 -       -       0          1       1
Process Logs                -       -       8       1512     176
Remote Logs                 -       -       0          0       0
Load Rate                                0.0%       5.79     0.0%
```

show task sipls

The SIP Location Server (SIPLS) task statistics are displayed as follows:

```
ACMEPACKET# show task sipls
12:43:10-122 (sipls@0.3.0) ID=c62bd010
```

```
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   13      13       0         13      13      13
Messages                   19      19      62      16713     181      23
Alloc Buffers              39      39       0         39      39      39
Free Buffers                0       0       0          0       0       0
Transactions                8       8      30       8277      25      11
Timed Objects              25      25      30       8297      33      28
TOQ Entries                 9       9      54      14941      56      12
Operations                  -       -      95      26191      80
Messages Received           -       -      31       8347      81
Messages Sent               -       -      30       8368     103
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Timed Events                -       -      54      14931      46
Alarms                      -       -       0          0       0
System Logs                 -       -       0          1       1
Process Logs                -       -      10       1853     183
Remote Logs                 -       -       0          0       0
Load Rate                                0.0%      3.78    0.0%
```

show task sipt

The SIP Transport (SIPT) task statistics are displayed as follows:

```
ACMEPACKET# show task sipt
12:43:22-133 (sipt@0.1.0) ID=c631d950
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   14      14       0         14      14      14
Messages                   21      21      68      16692     168      25
Alloc Buffers              39      39       0         39      39      39
Free Buffers                0       0       0          0       0       0
Transactions                8       8      33       8273      25      11
Timed Objects              25      25      33       8293      33      28
TOQ Entries                 8       8      33       8297      37      11
Operations                  -       -      79      19819      61
Messages Received           -       -      34       8334      72
Messages Sent               -       -      33       8357      96
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Timed Events                -       -      33       8288      27
Alarms                      -       -       0          0       0
System Logs                 -       -       0          1       1
Process Logs                -       -       8       1527     191
Remote Logs                 -       -       0          0       0
Load Rate                                0.0%      3.28    0.0%
```

show task sm

The system manager (SM) task statistics are displayed as follows:

```
ACMEPACKET# show task sm@0.0.0
12:43:38-189 (sm@0.0.0) ID=e19fead0
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
```

```
Services              17      17       0        17      17      17
Messages               4       4     321     49279     827       5
Alloc Buffers         49      49       0        49      49      49
Free Buffers           0       0       0         0       0       0
Transactions           0       0       0         0       0       0
Timed Objects         49      49       0        49      49      49
TOQ Entries            8       8     269     47617     159       9
Operations             -       -     296     48595     405
Messages Received      -       -     289     47242     393
Messages Sent          -       -      74      9814     444
Partial Message        -       -       0         0       0
Part Msg Expired       -       -       0         0       0
Part Msg Dropped       -       -       0         0       0
Timed Events           -       -       6      1093       6
Alarms                 -       -       0         0       0
System Logs            -       -       0         4       3
Process Logs           -       -       4      1663     627
Remote Logs            -       -       0         0       0
Load Rate                              0.0%    13.00    0.3%
```

show task snmpd The SNMP daemon task statistics are displayed as follows:

```
ACMEPACKET# show task snmpd
12:43:48-199 (snmpd@0.0.0) ID=e20fb6e0
Task Status               ---- Recent ---- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
Services                17      17       0         18      17      17
Messages                 3       3       2         20       8       5
Alloc Buffers           48      48       0         48      48      48
Free Buffers             0       0       0          0       0       0
Transactions             0       0       0          0       0       0
Timed Objects           18      18       0         19      18      18
TOQ Entries              0       0       0          0       0       0
Operations               -       -       2        340       3
Messages Received        -       -       1         10       4
Messages Sent            -       -       0          8       3
Partial Message          -       -       0          0       0
Part Msg Expired         -       -       0          0       0
Part Msg Dropped         -       -       0          0       0
Timed Events             -       -       0          0       0
Alarms                   -       -       0          0       0
System Logs              -       -       0          1       1
Process Logs             -       -       4        728      48
Remote Logs              -       -       0          0       0
Load Rate                              0.0%      0.10    0.0%
```

show task soapd The SOAP daemon task statistics are displayed as follows:

```
ACMEPACKET# show task soapd
12:44:05-109 (soapd@0.0.1) ID=d431a9e0
Task Status               ---- Recent ---- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
Services                16      16       0         16      16      16
Messages                20      20      56      16595      50      24
```

```
Alloc Buffers             48      48       0        48      48      48
Free Buffers               0       0       0         0       0       0
Transactions               8       8      27      8288      25      11
Timed Objects             27      27      27      8307      25      30
TOQ Entries                8       8      27      8288      25      11
Operations                 -       -      56     16895      51
Messages Received          -       -      28      8297      25
Messages Sent              -       -      27      8298      25
Partial Message            -       -       0         0       0
Part Msg Expired           -       -       0         0       0
Part Msg Dropped           -       -       0         0       0
Timed Events               -       -      27      8280      25
Alarms                     -       -       0         0       0
System Logs                -       -       0         2       2
Process Logs               -       -       4       741      71
Remote Logs                -       -       0         0       0
Load Rate                              0.0%      3.13    0.0%
```

show task sshd

The SSH daemon task statistics are displayed as follows:

```
ACMEPACKET# show task sshd
12:44:16-127 (sshd@0.0.0) ID=e1e82b80
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   17      17       0         17      17      17
Messages                    3       3       2          8       3       3
Alloc Buffers              48      48       0         48      48      48
Free Buffers                0       0       0          0       0       0
Transactions                0       0       0          0       0       0
Timed Objects              18      18       0         18      18      18
TOQ Entries                 0       0       0          0       0       0
Operations                  -       -       2        339       3
Messages Received           -       -       1          4       2
Messages Sent               -       -       0          4       2
Partial Message             -       -       0          0       0
Part Msg Expired            -       -       0          0       0
Part Msg Dropped            -       -       0          0       0
Timed Events                -       -       0          0       0
Alarms                      -       -       0          0       0
System Logs                 -       -       0          1       1
Process Logs                -       -       0        159      43
Remote Logs                 -       -       0          0       0
Load Rate                              0.0%      0.08    0.0%
```

show task xserv

The Transcoder Server task statistics are displayed as follows:

```
ACMEPACKET# show task xserv
12:45:13-154 (xserv@4.0.0) ID=d4185120
Task Status                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Services                   21      21       0         21      21      21
Messages                  299     299    1466     317217     949     301
Alloc Buffers              60      60       0         60      60      60
Free Buffers                0       0       0          0       0       0
```

```
Transactions            148     148     713     154550     462     150
Timed Objects           172     172     713     154574     462     174
TOQ Entries             148     148     713     154550     462     150
Operations                -       -    1460     315964     946
Messages Received         -       -     752     162662     487
Messages Sent             -       -     713     154562     464
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              -       -     713     154402     463
Alarms                    -       -       0          0       0
System Logs               -       -       0          8       6
Process Logs              -       -       4        817     137
Remote Logs               -       -       0          0       0
Load Rate                                0.1%     65.14     0.2%
```

Chassis Management Application Statistics

The show commands described in this section relate to system-level tasks and processes on the Net-Net system. These tasks generally do not have any direct involvement with passing traffic or other media and signaling applications.

Socket Front End (SFE)

The Socket Front End (SFE) manages TCP streams and connectionless UDP sessions within the Net-Net 9200 signaling plane. It is used by signaling components to communicate bi-directionally with addressable entities accessible via the external network. You can view SFE statistics with the **show sfe** command.

```
ACMEPACKET# show sfe [summary | pending | clients | socket]
```

show sfe summary

The **show sfe summary** command is displayed as follows:

```
ACMEPACKET# show sfe summary
***********************************************
SFE at 169.254.160.1:8013
***********************************************
Handles                     2(free:249998)
Host Path Transmit Port     169.254.177.0:8016
Server State                Active

12:49:31-135
Summary                        ---- Recent ---- -------- Lifetime --------
                         Active    High   Total      Total  PerMax    High
UDP Sockets                   2       2       0          2       2       2
TCP Listen Sockets            0       0       0          0       0       0
TCP Inbound Connections       0       0       0          0       0       0
TCP Outbound Connections      0       0       0          0       0       0
Free TCP Timers            5000    5000       0       5000    5000    5000
Alloc TCP Timers              0       0       0          0       0       0
Internal Errors               -       -       0          0       0
RDP Send Errors               -       -       0          0       0
No Socket For Net Packet      -       -       0          0       0
Bad Packet From Network       -       -       0          0       0
Send to Network Failed        -       -       0          0       0
Rcvd Fragments                -       -       0          0       0
```

```
Rcvd Fragment Errors           -       -       0          0       0
Sent Fragments                 -       -       0          0       0
Sent Fragment Errors           -       -       0          0       0

Total Active Clients        2
```

show sfe pending

The **show sfe pending** command displays pending socket open requests.

```
ACMEPACKET# show sfe pending

<ENTER>  no further known parameters
```

show sfe clients

The **show sfe clients** command displays the SFE's current clients (as tasks) and the number of sockets each client has opened to the SFE. For example:

```
ACMEPACKET# show sfe clients
------------------- ----------
Client              SockCount
------------------- ----------
dnsres@0.0.1        2
sipt@0.1.0          2
------------------- ----------
Total Active Clients: 2
```

show sfe load

The **show sfe load** command displays the SFE's current load as well as its load limit. For example:

```
ACMEPACKET# show sfe load
sfe@0.1.0: Load is 0.1; Limit is 95
```

show sfe sockets

The **show sfe sockets** command displays the SFE's open sockets in detail. This display includes the task, protocol, IP address and port, and number of messages received, sent, and errors. In addition, details about the recorded errors are listed. For example:

```
ACMEPACKET# show sfe sockets
Server State                Active
------ ------------------------------------ ---------- ---------- ---
Handle Socket                                  MsgRcvd   MsgSent   Err
------ ------------------------------------ ---------- ---------- ---
1     sipt@0.2.0 UDP[0:3/0]172.16.0.77:5060         0         0         0
2     sipt@0.1.0 UDP[0:0/0]192.168.0.77:5060        0         0         0
------ ------------------------------------ ---------- ---------- ---

12:50:48-112
Summary                    ---- Recent ---- -------- Lifetime --------
                         Active    High   Total     Total  PerMax    High
UDP Sockets                   2       2       0         2       2       2
TCP Listen Sockets            0       0       0         0       0       0
TCP Inbound Connections       0       0       0         0       0       0
TCP Outbound Connections      0       0       0         0       0       0
Free TCP Timers            5000    5000       0      5000    5000    5000
Alloc TCP Timers              0       0       0         0       0       0
Internal Errors               -       -       0         0       0
```

```
RDP Send Errors                -       -       0          0       0
No Socket For Net Packet       -       -       0          0       0
Bad Packet From Network        -       -       0          0       0
Send to Network Failed         -       -       0          0       0
Rcvd Fragments                 -       -       0          0       0
Rcvd Fragment Errors           -       -       0          0       0
Sent Fragments                 -       -       0          0       0
Sent Fragment Errors           -       -       0          0       0
```

Management Socket Front End (MSFE)

The Management Socket Front End (SFE) manages TCP streams and connectionless UDP sessions within the Net-Net 9200 management plane. It is used by components to communicate bi-directionally with addressable entities accessible via the external network. You can view MSFE statistics with the **show msfe** command.

```
ACMEPACKET# show msfe [summary | pending | clients | sockets]
```

show msfe summary

The **show msfe summary** command is displayed as follows:

```
ACMEPACKET# show msfe summary
*********************************************
mSFE at 169.254.160.0:8037
*********************************************
Handles                    0(free:1000)
Management Utility Address  172.30.92.92
Management Virtual Address  172.30.92.96
Server State                Active

12:51:45-176
Summary                    ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
UDP Sockets                 0       0       0          0       0       0
TCP Listen Sockets          0       0       0          0       0       0
TCP Inbound Connections     0       0       0          0       0       0
TCP Outbound Connections    0       0       0          0       0       0
Free TCP Timers             0       0       0          0       0       0
Alloc TCP Timers            0       0       0          0       0       0
Internal Errors             -       -       0          0       0
RDP Send Errors             -       -       0          0       0
No Socket For Net Packet    -       -       0          0       0
Bad Packet From Network     -       -       0          0       0
Send to Network Failed      -       -       0          0       0
Rcvd Fragments              -       -       0          0       0
Rcvd Fragment Errors        -       -       0          0       0
Sent Fragments              -       -       0          0       0
Sent Fragment Errors        -       -       0          0       0

Total Active Clients        0
```

show msfe pending

The **show msfe pending** command displays pending socket open requests.

show msfe clients

The **show msfe clients** command displays the MSFE's current clients (as tasks) and the number of sockets each client has opened to the MSFE. For example:

```
ACMEPACKET# show msfe clients
------------------ ----------
Client             SockCount
------------------ ----------
------------------ ----------
Total Active Clients        0
```

show msfe load

The **show msfe load** command displays the MSFE's current load as well as it's load limit. For example:

```
ACMEPACKET# show msfe load
sfe@0.0.0: Load is 2.6; Limit is 80
```

show msfe sockets

The **show msfe sockets** command displays the MSFE's open sockets in detail. This display includes the task, protocol, IP address and port, and number of messages received, sent, and errors. In addition, details about the recorded errors are listed. For example:

```
ACMESYSTEM# show msfe sockets
Server State                Active
------ ------------------------------------ ---------- ---------- ---
Handle Socket                                  MsgRcvd   MsgSent   Err
------ ------------------------------------ ---------- ---------- -
------ ------------------------------------ ---------- ---------- -

09:58:53-127
Summary                    ---- Recent ---- -------- Lifetime --------
                        Active   High   Total     Total  PerMax    High
UDP Sockets                  0      0      0         0      0       0
TCP Listen Sockets           0      0      0         0      0       0
TCP Inbound Connections      0      0      0         0      0       0
TCP Outbound Connections     0      0      0         0      0       0
Free TCP Timers              0      0      0         0      0       0
Alloc TCP Timers             0      0      0         0      0       0
Internal Errors              -      -      0         0      0
RDP Send Errors              -      -      0         0      0
No Socket For Net Packet     -      -      0         0      0
Bad Packet From Network      -      -      0         0      0
Send to Network Failed       -      -      0         0      0
Rcvd Fragments               -      -      0         0      0
Rcvd Fragment Errors         -      -      0         0      0
Sent Fragments               -      -      0         0      0
Sent Fragment Errors         -      -      0         0      0
```

Acme Messaging Protocol (AMP)

AMP is the messaging protocol used by all application tasks to communicate with each other. The Net-Net system provides counts of AMP message protocol types as sent or received by a supplied task. Counts are further delineated by Recent, Lifetime Total, and Lifetime Period Maximum. The Net-Net OS displays the appropriate AMP message counts for the task you specify.

Additionally, if one task makes synchronous communication with another task, the ACLI displays counts for the synchronous interprocess communication in the **ToServer** section of a specific task instance.

The **show amp** command usage is as follows:

```
ACMEPACKET# show amp <task>
```

where task is:

```
<name>@<card>.<cpu>.<core>
```

show amp acli

The **show amp acli** command displays AMP message statistics for the ACLI. For example:

```
ACMESYSTEM# show amp acli
10:00:27-121 (acli@0.0.0) ID=10000
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total           34       2395     120       33       2397     123
SNR              3        106      89        3        106      89
MAN              0          3       2        0          4       2
CLIP             4         20       4        3         17       3
LOG              0          0       0        0          4       2
CFG              2         43      16        2         43      16
AUTH            25       2223      24       25       2223      24

ToServer         5        159     107
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp arpm

The **show amp arpm** command displays AMP message statistics for the ARP manager (ARPM) . For example:

```
ACMEPACKET# show amp arpm@2.0.0
13:16:27-126 (arpm@2.0.0) ID=d46f4000
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total          126      34604     100      124      34606     100
MAN              0          1       1        0          2       2
CLIP             1          5       1        0          4       1
LOG              0          0       0        0          1       1
SP               0          0       0        0          4       4
ARP              0          3       3        0          0       0
CFG              0          2       2        0          2       2
REDUNDANCY     125      34593      99      124      34593      99

ToServer         0          2       2
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp auth

The **show amp auth** command displays AMP message statistics for the user authentication process. For example:

```
ACMEPACKET#  show amp auth@0.0.0
13:16:45-176 (auth@0.0.0) ID=e23c11a0
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total          180      36103     117      179      36109     120
SNR              0          1       1        0          1       1
MAN              0          3       2        0          3       1
CLIP             1          5       1        0          4       1
LOG              0          0       0        0          3       2
AUTH             6       1287       9        6       1291      11
REDUNDANCY     173      34807     106      173      34807     106

ToServer         0          2       1
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp broker

The **show amp broker** command displays AMP message statistics for the broker daemon. For example:

```
ACMEPACKET# show amp broker@0.0.1
13:16:59-183 (broker@0.0.1) ID=d40a7e50
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            1          5       3        0         38      37
MAN              0          2       2        0         36      36
CLIP             1          2       1        0          1       1
CFG              0          1       1        0          1       1

ToServer         0          1       1
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp cm

The **show amp cm** command displays AMP message statistics for the chassis manager (CM). For example:

```
ACMEPACKET# show amp cm@0.0.0
13:18:09-128 (cm@2.0.0) ID=d3b191b0
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total           53      14043      42       26       7028      27
MAN             51      14036      40       25       7017      20
CLIP             2          3       2        1          2       1
LOG              0          0       0        0          1       1
ARP              0          0       0        0          1       1
CFG              0          4       4        0          4       4
ALARM            0          0       0        0          3       3
```

```
ToServer         0          4       4
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp collect

The **show amp collect** command displays AMP message statistics for the HDR collector application. For example:

```
ACMESYSTEM# show amp collect
10:02:09-123 (collect@0.0.0) ID=e4e21f40
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            1          5       3        0          5       2
MAN              0          3       3        0          3       2
CLIP             1          2       1        0          1       1
LOG              0          0       0        0          1       1

ToServer         0          1       1
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp dnsres

The **show amp dnsres** command displays AMP message statistics for the DNS resolution server. For example:

```
ACMEPACKET# show amp dnsres@0.0.1
13:18:42-186 (dnsres@0.0.1) ID=d431a180
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            1         26      23        0         55      53
SNR              0          2       2        0          2       2
MAN              0          5       5        0         34      34
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          1       1
CFG              0         16      16        0         16      16

ToServer         0         21      21
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp ftpdalg

The **show amp ftpdalg** command displays AMP message statistics for the FTP ALG server. For example:

```
ACMEPACKET# show amp ftpdalg@0.0.0
13:19:39-150 (ftpdalg@0.0.0) ID=e19fe510
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
```

```
Total           1          4       2        0          6       4
MAN             0          2       2        0          2       1
CLIP            1          2       1        0          1       1
LOG             0          0       0        0          3       3
```

show amp h323GkGw

The **show amp h323GkGw** command displays H.323 Gatekeeper/Gateway AMP statistics. For example:

```
ACMEPACKET# show amp h323GkGw
14:18:09-193 (h323GkGw@0.1.1) ID=d54af390
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            1         16       8        0         15       7
SNR              0          3       3        0          3       3
MAN              0          3       2        0          2       1
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          1       1
CFG              0          7       4        0          7       4

ToServer         0         10       6
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp h323RasGk

The **show amp h323RasGk** command displays H.323 RAS Gatekeeper AMP statistics. For example:

```
ACMEPACKET# show amp h323RasGk
14:21:09-175 (h323RasGk@0.4.1) ID=d54b0c90
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total           45      86608      30       44      86607      29
SNR              0          3       3        0          3       3
MAN              0          3       2        0          2       1
CLIP             2          7       4        1          6       4
LOG              0          0       0        0          1       1
CFG              0          7       4        0          7       4
REDUNDANCY      43      86588      25       43      86588      25

ToServer         0         10       6
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp ipc

The **show amp ipc** command takes a task name as a final argument. This command displays AMP send/recieve statistics for the identified task. The show amp ipc command usage is as follows:

```
ACMEPACKET# show amp ipc <task>
```

For example:

```
ACMEPACKET# show amp ipc sipls@0.3.0
13:20:04-135 (sipls@0.3.0) ID=c62bd010
Task AMP Statistics        ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
AMP Msgs Received           -       -      35       8899      81
  Partial Parse             -       -       0          0       0
AMP Msgs Sent               -       -      34       8920     103
  Blocked                   -       -       0          0       0
  Queued                    0       0       0          0       0       0
  Queued Retries            -       -       0          0       0
  Queued Sent               -       -       0          0       0
  Queued Expired            -       -       0          0       0
  Errors                    -       -       0          0       0

Avg Queued=0.000 for 0
Max Queued=0.000
```

show amp lcm

The **show amp lcm** command displays AMP message statistics for the local core manager (LCM). For example:

```
ACMEPACKET# show amp lcm@0.0.0
13:15:08-172 (lcm@0.0.1) ID=d3a9dec0
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            4        169     160       37       7056      40
SNR              0          5       5        0          5       5
MAN              0        153     153       34       7039      31
CLIP             4          9       4        3          8       3
LOG              0          0       0        0          2       2
CFG              0          2       2        0          2       2

ToServer         0          2       2
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp lem

The **show amp lem** command displays AMP message statistics for the local element manager (LEM). For example:

```
ACMEPACKET# show amp lem@0.0.0
13:20:58-122 (lem@0.0.1) ID=d3b54110
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            2         43      40        1         80      78
MAN              0          2       2        0         39      39
CLIP             2          3       1        1          2       1
LOG              0          0       0        0          1       1
CFG              0         38      38        0         38      38

ToServer         0          2       2
  Retries        0          0       0
```

```
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp logman

The **show amp logman** command displays AMP message statistics for the log manager. For example:

```
ACMEPACKET# show amp logman@0.0.0
13:49:20-131 (logman@0.0.0) ID=e1657e30
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            6       1633     238        0          9       4
MAN              0          4       3        0          2       1
CLIP             1          3       1        0          2       1
LOG              0        284     225        0          0       0
ALARM            5       1342      87        0          3       2
SNMP             0          0       0        0          2       2
```

show amp mbcd

The **show amp mbcd** command displays AMP message statistics for the middlebox control daemon (MBCD). For example:

```
ACMEPACKET# show amp mbcd@2.0.1
13:49:41-118 (mbcd@2.0.1) ID=d3dc14c0
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total           29       9060      77      114      36091     167
SNR              0          4       4        0          4       4
MAN              0          4       4        0         25      25
CLIP             1          3       1        0          2       1
XCODE           28       9002      25      114      36012      97
LOG              0          0       0        0          1       1
NAT              0          4       4        0          4       4
CFG              0         42      42        0         42      42
REDUNDANCY       0          1       1        0          1       1

ToServer         0         49      49
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp msfe

The **show amp msfe** command displays AMP message statistics for the management socket front end process. For example:

```
ACMEPACKET# show amp msfe@0.0.0
13:50:01-172 (sfe@0.0.0) ID=e20a7900
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total          171      36772     104      170      36806     104
MAN              0          3       3        0         35      33
CLIP             1          7       4        0          8       6
```

```
LOG              0          0       0        0          1       1
REDUNDANCY     170      36762     101      170      36762     101

ToServer         0          1       1
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp natm

The **show amp natm** command displays AMP message statistics for the NAT manager. For example:

```
ACMEPACKET# show amp natm@2.0.0
13:50:26-165 (natm@2.0.0) ID=d53298c0
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            1         13      10        0         14      12
SNR              0          2       2        0          2       2
MAN              0          1       1        0          2       2
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          1       1
NAT              0          4       4        0          4       4
CFG              0          3       3        0          3       3

ToServer         0          5       5
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

Note: natm statistics are absent from SPU2/NPU2-based systems for architectural reasons.

show amp npm

The **show amp nmp** command displays AMP message statistics for NPM. For example:

```
ACMEPACKET# show amp npm
14:22:03-143 (npm@2.0.0) ID=c4950010
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            1         70      28        0        116      46
SNR              0          5       5        0          5       5
MAN              0         15       7        0         55      31
CLIP             1          1       1        0          0       0
LOG              0          0       0        0          3       3
ARP              0          0       0        0          2       2
CFG              0         49      24        0         51      24

ToServer         0         62      27
  Retries        0          2       2
  Rejects        0          0       0
  Timeouts       0          0       0
```

```
  Stray          0          0       0
```

show amp ntpd

The **show amp ntpd** command displays AMP message statistics for the NTP application. For example:

```
ACMESYSTEM#  show amp ntpd
10:01:48-102 (ntpd@0.0.0) ID=c767e310
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            1          4       2        0          3       1
MAN              0          2       2        0          2       1
CLIP             1          2       1        0          1       1
10:01:48-195 (ntpd@0.0.1) ID=cfcfeaf0
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            1          5       2        0          5       3
MAN              0          2       2        0          2       1
CLIP             1          2       1        0          1       1
LOG              0          0       0        0          1       1
CFG              0          1       1        0          1       1

ToServer         0          1       1
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp rasm

The **show amp rasm** command displays AMP message statistics for the RADIUS Accounting System Manager (RASM). For example:

```
ACMEPACKET# show amp rasm@0.0.0
13:50:43-114 (rasm@0.0.0) ID=e2a73160
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total          114      36811     104      113      36836     103
MAN              0          2       2        0         27      26
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          1       1
CFG              0          2       1        0          2       1
REDUNDANCY     113      36804     101      113      36804     101

ToServer         0          2       1
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp secured

The **show amp secured** command Displays Security Daemon AMP statistics. For example:

```
ACMEPACKET# show amp secured
```

```
14:22:21-148 (secured@0.2.0) ID=d54c4910
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total          149     346461     121      148     346455     120
SNR              0          1       1        0          1       1
MAN              0          8       3        0          7       4
CLIP             1          1       1        0          0       0
CFG              0         35      18        0         35      18
REDUNDANCY     148     346412     100      148     346412     100
AMP-Unk          0          4       4        0          0       0

ToServer         0         41      20
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp sem

The **show amp sem** command displays AMP message statistics for the system element manager (SEM). For example:

```
ACMEPACKET# show amp sem@0.0.0
13:20:58-122 (lem@0.0.1) ID=d3b54110
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            2         43      40        1         80      78
MAN              0          2       2        0         39      39
CLIP             2          3       1        1          2       1
LOG              0          0       0        0          1       1
CFG              0         38      38        0         38      38

ToServer         0          2       2
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp sfe

The **show amp sfe** command displays AMP message statistics for the socket front end (SFE). For example:

```
ACMEPACKET# show amp sfe@0.0.1
13:58:26-170 (sfe@0.0.1) ID=cb0ce030
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total          169      37276     100      168      37313     101
MAN              0          2       2        0         38      38
CLIP             1          7       2        0          8       3
LOG              0          0       0        0          3       3
RDPCNTRL         0          3       3        0          0       0
SFE              0          2       2        0          2       2
REDUNDANCY     168      37262      99      168      37262      99
```

show amp sipc

The **show amp sipc** command displays AMP message statistics for the SIP core function. For example:

```
ACMEPACKET# show amp sipc@0.1.1
13:58:40-149 (sipc@0.1.1) ID=cfcff470
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total           75      18640      85       74      18661     107
SNR              0         11      11        0         11      11
MAN              0          5       5        0         26      26
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          1       1
CFG              0         46      46        0         46      46
REDUNDANCY      74      18575      50       74      18575      50

ToServer         0         60      60
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp sipls

The **show amp sipls** command displays AMP message statistics for the SIP location server. For example:

```
ACMEPACKET# show amp sipls@0.3.0
13:58:55-167 (sipls@0.3.0) ID=c62bd010
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total           42       9478      81       41       9499     103
SNR              0          9       9        0          9       9
MAN              0          5       5        0         28      28
CLIP             1          5       1        0          4       1
LOG              0          0       0        0          1       1
CFG              0         52      52        0         52      52
REDUNDANCY      41       9405      25       41       9405      25
PEG              0          2       2        0          0       0

ToServer         0         64      64
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp sipt

The **show amp sipt** command displays AMP message statistics for the SIP transport function. For example:

```
ACMEPACKET# show amp sipt@0.1.0
13:59:02-173 (sipt@0.1.0) ID=c631d950
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total           44       9460      72       43       9483      96
SNR              0         12      12        0         12      12
```

```
MAN              0          5       5        0         27       27
CLIP             1          3       1        0          2        1
LOG              0          0       0        0          1        1
CFG              0         41      41        0         41       41
SFE              0          1       1        0          1        1
REDUNDANCY      43       9398      25       43       9398       25
PEG              0          0       0        0          1        1

ToServer         0         56      56
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp sm

The **show amp sm** command displays AMP message statistics for the system manager (SM). For example:

```
ACMEPACKET# show amp sm@0.0.0
13:59:21-132 (sm@0.0.0) ID=e19fead0
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total          204      53777     393       53      11229     444
SNR             19        783     218       19        783     218
MAN            184      52977     176       26       7888     221
CLIP             1         12       4        0         15       8
LOG              0          0       0        0          4       3
RDPCNTRL         0          2       1        0          0       0
ALARM            0          0       0        8       2536      45
CHASSIS          0          3       2        0          3       2
```

show amp snmpd

The **show amp snmpd** command displays AMP message statistics for the SNMP daemon. For example.

```
ACMEPACKET# show amp snmpd@0.0.0
13:59:37-148 (snmpd@0.0.0) ID=e20fb6e0
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            1         11       4        0          9       3
MAN              0          2       2        0          2       1
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          1       1
CFG              0          1       1        0          1       1
CHASSIS          0          3       2        0          3       2
SNMP             0          2       2        0          0       0

ToServer         0          4       2
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp soapd

The **show amp soapd** command displays AMP message statistics for the SOAP daemon. For example:

```
ACMEPACKET# show amp soapd@0.0.1
13:59:51-155 (soapd@0.0.1) ID=d431a9e0
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total           39       9425      25       38       9426      25
SNR              0          3       3        0          3       3
MAN              0          2       2        0          2       2
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          2       2
CFG              0          2       2        0          2       2
REDUNDANCY      38       9415      25       38       9415      25

ToServer         0          5       5
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
  Stray          0          0       0
```

show amp sshd

The **show amp sshd** command displays AMP message statistics for the SSH daemon. For example:

```
ACMEPACKET# show amp sshd@0.0.0
14:00:06-177 (sshd@0.0.0) ID=e1e82b80
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            1          5       2        0          5       2
MAN              0          2       2        0          2       1
CLIP             1          3       1        0          2       1
LOG              0          0       0        0          1       1
```

show amp xserv

The **show amp xserv** command displays AMP message statistics for the transcoder server. For example:

```
ACMEPACKET# show amp xserv
14:00:14-154 (xserv@4.0.0) ID=d4185120
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total          753     184522     487      715     175334     464
MAN              0          2       2        0          2       2
CLIP             1          3       1        0          2       1
XCODE           37       9195      25        0          0       0
LOG              0          0       0        0          8       6
CFG              0          1       1        0          1       1
REDUNDANCY     715     175321     462      715     175321     462

ToServer         0          1       1
  Retries        0          0       0
  Rejects        0          0       0
  Timeouts       0          0       0
```

```
      Stray          0          0       0
```

Reliable Datagram Protocol (RDP)

RDP is the transport protocol that carries AMP. Tasks use RDP to transport AMP messages among each other.

The **show rdp** command usage is as follows:

```
ACMEPACKET# show rdp <slot #> <cpu #> <core #> [all | links <peer> |
linkstats <peer> | serv <task> | servstats <task> | conn <task> |
connstats <task>]
```

show rdp

The **show rdp** command with only core location as an argument presents a quick summary and current links. For example:

```
ACMEPACKET# show rdp 0 0 0
****************************** 0.0.0 Summary ***************************
  RxTotal    :    7356723   TxTotal    :    7349011   LclTotal   :     12684
  RxBadHdrLen:          0   RxCksumErr :          0   RxBadLen   :         0
  TxIpErrs   :          0   RxNoPort   :          8   RxFullSock :         0
  TxRej      :          0   LclNoPort  :          0   LclFullSock:         0
  TxTooBig   :          0   TxWrongNet :          0   TxLinkDown :         0
  LclFcBlock :          0   LclFcErSelf:          0   LclFcTmout :         0
  TxFcBlock  :          0   TxOflowQBlk:          0   TxFcTimeout:         0
  TxWouldBlk :          0   LclWouldBlk:          0
  Servers    :        144   LogCount   :        266   LogDropCnt :         0
  Errors     :          0   AlarmSet   :          0   AlarmClear :         0
************************************************************************
169.254.96.0   ==> 169.254.97.0    1.0.0/1     Resets: 0   Conn: 1    UP
169.254.160.0  ==> 169.254.160.1   0.0.1/vc    Resets: 0   Conn: 3    UP
```

show rdp all

The **show rdp all** command displays the RDP stack information for a given CPU/core. In addition, the command shows all connections on the specified core and statistics for that connection. The following is an abbreviated display of this show command:

```
ACMEPACKET# show rdp 0 0 0 all
***************************** 0.0.0 Summary ****************************
  RxTotal    :    8853100   TxTotal    :    8844130   LclTotal   :     15242
  RxBadHdrLen:          0   RxCksumErr :          0   RxBadLen   :         0
  TxIpErrs   :          0   RxNoPort   :          8   RxFullSock :         0
  TxRej      :          0   LclNoPort  :          0   LclFullSock:         0
  TxTooBig   :          0   TxWrongNet :          0   TxLinkDown :         0
  LclFcBlock :          0   LclFcErSelf:          0   LclFcTmout :         0
  TxFcBlock  :          0   TxOflowQBlk:          0   TxFcTimeout:         0
  TxWouldBlk :          0   LclWouldBlk:          0
  Servers    :        144   LogCount   :        347   LogDropCnt :         0
  Errors     :          0   AlarmSet   :          0   AlarmClear :         0
************************************************************************
------------------------------------------------------------------------
----
169.254.96.0   ==> 169.254.97.0    1.0.0/1     Resets: 0   Conn: 1    UP
------------------------------------------------------------------------
----
 TX                                    RX
```

```
-------------------------------------------------------------------------
----
 Total Packets           :    348203  Total Packets           :    348202
 SYNs                    :         1  SYNs                    :         1
 ACKs                    :         1  ACKs                    :         1
 NAKs                    :         0  NAKs                    :         0
 Keepalives              :    348200  Keepalives              :    348199
 GratAcks                :         0  Rej ConnDel             :         0
 Rejects                 :         0  Rejects                 :         0
 Conn Deletes            :         0  Conn Deletes            :         1
 FC Asserts              :         0  FC Asserts              :         0
 FC Deasserts            :         0  FC Deasserts            :         0
 RxDups     :         0  RxSockDeliv :         1  RxFullSock  :         0
 RxOflProtect:        0  RxDropFull  :         0  RxOoOSeqs   :         0
 TxPendQFull :         0  TxWouldBlock:         0
 RxBadCcbStat:        0  RxBadCcbSeqs:         0  RxSeqTooFar :         0
 InactInterv :        0  MissInterv  :         1  TxSeqNum    :         2
 Rx1stExpSeq :        3  ExpRxSeqNum :         3  LastRxAck   :         2
 OflowHead   :        0  OflowTail   :         0  OflowQDepth :         0
 PendQHead   :        0  PendQTail   :         0  PendQDepth  :         0
 LinkFlags   :       24  RxOnDelCcb  :         0  Reliable Tx :         1
```

show rdp links

The **show rdp links** command displays the RDP link information from a supplied CPU/core to all external sockets within the chassis. The following is an abbreviated display of this show command:

```
ACMEPACKET# show rdp 0 0 0 links
-------------------------------------------------------------------------
169.254.96.0   ==> 169.254.97.0    1.0.0/1     Resets: 0   Conn: 1    UP
-------------------------------------------------------------------------
 TX                                    RX
-------------------------------------------------------------------------
 Total Packets           :    290115  Total Packets           :    290114
 SYNs                    :         1  SYNs                    :         1
 ACKs                    :         1  ACKs                    :         1
 NAKs                    :         0  NAKs                    :         0
 Keepalives              :    290112  Keepalives              :    290111
 GratAcks                :         0  Rej ConnDel             :         0
 Rejects                 :         0  Rejects                 :         0
 Conn Deletes            :         0  Conn Deletes            :         1
 FC Asserts              :         0  FC Asserts              :         0
 FC Deasserts            :         0  FC Deasserts            :         0
 RxDups     :         0  RxSockDeliv :         1  RxFullSock  :         0
 RxOflProtect:        0  RxDropFull  :         0  RxOoOSeqs   :         0
 TxPendQFull :         0  TxWouldBlock:         0
 RxBadCcbStat:        0  RxBadCcbSeqs:         0  RxSeqTooFar :         0
```

show rdp linkstats

The **show rdp linkstats** command displays the RDP link information from a supplied CPU/core to all external sockets within the chassis. This show command includes the show rdp links command plus additional statistics. The following is an abbreviated display of this show command:

```
ACMEPACKET# show rdp 0 0 0 linkstats
-------------------------------------------------------------------------
```

```
169.254.96.0   ==> 169.254.97.0    1.0.0/1     Resets: 0   Conn: 1    UP
-------------------------------------------------------------------------
 TX                                    RX
-------------------------------------------------------------------------
 Total Packets           :    290578  Total Packets           :    290577
 SYNs                    :         1  SYNs                    :         1
 ACKs                    :         1  ACKs                    :         1
 NAKs                    :         0  NAKs                    :         0
 Keepalives              :    290575  Keepalives              :    290574
 GratAcks                :         0  Rej ConnDel             :         0
 Rejects                 :         0  Rejects                 :         0
 Conn Deletes            :         0  Conn Deletes            :         1
 FC Asserts              :         0  FC Asserts              :         0
 FC Deasserts            :         0  FC Deasserts            :         0
 RxDups     :         0  RxSockDeliv :         1  RxFullSock  :         0
 RxOflProtect:        0  RxDropFull  :         0  RxOoOSeqs   :         0
 TxPendQFull :         0  TxWouldBlock:         0
 RxBadCcbStat:        0  RxBadCcbSeqs:         0  RxSeqTooFar :         0
 InactInterv :        0  MissInterv  :         1  TxSeqNum    :         2
 Rx1stExpSeq :        3  ExpRxSeqNum :         3  LastRxAck   :         2
 OflowHead   :        0  OflowTail   :         0  OflowQDepth :         0
 PendQHead   :        0  PendQTail   :         0  PendQDepth  :         0
 LinkFlags   :       24  RxOnDelCcb  :         0  Reliable Tx :         1
```

show rdp serv

The **show rdp serv** command displays the RDP server socket information from a supplied CPU/core to all external sockets within the chassis. Specifying a task name at the end of this command filters for the supplied task. The following is an abbreviated display of this show command:

```
ACMEPACKET# show rdp 0 0 0 serv acli
-------------------------------------------------------------------------
Local Address  TaskId   Task        Fd  FC  Blk Conn ChrCnt RSpace
-------------------------------------------------------------------------
a9fe6000:1095  e3697850 iAcli       18  no  yes 0    0      166400
a9fe6000:8006  e3697850 iAcli       16  no  yes 0    0      262144
a9fe2000:1094  e3697850 iAcli       14  no  yes 0    0      166400
a9fe2000:8006  e3697850 iAcli       12  no  yes 0    0      262144
a9feb000:1093  e3697850 iAcli       10  no  yes 0    0      166400
a9feb000:8006  e3697850 iAcli       8   no  yes 0    0      262144
a9fea000:1092  e3697850 iAcli       6   no  yes 5    0      166400
a9fea000:8006  e3697850 iAcli       4   no  yes 2    0      262144
```

show rdp servstats

The **show rdp servstats** command displays the same data as the show rdp serv command. In addition, the following counts are displayed for each local address:

- RxDeliver
- RxFullSock
- TxFcAssert
- TxFcDAsser
- LclDeliver
- LclFullSok
- LclWouldBl
- LclFcBlock
- LclFcDisca
- hiwat
- mbcnt
- mbmax
- maxCc

show rdp conn

The **show rdp conn** command displays the RDP connection information between tasks running on a supplied CPU/core to all external sockets within the chassis. Specifying a task name at the end of this command filters for the supplied task. The following is an abbreviated display of this show command:

```
ACMEPACKET# show rdp 0 0 0 conn iacli
-----------------------------------------------------------------------
Local Address  TaskId   Task        Fd  FC  Blk Conn ChrCnt RSpace
-----------------------------------------------------------------------
a9fe6000:1095  e3697850 iAcli       18  no  yes 0    0      166400
a9fe6000:8006  e3697850 iAcli       16  no  yes 0    0      262144
a9fe2000:1094  e3697850 iAcli       14  no  yes 0    0      166400
a9fe2000:8006  e3697850 iAcli       12  no  yes 0    0      262144
a9feb000:1093  e3697850 iAcli       10  no  yes 0    0      166400
a9feb000:8006  e3697850 iAcli       8   no  yes 0    0      262144
a9fea000:1092  e3697850 iAcli       6   no  yes 5    0      166400
    ------------------------------
    Foreign Addr   SNR Name fefc
    ------------------------------
    a9fea100:8034          no
    a9feb000:8034          no
    a9feb000:8003  sm       no
    a9fea100:8003  sm       no
    a9feb000:8004  sem      no
-----------------------------------------------------------------------
Local Address  TaskId   Task        Fd  FC  Blk Conn ChrCnt RSpace
-----------------------------------------------------------------------
a9fea000:8006  e3697850 iAcli       4   no  yes 2    0      262144
    ------------------------------
    Foreign Addr   SNR Name fefc
    ------------------------------
    a9feb000:8034          no
    a9feb000:8020  logman   no
-----------------------------------------------------------------------
```

show rdp connstats

The **show rdp conntats** command displays the same data as the show rdp conn command. In addition, the following counts are displayed for each address:

- RxDeliver (local address only)
- RxFullSock
- TxFcAssert
- TxFcDAsser
- LclDeliver (local address only)
- LclFullSok (local address only)
- LclWouldBl (local address only)
- LclFcBlock (local address only)
- LclFcDisca (local address only)
- hiwat (local address only)
- mbcnt (local address only)
- mbmax (local address only)
- Rx (foreign address only)
- Tx (foreign address only)
- RxFcAssert (foreign address only)
- RxFcDAsser (foreign address only)
- TxWouldBlk (foreign address only)
- RxRejects (foreign address only)
- RxDropFull (foreign address only)
- RxOProtect (foreign address only)
- DeadlkProt (foreign address only)

System Name Registry (SNR)

The SNR is a service provided by the SM, CM and LCM. Applications can register a mapping of a name to a transport address with their local LCM. The LCM stores these registrations, and forwards them to CM, which stores and forwards them to SM.

The **show snr** command usage is as follows:

```
ACMEPACKET# show snr [core | relay]
```

show snr core

The SNR core display shows all tasks active on the Net-Net system and their mapping to an IP address and socket pair. The following is an abbreviated display of this show command:

```
ACMEPACKET# show snr core
122 Names
arpm@2.0.0 169.254.162.0:8014
bcm56k@0.0.0 169.254.160.0:8025
broker@0.0.0 169.254.160.0:8025
broker@0.0.1 169.254.160.1:8025
broker@0.1.0 169.254.160.16:8025
broker@0.1.1 169.254.160.17:8025
```

```
broker@0.2.0 169.254.160.32:8025
broker@0.2.1 169.254.160.33:8025
broker@0.3.0 169.254.160.48:8025
broker@0.3.1 169.254.160.49:8025
broker@0.4.0 169.254.160.64:8025
broker@0.4.1 169.254.160.65:8025
broker@2.0.0 169.254.162.0:8025
broker@2.0.1 169.254.162.1:8025
94 Numbers
8001 169.254.160.0:8001
8001 169.254.160.1:8001
8001 169.254.160.16:8001
8001 169.254.160.17:8001
8001 169.254.160.32:8001
8001 169.254.160.33:8001
8001 169.254.160.48:8001
8001 169.254.160.49:8001
8001 169.254.160.64:8001
8001 169.254.160.65:8001
8001 169.254.162.0:8001
8001 169.254.162.1:8001
8002 169.254.160.0:8002
8002 169.254.162.0:8002
```

show snr relay

The SNR relay display shows the SNR relay (lookup) counters.

```
ACMEPACKET#   show snr relay
  Rx Request Msgs    307  Request Msg Failures    0
  Rx Register Msgs   2  Register Msg Failures   0
  Rx Deregister Msgs 2  Deregister Msg Failures 0
  Tx Relayed Msgs    311  Rx Unexpected Msgs      0
```

Redundancy Statistics

The Net-Net 9200 needs to share task information between redundant cards in order for failovers to occur without any system state or call loss.

The **show redundancy** command is used to display statistics and counts for transactions that occur between cards. This command takes a task as an arguments. The command is entered as follows:

```
show redundancy [arp | auth | cache | collect | configuration | core |
mbcd | rasm | sfe | soapd | standby | transport | xserv <slot> <core>
<cpu>]
```

Each task you use as an argument returns the same set of statistics. Client transactions are from the perspective of the tasks on the active card. Server transactions are from the perspective of the tasks on the standby card. For example:

```
ACMEPACKET: show redundancy cache
07:26:16-127 sipls@0.3.0 Redundancy Statistics
                          ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Total Records             0       0       0          0       0       0
Records Queued            0       0       0          0       0       0
Records Dropped             -       -       0          0       0
```

```
Client Transactions          0       0       0          0       0       0
  Requests Sent               -       -       0          0       0
  Requests Re-Trans           -       -       0          0       0
  Sync Resp Received          -       -       0          0       0
  Syncing Resp Receive        -       -       0          0       0
  Errors Received             -       -       0          0       0
  Transaction Timeouts        -       -       0          0       0
Server Transactions          0       0       0          0       0       0
  Requests Received           -       -       0          0       0
  Dup Req Received            -       -       0          0       0
  Sync Resp Sent              -       -       0          0       0
  Syncing Resp Sent           -       -       0          0       0
  Errors Sent                 -       -       0          0       0
```

show redundancy standby

By adding the standby argument to the the **show redundancy** command, the ACLI displays the redundancy statistics for the task you identify that exists on the standby card. The command is entered as follows:

```
show redundancy standby [arp | auth | cache | collect | configuration
| core | mbcd | rasm | sfe | soapd | transport]
```

For example:

```
ACMEPACKET> show redundancy standby arp
17:18:08-102 arpm@3.0.0 Redundancy Statistics
                           ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Total Records             2       2       2          2       2       2
Records Queued            0       0       0          0       0       0
Records Dropped             -       -       0          0       0
Client Transactions       0       2     154        154     151       2
  Requests Sent             -       -       0          0       0
  Requests Re-Trans         -       -       0          0       0
  Sync Resp Received        -       -      43         43      40
  Syncing Resp Receive      -       -       4          4       4
  Errors Received           -       -     107        107     107
  Transaction Timeouts      -       -       0          0       0
Server Transactions       0       0       0          0       0       0
  Requests Received         -       -       0          0       0
  Dup Req Received          -       -       0          0       0
  Sync Resp Sent            -       -       0          0       0
  Syncing Resp Sent         -       -       0          0       0
  Errors Sent               -       -       0          0       0
```

Chassis Hardware Statistics

The show commands described in this section provide information about the Net-Net 9200 chassis hardware.

Card and Hardware Status

The Net-Net OS keeps track of operational status of all major component. These components include all of the possible 13 feature and interface cards, and power and cooling components.

show status

The **show status** command lists all possible feature and interface cards, power supplies, and fan trays. For each of these components, State, HA role, environmental conditions, and a memory usage summary are given. For example:

```
ACMEPACKET# show status

Slot   Type     State          Role         Temperature CPU      Memory
  0    SPU0     CARD RUNNING   STANDBY      Normal      Normal   Normal
  1    SPU1     CARD RUNNING   ACTIVE       Normal      Normal   Normal
  2    NPU0     CARD RUNNING   STANDBY      Normal      Normal   Normal
  3    NPU1     CARD RUNNING   ACTIVE       Normal      Normal   Normal
  4    TCU0     CARD RUNNING   STANDBY      Normal      Normal   Normal
  5    TCU1     CARD RUNNING   ACTIVE       Normal      Normal   Normal
  6     TCU2      Not Installed
  7    MIU0      CARD RUNNING   STANDBY      Normal      N/A      N/A
  8    MIU1      CARD RUNNING   ACTIVE       Normal      N/A      N/A
  9    PHY0      CARD RUNNING   ACTIVE       Normal      N/A      N/A
  10    PHY1      Not Installed
  11    PHY2      Not Installed
  12    PHY3      Not Installed
  13   FANCTRL 0 CARD RUNNING   ACTIVE       Normal      N/A      N/A
  14   FANCTRL 1 CARD RUNNING   ACTIVE       Normal      N/A      N/A
  15   POWER0    CARD RUNNING   ACTIVE       Normal      N/A      N/A
  16   POWER1    CARD RUNNING   ACTIVE       Normal      N/A      N/A
  17   POWER2    CARD RUNNING   ACTIVE       Normal      N/A      N/A
  18    POWER3    Not Installed
```

show health

The **show health** command displays health information for major system components:

- System
- Feature / Interface card
- CPU
- Core

In addition, you can view health information for the power supplies and fan units at the system level.

The show health command displays the Redundancy Event List, which is a log of all major events associated with card switchovers. This is followed by a list of all current alarms at the component level you are viewing.

- If you type show health at the system level, all alarms will be displayed
- If you type show health at the card level, all alarms for that card will be displayed
- If you type show health at the CPU level, all alarms for that CPU will be displayed
- If you type show health at the core level, all alarms for that core will be displayed

The show health command usage follows:

```
show health [<slot #> [<CPU #> [<core #>]]]
```

The following example displays system-wide health with redundancy and current alarm information:

```
ACMEPACKET> show health

  Slot            Type            Health Score    Role
  0               SPU0            100             ACTIVE
  1               SPU1            0               RECOVERY
  2               NPU0            100             STANDBY
  3               NPU1            100             ACTIVE
  4               TCU0            Not Installed
  5               TCU1            Not Installed
  6               TCU2            Not Installed
  7               MIU0            100             ACTIVE
  8               MIU1            100             STANDBY
  9               PHY0            50              ACTIVE
  10              PHY1            100             UNASSIGNED
  11              PHY2            Not Installed
  12              PHY3            Not Installed
  13              FANCTRL 0       100             ACTIVE
  14              FANCTRL 1       100             ACTIVE
  15              POWER0          100             ACTIVE
  16              POWER1          100             ACTIVE
  17              POWER2          100             ACTIVE
  18              POWER3          100             ACTIVE

                              Redundancy Event List
Event  Card   Time                      Description                      Reason
1      NPU1   2008-08-22 14:56:17       Assumed Active from NPU0         Gateway Unreachable

done
8 alarms to show
Alarm Id    Task Id        Severity    Last Occurrence         Count   Description
--------    -------        --------    -------------           -----   -----------
21e11210    tSM@1.0.0      NOTICE      2008-08-22 14:57:24.241 1       Health Score 0 on Card SPU1
20a00101    tLCM@1.0.0     EMERGENCY   2008-08-22 14:57:23.943 1       Task tLOGMAN on 1.0.0 with PID
31000134    tBROKER@3.0.0  MAJOR       2008-08-22 14:56:17.842 1       gateway 10.10.140.1 unreachable
22621222    tSM@3.0.0      NOTICE      2008-08-22 14:56:17.784 1       NPU1 Switchover to Active Role
```

Temperature and I2C Status and Alarms

When the Net-Net 9200 chassis or any of its components exceeds temperature thresholds, it triggers an alarm and an SNMP trap. When the temperature returns to an acceptable level, the system immediately clears the alarm. There are two types of temperature sensors in the Net-Net 9200 chassis: LM84 sensors and LM75 sensors.

The **show i2c** command displays temperature properties for all i2c devices.

LM84 sensors monitor the temperature of individual CPUs and FPGAs. These sensors take both a local reading and a remote reading. The local reading indicates the temperature of the sensor itself, while the remote reading indicates the temperature of the CPU or FPGA it monitors. LM84 sensors use a single threshold to trigger and clear an alarm; when the temperature rises above the Minor threshold value, an alarm is triggered. An alarm is cleared when the temperature falls below this threshold.

LM75 sensors monitor the temperature of a particular site within the Net-Net 9200 chassis. These sensors have a seperate threshold to clear an alarm.

For both sensors, the temperature thresholds are fixed - as detailed in the tables below. The thresholds are determined by the sensor's position on the feature card,

and the feature card's position within the chassis. These thresholds can not be modified, and are pre-programmed based upon thermal chamber testing.

SPU Sensors

The following table identifies LM85 sensors and corresponding temperature thresholds for SPU cards.

LM84 Sensor Type	Local Temperature Threshold		Remote Temperature Threshold	
	Minor	Major	Minor	Major
SPU CPU 0 Temp Sensor	70	85	85	95
SPU CPU 1 Temp Sensor	70	85	85	95
SPU CPU 2 Temp Sensor	70	85	85	95
SPU CPU 3 Temp Sensor	70	85	85	95
SPU CPU 4 Temp Sensor	70	85	85	95

The following table identifies LM75 sensors and corresponding temperature thresholds for SPU cards.

LM75 Sensor Type	Temperature Thresholds		
	Clear Alarm	Minor	Major
SPU Board Temp Sensor	60	65	75
SPU Board Left Center Temp Sensor	60	65	75
SPU Board Back Temp Sensor	60	65	75
SPU Board Middle Back Temp Sensor	60	65	75

NPU Sensors

The following table identifies LM85 sensors and corresponding temperature thresholds for NPU cards.

LM84 Sensor Type	Local Temperature Threshold		Remote Temperature Threshold	
	Minor	Major	Minor	Major
NPU CPU Temp Sensor	70	85	85	95
NPU FPGA Temp Sensor	65	75	70	80

The following table identifies LM75 sensors and corresponding temperature thresholds for NPU cards.

LM75 Sensor Type	Temperature Thresholds		
	Clear Alarm	Minor	Major
NPU Board Temp Sensor	60	65	75
NPU NP0 Temp Sensor	60	65	75

LM75 Sensor Type	Temperature Thresholds		
	Clear Alarm	Minor	Major
NPU NP1 Temp Sensor	60	65	75
NPU DX240 Temp Sensor	60	65	75
NPU CAM Temp Sensor	60	65	75

TCU Sensors

The following table identifies LM85 sensors and corresponding temperature thresholds for TCU cards.

LM84 Sensor Type	Local Temperature Threshold		Remote Temperature Threshold	
	Minor	Major	Minor	Major
TCU CPU 0 Temp Sensor	70	85	85	95
TCU CPU 1 Temp Sensor	70	85	85	95
TCU FPGA Temp Sensor	65	75	70	80

The following table identifies LM75 sensors and corresponding temperature thresholds for TCU cards.

LM75 Sensor Type	Temperature Thresholds		
	Clear Alarm	Minor	Major
TCU Board Temp Sensor	60	65	75
TCU Board Corner Sensor	73	78	88
TCU TCM 0 Temp Sensor	88	93	103
TCU TCM 1 Temp Sensor	91	96	106
TCU TCM 2 Temp Sensor	62	67	77
TCU TCM 3 Temp Sensor	62	67	77

Interface Card and Fan Sensors

The following table identifies LM75 sensors and corresponding temperature thresholds for interface cards and fan temperature.

LM75 Sensor Type	Temperature Thresholds		
	Clear Alarm	Minor	Major
MIU Temp Sensor	60	65	75
PHY Temp Sensor	60	65	75
Fan Temp Sensor	55	60	70

MIB Information

The following table lists the temperature alarms and the traps generated.

Name/ID	Severity/ Health Degradation	Cause(s)	Log Message	Traps Generated
I2C TEMP WARNING/ 128XX270 . . . . . . 128XX27F	MINOR/ 20	• Temperature fault detected. • Minor temperature fault detected on fan controller.	• Temperature Warning on X in Slot N • Setting Minor Temperature Fault on FAN Controller X. Temp is XX.	apEnvMonTempChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C TEMP HIGH/ 128XX280 . . . . . . 128XX28F	MAJOR/ 50	• Temperature fault detected. • Major temperature fault detected on fan controller.	• Over Temperature Fault on X in slot N • Setting Major Temperature Fault on FAN Controller X. Temp is XX. • HIgh Temperature Alarm on X in Slot N	apEnvMonTempChangeNotification OR apSyslogMessageGenerated (See Note 1)

show i2c

The **show i2c** command displays temperature properties for all i2c devices.

`LM75 TEMPERATURE PROPERTIES` lists Over Temp values, Trigger Level values, and Reset Level values to support the seperate thresholds for triggering and reseting an alarm. Over Temp is a Boolean value which is set when there is an active temperature alarm. The Trigger Level is the high temperature threshold; when temperatures exceed this value, a minor temperature alarm is generated. The Reset Level is the threshold that clears a minor temperature alarm.

An example of the **show i2c** output is shown below:

```
ACMESYSTEM# show i2c

SPU0 I2C PROPERTIES

LM84 TEMPERATURE PROPERTIES
Name                          Local Temp     Remote Temp    Loc/Rem/Open Fault
SPU CPU 0 Temp Sensor         39             40             0/0/0
SPU CPU 1 Temp Sensor         39             40             0/0/0
SPU CPU 2 Temp Sensor         37             38             0/0/0
SPU CPU 3 Temp Sensor         37             38             0/0/0
SPU CPU 4 Temp Sensor         36             37             0/0/0

LM75 TEMPERATURE PROPERTIES
Name                                  Temperature    Over Temp Trigger Level Reset Level
SPU Board Temp Sensor                  36.5           0         65            60
SPU Board Left Center Temp Sensor      28.5           0         65            60
SPU Board Back Temp Sensor             33.5           0         65            60
SPU Board Middle Temp Sensor           34.5           0         65            60

DIGITAL POWER PROPERTIES
Name                          Uptime    Status
SPU DPM Temp Sensor           3895594   Group A: Normal
                                        Group B: Normal
                                        Group C: Normal
                                        Group D: Normal


NPU0 I2C PROPERTIES

LM84 TEMPERATURE PROPERTIES
Name                          Local Temp     Remote Temp    Loc/Rem/Open Fault
NPU CPU Temp Sensor           40             42             0/0/0
NPU FPGA Temp Sensor          32             33             0/0/0

LM75 TEMPERATURE PROPERTIES
Name                          Temperature    Over Temp Trigger Level Reset Level
NPU Temp Sensor               36             0         65            60
NPU NP0 Temp Sensor           28.5           0         65            60
NPU NP1 Temp Sensor           32.5           0         65            60
NPU DX240 Temp Sensor         26.5           0         65            60
NPU CAM Temp Sensor           32             0         N/A           N/A

DIGITAL POWER PROPERTIES
Name                          Uptime    Status
NPU DPM Sensor                3634813   Group A: Normal
                                        Group B: Normal
                                        Group C: Normal
                                        Group D: Normal
```

```
NPU0 I2C PROPERTIES

LM84 TEMPERATURE PROPERTIES
Name                          Local Temp     Remote Temp    Loc/Rem/Open Fault
NPU CPU Temp Sensor           40             42             0/0/0
NPU FPGA Temp Sensor          32             33             0/0/0

LM75 TEMPERATURE PROPERTIES
Name                          Temperature    Over Temp Trigger Level Reset Level
NPU Temp Sensor               36             0         65            60
NPU NP0 Temp Sensor           28.5           0         65            60
NPU NP1 Temp Sensor           32.5           0         65            60
NPU DX240 Temp Sensor         26.5           0         65            60
NPU CAM Temp Sensor           32             0         N/A           N/A

DIGITAL POWER PROPERTIES
Name                          Uptime    Status
NPU DPM Sensor                3634813   Group A: Normal
                                        Group B: Normal
                                        Group C: Normal
                                        Group D: Normal


TCU0 I2C PROPERTIES

LM84 TEMPERATURE PROPERTIES
Name                          Local Temp     Remote Temp    Loc/Rem/Open Fault
TCU CPU 0 Temp Sensor         39             40             0/0/0
TCU CPU 1 Temp Sensor         39             40             0/0/0
TCU FPGA Temp Sensor          0              0              0/0/0
TCU DPM Sensor                616820    Group A: Normal
                                        Group B: Normal
                                        Group C: Normal
                                        Group D: Normal

LM75 TEMPERATURE PROPERTIES
Name                          Temperature    Over Temp Trigger Level Reset Level
TCU Board Temp Sensor         46             0         65            60
TCU Board Corner Temp         39             0         78            73
TCU TCM 0 Temp Sensor         65             0         93            88
TCU TCM 1 Temp Sensor         Device Not Installed
TCU TCM 2 Temp Sensor         46             0         67            62
TCU TCM 3 Temp Sensor         43.5           0         67            62

DIGITAL POWER PROPERTIES
Name                          Uptime    Status
TCU DPM Sensor                616820    Group A: Normal
                                        Group B: Normal
                                        Group C: Normal
                                        Group D: Normal
```

```
MIU0 I2C PROPERTIES

LM75 TEMPERATURE PROPERTIES
Name                          Temperature    Over Temp Trigger Level Reset Level
MIU LM75 Temp Sensor          28.5           0         65            60

DIGITAL POWER PROPERTIES
Name                          Uptime    Status
MIU DPM Sensor                616449    Group A: Normal
                                        Group B: Normal

PHY0 I2C PROPERTIES

LM75 TEMPERATURE PROPERTIES
Name                          Temperature    Over Temp Trigger Level Reset Level
PHY LM75 Temp Sensor          28.5           0         65            60

PM8380 SERDES MUX PROPERTIES
Name                          Initialized    Channel
PM8380 SerDes Mux Sensor      True           A

DIGITAL POWER PROPERTIES
Name                          Uptime    Status
PHY DPM Sensor                617401    Group A: Normal
                                        Group B: Normal

FIBER PHY PLD PROPERTIES
Name                          Full BW   Tx Disabled    SFP Present    LOS       Tx Fault
Fiber PHY PLD Sensor Port 0    Yes       No             Yes            No        No
Fiber PHY PLD Sensor Port 1    Yes       No             Yes            No        No
Fiber PHY PLD Sensor Port 2    Yes       No             Yes            No        No
Fiber PHY PLD Sensor Port 3    Yes       No             Yes            Yes       No


FANCTRL 0 I2C PROPERTIES

FAN PROPERTIES
Name                          Temperature    Speed     Fan 1/2/3/4/Comm Faults
Fan Controller 0              26             8         0/0/0/0/0

POWER0 I2C PROPERTIES

POWER PROPERTIES
Name                          Temperature    Avg. Voltage  Avg. Current
Power Supply 0                32             12        18
```

Network Processor Card Statistics

The Network Processor Unit (NPU) is responsible for forwarding media packets along the data plane and propagating signaling packets up to the control plane. Traffic that crosses the NPU's internal GigE switch (DX240) is purely network traffic,

and is not used by system tasks as they talk to each other. A series of low-level statistics for the NPU's GigE switch are available.

show npu phy-port

The **show npu port** command displays the port configuration on the phy side of the dx240. This command takes a media slot and port argument. For example:

```
ACMEPACKET# npu phy-port 0 0 (fiber phy)
:14034200 00051c3e 00003748 000078cc

DX240 P00 MAC: fiber  disabled linkDOWN 1000M FD FC
        SYNC Fail Hi PCS Err PLL Locked

ACMEPACKET# show npu phy-port 1 0 (copper phy)
NPU240 PHY-Side Slot 0
P00 MAC:copper enabled  linkUP   100M  HD
        Copper PHY: linkUP   100M  HD AN Cmplt
        FORCE link pass
```

show npu phy-stats

The **show npu phy-stats** command displays Ethernet statistics on the phy side of the dx240. This command takes a media slot and port argument. For example:

```
ACMEPACKET# show npu phy-stats 0 0
NPU 240 PHY-side Slot 0 Port 0 Counters:
 goodOctetsSent                192 goodOctetsRcv            16352393
 goodPktsSent                    3 goodPktsRcv                36289
 brdcPktsSent                    3 brdcPktsRcv                  535
 mcPktsSent                      0 mcPktsRcv                      0
 badPktsRcv                     14 pkts64Octets                 736
 pkts65to127Octets            1239 pkts128to255Octets           270
 pkts256to511Octets          22703 pkts512to1023Octets        11341
 pkts1024tomaxOoctets            0 badOctetsRcv                15
 macTransmitErr                  0 excessiveCollisions            0
 unrecogMacCntrRcv               0 fcSent                         0
 goodFcRcv                       0 dropEvents                     0
 undersizePkts                   0 fragmentsPkts                 14
 oversizePkts                    0 jabberPkts                     0
 macRcvError                     0 badCrc                         0
 collisions                      0 lateCollisions                 0
 badFcRcv                        0
```

show npu phy-registers

The **show npu phy-registers** command displays register contents for each port on the NPU's DX240 switch. This command is ONLY applicable when a trispeed copper NIU is connected to the queried port. This command takes a media slot and port argument. Typing this command without any argument displays the NPU stats for port 0. This command is entered as:

```
ACMEPACKET# show npu phy-registers <slot> <port>
```

For example:

```
ACMEPACKET# show npu phy-registers 0 0
PHY Port 0 Page 0 regs:
Reg 00->1140 Reg 01->7949 Reg 02->0141 Reg 03->0cd4
Reg 04->05e1 Reg 05->0000 Reg 06->0004 Reg 07->2001
```

```
Reg 08->0000 Reg 09->0b00 Reg 10->0000 Reg 11->0000
Reg 12->0000 Reg 13->0000 Reg 14->0000 Reg 15->f000
Reg 16->0078 Reg 17->8140 Reg 18->0000 Reg 19->0040
Reg 20->0c68 Reg 21->0000 Reg 22->0000 Reg 23->0000
Reg 24->4100 Reg 25->0000 Reg 26->000a Reg 27->8684
Reg 28->0000 Reg 29->0000 Reg 30->0000
PHY Port 0 Page 1 regs:
Reg 00->0140 Reg 01->014d Reg 02->0141 Reg 03->0cd4
Reg 04->0801 Reg 05->0000 Reg 06->0004 Reg 07->2001
Reg 08->0000 Reg 09->0b00 Reg 10->0000 Reg 11->0000
Reg 12->0000 Reg 13->0000 Reg 14->0000 Reg 15->f000
Reg 16->0078 Reg 17->8410 Reg 18->0000 Reg 19->0000
Reg 20->0c68 Reg 21->0000 Reg 22->0001 Reg 23->0000
Reg 24->4100 Reg 25->0000 Reg 26->000a Reg 27->8684
```

show npu gmac-port

The **show npu gmac-port** command displays the port configuration on the GMAC side of the DX240. This command takes a media slot and port argument. For example:

```
ACMEPACKET# show npu gmac-port 0 0

NPU240 GMAC-Side Slot 0
P00 MAC:copper enabled  linkUP   1000M FD FC
```

show npu gmac-stats

The **show npu gmac-stats** command displays statistics on the GMAC side of the dx240. This command takes a media slot and port argument. For example:

```
ACMEPACKET# show npu gmac-stats 0 0
NPU 240 GMAC-Side Slot 0 Port 0 Counters:
 goodOctetsSent              183459 goodOctetsRcv              14946
 goodPktsSent                  1541 goodPktsRcv                159
 brdcPktsSent                   535 brdcPktsRcv                  0
 mcPktsSent                       0 mcPktsRcv                    0
 badPktsRcv                       0 pkts64Octets                 0
 pkts65to127Octets              159 pkts128to255Octets           0
 pkts256to511Octets               0 pkts512to1023Octets         0
 pkts1024tomaxOoctets             0 badOctetsRcv                0
 macTransmitErr                   0 excessiveCollisions         0
 unrecogMacCntrRcv                0 fcSent                      0
 goodFcRcv                        0 dropEvents                  0
 undersizePkts                    0 fragmentsPkts               0
 oversizePkts                     0 jabberPkts                  0
 macRcvError                      0 badCrc                      0
 collisions                       0 lateCollisions              0
 badFcRcv                         0
```

The **show npu gmac-stats** command has a different output when running with an NPU3 installed in the system.

```
ACMESYSTEM# show npu gmac-stats 0 0
--------------------
Dec 22 16:10:33.822
NPU Switch NP-Side Aggregate Counters for (Slot 0 Port 0) and (Slot 0
Port 2):
Npu3 FPGA SPI4.2 Stats dump:
SPI SINK_SOP_VIOLATION       :0x00000000
```

```
    SPI SINK_DATA_EOP_ERROR      :0x00000000
    SPI SINK_PYLD_CNTL_ERROR     :0x00000000
    SPI SINK_DIP4_ERROR_CNT      :0x00000000
    SPI SINK_RESERVED_CNTL       :0x00000000
    SPI SINK_NONZERO_ADDR        :0x00000000
    SPI SINK_BUS_SOP             :0x000002c0
    SPI SINK_BUS_EOP             :0x000002c0
    SPI SINK_BUS_ABORT_ERROR     :0x00000000
    SPI SOURCE_STATUS_ERROR      :0x00000000
    SPI SOURCE_DATA_ERROR        :0x00000000
    SPI SOURCE_SOP_COUNTER       :0x00000c26
    SPI SOURCE_EOP_COUNTER       :0x00000c26
    SPI SOURCE_EOP_ERR_COUNT     :0x00000000
    SPI SINK_DPA_ERR_COUNT       :0x00000000
SPI SINK_OOF_COUNT           :0x00000000
```

show npu cpu-stats

The **show npu cpu-stats** command displays statistics for the CPU port on the DX240. This is the interface port between the DX240 and the NPU's CPU. For example:

```
ACMEPACKET# show npu cpu-stats
Good Frames Sent 34559
MAC Tx Error Frames 0
Good Octets Sent 3416567
Good Frames Rxd 409
Bad Frames Rxd 0
Good Octets Rxd 46769
Bad Octets Rxd 0
```

show npu registers

The **show npu registers** command displays four key register contents for each of the DX240's ports. For example:

```
ACMEPACKET# show npu registers
DX240 00000000->00066003 00000004->204ca120 0000004c->0000d141
000000a0->0e03943f 000000a4->0001001d
DX240 P00 Ctrl 04000000->14030201 Stat    P00 04000004->00073009
DX240 P00 Auto 04000008->000033ec Serdes  P00 04000010->000078cc
DX240 P01 Ctrl 04000100->14030203 Stat    P01 04000104->00071000
DX240 P01 Auto 04000108->000033ec Serdes  P01 04000110->000078cc
DX240 P02 Ctrl 04000200->14030205 Stat    P02 04000204->00071000
DX240 P02 Auto 04000208->000033ec Serdes  P02 04000210->000078cc
DX240 P03 Ctrl 04000300->14030207 Stat    P03 04000304->00071000
DX240 P03 Auto 04000308->000033ec Serdes  P03 04000310->000078cc
DX240 P04 Ctrl 04000400->14034209 Stat    P04 04000404->00051c3e
DX240 P04 Auto 04000408->00003769 Serdes  P04 04000410->000078cc
DX240 P05 Ctrl 04000500->1403420b Stat    P05 04000504->00051c3e
DX240 P05 Auto 04000508->00003769 Serdes  P05 04000510->000078cc
DX240 P06 Ctrl 04800000->1403420d Stat    P06 04800004->00051c3e
DX240 P06 Auto 04800008->00003769 Serdes  P06 04800010->000078cc
DX240 P07 Ctrl 04800100->1403420f Stat    P07 04800104->00051c3e
DX240 P07 Auto 04800108->00003769 Serdes  P07 04800110->000078cc
DX240 P08 Ctrl 04800200->14030411 Stat    P08 04800204->0007303d
DX240 P08 Auto 04800208->00003368 Serdes  P08 04800210->000078cc
DX240 P09 Ctrl 04800300->14030413 Stat    P09 04800304->0007303d
```

```
DX240 P09 Auto 04800308->00003368 Serdes  P09 04800310->000078cc
DX240 P10 Ctrl 04800400->14030415 Stat    P10 04800404->0007303d
DX240 P10 Auto 04800408->00003368 Serdes  P10 04800410->000078cc
DX240 P11 Ctrl 04800500->14030417 Stat    P11 04800504->0007303d
DX240 P11 Auto 04800508->00003368 Serdes  P11 04800510->000078cc
DX240 P12 Ctrl 05000000->14030219 Stat    P12 05000004->00073009
DX240 P12 Auto 05000008->000033ec Serdes  P12 05000010->000078cc
DX240 P13 Ctrl 05000100->1403021b Stat    P13 05000104->00071000
DX240 P13 Auto 05000108->000033ec Serdes  P13 05000110->000078cc
DX240 P14 Ctrl 05000200->1403021d Stat    P14 05000204->00071000
DX240 P14 Auto 05000208->000033ec Serdes  P14 05000210->000078cc
DX240 P15 Ctrl 05000300->1403021f Stat    P15 05000304->00071000
DX240 P15 Auto 05000308->000033ec Serdes  P15 05000310->000078cc
DX240 P16 Ctrl 05000400->14034221 Stat    P16 05000404->00051c3e
DX240 P16 Auto 05000408->00003769 Serdes  P16 05000410->000078cc
DX240 P17 Ctrl 05000500->14034223 Stat    P17 05000504->00051c3e
DX240 P17 Auto 05000508->00003769 Serdes  P17 05000510->000078cc
DX240 P18 Ctrl 05800000->14034225 Stat    P18 05800004->00051c3e
DX240 P18 Auto 05800008->00003769 Serdes  P18 05800010->000078cc
DX240 P19 Ctrl 05800100->14034227 Stat    P19 05800104->00051c3e
DX240 P19 Auto 05800108->00003769 Serdes  P19 05800110->000078cc
DX240 P20 Ctrl 05800200->14030429 Stat    P20 05800204->0007303d
DX240 P20 Auto 05800208->00003368 Serdes  P20 05800210->000078cc
DX240 P21 Ctrl 05800300->1403042b Stat    P21 05800304->0007303d
DX240 P21 Auto 05800308->00003368 Serdes  P21 05800310->000078cc
DX240 P22 Ctrl 05800400->1403042d Stat    P22 05800404->0007303d
DX240 P22 Auto 05800408->00003368 Serdes  P22 05800410->000078cc
DX240 P23 Ctrl 05800500->1403042f Stat    P23 05800504->0007303d
DX240 P23 Auto 05800508->00003368 Serdes  P23 05800510->000078cc
```

dump npu-stats

The **dump npu-stats** command loops through a series of NPU statistics twice and writes the results to the log.npu_debug file.

Internal Switch Statistics

The Net-Net system's SPU contains a GigE switch which facilitates communication between every task on the Net-Net 9200 chassis. The **show switch** command usage is as follows:

```
ACMEPACKET# show switch <slot #> [portstate | portstats | linkstate |
l2table] <port #>
```

The port # argument is optional and filters for the given port.

show switch portstate

The **show switch portstate** command displays the state of each port on the specified switch. You must include the slot number to indicate which switch to query. For example:

```
ACMEPACKET# show switch 0 portstate
BCM Switch Port 0 State is Active
BCM Switch Port 1 State is Active
BCM Switch Port 2 State is Active
BCM Switch Port 3 State is Active
BCM Switch Port 4 State is Active
BCM Switch Port 5 State is Active
BCM Switch Port 6 State is Active
```

```
BCM Switch Port 7 State is Active
BCM Switch Port 8 State is Active
BCM Switch Port 9 State is Active
BCM Switch Port 10 State is Active
BCM Switch Port 11 State is Active
BCM Switch Port 12 State is Active
BCM Switch Port 13 State is Active
BCM Switch Port 14 State is Active
ACMEPACKET#
```

show switch linkstate

The **show switch linkstate** command displays the link state for each port on the specified switch. You must include the slot number to indicate which switch to query. Specifying a port number filters for that port. For example:

```
ACMEPACKET#  show switch 0 linkstate
BCM Switch Port 0 Link is Active
BCM Switch Port 1 Link is Active
BCM Switch Port 2 Link is Active
BCM Switch Port 3 Link is Active
BCM Switch Port 4 Link is Active
BCM Switch Port 5 Link is InActive
BCM Switch Port 6 Link is InActive
BCM Switch Port 7 Link is Active
BCM Switch Port 8 Link is InActive
BCM Switch Port 9 Link is InActive
BCM Switch Port 10 Link is InActive
BCM Switch Port 11 Link is InActive
BCM Switch Port 12 Link is InActive
BCM Switch Port 13 Link is InActive
BCM Switch Port 14 Link is InActive
ACMEPACKET#  show switch 0 linkstate 1
BCM Switch Port 1 Link is Active
```

show switch portstats

The **show switch portstats** command displays the statistics for each port on the specified switch. You must include the slot number to indicate which switch to query. Specifying a port number filters for that port. For example:

```
ACMEPACKET#  show switch 0 portstats 1
Statistics for Unit 0 port ge1
               3529142237      snmpIfInOctets (stat 0)
                 53518830      snmpIfInUcastPkts (stat 1)
                        8      snmpIfInNUcastPkts (stat 2)
                      201      snmpIfInErrors (stat 4)
               3553834235      snmpIfOutOctets (stat 6)
                 53515186      snmpIfOutUcastPkts (stat 7)
                     4882      snmpIfOutNUcastPkts (stat 8)
                     6638      snmpDot1dBasePortMtuExceededDiscards (stat 17)
                 53518838      snmpDot1dTpPortInFrames (stat 18)
                 53520068      snmpDot1dTpPortOutFrames (stat 19)
                     4890      snmpEtherStatsBroadcastPkts (stat 23)
                      153      snmpEtherStatsFragments (stat 25)
                106499036      snmpEtherStatsPkts64Octets (stat 26)
                   205155      snmpEtherStatsPkts65to127Octets (stat 27)
                    30733      snmpEtherStatsPkts128to255Octets (stat 28)
                   111558      snmpEtherStatsPkts256to511Octets (stat 29)
                   136274      snmpEtherStatsPkts512to1023Octets (stat 30)
                    49512      snmpEtherStatsPkts1024to1518Octets (stat 31)
                     6638      snmpEtherStatsOversizePkts (stat 32)
0x00000001a62da4d8      snmpEtherStatsOctets (stat 34)
                107038906      snmpEtherStatsPkts (stat 35)
                 53513478      snmpEtherStatsTXNoErrors (stat 38)
                 53518790      snmpEtherStatsRXNoErrors (stat 39)
                       48      snmpDot3StatsFrameTooLongs (stat 50)
               3529142237      snmpIfHCInOctets (stat 56)
                 53518830      snmpIfHCInUcastPkts (stat 57)
                        8      snmpIfHCInBroadcastPkts (stat 59)
               3553834235      snmpIfHCOutOctets (stat 60)
                 53515186      snmpIfHCOutUcastPkts (stat 61)
                     4882      snmpIfHCOutBroadcastPckts (stat 63)
                      136      snmpBcmEtherStatsPkts1522to2047Octets (stat 69)
                      350      snmpBcmEtherStatsPkts2048to4095Octets (stat 70)
                     6152      snmpBcmEtherStatsPkts4095to9216Octets (stat 71)
```

show switch l2table

The **show switch l2table** command displays the Layer 2, Ethernet table on the specified switch. The Ethernet address and vlan ID are shown for the port they are bound to. For example:

```
ACMEPACKET#  show switch 0 l2table

L2 Table for BCM 56304

[iCm]mac=00:11:22:01:02:01 vlan=1 modid=0 port=6/ge6[iCm]
[iCm]mac=00:11:22:01:00:21 vlan=1 modid=0 port=6/ge6[iCm]
[iCm]mac=00:11:22:00:00:41 vlan=1 modid=0 port=4/ge4[iCm]
[iCm]mac=00:11:22:01:06:01 vlan=1 modid=0 port=6/ge6[iCm]
```

```
[iCm]mac=00:11:22:00:03:01 vlan=1 modid=0 port=8/ge8[iCm]
[iCm]mac=00:11:22:01:05:11 vlan=1 modid=0 port=6/ge6[iCm]
[iCm]mac=00:11:22:00:00:11 vlan=1 modid=0 port=1/ge1[iCm]
[iCm]mac=00:11:22:aa:00:31 vlan=1 modid=0 port=3/ge3[iCm]
[iCm]mac=00:11:22:00:04:11 vlan=1 modid=0 port=10/ge10[iCm]
[iCm]mac=00:11:22:00:00:30 vlan=1 modid=0 port=3/ge3[iCm]
[iCm]mac=00:11:22:aa:00:10 vlan=1 modid=0 port=1/ge1[iCm]
[iCm]mac=00:11:22:00:06:10 vlan=1 modid=0 port=14/ge14[iCm]
[iCm]mac=00:11:22:00:05:00 vlan=1 modid=0 port=11/ge11[iCm]
[iCm]mac=00:11:22:01:00:00 vlan=1 modid=0 port=6/ge6[iCm]
[iCm]mac=00:11:22:00:01:00 vlan=1 modid=0 port=5/ge5[iCm]
[iCm]mac=00:11:22:aa:00:40 vlan=1 modid=0 port=4/ge4[iCm]
[iCm]mac=00:11:22:01:04:00 vlan=1 modid=0 port=6/ge6[iCm]
[iCm]mac=00:11:22:00:03:00 vlan=1 modid=0 port=8/ge8[iCm]
[iCm]mac=00:11:22:01:06:00 vlan=1 modid=0 port=6/ge6[iCm]
[iCm]mac=00:11:22:00:00:40 vlan=1 modid=0 port=4/ge4[iCm]
[iCm]mac=00:11:22:01:00:20 vlan=1 modid=0 port=6/ge6[iCm]
[iCm]mac=00:11:22:01:02:00 vlan=1 modid=0 port=6/ge6[iCm]
```

show switch

The **show switch** command has a different output when running with an NPU3 installed in the system.

```
ACMESYSTEM# show switch 2 portstate
NPU Switch Port 0 ( Phy 0 Port 0) State is Active
NPU Switch Port 1 ( Phy 0 Port 1) State is Active
NPU Switch Port 2 ( Phy 0 Port 2) State is Inactive
NPU Switch Port 3 ( Phy 0 Port 3) State is Inactive
NPU Switch Port 4 ( Phy 2 Port 0) State is Active
NPU Switch Port 5 ( Phy 2 Port 1) State is Active
NPU Switch Port 6 ( Phy 2 Port 2) State is Inactive
NPU Switch Port 7 ( Phy 2 Port 3) State is Inactive
NPU Switch Port 8 ( Arsenal 0 to EZChip ) State is Active
NPU Switch Port 9 ( Arsenal 0 to Cavium ) State is Active
NPU Switch Port 10 ( Arsenal 0 to Host ) State is Inactive
NPU Switch Port 11 ( Arsenal 0 Bridge SPI ) State is Active
NPU Switch Port 12 ( Phy 1 Port 0) State is Inactive
NPU Switch Port 13 ( Phy 1 Port 1) State is Inactive
NPU Switch Port 14 ( Phy 1 Port 2) State is Inactive
NPU Switch Port 15 ( Phy 1 Port 3) State is Inactive
NPU Switch Port 16 ( Phy 3 Port 0) State is Inactive
NPU Switch Port 17 ( Phy 3 Port 1) State is Inactive
NPU Switch Port 18 ( Phy 3 Port 2) State is Inactive
NPU Switch Port 19 ( Phy 3 Port 3) State is Inactive
NPU Switch Port 20 ( Arsenal 1 to EZChip ) State is Active
NPU Switch Port 21 ( Arsenal 1 to Cavium ) State is Active
NPU Switch Port 22 ( Arsenal 1 to Host ) State is Inactive
NPU Switch Port 23 ( Arsenal 1 Bridge SPI ) State is Active
NPU Switch Port 24 ( Arsenal 0 TCU MAC 0 ) State is Active
NPU Switch Port 25 ( Arsenal 0 TCU MAC 1 ) State is Active
NPU Switch Port 26 ( Arsenal 0 TCU MAC 2 ) State is Active
NPU Switch Port 27 ( Arsenal 0 TCU MAC 3 ) State is Active
NPU Switch Port 28 ( Arsenal 1 TCU MAC 0 ) State is Active
NPU Switch Port 29 ( Arsenal 1 TCU MAC 1 ) State is Active
NPU Switch Port 30 ( Arsenal 1 TCU MAC 2 ) State is Active
```

```
NPU Switch Port 31 ( Arsenal 1 TCU MAC 3 ) State is Active


ACMESYSTEM# show switch 2 linkstate
NPU switch Switch Port 0 ( Phy 0 Port 0) Link State is Inactive
NPU switch Switch Port 1 ( Phy 0 Port 1) Link State is Inactive
NPU switch Switch Port 2 ( Phy 0 Port 2) Link State is Inactive
NPU switch Switch Port 3 ( Phy 0 Port 3) Link State is Inactive
NPU switch Switch Port 4 ( Phy 2 Port 0) Link State is Active
NPU switch Switch Port 5 ( Phy 2 Port 1) Link State is Active
NPU switch Switch Port 6 ( Phy 2 Port 2) Link State is Inactive
NPU switch Switch Port 7 ( Phy 2 Port 3) Link State is Inactive
NPU switch Switch Port 8 ( Arsenal 0 to EZChip ) Link State is Active
NPU switch Switch Port 9 ( Arsenal 0 to Cavium ) Link State is Active
NPU switch Switch Port 10 ( Arsenal 0 to Host ) Link State is Active
NPU switch Switch Port 11 ( Arsenal 0 Bridge SPI ) Link State is Active
NPU switch Switch Port 12 ( Phy 1 Port 0) Link State is Active
NPU switch Switch Port 13 ( Phy 1 Port 1) Link State is Active
NPU switch Switch Port 14 ( Phy 1 Port 2) Link State is Active
NPU switch Switch Port 15 ( Phy 1 Port 3) Link State is Active
NPU switch Switch Port 16 ( Phy 3 Port 0) Link State is Active
NPU switch Switch Port 17 ( Phy 3 Port 1) Link State is Active
NPU switch Switch Port 18 ( Phy 3 Port 2) Link State is Active
NPU switch Switch Port 19 ( Phy 3 Port 3) Link State is Active
NPU switch Switch Port 20 ( Arsenal 1 to EZChip ) Link State is Active
NPU switch Switch Port 21 ( Arsenal 1 to Cavium ) Link State is Active
NPU switch Switch Port 22 ( Arsenal 1 to Host ) Link State is Active
NPU switch Switch Port 23 ( Arsenal 1 Bridge SPI ) Link State is Active
NPU switch Switch Port 24 ( Arsenal 0 TCU MAC 0 ) Link State is Active
NPU switch Switch Port 25 ( Arsenal 0 TCU MAC 1 ) Link State is Active
NPU switch Switch Port 26 ( Arsenal 0 TCU MAC 2 ) Link State is Active
NPU switch Switch Port 27 ( Arsenal 0 TCU MAC 3 ) Link State is Active
NPU switch Switch Port 28 ( Arsenal 1 TCU MAC 0 ) Link State is Active
NPU switch Switch Port 29 ( Arsenal 1 TCU MAC 1 ) Link State is Active
NPU switch Switch Port 30 ( Arsenal 1 TCU MAC 2 ) Link State is Active
NPU switch Switch Port 31 ( Arsenal 1 TCU MAC 3 ) Link State is Active
```

TCU Statistics

The Net-Net system's TCU can be queried for contains a GigE switch which facilitates communication between every task on the Net-Net 9200 chassis. The **show tcu** command usage is as follows:

```
show TCU [flair | gbe | hm | ibx | tcm] <slot> [<tcm-ID> <port>]
```

The TCM ID and port arguments are only used with the gbe and ibx arguments.

show tcu flair

The **show tcu flair** command displays the FLAIR statistics and counters of an identified TCU. The command is entered as:

```
show tcu flair <tcu slot>
```

For example:

```
ACMEPACKET# show tcu flair 4
=================== FLAIR Statistics ====================
```

```
version                                 :       0x6a0b0244
System Status                           :       0x00000065
Channel Select                          :       0x0000010c
Port 0 Link Error Counter               :       0x00000000
Port 1 Link Error Counter               :       0x00000000
Port 0 Data Error Counter               :       0x00000000
Port 1 Data Error Counter               :       0x00000000
Port 0 Catastrophic Error Counter       :       0x00000000
Port 1 Catastrophic Error Counter       :       0x00000000
Packet Counter                          :       0x00000000
Packet Error                            :       0x00f00baa
Ethernet to Swingline Packet Counter    :       0x00000014
Ethernet to Swingline Cell Counter      :       0x00000000
```

The **show tcu flair** command has a different output when running with an NPU3 and TCU installed in the system. This command displays the FLAIR statistics and counters of an identified TCU. The command is entered as:

```
ACMESYSTEM# show tcu flair 4
=================== FLAIR Statistics ====================
version                                 :       0x6a0b0244
System Status                           :       0x00000065
Channel Select                          :       0x00000104
Port 0 Link Error Counter               :       0x00000000
Port 1 Link Error Counter               :       0x00000000
Port 0 Data Error Counter               :       0x00000000
Port 1 Data Error Counter               :       0x00000000
Port 0 Good Packet Counter             :       0x00000000
Port 1 Good Packet Counter              :       0x00000000
```

show tcu gbe

The **show tcu gbe** command displays Ethernet statistics betwen the NPU and TCU. It requires a slot and TCM id argument where

slot = TCU slot number

tcm ID = TCM ID: 0, 1, 2, or 3

For example:

```
ACMEPACKET# show tcu gbe 4 0
========== Flair GbE unit: 0 Statistics ==========

rev                             :       0x00010003
mac_0                           :       0x00000000
mac_1                           :       0x00000000
frm_length                      :       0x00000600
pause_quant                     :       0x00000010
rx_section_empty                :       0x00000100
rx_section_full                 :       0x00000000
tx_section_empty                :       0x000001e0
tx_section_full                 :       0x00000000
rx_almost_empty                 :       0x00000000
rx_almost_full                  :       0x00000000
tx_almost_empty                 :       0x00000008
tx_almost_full                  :       0x00000020
```

```
mdio_addr0                      :       0x00000000
mdio_addr1                      :       0x00000001
phy_status                      :       0x0000001e
aFramesTransmittedOK            :       0x00000000
aFramesReceivedOK               :       0x00000000
aFramesCheckSequenceErrors      :       0x00000000
aAlignmentErrors                :       0x00000000
aOctetsTransmittedOK            :       0x00000000
aOctetsReceivedOK               :       0x00000000
aTxPAUSEMACCtrlFrames           :       0x00000000
aRxPAUSEMACCtrlFrames           :       0x00000000
ifInErrors                      :       0x00000000
ifOutErrors                     :       0x00000000
ifInUcastPkts                   :       0x00000000
ifInBroadcastPkts               :       0x00000000
ifInMulticastPkts               :       0x00000000
ifOutDiscards                   :       0x00000000
ifOutUcastPkts                  :       0x00000000
ifOutMulticastPkts              :       0x00000000
ifOutBroadcastPkts              :       0x00000000
DropEvent                       :       0x00000000
Octets                          :       0x00000000
Pkts                            :       0x00000000
UndersizePkts                   :       0x00000000
OversizePkts                    :       0x00000000
Pkts64Octets                    :       0x00000000
Pkts65to127Octets               :       0x00000000
Pkts128to255Octets              :       0x00000000
Pkts256to511Octets              :       0x00000000
Pkts512to1023Octets             :       0x00000000
Pkts1024to1518Octets            :       0x00000000
```

show tcu hm

The **show tcu hm** command displays health monitor statistics about a specified TCU on the screen. This command requires a slot argument which refers to the TCU in the slot you are querrying. The command is entered as:

```
show tcu hm <tcu slot>
```

For example:

```
ACMEPACKET# show tcu hm 4
        Initialized               : TRUE
        Paused                    : TRUE

        Packet matched VETH       : 0
        MAC Received packets      : 0
        MAC RX packets to Q       : 0
        MAC RX packets to Q Error : 0

        Received NPU packets      : 0
        Received NPU pkt UNK ADDR : 0

        Sent TCU packets          : 0
        Sent TCU packets ERROR    : 0
```

```
                    Link Down Count           : 0
```

show tcu ibx

The **show tcu ibx** command displays the IBX unit's statistics and counters of an identified TCU. The command is entered as:

```
show tcu ibx <tcu slot> <TCM number> <TCM switch port>
```

- slot—TCU slot number, 4, 5, or 6
- tcm ID—TCM ID, 0, 1, 2, or 3
- port—DSP port 0 ~ 9, DBG port is 15, FLAIR port is 25, BCM1250 port is 26

show tcu tcm

The **show tcu tcm** command displays the TCM configuration of an identified TCU. The command is entered as:

```
show tcu tcm <tcu slot>
```

For example:

```
ACMEPACKET# show tcu tcm 4
TCM 0 at CPU 0 core 0 is Present
TCM 1 at CPU 1 core 0 is Present
TCM 2 at CPU 0 core 1 is Present
TCM 3 at CPU 1 core 1 is Present
```

Internal Switch Port Mirroring

To mirror traffic from ports to port on the SPU's internal switch (BCM 56000), you use the **mirror** command. Mirroring is a way to sniff control traffic, that you can enable and disable as needed.

Enabling and disabling mirroring requires that you enter the SPU number, port number on the switch from which you want to mirror traffic (or you can mirror them all), the port number on the SPU to which you want that traffic mirrored , and either enabled or disabled. Traffic is ALWAYS mirrored to port 19. The **mirror** command usage is as follows:

```
mirror <SPU slot> <from-port> <to-port #> <enabled|disabled>
```

For example:

```
ACMEPACKET# mirror 0 10 19 enabled
```

Remember to disable mirroring when your debugging session ends.

BCM 56000 Ports

The following table lists the ports on the SPU's BCM 56K switch.

Port Number	Connection
0	Local SPU CPU 0
1	Local SPU CPU 1
2	Local SPU CPU 2
3	Local SPU CPU 3
4	Local SPU CPU 4
5	Other SPU CPU 0

Port Number	Connection
6	Other SPU BCM56K
7	NPU's CPU (slot 2)
8	NPU's CPU (slot 3)
9	TCU CPU 0 (slot 4)
10	TCU CPU 1 (slot 4)
11	TCU CPU 0 (slot 5)
12	TCU CPU 1 (slot 5)
13	TCU CPU 0 (slot 6)
14	TCU CPU 1 (slot 6)

Switching Cores from the ACLI

When you open a connection to the Net-Net 9200 and are using the ACLI, you are connected by default to the master core on the SPU (0.0.0). However, you can connect to and use the ACLI on other cores. Using the ACLI on other cores gives you the same range of ACLI functionality that you have on the master core.

Connecting to other cores can be useful for debugging purposes, and also for viewing local logs within `/ramdrv/logs`.To switch cores from the ACLI:

1. In Superuser mode, enter the command connect console and then the slot, CPU, and core numbers to which you want to connect. You enter the slot, CPU, and core numbers in the spaced format.

   ```
   ACMEPACKET# connect console 0 0 1
   ```

2. The system prompts you to confirm. To proceed, type a **y** and press <Enter>. To stay on the current core, type an **n** to cancel the connection.

   ```
   Are You Sure [y/n]?: y
   ```

3. Once you have connected to another core, note the change in your command line prompt. The command line prompt indicates the location where you are running the ACLI.

   ```
   ACMEPACKET@0.0.1#
   ```

System Card Communication Integrity

The Net-Net OS has mechanisms to verify internal connections between feature and interface cards. These processes are enabled within the appropriate configuration elements.

SPU to MIU Communication

A ping mechanism is used to test link integrity between an SPU and its dedicated MIU. The SPU sends a ping request out of the MIU's wancom/management IP ports into the network. When a ping reply is received, the SPU-MIU link integrity is verified. If no reply is received, the SPU-MIU link integrity is considered failed.

In order to use this feature, you must configure a remote network device connected to the MIU's Ethernet ports. This device must be capable of responding to ICMP ping request messages.

SPU to MIU communication verification is enabled with the **miu0-monitor-ip-address** or **miu1-monitor-ip-address** parameter located in the **system-config** configuration element.

- **miu0-monitor-ip-address**—Enter the remote IP address of a device that will return a ping, located in MIU0's network.
- **miu1-monitor-ip-address**—Enter the remote IP address of a device that will return a ping, located in MIU1's network.

NPU to TCU Communciation

For transcoding applications, the NPU and TCU must communicate with each other. The Net-Net 9200 uses an internal process to verify the link between these two feature cards. NPU to TCU communication verification is enabled or disabled with the xcode-path-monitor parameter located in the system-config configuration element.

Password Strength

Password Policy

You can configure the minimum acceptable length for a password if you have Superuser (administrative) privileges. The maximum password length is 64 characters.

To increase password strength, new passwords must include at least one character from three out of four of the following character sets:

- Upper case letters
- Lower case letters
- Numbers
- Punctuation marks

However, passwords cannot contain any of the following strings in any variation of case: `default, password, acme, user, admin, packet`.

Any change you make to the password length requirement does not go into effect until you configure a new password. Pre-existing passwords can continue to be used until you change them.

Setting the Password Policy

In the security ACLI path, you will find the **password-policy** configuration. It contains the **min-secure-pwd-len** parameter where you set the length requirement—between 8 and 64 characters—to use for passwords when password secure mode is enabled. For example, if you set this value to 15, then your password must be a minimum of 15 characters in length.

To set the minimum password length to use for password secure mode:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type **security** and press <Enter>.

   ```
   ACMEPACKET(configure)# security
   ACMEPACKET(security)#
   ```

3. Type **password-policy** and press <Enter>.

```
ACMEPACKET(system-config)# password-policy
ACMEPACKET(password-policy)#
```

4. **min-secure-pwd-len**—Enter a value between 8 and 64 characters that defines the minimum password length to use when in password secure mode. This parameter defaults to 8.
5. Save your work using the ACLI **done** command.
6. Save and activate your configuration.

Setting a New Password

After setting a new minimum password length, you can change your password for either the User mode or the Superuser mode. The **set password** command is entered as follows:

```
set password [login | enable | reset]
```

Where

- login—Sets the User mode password
- enable—Sets the Superuser mode password
- reset—resets all passwords

1. Type **set password login** in User mode.

```
ACMEPACKET# set password login
```

2. Enter your new password at the Enter new password prompt. Your typing will not be echoed to the screen.

```
Enter new password:
```

3. If your password doesn't conform to the requirements, the ACLI prints a summary of your password's characteristics so you can see how to enter a valid password. For example:

```
ACMEPACKET# set password login
Enter new password:
% Summary:
%       password length: 9
%       alpha character count: 9
%       numeric character count: 0
%       upper-case character count: 0
%       lower-case character count: 9
%       punctuation character count: 0
%       invalid character count: 0
%
% Only alphabetic (upper or lower case), numeric and punctuation
% character are allowed in the password.
% Password must be 10 - 64 characters,
% and have 3 of the 4 following character classes :
%       - lower case alpha
%       - upper case alpha
%       - numerals
%       - punctuation
Enter new password:
```

4. Enter a new valid password, and then confirm the password.

Resetting Passwords

You can use the `set password [login | enable] reset` command to restore the associated password to the default.

Tech Support Show Command

The **show support-info** command allows you to gather a set of information commonly requested by the Acme Packet TAC when troubleshooting customer issues.

The **show support-info** usage is as follows:

```
show support-info [standard | custom]
```

- `standard`—Displays information for all commands the **show support-info** command encompasses.
- `custom`—Uses the `/code/supportinfo.cmds` file to determine what commands should be encompassed. If the file does not exist, then the system notifies you.
- media—Executes and writes out only the *show media* commands to the `support-info.log file`.
- signaling—Executes and writes all but the *show media* commands to the `support-info.log file`.

In all cases, the system displays the command's output on the screen and writes the output to the `support-log.info` file (stored in `/ramdrv/logs`).

Each time the **show support-info** command is executed a new `support-info.log` file is created. The previous `support-info.log` file is renamed by appending a .1 to the end of the file name. All additional `support-info.log` files are renamed to their previous number, plus 1. The Net-Net SBC maintains up to 6 support-info files: `support-info.log` and `support-info.log.1` through `support-info.log.5`.

For example, when executing the **show support-info** command, a new `support-info.log` file is created. The existing `support-info.log` file is renamed to `support-info.log.1`. The existing `support-info.log.1` file is renamed to `support-info.log.2`, and so on. If a `support-info.log.5` exists prior to executing the **show support-info** command, it is deleted from the system when rotating the files.

The **show support-info** command combines the output of several ACLI commands into a single command. These include:

General System Commands

```
show bootparams
show version all
show i2c
show alarm current
show clock
show system
show log level * all
show task active
show task standby
show arp
show sip sessions
show features
```

```
show health
show status
show status slot
show user
show space
show ip connections
show acl all
show cpu summary
```

Physical Interface Commands

```
show interfaces
show media network
show media frame-statistics
show media phy-statistics <slot> <port>
show media host-statistics <slot> <port>
show media classify <slot> <port>
show media gmac-statistics <slot> <port>
```

SIP Commands

```
show sip realm
show sip cache
show sip all
show sip agents
show log level sip*@*all
```

Call Media Commands

```
show mbcd all
show mbcd realms
```

xserver Commands

```
show xserv <4.0.0,5.0.0,6.0.0> stats
show xserv <4.0.0,5.0.0,6.0.0> audit alloc
show xclient xlist
show xclient api-stats
show arp
show arp-statistics-all
show arp info
show arp standby
show nat statistics
show npu hm
```

Security Commands

```
show security certificates brief
show security ssh-pub-key
show ssm-accelerator
show tls session-cache
```

Display Information to the Screen

To Display information on the screen gathered from the `show support-info` command:

1. In either User or Superuser mode, type **show support-info** at the prompt. Include `more` if you want to view the information one page at a time.

   ```
   ACMEPACKET# show support-info standard
   ```

2. At the prompt at the bottom of the window, select one of the following ways to view further information:

- Enter a **q** to exit and return to the system prompt
- Press the <enter> key to view the next page
- Press the <space> bar to view the information through the end

System Configuration Listing

The show support info command can append the complete running config output (**show running-config**) to the end of the support output file by adding the "config" argument to the end of any show support-info command, except show support-info custom. For example:

```
ACMEPACKET# show support-info standard config
```

ACLI Management

ACLI Terminal Settings

The height and width of the ACLI display, in characters is customizable. You can also control the use of the **more** prompt.

show terminal

You can view a summary for all these settings using the ACLI **show terminal** command. For example:

```
ACMEPACKET# show terminal
Terminal settings:
   Height: 40
   Width: 80
   More: enabled
```

Setting the Terminal Height

Using the **set terminal height** command, you can configure the number of rows to set the height of the display. The default is 40 rows, and valid values range from 5-1000. You can also set the terminal height to zero (`0`), which turns off the **more** prompt.

To set the terminal height:

1. Type the command **set terminal height** followed by the number of rows corresponding to the height. You can choose between 5-1000 rows, and setting the terminal height to `0` turns the **more** prompt feature off. Then press <Enter>. For example:

   ```
   ACMEPACKET# set terminal height 50
   ```

Setting the Terminal Width

Using the **set terminal width** command, you can configure the number of columns to set the width of the display. The default is 80 columns, and valid values range from 10-256.

To set the terminal width:

1. Type the command **set terminal width** followed by the number of columns corresponding to the width. Then press <Enter>. For example:

   ```
   ACMEPACKET# set terminal width 100
   ```

Controlling the "more" Prompt

When the output of a command is too large to fit your configured terminal size, the system displays the output in smaller sections. At the end of a section a message is displayed with your options:

- <Space>—Display the next section of output
- <q>—Quits and returns to the system prompt
- <c>—Displays the rest of the output in its entirety

To turn the more prompt feature on:

1. Type the command **set terminal more enabled**, and then press <Enter>.

```
ACMEPACKET# set terminal more enabled
```

To turn the more prompt feature off:

1. Type the command **set terminal more disabled**, and then press <Enter>.

```
ACMEPACKET# set terminal more disabled
```

Configuration Mismatch Warning

The Net-Net 9200 can alert you when a configuration has been changed and you've applied the **done** command, but have not saved and activated yet. When you issue the `done` command and return to Superuser mode, the system prefixes the ACLI prompt with two asterisks (**). For example:

```
**ACMEPACKET#
```

When you have saved the configuration, but not yet activated it, the system prefixes the ACLI prompt with one asterisk (*). For example:

```
*ACMEPACKET#
```

When the saved configuration and the activated configuration are synchronized after activating the saved configuration, the ACLI prompt does not contain any asterisks. For example:

```
ACMEPACKET#
```

Although the `**ACMEPACKET#` prompt is lost on reboot, logging out of an ACLI session will not affect the `done` configuration prompt. In such a case, the `**ACMEPACKET#` prompt persists across ACLI sessions.

Setting the Configuration Mismatch Warning

To enable the configuration mismatch warning:

1. At the Superuser prompt, type **set cfgchange-prompt enable**. For example:

```
ACMEPACKET# set cfgchange-prompt enable
```

To confirm the configuration version mismatch alert functionality:

1. At the Superuser prompt, type **show cfgchange-prompt**. For example:

```
ACMEPACKET# show cfgchange-prompt
```

Save Configuration Warning

The ACLI alerts you if a configuration change has not been saved before you perform a reboot. For example:

```
**ACMEPACKET# reboot
-----------------------------------------------
WARNING: configuration changes have not been saved!
Rebooting without performing a "save config" will
result in all configuration changes being lost!
-----------------------------------------------
```

```
Are You Sure [y/n]?:
```

At this point, you should type **n** <enter>, and save and activate your configuration. If you only save the configuration, but do not activate it prior to reboot. The following message appears inline during the boot process:

```
Using last running configuration, issue "activate config" to load
current configuration
```

CLI Audit Trail

You can configure your Net-Net SBC to save a history of all user-entered commands to a common audit log file. When you enable this feature, all commands entered from any ACLI session are written to the `/ramdrv/logs/cli.audit.log` file. This file is lost when the Net-Net 9200 reboots. The ACLI audit trail is enabled by default, but you can turn it off by changing the system configuration's **cli-audit-trail** parameter to **disabled**.

The `cli.audit.log` file is closed when it reaches 1,000,000 bytes. The Net-Net 9200 maintains 5 closed files at any time before the oldest file is overwritten.

The system records details like what configuration a user selects when using the select command. Prompted passwords are not saved, but the requests for changes to them are.

The cli.audit.log file resembles the following example:

```
Dec 23 19:44:06.479 OPENED 0.0.0 /ramdrv/logs/cli.audit.log
Dec 23 2009 19:48:12.330 Task: console@0,0,0 user@console : 'enable'
Dec 23 2009 19:51:53.918 Task: console@0,0,0 admin@console : 'configure
terminal
'
Dec 23 2009 19:51:54.951 Task: console@0,0,0 admin@console : 'system'
Dec 23 2009 19:51:57.398 Task: console@0,0,0 admin@console : 'system-config'
Dec 23 2009 19:52:06.132 Task: console@0,0,0 admin@console : 'select'
Dec 23 2009 19:52:06.750 Task: console@0,0,0 admin@console : 'show'
Dec 23 2009 19:52:16.889 Task: console@0,0,0 admin@console : 'done'
Dec 23 2009 19:52:18.151 Task: console@0,0,0 admin@console : 'exit'
Dec 23 2009 19:52:19.158 Task: console@0,0,0 admin@console : 'exit'
Dec 23 2009 19:52:21.389 Task: console@0,0,0 admin@console : 'exit'
Dec 23 2009 19:52:23.038 Task: console@0,0,0 admin@console : 'show interfaces'
Dec 23 2009 19:58:30.794 Task: console@0,0,0 admin@console : 'show auditlog 0'
```

Viewing the CLI Audit Trail

You can use the **show auditlog** command to view CLI Audit Trail files (cli.audit.log) directly at the ACLI. Without specifying any arguments, the system displays the file currently being written to.

You can specify the closed log to view by including an optional number argument at the end of the command. For example, typing **show auditlog 3** displays `cli.audit.log.3.gz` on the screen.

Note that rolled over files are large (1 Mb in uncompressed size) and content will take several seconds or minutes to be displayed on the screen.

ACLI Instructions and Examples

To enable CLI audit trail:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **system** and press <Enter> to access the system-level configuration elements.

```
ACMEPACKET(configure)# system
```

3. Type **system-config** and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

```
ACMEPACKET(system)# system-config
ACMEPACKET(system-config)#
```

4. **cli-audit-trail**—Set this to enabled for the CLI audit trail feature to run.
5. Save and activate your configuration.

Support for Last Modified By

The Last Modified By feature appends a new field to all configuration elements, which is displayed when viewing any configuration element instance on the ACLI. The new field indicates whether the last configuration element change was performed from the ACLI or from the Net-Net EMS, and identifies the user who performed the change.

Note: The last-modified-by field is blank after an upgrade from a Net-Net OS version that does not support this feature.

EMS derived modification

When a configuration element was last modified via EMS, the `last-modified-by` line appears as follows:

```
last-modified-by                EMS_admin_172.30.80.2_UTC
```

In the above example, the `EMS` identifier indicates that the modification was made by EMS. The `admin` identifier indicates that the modifications was made from the EMS admin account. Next, the IP address identifies the host machine of the system on which EMS was hosted. Finally, the `UTC` identifier indicates the time zone where the EMS user made the modifications, as configured.

ACLI Derived Modification

When a configuration element was last modified via the ACLI, the `last-modified-by` line of a configuration element output can take two forms, based on how the user accessed the Net-Net SBC.

Console Access

When configuring the Net-Net SBC via a console connection, the `last-modified-by` line appears as `admin` separated from the word `console` by an ampersand. For example:

```
last-modified-by                admin@console
```

Telnet/SSH Access

When configuring the Net-Net SBC via a Telnet or SSH connection, the `last-modified-by` line appears as `admin` separated from the remote access machine's IP address by an ampersand. For example:

```
last-modified-by                admin@172.30.0.78
```

RADIUS Authentication

When a Telnet or SSH login has been authenticated via RADIUS, the `last-modified-by` user takes a slightly different format than that used for internally authenticated users.

Console Access

For a RADIUS authenticated console login, the `last-modified-by` line takes the same form as when the console connection was internally authenticated. For example:

```
last-modified-by                admin@console
```

Telnet/SSH Access

For a RADIUS authenticated Telnet or SSH login, the `last-modified-by` line appears as the RADIUS user-name separated from the remote access system's IP address by an ampersand. For example:

```
last-modified-by                radius-username@172.30.0.78
```

FTP/SFTP Session Management

When listing the current user sessions on the Net-Net SBC, the ACLI now displays FTP and SFTP sessions.

Viewing Sessions

The **show users** ACLI command includes console, Telnet, SSH, FTP and SFTP entry applications as listed in the **type** column. The **state** column shows either **login** or user name, where **login** signifies that the user has yet to login. Because SFTP sessions are initiated over an SSH session, the **type** column shows up as **ssh** before login. Once the SFTP session has been initiated, the **type** column changes to **sftp**. For example:

```
ACMEPACKET# show users
Index task-id    remote-address        IdNum duration type    state
----- ---------- --------------------- ----- -------- ------- ------
    0 0x193348a0                          0   6d:03h console  user
    1 0x0f22c250     10.0.200.204:4065   100 00:01:56     ssh  priv *
   11 0x195b7290     10.0.200.204:4068    11 00:00:07     ftp  user
   21 0x196298c0     10.0.200.204:4065    21 00:01:59    sftp  user
```

Terminating Sessions

The **kill** command now supports terminating FTP and SFTP sessions. The **kill** command is used in conjunction with the **IdNum** column output, corresponding to a user session, in the **show users** command. For example:

```
ACMEPACKET# kill 11
Killing ftp session at Index 11
```

The above example terminates the FTP session in the **show users** example above.

Historical Data Recording

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

How It Works

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

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

- Turn the HDR function on and off
- Set the sample rate in minutes, or the time between individual sample collections
- Set the time in minutes 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 settings for each group of data you want to collect, and the push receiver (server) to which you want data sent.

About the CSV File

When you enable HDR and configure one or more servers to which you want records sent, data is transmitted in a CSV file in standard format. There is one CSV file per record group type, and the first record for each file is a header containing the field name for each attribute in that file.

Collection Interval and Push

In your HDR configuration, you set parameters that govern:

- The groups for which the Net-Net SBC collects records
- How frequently the Net-Net SBC collects records
- How frequently the Net-Net SBC sends records off-box

Groups, collections, and records are determined as follows:

- Number of groups you configure corresponds to the number of push files sent.
- Number of collections per file is the push interval divided by the sample interval.
- Number of records per collection is depnedent on the group you are collecitng.

For example, for a collection group of ten records, with a push interval time of 5 minutes and a sample interval time of 1 minute, the Net-Net SBC would send 50 group records and 1 header record for each push.

Note that after each successful push, the Net-Net SBC clears (deletes) all records. The Net-Net SBC also clears files on system reboot, and after three consecutive push failures.

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 that groups are sent.

Collection Object—ACLI parameter	Metrics Included
Card Group—card	• Slot Number • Description • Card state • Health score • Redundancy state
CPU Core Group—core	• Core number • Core description • Core state • CPU utilization • RAM description • RAM utilization
Environmental fan statistics (fan)	• Fan location • Description • Speed
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
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 • Maximum one way signaling latency

Collection Object—ACLI parameter	Metrics Included
ACL Group—sip-ACL	• Total entries • Trusted • Blocked • ACL requests • Bad messages • Promotions • Demotions
SIP-b2bua	• INVITE sessions • licensed sessions • subsciptions • Dialogs • CallID Map • Exceeded License Capacity • Missing Dialogs • Expired Sessions • Terminated Sessions • Multiple OK Drops • Mapped Dialogs • Map dialog forwards • Map dialog miss • XML bodies parsed • XML bodies updated • XML Bodies NATed • XML errors • Transaction errors • Application Errors • Redundancy Errors • INVITE Session Rate
SIP Client Group—sip-client	• Total • Initial • Trying • Calling • Proceeding • Cancelling • Completed • Established • Confirmed • Terminated
SIP-core	• Response Contexts • Forwarded Requests • Saved Contexts • Challenge Found • Challenge Not Found • Challenge Dropped • Overload Rejects • DNS Errors • No Target/Route • Transaction Errors • Application Errors

Collection Object—ACLI parameter	Metrics Included
SIP Errors—sip-errors	• Transport Overload • Core Overload • LS Overload • Connections Rejected • Connection Errors • Pending Msg Dropped • Suppressed Retransmit • Response Retransmit • Req Dropped • Invalid Requests • Invalid Responses • Invalid Messages • ACL Demotions • Transaction Timeouts • Duplicate Transactions • Transport Errors • Transport App Errors • Trans Redundancy Errs • Challenge Not Found • Challenge Dropped • DNS Errors • No Target/Route • XML Errors • Core Trans Errors • Core App Errors • Exceeded License Cap • Missing Dialog • Expired Sessions • Terminated Sessions • Multiple OK Drops • B2BUA Trans Errors • B2BUA App Errors • B2BUA Redundancy Errs • Reg Rejects • Reg Cache Timeouts • Reg w/o Contacts • Forced UnRegister • Out of Map Ports • NMC Rejected • NMC Diverted • No Routes Found • Next Hop OOS • Anonymous Source • Invalid Trunk Group • Inb SA Constraints • Outb SA Constraints • Inb REG SA Constraint • Outb REG SA Constraint • LS Trans Errors • LS App Errors • LS Redundancy Errors • Media Overload • SDP Offer Errors • SDP Answer Errors • Drop Media Errors • Invalid SDP • Media Failure Drops • Media Exp Events • Early Media Exps • Exp Media Drops • Media Trans Errors • Media App Errors

Collection Object—ACLI parameter	Metrics Included
SIP Policy Group—sip-policy	• Local Policy Lookups • Local Policy Hits • Local Policy Misses • Local Policy Drops • Agent Group Hits • Agent Group Misses • NMC Calls • NMC Priority Calls • NMC Rejected • NMC Diverted • No Routes Found • Next Hop OOS • Anonymous Source • Invalid Trunk Group • Inb SA Constraints • Outb SA Constraints • Inb REG SA Constraint • Outb REG SA Constraint • Overload Rejects
SIP Server Group—sip-server	• Total • Initial • Trying • Calling • Proceeding • Cancelled • Established • Completed • Confirmed • Terminated
SIP Sessions Group—sip-sessions	• Invite Sessions • Licensed Sessions • Total Sessions • Total Sessions: • Total Sessions:Initial • Total Sessions:Early • Total Sessions:Established • Total Sessions:Terminated • Dialogs • Dialogs:Initial • Dialogs:Early • Dialogs:Confirmed • Dialogs:Terminated • Subscriptions • Subscriptions:Initial • Subscriptions:Pending • Subscriptions:Active • Subscriptions:Terminated

Collection Object—ACLI parameter	Metrics Included
SIP Transport Group—sip-transport	• Server Trans • Client Trans • Context IDs • Sockets • Sockets:Inbound Connections • Sockets:Outbound Connections • Sockets:Connection Aliases • Sockets:Pending Messages • Sockets:Connections Rejected • Sockets:Connection Errors • Sockets:Pending Msg Dropped • Reg Cache Updates • Overload Rejects • Supressed Retransmit • Response Retransmit • Request Dropped • Response Dropped • Invalid Requests • Invalid Responses • Invalid Messages • Transaction Timeouts • Duplicate Transactions • Transaction Errors • Application Errors • Redundancy Errors • Rejected Messages
SIP Media Group—sip-media	• Media Sessions • Media Pending • Media Refreshed • Media Overload • SDP Offer Errors • SDP Answer Errors • Drop Media Errors • Invalid SDP • Media Failure Drops • Media Exp Events • Early Media Exps • Exp Media Drops • Transaction Errors • Application Errors

Collection Object—ACLI parameter	Metrics Included
SIP Registry Group—sip-register	• User Entries • Local Contacts • HNT Contacts • Non-HNT Contacts • AURI Entries • Free Map Ports • Used Map Ports • Transactions • Forwards • Refreshes • Updates Sent • Challenges • Rejects • Timeouts • Fwd Postponed • Fwd Rejects • Refr Extension • Refresh Extended • Reg Cache Hits • Reg Cache Misses • Route to Registrar • Reg w/o Contacts • Forced UnRegister • Out of Map Ports • Transaction Errors • Application Errors • Redundancy Errors • Surrogate Regs • Surrogate Sent • Surrogate Reject • Surrogate Timeout
System Group—system	• Current signaling sessions • Current signaling session rate (CPS) • CAM utilization NAT • CAM utilization ARP • License capacity • Cached SIP Local Contact Registrations • Current H323 Number of Registrations
SIP Invite Group—sip-invites	• Timestamp • Message/Event • Server Totals • Client Totals
H.323 Statistics (h323-stats)	• Incoming Calls • Outgoing Calls • Connected Calls • Incoming Channels • Outgoing Channels • Contexts • Queued Messeges • TPKT Channels • UDP Channels

Collection Object—ACLI parameter	Metrics Included
Combined session agent statistics (session-agent)	• Hostname • System Type • Status • Inbound Active Sessions • Inbound Session Rate • Outbound Active Sessions • Outbound Session Rate • Inbound Sessions Admitted • Inbound Sessions Not Admitted • Inbound Concurrent Sessions High • Inbound Average Session Rate • Outbound Sessions Admitted • Outbound Sessions Not Admitted • Outbound Concurrent Sessions High • Outbound Average Sessions Rate • Max Burst Rate • Total Seizures • Total Answered Sessions • Answer/Seizure Ratio • Average One-Way Signaling Latency • Maximum One-Way Signaling Latency
Environmental temperature statistics—temperature	• Slot • Sensor Type • Description • Temperature (Celsius) • State
ENUM Group—enum-stats	• ENUM Agent • Transactions • Queries Sent • Queries Send:Success • Queries Sent:NoResults • Queries Sent:Timeout • Queries Sent:Failure • Resolvers • Cached Results • Cached NoResult • Cache Hits (Results) • Cache Hits (NoResult) • Cache Drops

Collection Object—ACLI parameter	Metrics Included
Storage space for CDR collection—space	• Partition • Space used • Space available
Diameter Group—eps-bw	• PS Name • SocketsConnections • Client Transactions • Client Transactions:Reserve Requests Sent • Client Transactions:Update Requests Sent • Client Transactions:Remove Requests Sent • Client Transactions:Requests Re-Trans • Client Transactions:Install Resp Received • Client Transactions:Reject Resp Received • Client Transactions:Remove Resp Received • Client Transactions:Errors Received • Client Transactions:Transaction Timeouts • Client Transactions:Errors,Server Transactions • Server Transactions:Requests Received • Server Transactions:Dup Req Received • Server Transactions:Success Resp Sent • Server Transactions:Error Resp Sent • Server Transactions:Requests Dropped

ACLI Instructions and Examples

This section shows you how to configure HDR. You need to set up:

- The collection configuration to govern default sample and push intervals, start and end times for collection
- The group settings configuration that tells the Net-Net SBC what groups of records to collect, when to start and stop collecting them, and how often to sample for that group
- Push receivers that take the records the Net-Net SBC sends

All HDR parameters are RTC-supported, so you can save and activate your configuration for them to take effect. Typing **reset collection** is required to actually execute a newly configured collection after a change.

Accessing the HDR Configuration Parameters

You access the parameters that enable and support HDR using the ACLI **system** path.

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **system** and press <Enter>.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **collect** and press <Enter>.

   ```
   ACMEPACKET(system)# collect
   ACMEPACKET(collect)#
   ```

   From here, you can type a question mark (?) to see individual parameters for the configuration.

Global Collection Settings: Boot State, Collection Start and Stop, Sample and Push Intervals

You access the collection configuration through the ACLI **system-configuration** menu. Once in the collection configuration, you can establish the global settings for HDR collection.

Note that the push receiver is configured in a sub-configuration; refer to the Push Receiver Settings (155) for details.

To configure global settings for HDR support:

1. **boot-state**—Set this parameter to `enabled` to start group collection, or to `disabled` (default) to prevent the Net-Net SBC from collecting HDR statistics. This parameter does not go into effect until the system is rebooted. You can also use the ACLI request **reset collect** command to start collection; using this command, you can reset collection for all groups, or for one specified group.
2. **sample-interval**—Enter the time in minutes for how often you want the Net-Net SBC to sample data records. The maximum value for this parameter is 120 minutes (2 hours).
3. **push-interval**—Enter the time in minutes for how often you want the Net-Net SBC to send collected records to push receiver(s). The default is 15.
4. **start-time**—Enter the exact date and time (for your local time zone) when you want the Net-Net SBC to start HDR collection; this time is either `now` (default) or a time in the future. Your entry must be in the format `yyyy-mm-dd-hh:mm:ss`, where: `yyyy` is the year, `mm` is the month, `dd` is the day, `hh` in the hour, `mm` is the minutes, and `ss` is the second.
5. **end-time**—Enter the exact date and time (for your local time zone) when you want the Net-Net SBC to finish HDR collection; this time is either `never` (default) or a time in the future. Your entry must be in the format `yyyy-mm-dd-hh:mm:ss`, where: `yyyy` is the year, `mm` is the month, `dd` is the day, `hh` in the hour, `mm` is the minutes, and `ss` is the second. There is no default for this parameter.

Collection Group Settings

You can configure multiple collection groups on your Net-Net SBC; the names of these groups appear in the Group Record Types (146) section above. Collection group settings are accessible through the collection configuration.

Note that the sample collection interval, start time, and end time you set here override the ones established in the global collection settings. The largest value you can enter for an group's sample collection must be smaller than the global push interval value. Default group-settings are inherreted from the collection configuration element. If you do not configure any group-settings, all groups will be collected.

To configure collection group settings:

1. Access the collection group (**group-settings**) configuration by way of the collection configuration. Once

```
ACMEPACKET(system-config)# collect
ACMEPACKET(collect)# group-settings
```

2. **group-name**—Enter the group name corresponding to the records that you want to collect; there are 21 possible groups for which the Net-Net SBC can collect data. The system group name is the default for this parameter; the other possible names to which you can refer are listed in the Group Record Types (146) table above.

3. **boot-state**—To turn HDR for this collection group on, set this parameter to `enabled`. If the collect configuration element's boot-state is set to disabled, this group-settings configuration element is ignored.
4. **sample-interval**—Enter the time in minutes for how often you want the Net-Net SBC to sample data records for the specified group. The maximum value for this parameter is 120 minutes (2 hours).
5. **start-time**—Enter the exact date and time (for your local time zone) when you want the Net-Net SBC to start collecting records for this group; this time is either now or a time in the future. Your entry must be in the format `yyyy-mm-dd-hh:mm:ss`, where: `yyyy` is the year, `mm` is the month, `dd` is the day, `hh` in the hour, `mm` is the minutes, and `ss` is the second. There is no default for this parameter.
6. **end-time**—Enter the exact date and time (for your local time zone) when you want the Net-Net SBC to stop collecting records for this group; this time is either never or a time in the future. Your entry must be in the format `yyyy-mm-dd-hh:mm:ss`, where: `yyyy` is the year, `mm` is the month, `dd` is the day, `hh` in the hour, `mm` is the minutes, and `ss` is the second. There is no default for this parameter.

Push Receiver Settings

You can configure multiple servers to receive the records that the Net-Net SBC. Push receiver settings are accessible through the collection configuration. To provide added security, you can transfer the HDR record files using SFTP as well as FTP. Note that public key authentication is not available for this feature. Instead, the Net-Net SBC uses password authentication.

If you configure more than one server, then the Net-Net SBC sends data to all of the servers. If one server fails, the Net-Net SBC generates an SNMP trap. In terms of clearing data, this means that if there are four servers configure and the Net-Net SBC successfully pushes data to three of them, then it will clear the data.

To configure servers to act as push receivers for HDR data:

1. Access the collection group (**group-settings**) configuration by way of the collection configuration. Once

   ```
   ACMEPACKET(system-config)# collect
   ACMEPACKET(collect)# push-receiver
   ```

2. **address**—Enter the IP address of the push receiver (server) to which you want records sent. The default for this parameter is `0.0.0.0`.
3. **username**—Enter the username that the Net-Net SBC will use when it tries to send records to this push server using FTP. There is no default for this parameter.
4. **password**—Enter the password (corresponding to the username) that the Net-Net SBC will use when it tries to send records to this push server using FTP. There is no default for this parameter.

   Note: Passwords appear in clear text and are viewable by anyone loged into the Net-Net SBC.

5. **data-store**—Enter the directory on the push receiver where you want collected data placed. There is no default for this parameter.
6. **protocol**—Valid values for this parameter are **FTP** (default) and **SFTP**. You only need to set this parameter if you want to use SFTP to send HDR collection record files.

Controlling HDR from the Command Line

For added ease-of-use, you can stop and start record collection from the command line in Superuser Mode. You can stop and start record collection for the entire HDR process, or you can specify a group name for which you want to stop and start collection.

When you stop collection using this command, it will not restart it using this command.

To start record collection from the command line:

1. In Superuser mode, type the ACLI **start collection all** command. If you press <Enter> at this point, the Net-Net SBC will start all record collection. If you enter a specify a group-name instead of the **all** arguement and press <Enter>, collection for that record group only will be started.

   ```
   ACMEPACKET# start collection voltage
   ```

To stop record collection from the command line:

1. In Superuser mode, type the ACLI **stop collection all** command. If you press <Enter> at this point, the Net-Net SBC will stop all record collection. If you enter a specify a group-name instead of the **all** arguement and press <Enter>, collection for that record group only will be stopped.

   ```
   ACMEPACKET# stop collection voltage
   ```

To restart record collection from the command line:

1. In Superuser mode, type the ACLI **reset collection** command. If you press <Enter> at this point, the Net-Net SBC will restart all record collection.

   ```
   ACMEPACKET# reset collection
   ```

   Resetting a collection lets the current sample interval and push interval cycle complete, and then reads and uses the sample interval and push interval times from the collect configuration element.

To delete all collection data files resident on the Net-Net SBC:

1. In Superuser mode, type the ACLI **delete collection** command. If you press <Enter> at this point, the Net-Net SBC will delete all record collections.

   ```
   ACMEPACKET# delete collection
   ```

To display the status of collection groups and push servers:

1. In Superuser mode, type the ACLI **show collection** command to view groups currently collected, next push time and next push interval. Also, the configured collectors and their states are displayed. If you press <Enter> at this point, the Net-Net SBC will show record collection status.

   ```
   ACMEPACKET# show collection

   Collector is currently collecting on:
   Group           Boot-State   Start Time          End Time

   fan             disabled     now                 never


   Next Push Scheduled for: 2008-01-11-11:12:06
   Subsequent Push Interval: 15 minutes

   Registered push receivers are:
   ```

```
IP Address          Status

172.30.11.16        reachable
```

CPU Core Index Mapping

The following table lists CPU CoreID values seen in HDR and SNMP statistics.

CPU and Core value	Core ID
cpu 0 core 0	CoreID 0
cpu 0 core 1	CoreID 1
cpu 1 core 0	CoreID 256
cpu 1 core 1	CoreID 257
cpu 2 core 0	CoreID 512
cpu 2 core 1	CoreID 513
cpu 3 core 0	CoreID 768
cpu 3 core 1	CoreID 769
cpu 4 core 0	CoreID 1024
cpu 4 core 1	CoreID 1025

NTP Features

NTP is a fully RTC-enabled service on the Net-Net 9200.

NTP Application Debugging

The commands listed in this section are used to debug NTP-application level issues. They show operating status for the NTP daemons, one of which runs on each core of the Net-Net 9200.

show ntp status

The **show ntp status** command displays information about the synchronization and running status of the specified NTP daemon. If no argument is supplied, the command displays NTPD status for the master active core. This includes the state of the NTP daemon, and the server to which it's synced. For example:

```
ACMEPACKET# show ntp status

NTPD 0.0.0                                    TUE NOV  19:18:08  2007

NTPD NTPD active server is running.
NTP synchronized to server at: 172.30.0.25
```

If you include a core argument, the ACLI displays NTPD status on that core. A core is specified by <slot> <CPU> <core>, separated by spaces. For example:

```
ACMEPACKET# show ntp status 0 1 0

NTPD 0.1.0                                    TUE NOV  19:18:58  2007

NTPD NTPD client is running.
NTP synchronization in progress...
```

show ntp server

The **show ntp server** displays the state of each NTP core daemon you query. If you type this command without any arguments, the ACLI displays information about the master active core's NTP daemon. The ACLI displays the statistics listed in the following table for each NTP daemon.

Display Column	Definition
server	Lists the NTP servers configured on the Net-Net 9200 by IP address. Entries are accompanied by characters: • Plus sign (+)—Symmetric active server • Dash (-)—Symmetric passive server • Equal sign (=)—Remote server being polled in client mode • Caret (^)—Server is broadcasting to this address • Tilde (~)—Remote peer is sending broadcast to * • Asterisk (*)—The peer to which the server is synchronizing
st	Stratum level—Calculated from the number of computers in the NTP hierarchy to the time reference. The time reference has a fixed value of 0, and all subsequent computers in the hierarchy are n+1.
poll	Maximum interval between successive polling messages sent to the remote host, measured in seconds.
reach	Measurement of successful queries to this server; the value is an 8-bit shift register. A new server starts at 0, and its reach augments for every successful query by shifting one in from the right: 0, 1, 3, 7, 17, 37, 77, 177, 377. A value of 377 means that there have been eight successful queries.
delay	Amount of time a reply packet takes to return to the server (in milliseconds) in response.
offset	Time difference (in milliseconds) between the client's clock and the server's.
disp	Difference between two offset samples; error-bound estimate for measuring service quality.

For example:

```
ACMEPACKET# show ntp server

NTPD 0.0.0                                        TUE NOV  19:23:57  2007

NTPD NTPD active server is running.
  peer                st  poll   reach     delay       offset      disp
----------------------- --  ----  ------   --------   --------   -----
*172.30.0.25           2   512     37    0.015625   0.005153   0.046539
```

If you include a core argument, the ACLI displays NTPD status on that core. A core is specified by <slot> <CPU> <core>, separated by spaces. For example:

```
ACMEPACKET# show ntp server 0 1 1

NTPD 0.1.1                                        TUE NOV  19:24:08  2007

NTPD NTPD client is running.
  peer                st  poll   reach     delay       offset      disp
----------------------- --  ----  ------   --------   --------   -----
=169.254.176.0         3   512     37    0.015625   -0.016335    0.52643
```

NTP System Level Debugging

The following commands display NTP system statistics and counters. This information reflects how NTP daemons interact with each other and the system processes that support the Net-Net 9200's operation.

show task ntp

This command displays the statistics for each NTP daemon (NTPD) running on every core. For example:

```
ACMEPACKET# show task ntp
19:21:05-137 (ntpd@0.0.0) ID=e2560ec0
Task Status                ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Services                 17      17       0         18      18      18
Messages                  4       4      36        163      43       4
Alloc Buffers            50      50       0         52      52      52
Free Buffers              2       2       0          2       2       2
Transactions              0       0       0          0       0       0
Timed Objects            19      19       0         21      21      21
TOQ Entries               1       1     130        691      97       2
Operations                -       -     161        842     126
Messages Received         -       -      33        156      42
Messages Sent             -       -       2          7       3
Partial Message           -       -       0          0       0
Part Msg Expired          -       -       0          0       0
Part Msg Dropped          -       -       0          0       0
Timed Events              -       -     130        690      97
Alarms                    -       -       0          0       0
System Logs               -       -       0          0       0
Process Logs              -       -       4         87      72
Remote Logs               -       -       0          0       0
Load Rate                                0.0%      0.26    0.1%
```

You can also use the **show task ntp 2.0.1** syntax, for example, to query a specific core.

show amp ntpd

This command shows AMP statistics for the NTP daemon (NTPD) running on each core. For example:

```
ACMEPACKET# show amp ntpd
19:22:09-100 (ntpd@0.0.0) ID=e2560ec0
            -------- Received -------   ---------- Sent ---------
Protocol    Recent      Total  PerMax   Recent      Total  PerMax
            ------  ---------  ------   ------  ---------  ------
Total            2          7       3        1          7       3
MAN              0          0       0        0          1       1
CLIP             2          7       3        1          6       3
```

You can also use the **show amp ntpd x.0.x** syntax to query a specific core.

4 Network Management

Commands discussed in this chapter primarily concern OSI model layers 2-4 information on the Net-Net 9200.

Network Connections

The commands listed in this section are used to view physical interfaces and logical network connections as currently in use on the Net-Net 9200.

show interfaces

The **show interfaces** command is used to list all configured Ethernet interfaces, their IP settings, and ethernet statistics. Configured media interfaces are displayed by their phy-interface configuration element name followed by the hardware location in parenthesis). The following is an abbreviated display of this show command:

```
ACMEPACKET# show interfaces
eth (unit number 2, MIU1)
     Flags : UP
     Type: ETHERNET_CSMACD
     inet: 172.30.92.92
     Broadcast address: 172.30.255.255
     Netmask: 0xFFFF0000 Subnetmask: 0xFFFF0000
     Ethernet address is 00:08:25:02:65:b2
     Metric is 0
     Maximum Transfer Unit size is 1500
     47046434 octets received
     49199787 octets sent
     52427 unicast packets received
     977093 unicast packets sent
     205814 non-unicast packets received
     2 non-unicast packets sent
     0 incoming packets discarded
     0 outgoing packets discarded
     0 incoming errors
     0 outgoing errors
     0 unknown protos
     0 collisions; 0 dropped
private(media slot 0 port 0):
     Flags : UP
     Type: ETHERNET_CSMACD (COPPER)
     Admin State: enabled
     Auto Negotiation: enabled
     Duplex Mode: HALF
     Force Speed Selection: 100 Mbps
     inet: 192.168.0.77 vlan: 0
     Broadcast address: 192.168.255.255
     Netmask: 0xFFFF0000
     Gateway: 192.168.0.10
```

```
Ethernet address is 20:68:02:25:08:04
Virtual Ethernet address is 00:08:25:fe:1c:00
Metric is 0
Maximum Transfer Unit size is 1500
3552470 octets received
192 octets sent
54537 unicast packets received
3 unicast packets sent
54036 non-unicast packets received
3 non-unicast packets sent
1 incoming packets discarded
0 outgoing packets discarded
0 incoming errors
0 outgoing errors
0 unknown protos
0 collisions; 0 dropped
```

show ip connections

In order to quickly view all active network connections on the Net-Net 9200, the **show ip connections** command is used. This command first displays a list of the network connections on active cards. The command next lists all network connections on standby cards. For example:

```
ACMEPACKET# show ip connections
Internet Connections on Active (including servers)
Proto   Local Address           Foreign Address         (state)
-------------------------------------------------------------
TCP     172.30.92.96:23         10.0.200.204:1749
TCP     0.0.0.0:21              0.0.0.0:0               LISTEN
TCP     0.0.0.0:22              0.0.0.0:0               LISTEN
TCP     0.0.0.0:23              0.0.0.0:0               LISTEN
TCP     0.0.0.0:41              0.0.0.0:0               LISTEN
TCP     0.0.0.0:111             0.0.0.0:0               LISTEN
TCP     0.0.0.0:6666            0.0.0.0:0               LISTEN
TCP     172.30.92.96:8080       0.0.0.0:0               LISTEN
UDP     0.0.0.0:111             0.0.0.0:0
UDP     0.0.0.0:123             0.0.0.0:0
UDP     172.30.92.96:161        0.0.0.0:0
UDP     172.30.92.96:1125       0.0.0.0:0
UDP     172.30.92.96:1812       0.0.0.0:0
UDP     172.16.0.77:5060        0.0.0.0:0
UDP     192.168.0.77:5060       0.0.0.0:0

Internet Connections on Standby (including servers)
Proto   Local Address           Foreign Address         (state)
-------------------------------------------------------------
TCP     0.0.0.0:21              0.0.0.0:0               LISTEN
TCP     0.0.0.0:22              0.0.0.0:0               LISTEN
TCP     0.0.0.0:23              0.0.0.0:0               LISTEN
TCP     0.0.0.0:41              0.0.0.0:0               LISTEN
TCP     0.0.0.0:111             0.0.0.0:0               LISTEN
TCP     0.0.0.0:6666            0.0.0.0:0               LISTEN
UDP     0.0.0.0:111             0.0.0.0:0
UDP     0.0.0.0:123             0.0.0.0:0
UDP     172.30.92.94:161        0.0.0.0:0
```

```
UDP     172.30.92.94:1051       0.0.0.0:0
UDP     172.30.92.94:1812       0.0.0.0:0
```

show ip statistics

The **show ip statistics** command allows you to display a list of IP statistics including the number of ACL denials and the last IP address denied. For example:

```
ACMEPACKET# show ip statistics
system-acl statistics
         acl-denials          0
   last-srcip-denied         0.0.0.0
```

ARP Statistics

The commands listed in this section are used to view ARP table statistics and related information.

show arp commands

The **show arp** commands are used to display ARP tables, ARP table statistics for media interfaces, and management routes. The **show arp** command usage is as follows:

```
ACMEPACKET# show arp [statistics-all | statistics-by-interface | table-
all | table-by-interface | info] <slot> <port>
```

show arp statistics-by-interface

This **show** command displays the counts and statistics for a specified media interface's ARP table. Information displayed includes receive, transmit, and CAM statistics. This command is entered as:

```
ACMEPACKET# show arp statistics <slot> <port>
 <slot>: 0,1
 <port>: 0,1,2,3
```

For example:

```
Manifestoo# show arp statistics-by-interface 0 0

Interface: 0/0

-- Receive --
      Add intf:          1, Error:           0
   Delete intf:          0, Error:           0
    Flush intf:          0, Error:           0
    Arp enable:          0, Error:           0
   Arp disable:          0, Error:           0
   Add dynamic:          0, Error:           0
    Add static:          0, Error:           0
Delete dynamic:          0, Error:           0
 Delete static:          0, Error:           0
      Info Req:          0, Error:           0
          Pend:          0, Error:           0, Drop:          0
       Request:      57288, Update:          0, Drop:      57288
         Reply:          1, Update:          1, Drop:          0
       Network:      57289, Error:           0
                              ARP:           0
                           Subnet:           0
                             Intf:           0
```

```
                                IP:          0
                         Operation:          0

-- Transmit --
Request:          5, Error:          0
  Reply:          0, Error:          0
   Pend:          0, Error:          0
Network:          5, Error:          0
    Hip:          1, Error:          0
 Expire:          0, Error:          0
   Info:          0, Error:          0

-- CAM --
   Add error: 0
Delete error: 0
Update error: 0
Search error: 0
  Miss error: 0
Rate Control: 0
```

show arp statistics-all

This **show** command works similarly to the **show arp statistics-by-interface** command except that it does not take any arguments, and it displays statistics for all configured media interfaces.

```
ACMEPACKET# show arp statistics-all

ARPM STATUS: ACTIVE

Interface: ALL

-- Receive --
      Add intf:          2, Error:          0
   Delete intf:          0, Error:          0
    Flush intf:          0, Error:          0
    Arp enable:          0, Error:          0
   Arp disable:          0, Error:          0
   Add dynamic:          0, Error:          0
    Add static:          0, Error:          0
Delete dynamic:          0, Error:          0
 Delete static:          0, Error:          0
      Info Req:          1, Error:          0
          Pend:          0, Error:          0, Drop:          0
       Request:     114541, Update:          0, Drop:     114541
         Reply:          2, Update:          2, Drop:          0
       Network:     120033, Error:       5490
                              ARP:          0
                           Subnet:       5490
                             Intf:          0
                               IP:          0
                         Operation:          0

-- Transmit --
Request:         10, Error:          0
  Reply:          0, Error:          0
```

```
   Pend:          0, Error:          0
Network:         10, Error:          0
    Hip:          2, Error:          0
 Expire:          0, Error:          0
   Info:          0, Error:          0

-- CAM --
   Add error: 0
Delete error: 0
Update error: 0
Search error: 0
  Miss error: 0
Rate Control: 0
```

show arp table-all

This **show** command displays the complete arp table for management and media interfaces, including ARP table entry type, MAC address, IP address, interface (slot/port) and VLAN, time added to the table for each entry, and Secondary gateways. For example:

```
Manifestoo# show arp table-all

--- Management ARP Table ---

destination     gateway           flags  Refcnt  Use         Interface
-------------------------------------------------------------------
172.30.0.1      00:0f:23:4a:d8:80  33686533  2      0           eth2
172.30.0.25     00:11:2f:74:88:5f  33686533  1      852551      eth2
-------------------------------------------------------------------


--- Media and Signaling ARP Table ---

               Total ARP Entries = 6
               ----------------------
Intf  VLAN     IP-Address            MAC         time-stamp   type
active-count
 0/3   0  172.016.000.010    00:15:F2:4C:FC:F7  1193227957  dynamic
1
 0/0   0  192.168.000.010    00:0E:0C:9B:FE:B5  1193227957  dynamic
1


Special Entries:
 0/3    0   000.000.000.000     00:15:F2:4C:FC:F7  1193170829  gateway
 0/3    0   172.016.000.000     00:00:00:00:00:00  1193170829  network
 0/0    0   000.000.000.000     00:0E:0C:9B:FE:B5  1193170829  gateway
 0/0    0   192.168.000.000     00:00:00:00:00:00  1193170829  network


Gateway Status:
Intf  VLAN     IP-Address          MAC          time-stamp hb status
 0/3    0   172.016.000.010  00:15:F2:4C:FC:F7  1193227957    reachable
 0/0    0   192.168.000.010  00:0E:0C:9B:FE:B5  1193227957    reachable
```

```
Secondary Gateway Status:
Intf  VLAN     IP-Address          MAC          time-stamp hb status
```

show arp table-by-interface

By adding a slot and port argument to the **show arp table** command, the ACLI displays the arp table for a given media interface. This table lists ARP table entry type , MAC address, IP address, interface (slot/port) and VLAN, and time added to the table for each entry. This command is entered as:

```
ACMEPACKET# show arp table-by-interface <slot> <port>
 <slot>: 0,1
 <port>: 0,1,2,3
```

For example:

```
ACMEPACKET# show arp table 0 0

               Total ARP Entries = 9
               ----------------------
Intf  VLAN     IP-Address             MAC          time-stamp   type
 0/0    0   172.016.000.199     00:0B:82:08:1E:A9  1152879227  dynamic
 0/0    0   172.016.000.099     00:14:BF:B3:41:4E  1152878833  dynamic
 0/0    0   172.016.000.010     00:0E:0C:37:B4:7A  1152878941  dynamic


Special Entries:
 0/0    0   000.000.000.000     00:0E:0C:37:B4:7A  1152837989  gateway
 0/0    0   172.016.000.000     00:00:00:00:00:00  1152837989  network


Gateway Status:
Intf  VLAN     IP-Address          MAC          time-stamp hb status
 0/0    0   172.016.000.010  00:0E:0C:37:B4:7A  1152878941    reachable
```

show arp info

This **show** command displays the ARP table statistics. This command does not take a slot and port argument. For Example:

```
ACMEPACKET# show arp info
-- ARP table info --
Maximum number of entries  : 4096
Number of used entries     : 9
Length of search key       : 1 (x 64 bits)
First search entry address : 0x1f000
length of data entry       : 2 (x 64 bits)
First data entry address   : 0x3e000
Enable aging               : 0
Enable policing            : 0
```

show arp standby

This **show** command displays ARP table statistics for the task you identify that exists on the standby card. For example:

```
ACMEPACKET# show arp standby info
--------------------
Mar 24 19:59:59.594
Retrieving info from standby NPU [3.0.0]
```

```
-- ARP table info --
Maximum number of entries  : 4096
Number of used entries     : 4
Length of search key       : 1 (x 64 bits)
First search entry address : 0x1f000
length of data entry       : 2 (x 64 bits)
First data entry address   : 0x3e000
Enable aging               : 0
Enable policing            : 0
```

show arp

The **show arp** command only changes in the Management ARP section. For example:

```
Manny# show arp

--- Management ARP Table ---

  172.16.203.195 at 00:a0:a9:00:00:24 [hip1]
     172.30.0.27 at bc:ae:c5:60:12:4c [eth0]
   172.30.10.209 at 00:04:96:51:c1:40 [eth0]
    172.30.68.69 at 00:04:96:37:13:ca [eth0]
  182.16.203.188 at 00:1b:21:9f:07:a8 [hip2]


--- Media and Signaling ARP Table ---
--------------------
Dec  6 20:45:21.354
               Total ARP Entries = 3
               ----------------------
Intf VLAN     IP-Address        MAC            time-stamp  type   active-count
 0/3 0     182.16.203.188   00:1B:21:9F:07:A8  1323203352  dynamic    1
 0/1 101   172.16.203.195   00:A0:A9:00:00:24  1323203347  dynamic    1
 0/0 100   192.168.203.195  02:03:04:05:06:07  1323203308  dynamic    1
Gateway Status:
Intf VLAN     IP-Address        MAC            time-stamp  hb  a  status
 0/3 0     182.16.203.188   00:1B:21:9F:07:A8  1323203313      *  reachable
 0/1 101   172.16.203.195   00:A0:A9:00:00:24  1323203308      *  reachable
 0/0 100   192.168.203.195  02:03:04:05:06:07  1323203308      *  reachable
Secondary Gateway Status:
Intf VLAN     IP-Address        MAC            time-stamp  hb  a  status
 0/3 0     182.16.203.189   00:1B:21:9F:07:A9  1323203313      *  reachable
 0/1 101   172.16.203.196   00:A0:A9:00:00:25  1323203308      *  reachable
 0/0 100   192.168.203.196  02:03:04:05:06:08  1323203308      *  reachable
```

Manual ARP Table Changes

You can manually modify entries in the ARP table with the add, delete, and check commands. If your deployment does not use VLANs, set all VLAN arguments to 0.

check arp

The **check arp** command sends a test message to the indicated physical interface. The **check arp** command usage is as follows:

```
ACMEPACKET# check arp <slot> <port> <vlan> <ip>
```

```
 <slot>: 0,1
 <port>: 0,1,2,3
 <vlan>: 0,1,2, etc
 <ip>: IP address in the form x.x.x.x
```

For example:

```
ACMEPACKET# check arp 1 0 0 172.16.0.123
Invalid arp request
```

add arp

The **add arp** command adds an ARP entry to the ARP table. Since some network devices do not support ARP, static ARP entries sometimes need to be added to the ARP table manually. The add arp command usage is as follows:

```
ACMEPACKET# add arp <slot> <port> <vlan> <ip> <mac>
 <slot>: 0,1
 <port>: 0,1,2,3
 <vlan>: 0,1,2, etc
 <ip>: IP address in the form x.x.x.x
 <mac>: MAC address in the form x:x:x:x:x:x
```

For example:

```
ACMEPACKET# add arp 0 0 0 172.16.0.102 ab:cd:ef:01:23:45
```

delete arp

The **delete arp** command removes ARP entries from the ARP table. You only need to identify the IP address, VLAN tag, and slot and port pair to be removed. The delete arp command usage is as follows:

```
ACMEPACKET# delete arp <slot> <port> <vlan> <ip>
 <slot>: 0,1
 <port>: 0,1,2,3
 <vlan>: 0,1,2, etc
 <ip>: IP address in the form x.x.x.x
```

For example:

```
ACMEPACKET# delete arp 0 0 0 172.16.0.102
```

Other ARP Commands

You can reset the accumulated ARP statistics with the **reset arp statistics** command. For example:

```
ACMEPACKET# reset arp statistics
Clearing arp stats
```

ACL Statistics

The commands listed in this section are used to view ACL table statistics and related information.

Show ACL commands

The **show acl** commands are used to display ACL entries in the ACL table for media interfaces. The **show acl** command usage is as follows:

```
ACMEPACKET# show acl [all | denied | info | ip | summary | trusted |
untrusted]
```

show acl denied

The **show acl denied** command displays the list of denied ACL entries. Once an endpoint is added to the denied list, it appears in this show command's output. Information for each entry includes:

- Connecting media port, slot, and VLAN tag
- Source IP Address, bit mask, port, and port mask
- Destination IP address, bit mask, port, and port mask
- Protocol
- ACL entry as static or dynamic
- ACL entry index

For example:

```
ACMEPACKET# show acl denied
--------------------
Dec  6 20:31:16.991
DENIED entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask  prot type
index
Total number of DENIED entries = 0
DYNAMIC_DENIED entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask  prot type
index
0:/1:101  200.2.0.10:5060        0.0.0.0               udp  dynamic 17
0:/1:101  200.2.0.11:5060        0.0.0.0               udp  dynamic 18
0:/1:101  200.2.0.12:5060        0.0.0.0               udp  dynamic 19
Total number of DYNAMIC_DENIED entries = 3
```

show acl info

The **show acl info** command displays ACL table statistics. For each type of ACL entry, configured-trusted, configured-denied, untrusted, dynamic-trusted, dynamic-denied, and media, statistics are given for the number of active entries, % utilization of total entries, and max entries. In addition, errors due to exceeding ACL constraints are listed.

```
ACMEPACKET# show acl info
--------------------
Dec  6 20:35:15.243
Access Control List Statistics:
               | # of entries | % utilization | Max Entries
-------------------------------------------------------------------
Config Trusted  |          3            *            *
Config Denied   |          0            *            *
Untrusted       |          3            *            *
Dynamic Trusted |          8          0.002%      500000
Dynamic Denied  |          3          0.001%       64000
Media           |          0          0.000%      524288
-------------------------------------------------------------------
*  = Configured Trusted, Contigured Deny, and Untrusted are shared
Total Signaling space used = 6 of 16384 (99.963% free)
-------------------------------------------------------------------
Dynamic Trusted Entries not allocated due to ACL constraints:       0
Dynamic Denied Entries not allocated due to ACL constraints:        0
Media Entries not allocated due to ACL constraints:                 0
```

show acl ip

You can filter the output of **show acl** based on IP address. This command is useful if you want to check the ACL properties of a specific IP address. For example:

```
ACMEPACKET# show acl ip 200.3.0.1
--------------------
Dec  6 20:37:05.978
DENIED entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot type    index
Total number of DENIED entries = 0
DYNAMIC_DENIED entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot type    index
Total number of DYNAMIC_DENIED entries = 0
TRUSTED entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot type    index  recv    drop
Total number of TRUSTED entries = 3
DYNAMIC_TRUSTED entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot type    index
0/1:101   200.3.0.1               172.16.203.190:5060      udp  dynamic 7
Total number of DYNAMIC_TRUSTED entries = 8
UNTRUSTED entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot type    index
Total number of UNTRUSTED entries = 3
```

show acl summary

The **show acl summary** command summarizes global ACL action counts. For example:

```
ACMEPACKET# show acl summary
--------------------
Dec  6 20:38:16.880
                                Entries          Packets         Dropped
Total config deny entries:            0              n/a             n/a
Total dynamic deny enttries:          0              n/a             n/a
Total all deny entries:               0              n/a               0

Total media entries:                  0              n/a             n/a
Total untrusted entries:              3                0               0

Total config trusted entries:         3                0               0
Total dynamic trusted entries:        8                0               0
    by interface:
         0/0:                       n/a                0               0
         0/1:                       n/a                0               0
         0/3:                       n/a                0               0
Total all trusted entries            11                0               0
```

show acl trusted

The **show acl trusted** command displays the list of trusted and dynamic-trusted ACL entries. Once an endpoint is added to the trusted list, it appears in this show command's output. Information for each entry includes:

- Connecting media port, slot, and VLAN tag
- Source IP Address, bit mask, port, and port mask
- Destination IP address, bit mask, port, and port mask
- Protocol
- ACL entry as static or dynamic
- ACL entry index
- Packets received
- Packets dropped

For example:

```
ACMEPACKET# show acl trusted
--------------------
Dec  6 20:39:34.723
TRUSTED entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot type    index  recv
0/0:100   0.0.0.0                  192.168.203.190          icmp static  4      0
0/1:101   0.0.0.0                  172.16.203.190           icmp static  5      0
0/3:0     0.0.0.0                  182.16.203.199           icmp static  6      0
Total number of TRUSTED entries = 3
DYNAMIC_TRUSTED entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot type    index
0/1:101   200.3.0.1                172.16.203.190:5060      udp  dynamic 7
0/1:101   200.3.0.2                172.16.203.190:5060      udp  dynamic 8
0/1:101   200.1.0.1                172.16.203.190:5060      udp  dynamic 9
Total number of DYNAMIC_TRUSTED entries = 3
```

show acl untrusted

The **show acl untrusted** command displays the list of untrusted ACL entries. Once an endpoint is added to the untrusted list, it appears in this show command's output. Information for each entry includes:

- Connecting media port, slot, and VLAN tag
- Source IP Address, bit mask, port, and port mask
- Destination IP address, bit mask, port, and port mask
- Protocol
- ACL entry as static or dynamic
- ACL entry index

For example:

```
ACMEPACKET# show acl untrusted

untrusted entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot type    index
0/0:0     0.0.0.0                  192.168.0.77:5060        UDP  static  3
0/3:0     0.0.0.0                  172.16.0.77:5060         UDP  static  4

Total number of untrusted entries = 2
```

show acl all

The **show acl all** command displays the concatenation of all other **show acl** commands and a final summary.

NAT Statistics

The commands listed in this section are used to view NAT statistics for media interfaces.

Show NAT commands

The **show nat** commands are used to display the NAT table for the Net-Net system. You can query a NAT table entry by its address, NAT table index, or display a shortened tabular form of the NAT table. The **show nat** command usage is as follows:

```
show nat [by-addr | by-index | in-tabular | info | statistics]
```

show nat by-addr

The **show nat by-addr** command displays a tabular output of the NAT table for a given IP address. The IP address that you supply is used to match for the source IP, destination IP, translated source IP, or translated destination IP addresses. Information for each entry includes:

- NAT table index number
- Protocol of this NAT flow
- Slot / Port : Vlan ID on source side of the flow
- Source IP address and port
- Destination IP address and port

The show nat by-addr command usage is as follows:

```
ACMEPACKET# show nat by-addr <IP Address>
```

For example:

```
ACMEPACKET# show nat by-addr 172.16.0.123

Index Proto  Intf:Vlan      Src IP:Port              Dst IP:Port
-------------------------------------------------------------------
1     6      I=0/0:0        172.16.0.10:23           172.16.0.123:0
             O=1/0:0        192.168.0.123:23         192.168.0.10:0
2     6      I=1/0:0        192.168.0.0:0            192.168.0.123:23
             O=0/0:0        172.16.0.123:0           172.16.0.10:23
6     6      I=0/0:0        0.0.0.0:0                172.16.0.123:0
7     6      I=0/0:0        0.0.0.0:0                172.16.0.123:1
             O=0/0:0        0.0.0.0:0                172.16.0.123:1
8     17     I=0/0:0       0.0.0.0:0                172.16.0.123:5060
```

show nat by-index

The **show nat by-index** command displays full statistics for the NAT table entries specified in a supplied entry index range. If you do not specify a range, the system uses the default range of 1 through 200. The range you enter here corresponds to line

numbers in the table, and not to the number of the entry itself. Information for each entry includes:

Parameter	Description
SA_flow_key	Source IP address key used for matching in the look-up process.
DA_flow_key	Destination IP address key used for matching in the look-up process.
SP_flow_key	Source port used for matching in the look-up process.
DP_flow_key	Destination port used for matching in the look-up process.
VLAN_flow_key	If this is a non-zero value, then there is an associated VLAN. If this value is zero, then there is no associated VLAN.
SA_prefix	These values determine how many bits in the key are considered in the look-up process for a match, where SA is the source IPv4 address, DA is the destination IPv4 address, SP is the UDP source port, and DP is the UDP source port.
DA_prefix	
SP_prefix	
DP_prefix	
Protocol_flow_key	This value stands for the protocol used, where the following values and protocols correspond: • 1 = ICMP • 6 = TCP/IP • 17 = UDP
Ingress_flow_key	This value uniquely identifies from where the packet came, and it is a combination of the Ingress Slot and Ingress Port values.
Ingress Slot	Together with the Ingress Port, this value makes up the Ingress_flow_key.
Ingress Port	Together with the Ingress Slot, this value makes up the Ingress_flow_key.
XSA_data_entry	This is the translated (i.e., post-lookup) source IPv4 address value.
XDA_data_entry	This is the translated (i.e., post-lookup) destination IPv4 address value.
XSP_data_entry	This is the translated (i.e., post-lookup) source port value.
XDP_data_entry	This is the translated (i.e., post-lookup) destination port value.
Egress_data_entry	This value uniquely identifies the outbound interface for the packet, and it is a combination of the Egress Slot and Egress Port values. This is the functional equivalent to the Ingress_flow_key.
Egress Slot	Together with the Egress Port, this value makes up the Egress_data_entry.
Egress Port	Together with the Egress Slot, this value makes up the Egress_data_entry.
flow_action	This value displays the defined flow_action (i.e., flag) bits. The flow action bit mask includes the following bit options: • bit 1 - 1=MPLS strip • bit 2 - 1=Diffserv clear • bit 5 - 1=Latch source address • bit 6 - 1=Collapse flow • bit 7 - 1=Slow Path • bit 8 - 1=QoS Requirement • bit 9 - 1=RTCP, 0=RTP is bit 8 is set • bit 10 - 1=HIP • bit 11 - 1=TCU (transcoding) • bit 12 - 1 Diagnostics (testing only) • bit 13 - 1 NAT ALG packets

Parameter	Description
optional_data	This value specifies DSP device ID or session ID of transcoded traffic.
VLAN_data_entry	This value refers to the outbound VLAN look-up process. A non-zero value means that there is an associated VLAN, while a zero value means that there is no associated VLAN.
host_table_index	This value refers to the virtual index for the host management of CAM processing.
init_flow_guard	This timer is used to age the entries in the CAM.
inact_flow_guard	This timer is used to age the entries in the CAM.
max_flow_guard	This timer is used to age the entries in the CAM.

The show nat by-index command usage is as follows:

```
ACMEPACKET# show nat by-index <index range start> <index range finish>
```

For example:

```
ACMEPACKET# show nat by-index 1 63488
--------------------
Nov 23 15:38:45.665
------------------------------------------------------------
Total number of NAT entries = 6
------------------------------------------------------------
------------------------------------------------------------------------------
NAT host index 7, search table index 5,0:
Flow type: Unresolved non-latching flow
KEY: src info   : 0.0.0.0/0 : 0/0
KEY: dst info   : 192.168.201.34/32 : 0/0
KEY: ingres info: slot/port 0/0 (intf 0),  vlan 33,  proto icmp(1)

RES:  src result: sa 0.0.0.0 : 0
RES:  dst result: da 0.0.0.0 : 0
RES: egress info: slot/port 0/0 (intf 0), vlan 33

Table Index     : fg index             7    srch tbl id       5, 0
                : reverse id           0    intf id           0
Host Data       : flow_action     0x0400    op_data           0
DOS Data        : avrg-rate         8192    rtcp-lm           0
                : min-rs-rt            0
Flow Guard     : init       4294967295    inact    4294967295   max 4294967295
------------------------------------------------------------------------------
NAT host index 8, search table index 6,0:
Flow type: Unresolved non-latching flow
KEY: src info   : 0.0.0.0/0 : 0/0
KEY: dst info   : 172.16.10.34/32 : 0/0
KEY: ingres info: slot/port 0/1 (intf 2),  vlan 22,  proto icmp(1)

RES:  src result: sa 0.0.0.0 : 0
RES:  dst result: da 0.0.0.0 : 0
RES: egress info: slot/port 0/1 (intf 2), vlan 22

Table Index     : fg index             8    srch tbl id       6, 0
                : reverse id           0    intf id           0
Host Data       : flow_action     0x0400    op_data           0
DOS Data        : avrg-rate         8192    rtcp-lm           0
                : min-rs-rt            0
Flow Guard     : init       4294967295    inact    4294967295   max 4294967295
------------------------------------------------------------------------------
```

show nat in-tabular

The **show nat in-tabular** command displays a tabular output of the NAT table for a supplied entry index range. Information for each entry includes:

- NAT table index number
- Protocol of this NAT flow
- Slot / Port : Vlan ID on source side of the flow
- Source IP address and port
- Destination IP address and port

The show nat by-addr command usage is as follows:

```
ACMEPACKET# show nat in-tabular <index-start> <index-end>
```

For example:

```
ACMEPACKET# show nat in-tabular 1 5

Index Proto  Intf:Vlan      Src IP:Port              Dst IP:Port
-------------------------------------------------------------------
1     1      I=1/0:0        0.0.0.0:0                192.168.0.123:0
2     17     I=1/0:0       0.0.0.0:0               192.168.0.123:5060
3     17     I=0/0:0        0.0.0.0:0               172.16.0.123:5060
4     17     I=1/0:0        192.168.0.10:53          192.168.0.123:0
```

show nat info

The **show nat info** command lists summaries of the 3 main tables used for DOS/endpoint lookups. For example:

```
ACMEPACKET# show nat info
-----------------------------------------
------------  Media table info -----------
-----------------------------------------
Host Database:   size              : 524288
Host Database:   used entries      : 4
Host Database:   alloc failed      : 0
Media Hash:      used entries      : 4
Media Hash:      mem used          : 32768
Media Hash:      hsh mem free      : 49152
Media Hash:      sig mem free      : 156587264
Media Hash:      res mem free      : 156587264
-----------------------------------------
--------- Signaling Table Info -----------
-----------------------------------------
Host Database:   size              : 16384
Host Database:   used entries      : 4
Host Database:   alloc failed      : 0
Signaling Tree:  used entries      : 4
Signaling Tree:  mem used          : 262848
Signaling Tree:  hsh mem free      : 0
Signaling Tree:  sig mem free      : 0
Signaling Tree:  res mem free      : 0
-----------------------------------------
---------- Endpoint Table Info -----------
-----------------------------------------
Host Database:   size              : 589824
Host Database:   used entries      : 0
Host Database:   used trusted      : 0
Host Database:   used deny         : 0
Host Database:   max trusted       : 512000
```

```
Host Database:   max deny           : 65536
Host Database:   trusted alloc fail : 0
Host Database:   deny alloc fail    : 0
Endpoint Hash:   num entries        : 0
Endpoint Hash:   mem used           : 8388608
Endpoint Hash:   hsh mem free       : 49152
Endpoint Hash:   sig mem free       : 40177856
Endpoint Hash:   res mem free       : 40177856
```

show nat load

The **show nat load** command displays the CPU load of the natm task.

```
ACMEPACKET# show nat load
natm@2.0.0: NAT Load is 0.7; Limit is 80
```

The **show nat statistics** command displays NAT table transaction statistics. For example:

```
ACMEPACKET# show nat statistics
--------------------
Nov 23 15:38:46.223
NATM Status: ACTIVE
-- API Stats --
        Command   RX-Total      RX-OK   Rx-Error      TX-OK   TX-Error
         Nat Add         10         10          0         10          0
      Nat Delete          6          6          0          6          0
      Nat Update          0          0          0          0          0
   Nat Update-Add         0          0          0          0          0
Nat Update-Delete         0          0          0          0          0
       Nat Latch          2          2          0          2          0
   Flow Gd Notify         0          0          0          0          0
        Nat Info          0          0          0          0          0
       Nat Ready          0          0          0          0          0
       Stats Get          0          0          0          0          0
     Stats Clear          0          0          0          0          0
     Diag Enable          0          0          0          0          0
    Diag Disable          0          0          0          0          0
         Arp Add          0          0          0          0          0
      Arp Delete          0          0          0          0          0
-- CAM Stats --
Add errors          :   0
Delete errors       :   0
Update errors       :   0
Convert errors      :   0
Record errors       :   0
Duplicate errors    :   0
Number of  shuffles :   0
-- Flowguard Stats --
Add errors          :   0
Delete errors       :   0
Reserve errors      :   0
Invalid NAT IDs     :   0
Find CAM errors     :   0
```

show nat standby

The **show nat standby** command displays standby NAT statistics for the specified NAT task stored on the Net-Net SBC. For example:

```
ACMEPACKET# show nat standby info
--------------------
Mar 25 13:02:52.946
Retrieving info from standby NPU [3.0.0]

-- NAT table info --
Maximum number of entries  : 63488
Number of used entries     : 16
Length of search key       : 2 (x 64 bits)
First search entry address : 0x0
length of data entry       : 4 (x 64 bits)
First data entry address   : 0x0
Enable aging               : 1
Enable policing            : 0

-- TM info --
Flow ID list size     : 98303
Number of used flows  : 98
Number of free flows  : 98205
```

show nat statistics

The **show nat statistics** command displays NAT table transaction statistics. For example:

```
ACMEPACKET# show nat statistics

NATM Status: ACTIVE


-- API Stats --

        Command   RX-Total      RX-OK   Rx-Error      TX-OK   TX-Error
         Nat Add          3          3          0          3          0
      Nat Delete          0          0          0          0          0
      Nat Update          0          0          0          0          0
   Nat Update-Add         0          0          0          0          0
Nat Update-Delete         0          0          0          0          0
       Nat Latch          0          0          0          0          0
   Flow Gd Notify         0          0          0          0          0
        Nat Info          0          0          0          0          0
       Stats Get          0          0          0          0          0
     Stats Clear          0          0          0          0          0
     Diag Enable          0          0          0          0          0
    Diag Disable          0          0          0          0          0
         Arp Add          0          0          0          0          0
      Arp Delete          0          0          0          0          0

-- CAM Stats --
Add errors          :   0
Delete errors       :   0
Update errors       :   0
Convert errors      :   0
Record errors       :   0
Duplicate errors    :   0
Number of  shuffles :   0
```

```
-- Flowguard Stats --
Add errors          :   0
Delete errors       :   0
Reserve errors      :   0
Invalid NAT IDs     :   0
Find CAM errors     :   0
```

show nat table

The show nat table command displays the nat table sorted by the argument passed to it followed by the respective search term. This command is entered as:

```
show nat table [by denied | by trusted | by-src-port | by-src-addr |
by-media | bydest-port | by-dest-addr] <search term>
```

For example:

```
ACMEPACKET# show nat table by-denied
--------------------
Nov 23 15:38:46.326
Index   Prot   Intf:Vlan  Src IP:Port                  Dst IP:Port
-------------------------------------------------------------------------
ACMEPACKET# show nat table by-dest-addr 192.168.201.34
--------------------
Nov 23 15:38:46.376
Index   Prot   Intf:Vlan  Src IP:Port                  Dst IP:Port
-------------------------------------------------------------------------
7      icmp   I=0/0:33   0.0.0.0:0                    192.168.201.34:0
10     udp    I=0/0:33   0.0.0.0:0                  192.168.201.34:5060
14     udp    I=0/0:33   0.0.0.0:0                 192.168.201.34:10002
              O=0/1:22   172.16.10.34:10002          172.16.10.36:10000
ACMEPACKET# show nat table by-dest-port 5060
--------------------
Nov 23 15:38:46.429
Index   Prot   Intf:Vlan  Src IP:Port                  Dst IP:Port
-------------------------------------------------------------------------
9      udp    I=0/1:22   0.0.0.0:0                    172.16.10.34:5060
10     udp    I=0/0:33   0.0.0.0:0                  192.168.201.34:5060
ACMEPACKET# show nat table by-media
--------------------
Nov 23 15:38:46.478
Index   Prot   Intf:Vlan  Src IP:Port                  Dst IP:Port
-------------------------------------------------------------------------
13     udp    I=0/1:22   0.0.0.0:0                    172.16.10.34:10002
            O=0/0:33   192.168.201.34:10002        192.168.201.35:10000
14     udp    I=0/0:33   0.0.0.0:0                 192.168.201.34:10002
              O=0/1:22   172.16.10.34:10002          172.16.10.36:10000
ACMEPACKET# show nat table by-src-addr *
--------------------
Nov 23 15:38:46.530
Index   Prot   Intf:Vlan  Src IP:Port                  Dst IP:Port
-------------------------------------------------------------------------
7      icmp   I=0/0:33   0.0.0.0:0                    192.168.201.34:0
8      icmp   I=0/1:22   0.0.0.0:0                      172.16.10.34:0
9      udp    I=0/1:22   0.0.0.0:0                    172.16.10.34:5060
10     udp    I=0/0:33   0.0.0.0:0                  192.168.201.34:5060
13     udp    I=0/1:22   0.0.0.0:0                    172.16.10.34:10002
```

```
            O=0/0:33  192.168.201.34:10002       192.168.201.35:10000
14     udp   I=0/0:33  0.0.0.0:0                 192.168.201.34:10002
             O=0/1:22  172.16.10.34:10002          172.16.10.36:10000
ACMEPACKET# show nat table by-src-port *
--------------------
Nov 23 15:38:46.581
Index   Prot   Intf:Vlan  Src IP:Port                   Dst IP:Port
-------------------------------------------------------------------------
7       icmp   I=0/0:33   0.0.0.0:0                     192.168.201.34:0
8       icmp   I=0/1:22   0.0.0.0:0                      172.16.10.34:0
9       udp    I=0/1:22   0.0.0.0:0                    172.16.10.34:5060
10      udp    I=0/0:33   0.0.0.0:0                   192.168.201.34:5060
13      udp    I=0/1:22   0.0.0.0:0                    172.16.10.34:10002
            O=0/0:33  192.168.201.34:10002       192.168.201.35:10000
14     udp   I=0/0:33  0.0.0.0:0                 192.168.201.34:10002
             O=0/1:22  172.16.10.34:10002          172.16.10.36:10000
ACMEPACKET# show nat table by-trusted
--------------------
Nov 23 15:38:46.633
Index   Prot   Intf:Vlan  Src IP:Port                   Dst IP:Port
-------------------------------------------------------------------------
7       icmp   I=0/0:33   0.0.0.0:0                     192.168.201.34:0
8       icmp   I=0/1:22   0.0.0.0:0                      172.16.10.34:0
ACMEPACKET# show nat table by-untrusted
--------------------
Nov 23 15:38:46.683
Index   Prot   Intf:Vlan  Src IP:Port                   Dst IP:Port
-------------------------------------------------------------------------
9       udp    I=0/1:22   0.0.0.0:0                    172.16.10.34:5060
10      udp    I=0/0:33   0.0.0.0:0                   192.168.201.34:5060
ACMEPACKET# show nat table tabular
--------------------
Nov 23 15:38:46.734
Index   Prot   Intf:Vlan  Src IP:Port                   Dst IP:Port
-------------------------------------------------------------------------
7       icmp   I=0/0:33   0.0.0.0:0                     192.168.201.34:0
8       icmp   I=0/1:22   0.0.0.0:0                      172.16.10.34:0
9       udp    I=0/1:22   0.0.0.0:0                    172.16.10.34:5060
10      udp    I=0/0:33   0.0.0.0:0                   192.168.201.34:5060
13      udp    I=0/1:22   0.0.0.0:0                    172.16.10.34:10002
            O=0/0:33  192.168.201.34:10002       192.168.201.35:10000
14     udp   I=0/0:33  0.0.0.0:0                 192.168.201.34:10002
             O=0/1:22  172.16.10.34:10002          172.16.10.36:10000
```

show nat host

The **show nat host** command displays counts related to the types of flows sent to the system Host.

```
ACMEPACKET# show nat host
--------------------
Nov 23 15:38:45.970
15:38:45-109
Host Path Statistics                    ---- Lifetime ----
                                Recent      Total  PerMax
Received                          2986      52585    3263
```

```
  Signaling                          5         23      11
    Dropped                          0          0       0
    Not Dropped                      0          0       0
  HIP Packets                        0          0       0
  ARP Net                         2117      35095    2040
  ARP Pending                        0          0       0
  NP Latch                           0          0       0
  IP Fragments                       0          0       0
  Diagnostic                         0          0       0
  NAT ALG                            0          0       0
  IPSEC Packets                      0       1407     819
  ICMPV6 Packets                     0          0       0
Sent                               192       4234    1016
```

Other NAT Commands

You can reset the accumulated NAT statistics with the **reset nat statistics** command. For example:

```
ACMEPACKET# reset nat statistics
```

Media Interface Statistics

This commands listed in this section are used to view statistics about the media interface hardware.

Show media commands

The **show media** command displays information about the Net-Net system's media interfaces. This **show media** command usage is as follows:

```
ACMEPACKET# show media [classify | frame-statistics | gmac-statistics
| host-statistics | network | phy-statistics] [<slot> <port>]
```

show media classify

The **show media classify** command displays network processor statistics for a specified media interface.

The **show media classify** command usage is as follows:

```
ACMEPACKET# show media classify <slot> <port>
```

For example:

```
ACMEPACKET# show media classify 0 0
--------------------
Aug 14 13:10:09.914
Classifier Packets Dropped             :       0
IPv4 DIX Packets Received              :       902
IPv4 DIX-VLAN Packets Received         :       0
IPv4 Fragment Packets Received         :       0
IPv4 Error Packets Received            :       0
ARP Packets Received                   :       74
IPv4 Latch Events                      :       2
IPv6 DIX Packets Received              :       0
IPv6 DIX-VLAN Packets Received         :       0
IPv6 Error Packets Received            :       0
```

```
IPv6 Latch Events                       :       0
IPv6 Fragment Packets Received          :       0
IPv6 ICMP Packets Received              :       0
IPv6 Other ExtHdr Packets Received      :       0
TOP-PARSE Packets Dropped               :       0
TOP-RESOLVE Packets Dropped             :       516
TOP-MODIFY Packets Dropped              :       0
TOP Media Hash Misses                   :       0
TOP L2R Hash Misses                     :       0
TOP NETIF Hash Misses                   :       0
TOP Latch Misses                        :       0
Untrusted Packet Dropped                :       0
Trusted Packet Dropped                  :       0
Deny Packet Dropped                     :       0
Media Policed Packets Dropped           :       0
IPv4 to IPv4 NAT Packet Count           :       375
IPv4 to IPv6 NAT Packet Count           :       0
IPv6 to IPv4 NAT Packet Count           :       0
IPv6 to IPv6 NAT Packet Count           :       0
IPv4 to IPv6 UDP Checksum Gen Count     :       0
SPI-A Transmit Packet Count             :       412978
SPI-B Transmit Packet Count             :       2063102
Host  Transmit Packet Count             :       0
Standby Error Receive Packet Count      :       0
TCU-A Transmit Packet Count             :       0
TCU-B Transmit Packet Count             :       0
Cavium Transmit Packet Count            :       375
EZ Loopback Receive Packet Count        :       0
EZ Interrupt Receive Packet Count       :       0
EZ Host CPU Receive Packet Count        :       0
EZ TCU-A Receive Packet Count           :       0
EZ TCU-B Receive Packet Count           :       0
EZ Cavium Receive Packet Count          :       0
EZ Pre-NAT Packet-Trace Count           :       0
EZ Post-NAT Packet-Trace Count          :       0
EZ IPSec Control Packet Count           :       0
EZ Transmit Drain Drop Count            :       0
Last L2R Miss Key:     0x0000 0x0000 0x0000 0x0000 0x0000 0x0000 0x0000
0x0000
0x0000 0x0000
```

show media frame-statistics

The **show media frame-stats** command displays staistics about the traffic manager's CPU port. No arguments are used with this command.

For example:

```
ACMEPACKET# show media frame-statistics
  FRAME Total RX 5700    = 4
  FRAME Total RX END-L2  = 0
  FRAME Total RX END-L3  = 0

  FRAME Total TX END     = 0
  FRAME Total TX 5700    = 2
```

```
FRAME_RX_APP_Q_WRITE_ERR    = 0
FRAME_RX_APP_Q_READ_ERR     = 0
FRAME_RX_APP_ERR            = 0
FRAME_RX_APP_NPM            = 4

FRAME_RX_5700DFT_INIT_COUNT = 0
FRAME_RX_MBLK_ERR           = 0
FRAME_RX_CRC_ERR_COUNT      = 0
FRAME_RX_BAD_LEN_ERR_COUNT  = 0
FRAME_RX_IDMA5700_HCOUNT    = 0
FRAME_RX_5700DFT_STATUS_ERR = 0
FRAME_RX_END_STANDBY_ERR    = 0
FRAME_RX_ALG_PATH_ERR       = 0
FRAME_RX_TASK_ERR           = 0

FRAME_TX_APP_Q_WRITE_ERR    = 0
FRAME_TX_APP_Q_READ_ERR     = 0
FRAME_TX_TASK_ERR           = 0
FRAME_TX_5700DFT_STATUS_ERR = 0
FRAME_TX_5700DFT_INIT_ERR   = 0
FRAME_TX_5700SPD_TIME_ERR   = 0
FRAME_TX_5700_SEND_ERR      = 0

FRAME_TX_5700_PDU_DROPPED_ERR      = 0

FRAME_TX_5700_NO_LAST_PDU_ERR      = 0

FRAME_RX_ENDL2_NONAME_ERR = 0
FRAME_RX_ENDL3_NONAME_ERR = 0
FRAME_RX_END_NOMBLK_ERR   = 0

FRAME_TX_END_NOMBLK_ERR = 0
FRAME_TX_END_NOCLBUF_ERR= 0
FRAME_TX_END_STANDBY_ERR= 0
FRAME_TX_END_SEND_ERR   = 0
```

show media gmac-statistics

The **show media gmac-statistics** command displays GMAC statistics for a supplied GMAC device and interface.

The **show media gmac-statistics** command usage is as follows:

```
ACMEPACKET# show media gmac-statistics <GMAC Slot#> <GMAC Port#>
```

For Example:

```
ACMEPACKET# show media gmac-statistics 0 0
            Device 0 Port 0 IXF1104 Ethernet Statistics

                                    Tx Stats                 Rx Stats
                                    --------                 --------
Octets OK                         1428825567               1369464813
Octets BAD                              0                        0
Ucast Pkts                        3004034                  3003886
Mcast Pkts                              0                        0
Bcast Pkts                              0                     5652
Pkts 64 Octets                          0                      907
```

```
Pkts 65-127 Octets                    907                    4064
Pkts 128-255 Octets                     0                    1016
Pkts 256-511 Octets               2000161                 2003551
Pkts 512-1023 Octets              1002966                 1000000
Pkts 1024-1518 Octets                   0                       0
Pkts 1519-Max Octets                    0                       0
Tx Deferred                       0  Rx FCS Errors                0
Tx Ex.Len Drop                    0  Rx Tagged                    0
Tx Underrun                       0  Rx Data Errors               0
Tx Tagged                   3004034  Rx Align Errors              0
Tx CRC Errors                     0  Rx Long Errors               0
Tx Pause Frames                   0  Rx Jabber Errors             0
Tx Flow Ctrl Frms                 0  Rx Unkn MAC Ctrl             0
Rx Very Long Errs                 0  Rx Runt Errors               0
Rx Short Errors                   0  Rx Carrier Ext               0
Rx Sequence Errs                  0  Rx Symbol Errors             0
Tx FIFO Err Rmvd                  0  Rx FIFO Err Rmvd             0
Tx FIFO Ovr Rmvd                  0  Rx FIFO Ovr Rmvd             0
```

show media host-statistics

The **show media host-statistics** command displays statistics about traffic received on media interfaces destined for the system host. The **show media host-statistics** command usage is as follows:

```
ACMEPACKET# show media host-statistics <slot> <port>
 <slot>: 0,1
 <port>: 0,1,2,3
```

For Example:

```
ACMEPACKET# show media host-statistics 0 0
--------------------
Aug 14 13:11:05.974
Host Receive Packet Stats for Slot: 0 and Port: 0
Latch Flow Packets:      2
Packet Capture Packets:  0
SFE Packets:             11
IPv4 Fragments:          0
IPv6 Fragments:          0
Arp Packets:             74
    Arp Pkts Sent To SP Skt: 74
IcmpV6 Packets:          0
IP Stack Packets:        0
Phy stats Packets:       0
Diag Packets:            0
Nat Alg Packets:         0
IPsec Packets:           0
Total END Packets:       1650802
Total END Error Packets: 0
Total SFE Error Packets: 0
Total Frag Error Packets:0
Total Frag6 Error Packets:0
Total Arp Error Packets: 0
Total ICMPv6 Error Pkts: 0
Invalid Acme Hdr:        0
Invalid Port:            0
```

```
Invalid Forward Code:    0
Invalid Pkt Size(small): 0
Invalid Pkt Size(large): 0
Hostbound Pkt Drops    : 0
Host Transmit Packet Stats for Slot: 0 Port: 0
Layer 2 Packets:         108
Layer 3 Packets:         12
Pend Packets:            1
IPsec Packets:           0
TM Packets:              0
RFC2833 packets:         3
Failed Packets:          0
Failed Mblk:             0
Traced packets:          0
```

show media network

The **show media network** command displays network configuration details for all configured media interfaces (NIUs). Information for each entry includes:

- NIU interface slot / port
- VLAN ID
- IP Address configured for that slot / port / VLAN ID
- Netmask
- Configured gateway
- Secondary gateway
- Status

For example:

```
ACMEPACKET# show media network

Intf  Vlan   IP Address      Netmask         Gateway         Sec-Gateway     St
0/0   0      192.168.0.77    255.255.0.0     192.168.0.10    0.0.0.0         er
0/3   0      172.16.0.77     255.255.0.0     172.16.0.10     0.0.0.0         er
```

show media phy-statistics

The **show media phy-statistics** command displays staistics about the phy side of the dx240. This command outputs the same data as the show npu phy-stats command. This command takes a media slot and port argument.

For example:

```
ACMEPACKET# show media phy-statistics 1 0
NPU 240 PHY-side Slot 0 Port 0 Counters:
 goodOctetsSent                192 goodOctetsRcv             3691904
 goodPktsSent                    3 goodPktsRcv                 56682
 brdcPktsSent                    3 brdcPktsRcv                 56166
 mcPktsSent                      0 mcPktsRcv                       0
 badPktsRcv                      1 pkts64Octets                56014
 pkts65to127Octets             410 pkts128to255Octets            258
 pkts256to511Octets              0 pkts512to1023Octets              0
 pkts1024tomaxOoctets            0 badOctetsRcv                     0
 macTransmitErr                  0 excessiveCollisions              0
```

```
unrecogMacCntrRcv                0 fcSent                         0
goodFcRcv                        0 dropEvents                     0
undersizePkts                    0 fragmentsPkts                  1
oversizePkts                     0 jabberPkts                     0
macRcvError                      0 badCrc                         0
collisions                       0 lateCollisions                 0
badFcRcv                           0
```

When an NPU3 is installedin the system.

```
ACMESYSTEM# show media phy-statistics 0 0
--------------------
Dec 22 15:59:31.351
NPU Switch PHY-side Slot 0 Port 0 Counters:
Npu3 FPGA MAC Stats dump:
MAC Rx Stats
========
Rx Bytes           :0x00000000
Rx 64B Fr Ok       :0x00000000
Rx 65-127B Fr Ok   :0x00000000
Rx 128-255B Fr Ok  :0x00000000
Rx 256-511B Fr Ok  :0x00000000
Rx 512-1023B Fr Ok :0x00000000
Rx 1024-Max Fr Ok  :0x00000000
Rx Fr ChkSeq Err   :0x00000000
Rx Broadcast Fr Ok :0x00000000
Rx Multicast Fr Ok :0x00000000
Rx Vlan Tag Fr Ok  :0x00000000
Rx Pause Fr Ok     :0x00000000
Rx Bad Frame       :0x00000000
Rx Length Error    :0x00000000
Rx Good Frame      :0x00000000
MAC Tx Stats
========
Tx Bytes           :0x00000000
Tx 64B Fr Ok       :0x00000000
Tx 65-127B Fr Ok   :0x00000000
Tx 128-255B Fr Ok  :0x00000000
Tx 256-511B Fr Ok  :0x00000000
Tx 512-1023B Fr Ok :0x00000000
Tx 1024-Max Fr Ok  :0x00000000
Tx Broadcast Fr Ok :0x00000000
Tx Multic Fr Ok    :0x00000000
Tx Underrun Err    :0x00000000
Tx Vlan Tag Fr Ok  :0x00000000
Tx Pause Fr Ok     :0x00000000
Tx Good Frame      :0x00000000
```

Other Media Commands

You can reset the accumulated media card hardware statistics with the **reset media** commands.

The **reset media** command usage is as follows:

```
ACMEPACKET# reset media [gmac-statistics | host-statistics]
```

HIP Statistics

The commands listed in this section are used to view information about the host-in-path (HIP) traffic statistics. HIP functionality lets you direct a specific class of traffic through a media interface to the host application.

show hip commands

The **show hip** command displays information about the Net-Net system's HIP statistics. The **show hip** command usage is as follows:

```
ACMEPACKET# show hip [interfaces | statistics-all | statistics-by-
interface <slot> <port>]
```

show hip interfaces

The **show hip interfaces** command lists the physical interface and network interface where a HIP entry is configured on the Net-Net 9200. For example:

```
ACMEPACKET# show hip interfaces

HIP (unit number 1)
        Hip Intf     1
        Media Slot   0
        Media Port   3
        Media Intf   6
        Sub Port     0
        IP Address   172.16.0.77
        Netmask      255.255.0.0
        MAC Address  00:08:25:fe:1c:03
```

show hip statistics-all

The **show hip statistics-all** command displays receive and transmit statistics for all services that reach the host, from all media interfaces. In addition, overall HIP statistics are displayed on the the screen.

For example:

```
ACMEPACKET# show hip statistics-all

Intfs cfg:       0
Intfs added:     0
Intfs add fails: 0
Intfs deleted:   0
Invalid rtp fd:  FALSE
Invalid kern fd: FALSE

Interface: ALL

          Rx Stats    Tx Stats
 Total:          0           0
   ARP:          0           0
    IP:          0           0
   UDP:          0           0
  ICMP:          0           0
   TCP:          0           0
   FTP:          0           0
TELNET:          0           0
  SNMP:          0           0
```

show hip statistics-by-interface

The **show hip** command with supplied slot and port arguments displays receive and transmit statistics for each service you can allow to reach the host on the specified interface.

The **show hip** command usage is as follows:

```
ACMEPACKET# show hip statistics-by-interface <slot> <port>
```

For Example:

```
ACMEPACKET# show hip statistics-by-interface 0 1

Interface: 0/1

          Rx Stats    Tx Stats
 Total:          0           0
   ARP:          0           0
    IP:          0           0
   UDP:          0           0
  ICMP:          0           0
   TCP:          0           0
   FTP:          0           0
TELNET:          0           0
  SNMP:          0           0
```

Other HIP Commands

You can reset the accumulated HIP statistics with the **reset hip statistics** command. For example:

```
ACMEPACKET# reset hip statistics
Clearing hip stats
```

Route Statistics

This commands listed in this section are used to learn about host routes configured in the routing table, and their statistics.

show routes

The **show routes** command displays the current system routing table. Information includes the destination, gateway to use, flags, RefCnt, Use, protocol, ToS bit, and respective physical interface for that destination. For example:

```
ACMEPACKET# show routes

Destination/Pfx    Gateway         Flags    RefCnt Use     Proto Tos I/f

0.0.0.0/0          172.30.0.1      2010003  1      0          1   0 eth2
10.0.200.204       172.30.0.1      2020007  1      868        2   0 eth2
127.0.0.1          127.0.0.1       2200005  0      0          2   0 lo0
169.254.0.0/16     169.254.33.0    2000101  2      0          2   0 eth1
169.254.64.0/18    169.254.97.0    2000101  1      0          2   0 eth0
169.254.128.0/18   169.254.161.0   2000101  0      0          2   0 v_eth0
169.254.128.0/18   169.254.176.0   101      0      0          2   0 v_eth0
172.16.0.0/16      172.16.0.77     2000101  0      0          2   0 hip1
172.30.0.0/16      172.30.92.92    2000101  3      0          2   0 eth2
172.30.92.96       172.30.92.96    2000103  0      0          2   0 ve_eth2
192.168.0.0/16     192.168.0.77    2000101  0      0          2   0 hip0
```

show route-stats

The **show route-stats** command shows routing statistics including bad routing redirects, dynamically created routes, new gateway due to redirects, destinations found unreachable, and use of a wildcard route. For example:

```
ACMEPACKET# show route-stats

routing:
        0 bad routing redirect
        0 dynamically created route
        0 new gateway due to redirects
        4294952170 destination found unreachable
        0 use of a wildcard route
```

Pinging an IP Address

This section explains how to determine the existence of an IP address, whether it is up and accepting requests. The ACLI lets you ping external interfaces from the management ethernet ports. The output of the **ping** command includes:

- Time in milliseconds it took the ICMP packets to reach the destination and return
- Statistics that indicate the number of packets transmitted, the number of packets received, and the percentage of packet loss.
- Time in milliseconds for the minimum, average, and maximum RTTs. The default timeout is 64 milliseconds.

For example:

```
ACMEPACKET# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1): 56 data bytes
64 bytes from 10.0.0.1: icmp_seq=0 ttl=255 time=1.9 ms
64 bytes from 10.0.0.1: icmp_seq=1 ttl=255 time=1.8 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=255 time=1.9 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=255 time=1.8 ms

--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.8/1.8/1.9 ms
```

Specifying a Source Address for ICMP Pings

The Net-Net 9200 supports sending ICMP Pings out of a user-specified network-interface and VLAN by using optional arguments with the ping command. If a source network interface and IP address are not specified, the Net-Net 9200 will send the ping out of its active MIU's Ethernet port.

The ping command is entered as follows:

```
ping <host-address> [<network-interface-name:vlan>] <source-address>
```

For Example:

```
ACMEPACKET# ping 192.168.0.96 private:0 192.168.0.80
```

Configuring a Network Interface for pinging

Before sending pings from a Net-Net 9200 network interface, you must enable the **icmp** parameter on the network interface you plan to ping from. In addition, you must add the source-address you plan to ping from to the network-interface's **hip-ip-list** parameter.

To configure a network interface for pinging network hosts:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **system** and press <Enter> to access the system-level configuration elements.

   ```
   configure# system
   ```

3. Type **network-interface** and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

   ```
   system# network-interface
   network-interface#
   ```

4. **icmp**—Set this parameter to enabled to support ICMP traffic.
5. **hip-ip-list**—Enter one or more IP addresses you wish to ping from. You must type **add** immediately before the IP addresses you are configuring in the HIP list.
6. Save and activate the configuration.

DNS and ENUM Management

DNS Statistics

The Net-Net 9200 includes several commands used to debug, validate, and monitor DNS transactions and the status of the DNS configuration.

show dns cache

The **show DNS cache** command displays contents of DNS cache. This command can take a realm name to indicate the realm where to perform the query, a type to indicate the DNS query type (A, SRV or NAPTR), and a DNS name to query upon. The **show DNS cache** command can be entered as follows:

```
show dns cache all
show dns cache <realm> all
show dns cache <realm> <type> <name>
```

show dns lookup

The **show DNS lookup** command display results of DNS lookup for a number within the DNS cache. This command can take a realm name to indicate the realm where to perform the query, a type to indicate the DNS query type (A, SRV or NAPTR), and a DNS name to query upon. The **show DNS lookup** command can be entered as follows:

```
show dns lookup <realm> <type> <name>
```

show dns query

The **show DNS query** command performs an DNS lookup directly to the DNS server, without looking in the local cache. This command can take a realm name to indicate the realm where to perform the query, a type to indicate the DNS query type (A, SRV or NAPTR), and a DNS name to query upon. The **show DNS query** command can be entered as follows:

```
show dns query <realm> <type> <name>
```

show dns realm

The **show DNS realm** command display a DNS statistics for a supplied realm. The **show DNS server** command is entered as follows:

```
show dns realm <realm>
```

show dns server

The **show DNS server** command displays information about the local DNS resolution server. The **show DNS server** command is entered as follows:

```
show dns server
```

show dns sip

The **show DNS sip** command displays information about the Net-Net 9200's SIP applications' interactions with the DNS application. The **show dns SIP** command is entered as follows:

```
show dns sip
```

show dns sockets

The **show DNS sockets** command displays information about the system's DNS sockets. The **show dns sockets** command is entered as follows:

```
show dns sockets
```

clear dns

The **clear DNS** command is used to remove one or more entries from the DNS cache. Supplying only a realm argument clears the cache for that realm, while supplying type and name arguments clear that name from the cache. Use the **all** argument to remove all entries. The **clear DNS** command is entered as follows:

```
clear dns all
clear dns <realm> all
clear dns <realm> <type> <name>
```

ENUM Statistics

The Net-Net 9200 includes several commands used to debug, validate, and monitor ENUM transactions and the status of the ENUM configuration.

show enum cache

The **show enum cache** command displays contents of ENUM cache. This command can take an enum-server argument and a phone number argument. The enum-server argument is used to choose the cache statistics for the given ENUM server. The phone number argument is used to display cache statistics for that phone number on the entered enum server. The **show enum cache** command can be entered as follows:

```
show enum cache all
show enum cache <enum-server> all
show enum cache <enum-server> <number>
```

show enum lookup

The **show enum lookup** command display results of ENUM lookup for a number within the cache. This command can take an enum-server argument and a phone number argument. The enum-server argument is used to choose the lookup statistics for the given ENUM server. The phone number argument is used to display lookup statistics for that phone number on the entered enum server. The **show enum lookup** command is entered as follows:

```
show enum lookup <enum-server> <number>
```

show enum query

The **show enum query** command performs an ENUM lookup directly to the ENUM server. This command takes an enum-server argument and a phone number argument. The enum-server argument determines the server to query, and the phone number argument is the actual queried number. The **show enum query** command is entered as follows:

```
show enum query <enum-server> <number>
```

show enum server

The **show enum server** command display a specific ENUM server's statistics. The **show enum server** command is entered as follows:

```
show enum server <enum-server>
```

clear enum

The **clear enum** command is used to remove one or more entries from the ENUM cache. Supplying only an enum-server argument clears the cache for that server, while supplying a number argument clears that number from the cache. Use the all argument to remove all entries. The **clear enum** command is entered as follows:

```
clear enum all
clear enum <enum-server> all
clear enum <enum-server> <number>
```

Clearing ENUM and DNS Statistics

To clear statistics for ENUM and DNS, you can use additions to the ACLI **reset** command. Before you reset the counters, however, you might want to confirm the current statistics on the system are not zero. You can do so using the show command—by typing, for example, **show enum stats**.

The **reset** command takes the ENUM and DNS arguments to clear those sets of statistics. When you use the command, the system notifies you whether it has successfully cleared the statistics (even if the counter are zero) or if it has run into an error causing the command to fail.

ACLI Instructions and Examples

This section shows you how to clear ENUM and DNS statistics. The ENUM example confirms successful completion of the command; the second shows the error message that appears if the command fails.

To clear ENUM statistics:

1. At the command line, type **reset enum** and then press <Enter>.

```
ACMEPACKET# reset enum
Successful reset of the ENUM Agent stats
```

To clear DNS statistics:

1. At the command line, type **reset dns** and then press <Enter>.

```
ACMEPACKET# reset dns
SIP DNS statistics not available
```

DNS Server Status

The Net-Net SBC monitors the status of all configured DNS servers used by a SIP daemon. If a DNS server goes down, a major alarm is sent. If all DNS servers used by a SIP daemon are down, a critical alarm is sent. The **apAppsDnsServerStatusChangeTrap** is sent for both events.

Once the **apAppsDnsServerStatusChangeTrap** has been sent, a 30 second window elapses until the server status is checked again. At the 30 second timer expiration, if the server is still down, another trap and alarm are sent. If the server has been restored to service, the **apAppsDnsServerStatusChangeClearTrap** is sent.

SNMP

The **apAppsDNSServerStatusTable** contains the following objects:

Object Identifier Name: apAppsDnsServerStatusTable (.1.3.6.1.4.1.9148.3.16.1.2.2.1)		
Object Identifier Name: apAppsDnsServerStatusEntry (.1.3.6.1.4.1.9148.3.16.1.2.2.1.1)		
apAppsDnsInterfaceName	apAppsDnsServerStatusEntry: 1.3.6.1.4.1.9148.3.16.1.2.2.1.1.1	The name of the DNS interface that contains this DNS server.
apAppsDnsServerInetAddressType	apAppsDnsServerStatusEntry: 1.3.6.1.4.1.9148.3.16.1.2.2.1.1.2	The Inet address type of this DNS server.
apAppsDnsServerInetAddress	apAppsDnsServerStatusEntry: 1.3.6.1.4.1.9148.3.16.1.2.2.1.1.3	The IP address of this DNS server.
apAppsDnsServerStatus	apAppsDnsServerStatusEntry: 1.3.6.1.4.1.9148.3.16.1.2.2.1.1.4	The status of this DNS server.

Trap

A trap is sent in the event that a server becomes unreachable, and a clear trap is sent once service is restored to all OOS servers.:

Trap Name	Description
apAppsDnsServerStatusChangeTrap: 1.3.6.1.4.1.9148.3.14.2.2.0.1	This trap is generated if the reachability status of a DNS-ALG server changes from In-Service to either Timed out or Out of Service.

Alarm

The following alarm is generated in the event that one or more DNS servers go down:

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
APP_ALARM_LOST_DNS_CONN	0x50050049	CRITICAL: all DNS servers configured for a SIP daemon are down. MAJOR:One or more DNS servers configured for a SIP daemon are down.	DNS server configured for a SIP daemon is down.	One or more DNS Servers are currently unreachable!	apAppsDnsServerStatusChangeTrap

Packet Trace

The packet trace feature lets the Net-Net SBC mirror any communication between two endpoints running through the Net-Net SBC, or between itself and a specific endpoint. To accomplish this, the Net-Net SBC replicates the packets sent and received, and then sends them to a configured trace server. Using a protocol analyzer running on the trace server, you can then analyze the mirrored packets. Currently, the Packet Trace feature supports:

- One configurable trace server (on which you have installed your software protocol analyzer)
- Sixteen concurrent endpoint traces

How It Works

To use this feature, create a trace server configuration on the Net-Net SBC so that it knows where to send the mirrored packets. Once the trace server is configured, the Net-Net SBC uses one of its internally configured IP addresses (such as one for a SIP interface) on which to source the trace.

You start a packet trace using the ACLI Superuser command **start packet-trace**, entered with these pieces of information:

- Network interface—The name of the network interface on the Net-Net SBC from which you want to trace packets; this value can be entered either as a name alone or as a name and subport identifier value (name:subportid)

  This feature is supported for NIU (media) interfaces; it is not supported for MIU (management) interfaces.
- IP address—IP address of the endpoint to and from which the Net-Net SBC will mirror calls
- Local port number—Optional parameter; Layer 4 port number on which the Net-Net SBC receives and from which it sends; if no port is specified or if it is set to 0, then all ports will be traced
- Remote port number—Optional parameter; Layer 4 port number to which the Net-Net SBC sends and from which it receives; if no port is specified or if it is set to 0, then all ports will be traced

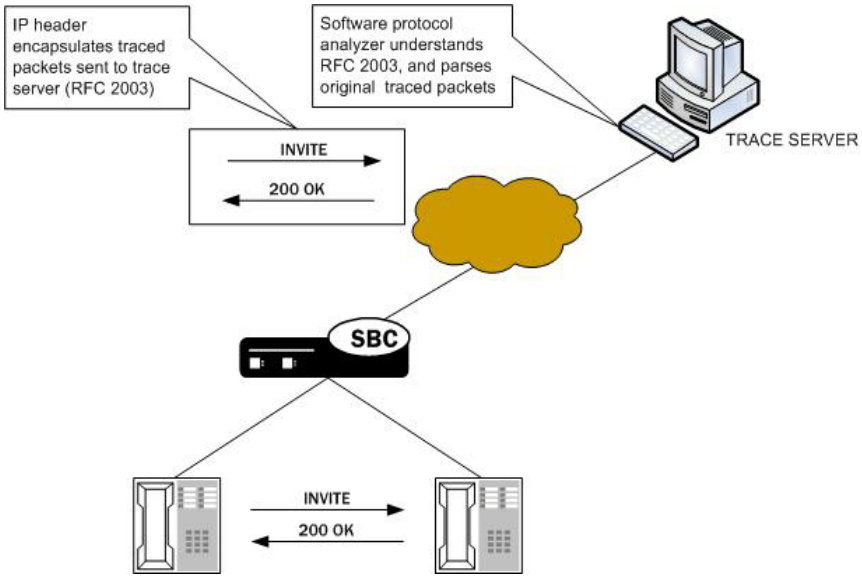
The usage is as follows:

```
start packet-trace <network-interface:subport ID> <IP address>
[<local-port>] [<remote-port>]
```

See the Starting a Packet Trace (198) section for an example.

Once the trace is initiated, the Net-Net SBC duplicates all packets sent to and from the endpoint identified by the IP address that are sent or received on the specified Net-Net SBC network interface.

The Net-Net SBC then encapsulates the original packets in accordance with RFC 2003 (IP Encapsulation within IP); it adds the requisite headers, and the payload contains the original packet trace with the Layer 2 header removed. Since software protocol analyzers understand RFC 2003, they can easily parse the original traced packets. In order to see only packet traces information in your software protocol analyzer, you can use a capture filter; for example, the Ethereal/Wireshark syntax is “ip proto 4.”



It is possible that—for large frames—when the Net-Net SBC performs the steps to comply with RFC 2003 by adding the requisite header, the resulting packet might exceed Ethernet maximum transmission unit (MTU). This could result in packets being dropped by external network devices, but widespread support for jumbo frames should mitigate this possibility.

If the Net-Net SBC either receives or transmits IP fragments during a packet trace, then it will only trace the first fragment. The first fragment is likely to be a maximum-sized Ethernet frame.

The Net-Net SBC continues to conduct the packet trace and send the replicated information to the trace server until you instruct it to stop. You stop a packet trace with the ACLI **stop packet-trace** command. With this command, you can stop either an individual packet trace or all packet traces that the Net-Net SBC is currently conducting. The usage is as follows:

```
stop packet-trace <network-interface:subport ID> <IP address> [<local-
port>] [<remote-port>]
```

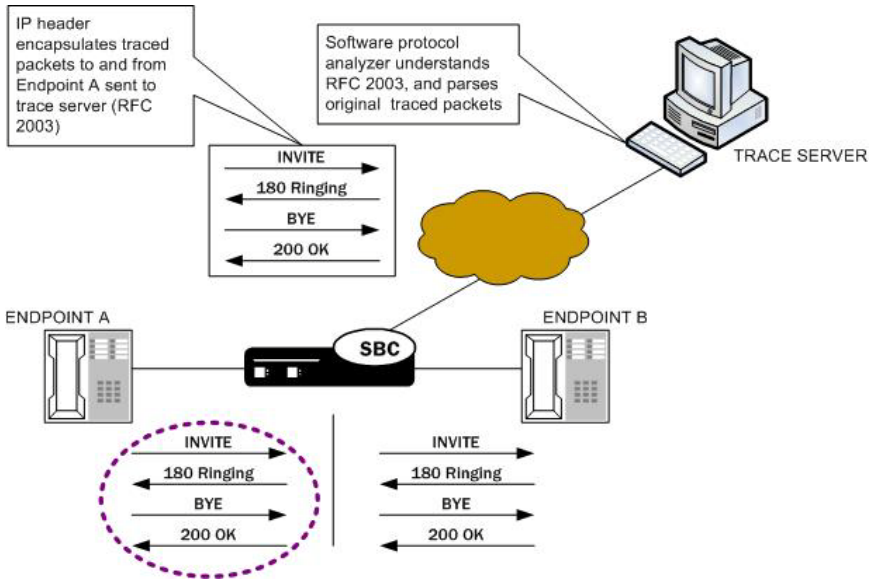
Packet Trace Scenarios

This section describes three possible ways that you might use the packet trace feature. You can examine communications sent to and from one endpoint, sent between two endpoints, or sent between ingress and/or egress Net-Net SBC interfaces to endpoints.

Packet Trace for One Endpoint

When you use the **start packet-trace** command, the Net-Net SBC sets up packet tracing for the traffic between itself and one endpoint. The Net-Net SBC collects and replicates the packets to and from one endpoint. All traffic on all ports is replicated to the trace server. To enable this kind of trace, you set up one packet trace using the **start packet-trace** command. For example:

```
ACMEPACKET# start packet-trace <Network Interface> <IP address of
Endpoint A>
```

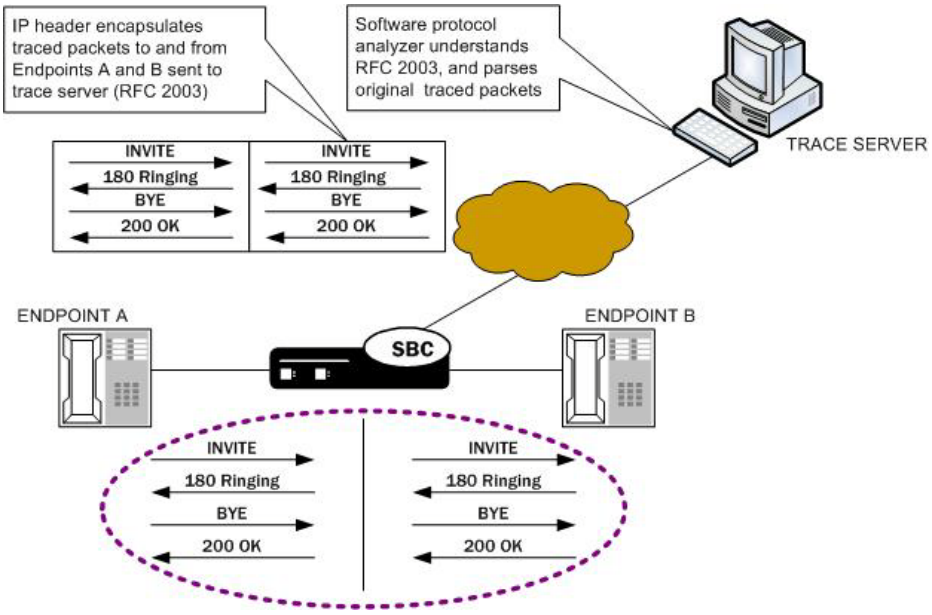


Packet Trace for Both Call Legs

If you want to trace both sides (both call legs) of a call that runs through the Net-Net SBC, then you must set up individual traces for each endpoint—meaning that you would initiate two packet traces. This trace gives you the communications for both call legs between the endpoints you specify. All traffic on all ports for both call legs is replicated to the trace server.

The commands you carry out would take the following form:

```
ACMEPACKET# start packet-trace <Destination Network Interface of
Endpoint A> <IP address of Endpoint A>
ACMEPACKET# pstart acket-trace <Destination Network Interface of
Endpoint B> <IP address of Endpoint B>
```

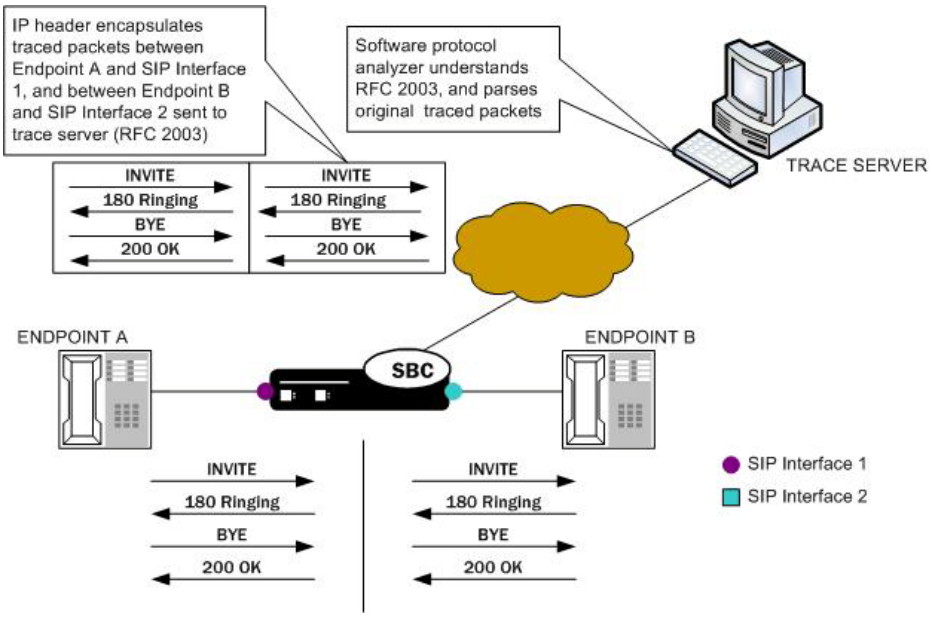


Packet Trace for a Net-Net SBC Signaling Address

You can perform a packet trace for addresses internal to the Net-Net SBC. Using signaling interface addresses puts the emphasis on the Net-Net SBC rather than on the endpoints by allowing you to view all traffic that traverses specified interfaces.

The commands you carry out would take the following form:

```
ACMEPACKET# start packet-trace <Network Interface where Endpoint A
connects> <SIP Interface 1 IP address> 5060
ACMEPACKET# start packet-trace <Network Interface where Endpoint B
connects> <SIP Interface 2 IP address> 5060
```



ACLI Instructions and Examples

There are three steps you can take when you use the packet trace feature:

- Configuring the Net-Net SBC with the trace server information so that the Net-Net SBC knows where to send replicated data
- Setting up the capture filter "ip proto 4" in your software protocol analyzer if you only want to see the results of the Net-Net SBC packet trace(s)
- Starting & Stopping a packet trace

This section provides information about how to perform all three tasks.

Configuring a Trace Server

You must configure a trace server on the Net-Net SBC; this is the device to which the Net-Net SBC sends replicated traffic. The Net-Net SBC supports one trace server.

To configure a trace server on your Net-Net SBC:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **system** and press <Enter>.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Enter **capture-receiver** and press <Enter>.

```
ACMEPACKET(system)# capture-receiver
ACMEPACKET(capture receiver)#
```

4. **state**—Type **enabled** so that you can use the trace server to which you want to send the mirrored packets for calls you are packet tracing. This parameter defaults to `disabled`.
5. **address**—Enter the IP address of the trace server; there is no default.
6. **network-interface**—Enter the name and subport of the Net-Net SBC network interface from which the Net-Net SBC is to send mirrored packets. Your entry needs to take the form `name:subport`. The default for this parameter is `:0`.
7. Save your work using the ACLI **done** command.
8. Save and activate your configuration.

Starting a Packet Trace

Start a packet trace by entering the appropriate ACLI command with these pieces of information:

- Network interface (`name:subport ID` combination)
- IP address to be traced; if you do not enter local and/or remote ports when you start the trace, the Net-Net SBC will trace all ports
- (Optional) Local UDP/TCP port on which the Net-Net SBC sends and receives traffic to be traced
- (Optional) Remote UDP/TCP port to which the Net-Net SBC sends traffic, and from which it receives traffic to be traced; you cannot enter the remote port without specifying a local port

To start a packet trace with local and remote ports specified:

1. Type **start packet-trace** followed by a <Space>. After another <Space>, type in the name and subport ID for the network interface followed by a <Space>, the IP address to be traced followed by a <Space>, the local port number followed by a <Space>, and then optionally the remote port number. Then press <Enter>.

```
ACMEPACKET# start packet-trace core:0 192.168.10.99 5060 5060
Trace started for 192.168.10.99
```

Stopping a Packet Trace

You use the stop a packet trace by entering the appropriate ACLI command with these pieces of information:

- Network interface (`name:subport ID` combination)
- IP address to be traced
- (Optional) Local UDP/TCP port on which the Net-Net SBC sends and receives traffic to be traced
- (Optional) Remote UDP/TCP port to which the Net-Net SBC sends traffic, and from which it receives traffic to be traced

If the packet trace you want to stop has no entries for local and/or remote ports, then you do not have to specify them.

To stop a packet trace with local and remote ports specified:

1. Type **stop packet-trace** followed by a <Space>. After another <Space>, type in the name and subport ID for the network interface followed by a <Space>, the

IP address to be traced followed by a <Space>, the local port number followed by a <Space>, and then optionally the remote port number. Then press <Enter>.

```
ACMEPACKET# stop packet-trace core:0 192.168.10.99 5060 5060
```

To stop all packet traces on the Net-Net SBC:

1. Type **stop packet-trace** followed by a <Space>and the word **all** and press <Enter>.

```
ACMEPACKET# stop packet-trace all
```

Viewing Active Packet Traces

You can see statistics for packet traces initiated on the Net-Net SBC by using the **show packet-trace** command. The display shows you a summary of the active packet traces on the Net-Net SBC. Displayed information includes: the IP address, local and remote port (which displays as 0 if no ports have been designated), slot, port, and VLAN.

```
ACMEPACKET# show packet-trace

IP Address      Local-Port  Remote-Port  Slot Port   VLAN
-------------------------------------------------------
192.168.10.1         0            0        0    1      0
192.168.10.99     5060         5060        0    1      0
10.0.0.1            23            0        1    0      0
```

5 Application Management

Commands discussed in this chapter are used for Net-Net OS application management. This class of commands refers to statistics and counters dealing with media and signaling traffic.

SIP Management

The Net-Net System provides numerous statistics and real-time operating parameters reflecting all aspects of its SIP implementation.

SIP Tasks Show Commands

SIP processing spans several tasks on the Net-Net 9200. The following SIP show commands display various details of SIP system functionality.

show sip transport

The **show sip transport** command displays statistics related to the SIP transport application (sipt). This application implements the Transport Layer and the Transaction Layer of the SIP Signaling Protocol. It is the entry and exit point for all SIP messages. It parses and validates all received SIP message requests and responses. It formats and transmits all outgoing SIP message requests and responses. It also performs all SIP-NAT encoding and decoding on SIP messages. For example:

```
ACMEPACKET# show sip transport
12:37:53-106 sipt
SIP Transport             ---- Recent ---- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
Server Trans             0       0       0      32574    6009    1982
Client Trans             0       0       0      32574    6010    1981
Context IDs              0       0       0      32574    6009    1982
Sockets                  2       2       0          3       3       3
Req Rejected             -       -       0          0       0
Req Dropped              -       -       0          0       0
DNS Trans                0       0       0          0       0       0
DNS Sockets              0       0       0          0       0       0
DNS Results              0       0       0          0       0       0
Invalid Requests         -       -       0          0       0
Invalid Responses        -       -       0          0       0
Invalid Messages         -       -       0          0       0
Transaction Errors       -       -       0          0       0
Application Errors       -       -       0          0       0
```

show sip server

The **show sip server** command displays statistics related to the server. For example:

```
ACMEPACKET# show sip server
08:07:38-146 sipls@0.3.0
SIP Server Trans          ---- Recent ---- -------- Lifetime --------
```

```
                      Active    High   Total      Total  PerMax    High
Total                      0       0       0          0       0       0
<Initial>                  0       0       0          0       0       0
<Trying>                   0       0       0          0       0       0
<Calling>                  0       0       0          0       0       0
<Proceeding>               0       0       0          0       0       0
<Cancelled>                0       0       0          0       0       0
<Established>              0       0       0          0       0       0
<Completed>                0       0       0          0       0       0
<Confirmed>                0       0       0          0       0       0
<Terminated>               0       0       0          0       0       0
```

show sip client

The **show sip client** command displays statistics related to the client. For example:

```
ACMEPACKET# show sip client
08:07:12-121 sipls@0.3.0
SIP Client Trans            ---- Recent ---- -------- Lifetime --------
                      Active    High   Total      Total  PerMax    High
Total                      0       0       0          0       0       0
<Initial>                  0       0       0          0       0       0
<Trying>                   0       0       0          0       0       0
<Calling>                  0       0       0          0       0       0
<Proceeding>               0       0       0          0       0       0
<Cancelling>               0       0       0          0       0       0
<Completed>                0       0       0          0       0       0
<Established>              0       0       0          0       0       0
<Confirmed>                0       0       0          0       0       0
<Terminated>               0       0       0          0       0       0
```

show sip codecs

The **show sip codecs** command displays realm codec statistics. For example:

```
ACMEPACKET# show sip codecs public
18:56:31-46 Realm public
Codec Statistics
                           ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Transcoded                0       0       0          0       0       0
Transrated                0       0       0          0       0       0
Transparent               0       0       0          0       0       0
PCMU Count                -       -       0          0       0
PCMA Count                -       -       0          0       0
G722 Count                -       -       0          0       0
G723 Count                -       -       0          0       0
G726-16 Count             -       -       0          0       0
G726-24 Count             -       -       0          0       0
G726-32 Count             -       -       0          0       0
G726-40 Count             -       -       0          0       0
G728 Count                -       -       0          0       0
G729 Count                -       -       0          0       0
GSM Count                 -       -       0          0       0
iLBC Count                -       -       0          0       0
H261 Count                -       -       0          0       0
H263 Count                -       -       0          0       0
T38 Count                 -       -       0          0       0
```

```
Other Count              -       -       0          0       0
```

show sip core

The **show sip core** command displays statistics related to the SIP core task (sipc). This is where the SIP proxy function is carried out and where requests are forwarded to one or more next hop target destinations. For example:

```
ACMEPACKET# show sip core
08:01:32-180 sipls@0.3.0
SIP Core                    ---- Recent ---- -------- Lifetime --------
                         Active    High   Total      Total  PerMax    High
Response Contexts             0       0       0          0       0       0
Forwarded Requests            0       0       0          0       0       0
Saved Contexts                0       0       0          0       0       0
Challenge Found               -       -       0          0       0
Challenge Not Found           -       -       0          0       0
Challenge Dropped             -       -       0          0       0
Overload Rejects              -       -       0          0       0
DNS Errors                    -       -       0          0       0
No Target/Route               -       -       0          0       0
Transaction Errors            -       -       0          0       0
Application Errors            -       -       0          0       0
```

show sip b2bua

The **show sip b2bua** command displays statistics related to the SIP Back To Back UA task (sipbb). The SIP B2B UA manages all SIP sessions and dialogs in addition to implementing the Back-to-Back User Agent functionality for SIP. For example:

```
ACMEPACKET# show sip b2bua
08:05:13-101 sipls@0.3.0
SIP B2BUA                   ---- Recent ---- -------- Lifetime --------
                         Active    High   Total      Total  PerMax    High
Dialogs                       0       0       0          0       0       0
Sessions                      0       0       0          0       0       0
CallID Map                    0       0       0          0       0       0
Pending Requests              0       0       0          0       0       0
Missing Dialog                -       -       0          0       0
Expired Sessions              -       -       0          0       0
Multiple OK Drops             -       -       0          0       0
Multiple OK Terms             -       -       0          0       0
Media Failure Drops           -       -       0          0       0
Non-ACK 2xx Drops             -       -       0          0       0
Transaction Errors            -       -       0          0       0
Application Errors            -       -       0          0       0
```

show sip sessions

The **show sip sessions** command displays statistics related to the states of SIP sessions and dialogs. For example:

```
ACMEPACKET# show sip sessions
12:38:29-142 sipbb
SIP Session                 ---- Recent ---- -------- Lifetime --------
                         Active    High   Total      Total  PerMax    High
Sessions                      0       0       0      10000    1837     154
  Initial                     0       0       0      10000    1837       3
  Early                       0       0       0      10000    1837       5
  Established                 0       0       0      10000    1837     149
```

```
  Terminated            0       0       0      10000    1837      75
Dialogs                 0       0       0      20000    3674     452
  None                  0       0       0      20000    3674       2
  Early                 0       0       0      20000    3674      10
  Confirmed             0       0       0      20000    3674     298
  Terminated            0       0       0      20000    3674     150
```

show sip cache

The **show sip cache** command displays statistics for the SIP Registration Cache (location service). For example:

```
ACMEPACKET# show sip cache
12:38:38-149 sipls
SIP Loc Server            ---- Recent ---- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Cached Entries          0       0       0          0       0       0
Local Entries           0       0       0          0       0       0
Free Map Ports          0       0       0          0       0       0
Used Map Ports          0       0       0          0       0       0
Transactions            0       0       0          0       0       0
Forwards                -       -       0          0       0
Refreshes               -       -       0          0       0
Rejects                 -       -       0          0       0
Timeouts                -       -       0          0       0
Fwd Postponed           -       -       0          0       0
Fwd Rejects             -       -       0          0       0
Refr Extension          0       0       0          0       0       0
Refresh Extended        -       -       0          0       0
Reg Cache Hits          -       -       0          0       0
Reg Cache Misses        -       -       0      10000    1837
Route to Registrar      -       -       0          0       0
Reg w/o Contacts        -       -       0          0       0
Transaction Errors      -       -       0          0       0
Application Errors      -       -       0          0       0
```

show sip policy

The **show sip policy** command displays statistics related to local policy lookups. This functionality is part of the SIP location service. For example:

```
ACMEPACKET# show sip policy
12:38:42-154 sipls
SIP Policy/Routing                      ---- Lifetime ----
                                Recent      Total  PerMax
Local Policy Lookups                 0      10000    1837
Local Policy Hits                    0      10000    1837
Local Policy Misses                  0          0       0
Local Policy Drops                   0          0       0
Agent Group Hits                     0          0       0
Agent Group Misses                   0          0       0
No Routes Found                      0          0       0
Inb SA Constraints                   0          0       0
Outb SA Constraints                  0          0       0
```

show sip media

The **show sip media** command displays statistics related to SIP media sessions. For example:

```
ACMEPACKET# show sip media
12:39:05-180 sipm
SIP Media                 ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Media Sessions            0       0       0      10000    1837     154
Media Pending             0       0       0      20000    3674       1
SDP Offer Errors          -       -       0          0       0
SDP Answer Errors         -       -       0          0       0
Drop Media Errors         -       -       0          0       0
Media Exp Events          -       -       0          0       0
Early Media Exps          -       -       0          0       0
Exp Media Drops           -       -       0          0       0
Transaction Errors        -       -       0          0       0
Application Errors        -       -       0          0       0
```

show sip load

The **show sip load** command displays the SIP transport task's current load. For example:

```
ACMEPACKET# show sip load
SIP Transport Load is 0.0; Limit is 80
```

SIP Messages Show Commands

The following show commands display statistics related to SIP messages of the type indicated. The Server columns display counts of the SIP message type received by the Net-Net 9200, and the Client columns display counts of the SIP message type sent by the Net-Net 9200.

show sip invite

```
ACMEPACKET# show sip invite
18:52:12-198 sipls@0.4.1
                   --------- Server --------  --------- Client --------
Message/Event        Recent     Total  PerMax   Recent     Total  PerMax
                    ------  ---------  ------  ------  ---------  ------
INVITE Requests           1          1       1       1          1       1
Retransmissions           0          0       0       0          0       0
100 Trying                1          1       1       0          0       0
180 Ringing               1          1       1       1          1       1
200 OK                    1          1       1       1          1       1
Response Retrans          0          0       0       0          0       0
Transaction Timeouts      0          0       0       0          0       0
Locally Throttled         0          0       0
Avg Latency=0.009 for 1
Max Latency=0.009
```

show sip ack

```
ACMEPACKET# show sip ack
12:39:13-187
                   --------- Server --------  --------- Client --------
Message/Event        Recent     Total  PerMax   Recent     Total  PerMax
                    ------  ---------  ------  ------  ---------  ------
ACK Requests              0      10000    1837       0      10000    1837
Retransmissions           0          0       0       0          0       0
Duplicate Response        0          0       0       0          0       0
Transaction Timeouts      0          0       0       0          0       0
```

```
Avg Latency=0.000 for 0
Max Latency=0.000
```

show sip bye

```
ACMEPACKET# show sip bye
12:39:19-192
                  --------- Server --------  --------- Client --------
Message/Event       Recent     Total  PerMax   Recent     Total  PerMax
                   ------  ---------  ------   ------  ---------  ------
BYE Requests             0     12574    2338        0     12574    2338
Retransmissions           0         0       0        0         0       0
200 OK                   0     12574    2339        0     12574    2339
Duplicate Response        0         0       0        0         0       0
Transaction Timeouts      0         0       0        0         0       0

Avg Latency=0.000 for 0
Max Latency=0.000
```

show sip register

```
ACMEPACKET# show sip register
13:59:17-135
                  --------- Server --------  --------- Client --------
Message/Event       Recent     Total  PerMax   Recent     Total  PerMax
                   ------  ---------  ------   ------  ---------  ------
REGISTER Requests         6     13343       5        1       287       2
Retransmissions           0         0       0        0         0       0
200 OK                   6     13343       5        1       287       2
Duplicate Response        0         0       0        0         0       0
Transaction Timeouts      0         0       0        0         0       0

Avg Latency=0.002 for 7
Max Latency=0.016
```

show sip cancel

```
ACMEPACKET# show sip cancel
14:13:56-114
                  --------- Server --------  --------- Client --------
Message/Event       Recent     Total  PerMax   Recent     Total  PerMax
                   ------  ---------  ------   ------  ---------  ------
CANCEL Requests           0         1       1        0         1       1
Retransmissions           0         0       0        0         0       0
200 OK                   0         1       1        0         1       1
Duplicate Response        0         0       0        0         0       0
Transaction Timeouts      0         0       0        0         0       0

Avg Latency=0.000 for 0
Max Latency=0.000
```

show sip prack

```
ACMEPACKET# show sip prack
---< NO DATA AVAILABLE >----
```

show sip options

```
ACMEPACKET# show sip options
---< NO DATA AVAILABLE >----
```

show sip info

```
ACMEPACKET# show sip info
---< NO DATA AVAILABLE >----
```

show sip sub

```
ACMEPACKET# show sip sub
---< NO DATA AVAILABLE >----
```

show sip subscribe

```
ACMEPACKET# show sip subscribe
---< NO DATA AVAILABLE >----
```

show sip notify

```
ACMEPACKET# show sip notify
---< NO DATA AVAILABLE >----
```

show sip refer

```
ACMEPACKET# show sip refer
---< NO DATA AVAILABLE >----
```

show sip update

```
ACMEPACKET# show sip update
---< NO DATA AVAILABLE >----
```

show sip message

```
ACMEPACKET# show sip message
---< NO DATA AVAILABLE >----
```

show sip publish

```
ACMEPACKET# show sip publish
---< NO DATA AVAILABLE >----
```

show sip other

```
ACMEPACKET# show sip other
---< NO DATA AVAILABLE >----
```

show sip forked

Using the ACLI **show sip forked** command, you can display the total number of forked sessions the Net-Net SBC received and the total number it rejected. The Net-Net SBC counts forked sessions when it receives a dialog-creating INVITE and is enabled to shared bandwidth. Further, it counts as forked all session with the P-Multiring-Correlator header.

```
ACMEPACKET# show sip forked
16:57:46-131 sipls@0.4.1
Forked Session Stats              ---- Recent ---- ---- Lifetime -----
                        Active   High   Total     Total  PerMax   High
Total Sessions                    -       -       0          0       0
Total Sessions Rej                -       -       0          0       0
```

SIP Networking Show Commands

The following **show** commands display statistics about logical SIP entities in the network and their connections to the Net-Net system.

show sip agents

The **show sip agents** command displays statistics related to defined SIP session agents. Entering this command without any arguments lists all SIP session agents. Adding the IP address or hostname of a session agent at the end of the command displays statistics for that session agent. For example:

```
ACMEPACKET# show sip agents
```

```
No Session Agents found
```

show sip sockets

The **show sip sockets** command displays connections and message counts on the Net-Net system. For example:

```
ACMEPACKET# show sip sockets
------ ------------------------------ ---------- ---------- --------
Handle Socket                         MsgRcvd    MsgSent    Errors
------ ------------------------------ ---------- ---------- --------
2      UDP[0:0]172.16.0.170:5060      32574      42574      0
3      UDP[2:0]192.168.24.170:5060    42574      32574      0
------ ------------------------------ ---------- ---------- --------
Total Open Sockets: 2
```

show sip endpoint

The **show sip endpoint** command displays registration information for a supplied endpoint. For example:

```
ACMEPACKET#  show sip endpoint 801
-------------------------------------------------------------
User sip:801@172.16.0.123 ID=2
  Contact: ID=2 exp-UA=1497 exp-SD=1493
    UA=<sip:801@172.16.0.199>
        realm=public local=172.16.0.123:5060 remote=172.16.0.199:5060
    SD=<sip:801@192.168.0.123:5060> realm=private
    Call-ID=8829479ed7557833@172.16.0.199
-------------------------------------------------------------
```

show sip realm

The **show sip realm** command displays current statistics for all configured realms used for SIP services. For example:

```
ACMEPACKET# show sip realm
07:39:21
              ----- Inbound -----  ---- Outbound ----- -- Latency --  Max
Realms         Active  Rate  ConEx  Active  Rate  ConEx   Avg    Max Burst
private             0   0.0     0       0   0.0      0  0.000  0.000     0
public              0   0.0     0       0   0.0      0  0.000  0.000     0
```

Entering a specific realm as the final argument returns statistics for the identified realm. For example:

```
ACMEPACKET# show sip realm public
15:01:38-38
Realm net200 ID=06 [In Service]
                          ---- Recent ---- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
Inbound Sessions         0       0       0          0       0       0
  Sustained Rate         -       -     0.0          -       -
  Rate Exceeded          -       -       0          0       0
  Num Exceeded           -       -       0          0       0
  Burst Rate(10s)        0       0       0          0       0       0
  RegRate Exceeded       -       -       0          0       0
Outbound Sessions        0       0       0          0       0       0
  Sustained Rate         -       -     0.0          -       -
  Rate Exceeded          -       -       0          0       0
```

```
  Num Exceeded          -       -       0          0       0
  Burst Rate(10s)       0       0       0          0       0       0
  RegRate Exceeded      -       -       0          0       0
Burst       (10s)       0       0       0          0       0       0
Trans Timeouts          0       0       0          0       0       0
Requests Sent           -       -       0          1       1
Requests Complete       -       -       0          1       1
Requests Received       -       -       0          0       0
Seizure                 -       -       0          0       0
Answer                  -       -       0          0       0
  ASR Exceeded          -       -       0          0       0
Minutes Exceed Rej      -       -       0          0       0
Short Sessio(10s)       0       0       0          0       0       0

Avg Latency=0.000 for 1
Max Latency=0.000
```

SIP CPU Load Limiting

See SIP Load Limiting (234) for a description on how to enable SIP CPU load limiting.

Call Protocol (SIP) Tracing

For debugging needs, you can capture and save a log of all VoIP application messages that reach and are sourced from the Net-Net 9200 as a signalling protocol log. This log file can be stored locally (RAM drive), remotely (process log server), or simultaneously locally and remotely.

This feature works similarly to the Process Log Files (28) feature.

SIP Protocol Trace Output

The SIPT process is the SIP task that generates a protocol trace. When writing a protocol trace locally, the sipmsg.log file is located on the file system local to the CPU/core where the SIPT runs, in the `/ramdrv/logs/` directory. You can use the **show manifest** command to find the location of SIPT.

When you set SIPT's task logging configuration to a specific level, all messages of that level and higher are written to the task log. By default, if you set the task's logging level to TRACE or DEBUG, it also outputs a protocol trace. Alternatively, you can use the call trace parameter to enable a protocol message trace, regardless of the task's logging level.

Configuration

Call protocol tracing is enabled in the system configuration. You must also set the call trace mode parameter, which determines the location of the call trace log files. You may choose one of four selectable call trace modes to specify what the Net-Net 9200 does with the call trace log.

- local—Writes the protocol trace file locally.
- remote—Sends protocol trace message to the configured Acme Process Log Server.
- both—Writes the protocol trace file to both the configured Acme Process Log Server and locally.
- none—Task does not write to local or remote location.

To enable SIP call tracing:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type **system** and press <Enter> to access the system path.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```

3. Type **system-config** and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

   ```
   ACMEPACKET(system)# system-config
   ACMEPACKET(system-config)#
   ```

4. **call-tracing**—Set this parameter to enabled for the Net-Net 9200 to generate a call trace log.

5. **call-trace-mode**—Set the call trace log mode that you want to use from these available choices:
   - remote—Send call trace logs to the Process log server only
   - local—Send call trace logs to the local file system only (default)
   - both—Send call trace logs to the Process log server and to the local file system
   - none—No call trace logging

6. Save your work using the ACLI **done** command.
7. Save and activate the configuration.

Displaying and Clearing Registration Cache Entries

The Net-Net SBC's registration cache management offers detailed information (beyond basic registration cache displays) and flexible ways to view the registration cache. You can query, clear, and audit entries.

Querying the SIP Registration Cache

You can view SIP registration cache information **by-user**, **by-realm**, **by-route**, and **by-registrar**. For each of these search criteria, you can specify the whole term, part of the search term, or a wildcard "*". If you only use part of a user name without adding the wildcard character, the Net-Net SBC only returns exact matches.

The SIP registration cache statistics include counters for free and allocated signaling ports. You can issue a show registration command to display the statistics:

```
17:36:55-190
SIP Registrations          -- Period -- -------- Lifetime --------
                  Active    High   Total      Total  PerMax    High
```

```
User Entries          4       4       0          7       4       4
Local Contacts        4       4       0          7       4       4
Free Map Ports    12284   12284       0      12291   12288   12288
Used Map Ports        4       4       0          7       4       4
Forwards              -       -       1         22       4
Refreshes             -       -       3         43       3
Rejects               -       -       0          0       0
Timeouts              -       -       0          1       1
Fwd Postponed         -       -       0          0       0
Fwd Rejected          -       -       0          0       0
Refr Extension        0       0       0          0       0       0
Refresh Extended      -       -       0          0       0
```

The labels for the first two items reflect the restructured registration cache:

- User Entries—Counts the number of unique SIP addresses of record in the cache. Each unique address of record represents a SIP user (or subscriber). The address of record is taken from the To header in the REGISTER request. There might be one or more registered contacts for each SIP user. The contacts come from the Contact header of the REGISTER request.
- Local Contacts—Counts the number of contact entries in the cache. Because the same user can register from multiple endpoints (user agents); the number of Local Contacts might be higher than the number of User Entries.
- Free Map Ports—Counts the number of ports available in the free signaling port pool.
- Used Map Ports—Counts the number of signaling ports allocated for registration cache entries. The value of Used Map Ports will equal the number of Local Contacts when the port mapping feature is used for all registrar/softswitch realms in the Net-Net 9200.

by-user

The registration cache can be searched by a specific username, phone number, or portion of a username or phone number. All of these user types are equivalent. This command is entered as:

```
show registration sip by-user <endpoint> [brief | extended | detail]
```

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 with 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*`). For example:

```
ACMEPACKET> show registration sip by-user user*

Registration Cache                          TUE JUL  11:29:50 UTC 2007
                                                Num
User                                         Contacts   Registered at
---------------------------------- --------   -------------------
sip:user@acme.com                               1   2007-07-26-11:29:50
sip:username@acme.com                           1   2007-07-26-11:29:51
sip:username2@acme.com                          1   2007-07-26-11:29:51
ACMEPACKET>
```

You can add the **detailed** argument only to the by-user query to view complete registration cache contents:

```
ACMEPACKET> show registration sip by-user user detailed

Registration Cache (Detailed View)              TUE JUL2 11:32:21 UTC
2007

User: sip:user@acme.com
  Registered at:  2007-07-26-11:32:21    Surrogate User: false

  Contact Information:
    Contact Name: sip:user@acme.com valid: false, challenged: false
      Via-Key: 172.30.80.4
      Registered at: 2007-07-26-11:32:21
      Last Registered at: 2007-07-26-11:32:21
      state:  <expired>

      Transport: <none>,   Secure: false
      Local IP: 172.30.80.180:5060

      User Agent Info:
       Contact: sip:user-acc-m2vm2n09kb@127.0.0.15:5060;transport=udp
          Realm: access,  IP: 172.30.80.4:5060

      SD Contact: sip:user-p3rrurjvp0lvf@127.0.0.10:5060
          Realm: backbone
```

by-realm

The registration cache can be searched for calls that have registered through a specified ingress realm. Wild cards will be supported as well. This command is entered as:

```
show registration sip by-realm <realm> [brief | extended]
```

The output will also be sorted alphabetically by the realm name which will be shown first in the output. For example:

```
ACMEPACKET# show registration sip by-realm *

Registration Cache                              THU OCT 2 15:02:12  2007


Realm           User                            Registered at
--------------- ------------------------------- -------------------
access          sip:420000002@172.16.34.10      2007-10-11-15:01:51
backbone        sip:17815552020@acmepacket.com  2007-10-11-14:10:26
--------------- ------------------------------- -------------------
Total 2 entries
```

You can add the **extended** argument to view this command's output with detailed information as shown in the Extended Registration Cache Output section.

by-route

The registration cache can be searched for calls by their Internet-routable IP address with the search type "by-route". This is useful for viewing the endpoints associated with public addresses. Wild cards are supported as well. Search values are checked

to be a valid IPv4 IP address, except in the case of use with the wild cards where only the first part of the address is checked. This command is entered as:

```
show registration sip by-route <IP-address> [brief | extended]
```

The output is sorted by the IP address. For example:

```
ACMEPACKET# show registration sip by-route *

Registration Cache                              THU OCT 2 15:02:12  2007

Routable
IP Address      User                             Registered at
--------------- -------------------------------- ------------------
172.16.34.10    sip:420000002@172.16.34.10       2007-10-11-15:01:51
192.168.34.10   sip:17815552020@acmepacket.com   2007-10-11-14:10:26
--------------- -------------------------------- ------------------
Total 2 entries
```

You can add the **extended** argument to view this command's output with detailed information as shown in the Extended Registration Cache Output section.

by-registrar

The registration cache can be searched for calls that use a specific registrar. The search will support wild cards so either complete name of the realm, partial name ending with the "*" or "*" by itself could be used. This command is entered as:

```
show registration sip by-registrar <IP-address> [brief | extended]
```

The output is sorted alphabetically by the registrar address. A delay before printing the output of the by-registrar command to the screen is likely. Before the number of entries there will be a note: "Searching entries…total n". The maximum supported number of entries is 999,999.

```
ACMEPACKET# show registration sip by-registrar *

Registration Cache                              THU OCT 2 15:02:12  2007

Registrar
IP Address      User                             Registered at
--------------- -------------------------------- ------------------
172.16.34.10    sip:420000002@172.16.34.10       2007-10-11-15:01:51
192.168.34.10   sip:17815552020@acmepacket.com   2007-10-11-14:10:26
--------------- -------------------------------- ------------------
Total 2 entries
```

You can add the **extended** argument to view this command's output with detailed information as shown in the Extended Registration Cache Output section.

Extended Registration Cache Output

You can add the **extended** argument to the show registration sip command's output. The output includes User, Registration Time, registration realm, registrar's

address, public IP address where that user can be reached. All information in the following example is conveyed whenever the **extended** argument is invoked:

```
ACMEPACKET# show registration sip by-user * extended

Registration Cache                                THU OCT  15:02:12  2007

                                                  Registrar     Routable
User                 Registered at       Realm    IP Address    IP Address
-------------------- ------------------- -------- ------------ -------------
sip:421@172.16.34.10 2007-10-11-15:01:51 access   192.168.1.10 172.16.34.10
sip:178120@acm.com   2007-10-11-14:10:26 backbone 198.168.10.1 172.168.34.25
-------------------- ------------------- -------- ------------ -------------
Total 2 entries
```

Writing Registration Queries to a File

You can write all output from the **show registration sip** commands to a file located on the local flash file system instead of to the ACLI. You use the **to-file** switch, followed by the output filename. The file is written to the `/ramdrv/` location, or any subdirectory as indicated in the filename. For example:

```
ACMEPACKET# show registration sip by-user * to-file /ramdrv/output.txt
```

If the file already exists, the old file is renamed to `file_name.bak`. Subdirectories are supported and will be created by the system if they do not exist.

Note: The contents of the /ramdrv/ is cleared on reboot. Therefore, you must FTP them off the Net-Net SBC if they require preservation.

Displaying H.323 Registration Cache Entries

The Net-Net SBC's registration cache management offers detailed information (beyond basic registration cache displays) and flexible ways to view the registration cache. You can query, clear, and audit entries.

by-alias

The H.323 registration cache can be searched by a specific endpoint . This command is entered as:

```
show registration h323 by-alias <endpoint> [brief | detail]
```

The **<endpoint>** portion of the command can be a single phone number or one of the terminal aliases. Use of the wildcard character '*' is supported as the last character of the endpoint string.

For example, an endpoint might be registered as `4278_endp` .

The phone number can be a single number (such as `7815551234`) or a single number wildcarded with 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*`). For example:

```
ACMEPACKET> show registration h323 by-alias 4278_endp

Registration Cache                          FRI MAR 10 20:22:00  2010


Endpoint                          Expiration      Registered at
--------------------------------- --------------- -------------------
4278_endp                         27              2007-08-03-19:58:34
```

```
-------------------------------- -------------- ------------------
Total 1 entry
```

You can add the **detailed** argument to view complete registration cache contents:

```
ACMEPACKET> show registration h323 by-alias 4224_endp detail

Registration Cache (Detailed View)            TUE APR 15 14:51:59 2010
Endpoint: 4224_endp,  state: Registered
  Registered at: 2007-04-24-14:50:05
  Expiration: 204
  Gatekeeper: open-gk1

  Endpoint NAT Address: 192.168.200.56:1372
  SD Call Signaling Address: 150.150.150.10:2048
  SD RAS Address: 150.150.150.10:8200

  Terminal Alias(s):
    Alias: e164: 17815552222,  Registered: true

  Call Signaling Address(s):
    Address: 192.168.200.56:1720

  RAS Address(s):
    Address: 192.168.200.56:1372
```

Clearing the SIP Registration Cache

You can clear a single user entry from the SIP registration cache, or you can clear the full registration cache with the **clear registration sip** command.

clear registration sip

You can clear the entire registration cache by using the **all** switch, or remove the registration cache entry for a single specified user or phone number. The phone number can be a single number (7815554400). You can also enter a user name for this value. This command takes the form:

```
clear registration sip [all | by-user <user> ]
```

After you use this command, all affected endpoints will have to register through the Net-Net SBC once again.

Note: You can wildcard user values with the clear registration sip command.

Entries Registered by a Surrogate Agent

Endpoints registered by a surrogate are uniquely displayed on the ACLI. These same endpoints can not be removed from the registration cache by regular means. You can disable the surrogate agent in the configuration to remove these entries from the cache.

Displaying Registrations

Entries created by the surrogate agents will have a "*" before the user name when running a show registration command. There will be also a separate count for those

entries. If no endpoints were registered by a surrogate agent, no extra line with the surrogate counter will be shown. For example:

```
ACMEPACKET> show registration sip by-user mike*

Registration Cache                              TUE MAR 10 11:29:50  2007
                                        Num
  User                                Contacts   Registered at
---------------------------------- --------   ------------------
  sip:mike@acme.com                        1   2007-03-06-11:29:50
* sip:mikesmith@acme.com                   1   2007-03-06-11:29:51
  sip:mikester@acme.com                    1   2007-03-06-11:29:51
---------------------------------- --------   ------------------

Total 3 entries
1 entry created by the surrogate agent(s)
```

Clearing Registrations

When using the clear-cache command, entries created by the surrogate agent will be skipped and will not be cleared if exist in the registry. The extra counter for the surrogate entries will point out how many of those are skipped. The original counter will print out the number of entries that where cleared.

If the clear-cache command is successful there are several possible outputs displayed to the screen. If there were no entries created by the surrogate agents then the output looks like this:

```
Successfully cleared 658 Registration Cache entries
```

When the registration cache contains mixed elements, both created normally and by the surrogate agents, the output looks like this:

```
Successfully cleared 658 Registration Cache entries
65 entries skipped (created by the surrogate agent(s))
```

If all of the entries in the registry were created by the surrogate agents, then the output looks like this:

```
No entries cleared!
65 entries skipped (created by the surrogate agent(s))
```

If requested search finds no matching entries, the output looks like this:

```
No matching entries found!
```

Clearing the H.323 Registration Cache

You can clear a single user entry from the H.323 registration cache, or you can clear the full registration cache with the **clear registration h323** command.

clear registration sip

You can clear the entire registration cache by using the **all** switch, or remove the registration cache entry for a single specified endpoint. This command takes the form:

```
clear registration h323 [all | by-alias <endpoint> ]
```

After you use this command, all affected endpoints will have to register through the Net-Net SBC once again.

You can wildcard user values with the clear-cache registration h323 command.

Session Agent Management

Manual Registration Invalidation

Session agents represent statically defined logical next-hops and previous-hops, for the purpose of providing hostname-to-IP Address resolution. You can provision admission control, constraints, and identification or provisioning properties for each session-agent.

After an endpoint registers to a registrar through the Net-Net SBC, its registration is cached to memory on the system. This cached registration exists for the time indicated by the expiration of the REGISTER response sent from the registrar. If an endpoint sends another REGISTER before the cached registration expires, the Net-Net SBC responds directly to the endpoint, rather than forwarding it to the real registrar. Additionally, if the registrar is configured as a session agent, this association is stored in the contact line within the registration-cache.

The Net-Net SBC includes provisions to explicitly invalidate current registrations in certain instances with the **reset session-agent** command. If the registrar, configured as a session agent, goes out of service, the SBC can invalidate the current endpoint registrations to that session agent. Thus, after resetting the session agent, the Net-Net SBC acts as if the registrations have expired, and forces the endpoints to re-register with the registrar. The command is entered as follows:

```
reset session-agent <session-agent-name>
```

To help identify when session agents have been marked as invalid, the associated session agent for a contact can now be displayed by the **show sip endpoint** ACLI command.

An asterisk '*' is displayed next to the session agent when it is in service and an 'X' is displayed when a session agent failover has occurred or if the session agent has been marked as invalid. For example:

```
ACMEPACKET# show sip endpoint-ip 9
User <sip:9580000001@192.168.201.86>
  Contact ID=1008 exp=597
    UA-Contact: <sip:sipp@192.168.200.254:9004> UDP
       realm=sip192 local=192.168.201.86:5060 UA=192.168.200.254:9004
SA=172.16.0.66 *
    SD-Contact: <sip:9580000001-hchse0jm171u2@172.16.10.86:5060>
realm=sip172
    Call-ID: 1-20622@192.168.200.254'
    Service-Route='<sip:172.16.0.66:5060;lr>'


ACMEPACKET# reset session-agent 172.16.0.66


ACMEPACKET#show sip endpoint-ip 9
User <sip:9580000001@192.168.201.86>
  Contact ID=1008 exp=597
    UA-Contact: <sip:sipp@192.168.200.254:9004> UDP
       realm=sip192 local=192.168.201.86:5060 UA=192.168.200.254:9004
SA=172.16.0.66 X
    SD-Contact: <sip:9580000001-hchse0jm171u2@172.16.10.86:5060>
realm=sip172
    Call-ID: 1-20622@192.168.200.254'
    Service-Route='<sip:172.16.0.66:5060;lr>'
```

MBCD Management

MBCD communicates with the networking control portions of the Net-Net OS to coordinate between signaling and media functions. MBCD is generally used to set up and manage media flows.

MBCD Show Command

The following **show** commands are used to query MBCD and display real time statistics. The **show mbcd** command usage is as follows:

```
ACMEPACKET# show mbcd [client | server | nat | acl | errors | add |
modify | subtract | notify | flows | cams | realms | rules-natalg |
sessions-natalg | forked-sessions]
```

show mbcd client

The **show mbcd client** command displays statistics related to MBCD transactions when MBCD acts as a client communicating with signaling tasks, acting as servers. For example:

```
ACMEPACKET# show mbcd client
12:08:15-130
MBCD Client                ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Client Trans                0       0       0      30000    5511       3
Server Trans                0       0       0          0       0       0
Trans Timeouts              -       -       0          0       0
Client Sessions             0       0       0      10000    1837     154
Client Errors               -       -       0          0       0
Open Streams Failed         -       -       0          0       0
Drop Streams Failed         -       -       0          0       0
Exp Flow Events             -       -       0          0       0
Exp Flow Not Found          -       -       0          0       0
```

show mbcd server

The **show mbcd server** command displays statistics related to MBCD transactions when MBCD acts as the server communicating with signaling tasks, acting as clients. These counts primarily reflect asynchronous transactions, such as the action to take after a flow guard expiration. For example:

```
ACMEPACKET# show mbcd server
12:08:21-133
MBC Server                 ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Client Trans                0       0       0          0       0       0
Server Trans                0       0       0      30000    5510    1767
Trans Timeouts              -       -       0          0       0
Contexts                    1       1       0      10001    1837     155
Flows                       2       2       0      20005    3674     313
Flow-Port                   0       0       0      20000    3674     308
Flow-NAT                    2       2       0      60010   11021     309
Flow-RTCP                   0       0       0          0       0       0
Flow-Hairpin                0       0       0          0       0       0
Flow-Released               0       0       0          0       0       0
MSM-Release                 0       0       0          0       0       0
NAT Entries                 2       2       0      30005    5511     308
Free Ports               3000    3000       0      43000    7624    3000
Used Ports                  0       0       0      40000    7348     616
```

```
Port Sorts                -       -       0          0       0
```

show mbcd nat

The **show mbcd nat** command displays statistics on MBCD's NAT table transactions. For example.

```
ACMEPACKET# show mbcd nat
12:08:24-136
NAT Entries               ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
NAT Entries               2       2       0      30005    5511     308
Transactions              0       0       0      60008   11020       7
Trans Queued              0       0       0          0       0       0
Trans Timeouts            -       -       0          0       0
Trans Errors              -       -       0          0       0
Adds                      -       -       0      30005    5511
Deletes                   -       -       0      30003    5510
Updates                   -       -       0          0       0
Non-Starts                -       -       0          0       0
Stops                     -       -       0          0       0
Expired                   -       -       0          0       0
ARP Timeouts              -       -       0          0       0
```

show mbcd acl

The **show mbcd acl** command displays statistics on MBCD's entries in the ACL list. For example:

```
ACMEPACKET# show mbcd acl
12:08:29-142
ACL Entries               ---- Recent ---- -------- Lifetime --------
                     Active    High   Total      Total  PerMax    High
Static Trusted            0       0       0          0       0       0
Static Blocked            0       0       0          0       0       0
Dynamic Trusted           0       0       0          0       0       0
Dynamic Blocked           0       0       0          0       0       0
App Requests              -       -       0          0       0
Added                     -       -       0          0       0
Removed                   -       -       0          3       3
Dropped                   -       -       0          0       0
```

show mbcd errors

The **show mbcd errors** command displays statistics related to MBCD task errors. The following fields are explained:

- Server Errors—Number of uncategorized errors in the MBC server.
- Flow Add Failed—Number of errors encountered when attempting to add an entry to the NAT table.
- Flow Delete Failed—Number of errors encountered when attempting to remove an entry from the NAT table.
- Flow Update Failed—Number of errors encountered when attempting to update an entry in the NAT table upon receipt of the first packet for a media flow.
- Flow Latch Failed—Number of errors when attempting to locate an entry in the NAT table upon receipt of the first packet for a media flow.
- Pending Flow Expired—Number of flow timer expirations for pending flows that have not been added to the NAT table.

- Exp CAM Not Found—This statistic shows the number that the NAT table entry for an expired flow could not find in the NAT table. This usually occurs due to a race condition between the removal of the NAT entry and the flow timer expiration notification being sent to MBCD from the NP.
- Drop Unknown Exp Flow—Number of flows deleted by the MBCD because of a negative response from the application to a flow timer expiration notification.
- Drop/Exp Flow Missing—Number of negative responses from the application to a flow timer expiration notification for which the designated flow could not be found in MBCD's tables. Also includes when a flow for a Subtract request to MBCD cannot be found.
- Exp Notify Failed—Number of errors encountered when the MBCD attempted to send a flow timer expiration notification to the application.
- Unacknowledged Notify—Number of flow expiration notification messages sent from MBCD to the application for which MBCD did not receive a response in a timely manner.
- No Ports Available—Number of steering port allocation requests not be satisfied due to a lack of free steering ports in the realm.
- Invalid Realm—Number of flow setup failures due to an unknown realm in the request from the application.
- Insufficient Bandwidth—Number of flow setup failures due to insufficient bandwidth in the ingress or egress realm.Exp Flow Events—Number of flow timer expiration notifications received from the MBCD by all applications.
- Stale Ports Reclaimed—Number of ports that were reclaimed when the standby card had a stale flow that the active card replaced; when the flow is replaced, the steering ports are also reallocated properly (i.e., according to the active system).
- Stale Flows Replaced—Number of times that the standby card had entries in its flow tables that did not match those on the active card; the active card replaced the standby's stale flows with valid ones.
- Pipe Alloc Errors—Number of times that buffer allocation failed for communication between application tasks and middlebox control protocol tasks.
- Pipe Write Errors—Number of times that messages were not sent between the application tasks and middlebox control protocol tasks, possibly because of a pipe/buffer allocation error.
- XCode Alloc Errors—Number of times opening a transcoding session was denied because of no remaining sessions.

```
ACMEPACKET# show mbcd errors
16:25:20-145
MBC Errors                    ---- Lifetime ----
                        Recent      Total  PerMax
Server Errors                0          0       0
Flow Add Failed              0          0       0
Flow Delete Failed           0          0       0
Flow Update Failed           0          0       0
Flow Latch Failed            0          0       0
Pending Flow Expired         0          0       0
Exp CAM Not Found            0          0       0
Drop Unknown Exp Flow        0          0       0
Drop/Exp Flow Missing        0          0       0
Exp Notify Failed            0          0       0
```

```
Unacknowledged Notify        0          0       0
Invalid Realm                0          0       0
No Ports Available           0          0       0
Insufficient Bandwidth       0          0       0
Stale Ports Reclaimed        0          0       0
Stale Flows Replaced         0          0       0
Natm Send Errors             0          0       0
Natm Timeout Errors          0          0       0
Natm Errors                  0          0       0
XCode Internal Errors        0          0       0
XCode Alloc Errors           0          0       0
XCode Update Errors          0          0       0
XCode Delete Errors          0          0       0
XCode Over License Cap      45         60      35
```

show mbcd add

The **show mbcd add** command displays statistics on MBCD's add transactions. Add transactions only occur when MBCD acts in a server role. For example:

```
ACMEPACKET# show mbcd add
12:08:40-151
                 --------- Server --------   --------- Client --------
Message/Event    Recent      Total  PerMax   Recent      Total  PerMax
                 ------  ---------  ------   ------  ---------  ------
Add Commands          0      10000    1837        0          0       0
Retransmissions       0          0       0        0          0       0
Success               0      10000    1837        0          0       0
Errors                0          0       0        0          0       0

Avg Latency=0.000 for 0
Max Latency=0.000
```

show mbcd modify

The **show mbcd modify** command displays statistics on MBCD's modify transactions. Modify transactions only occur when MBCD acts in a server role. For example:

```
ACMEPACKET# show mbcd modify
12:08:41-154
                 --------- Server --------   --------- Client --------
Message/Event    Recent      Total  PerMax   Recent      Total  PerMax
                 ------  ---------  ------   ------  ---------  ------
Modify Commands       0      10000    1837        0          0       0
Retransmissions       0          0       0        0          0       0
Success               0      10000    1837        0          0       0
Errors                0          0       0        0          0       0

Avg Latency=0.000 for 0
Max Latency=0.000
```

show mbcd subtract

The **show mbcd subtract** command displays statistics on MBCD's subtract transactions. Subtract transactions only occur when MBCD acts in a server role. For example:

```
ACMEPACKET# show mbcd subtract
12:08:49-160
                 --------- Server --------   --------- Client --------
Message/Event     Recent      Total  PerMax   Recent      Total  PerMax
                 ------  ---------  ------   ------  ---------  ------
Subtract Commands       0      10000    1837        0          0       0
Retransmissions         0          0       0        0          0       0
Success                 0      10000    1837        0          0       0
Errors                  0          0       0        0          0       0

Avg Latency=0.000 for 0
Max Latency=0.000
```

show mbcd notify

The **show mbcd notify** command displays statistics on MBCD's notify transactions. Notify transactions only occur when MBCD acts in a client role.

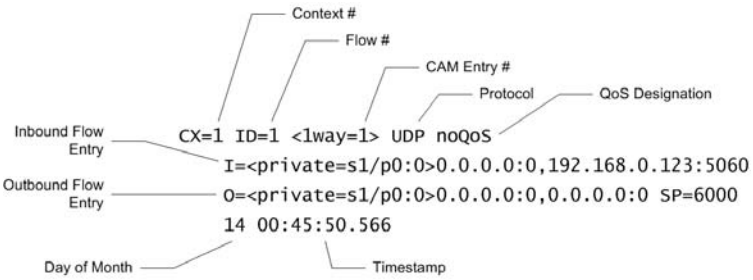
show mbcd flows

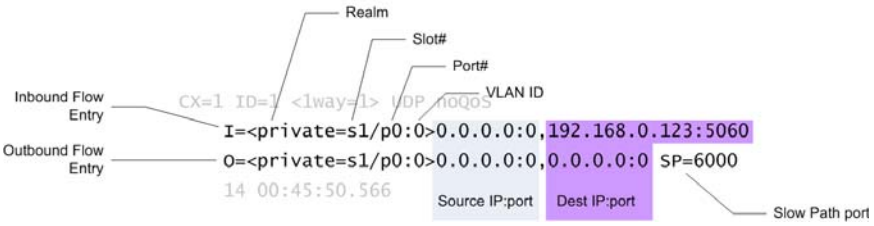
The **show mbcd flows** command displays statistics on the contexts and flows MBCD has established. For example:

```
ACMEPACKET# show mbcd flows
Contexts & Flows:
CX=1 ID=1 <1way=1> UDP noQoS
    I=<private=s1/p0:0>0.0.0.0:0,192.168.0.123:5060
    O=<private=s1/p0:0>0.0.0.0:0,0.0.0.0:0 SP=6000
    14 00:45:50.566

CX=1 ID=2 <1way=2> UDP noQoS
    I=<public=s0/p0:0>0.0.0.0:0,172.16.0.123:5060
    O=<public=s0/p0:0>0.0.0.0:0,0.0.0.0:0 SP=6000
    14 00:45:50.583

CX=1 ID=3 <1way=3> UDP noQoS
    I=<private=s1/p0:0>192.168.0.10:53,192.168.0.123:0
    O=<private=s1/p0:0>0.0.0.0:0,192.168.0.123:0 SP=6000
    14 00:45:50.583

1 contexts; 3 flows
```

Note: Do not execute the show mbcd flows command on a loaded production system. The output's load on the Net-Net 9200 could interrupt call processing.

The following explains the **show mbcd flows** output in detail:





forked calls

The **show mbcd flows** command displays the "forkedCallId" if the flows belong to a forked session. For example

```
ACMEPACKET# show mbcd flows
CX=65537.1E ID=65537-A <1way=12> UDP/2c noQoS brq=200(f) med=audio <lg>
    I=<net200=s0/p3:0>0.0.0.0,192.168.200.85:10000
    O=<net1=s0/p2:0>192.168.1.85:10000,192.168.1.139:9200
    23 21:04:56.318 last=23 21:04:56.455 other=65538; 4 ports:
     192.168.200.85:10000+10001
     192.168.1.85:10000+10001
    XCode=no:off xE= xW=
   2833ACT=NONE 2833InPL=101 2833OutPL=101 2833CLKFRQ=8000 2833INDEX=0
    DTIn=0 DTOut=0
    DigTypeIn=NONE DigTypeOut=NONE
ForkedCallId:pmultiringcorrelator@192.168.200.139
```

Note: Do not execute the **show mbcd flows** command on a loaded production system. The output's load on the Net-Net 9200 could interrupt call processing.

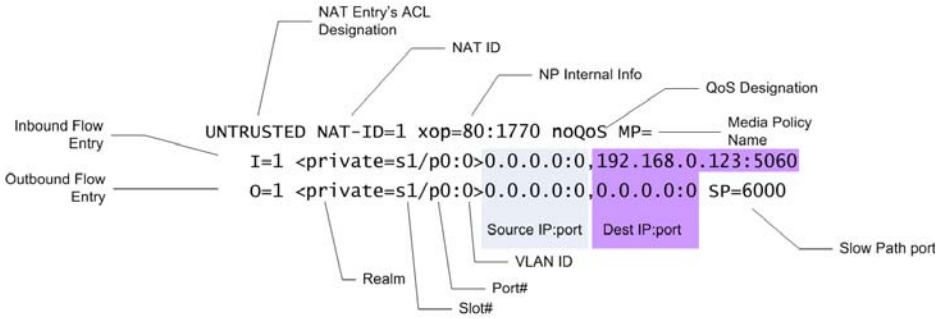
show mbcd cams

The **show mbcd cams** command displays statistics on the flows entries MBCD has entered in the CAM. For example:

```
ACMEPACKET# show mbcd cams
NatFlows:
UNTRUSTED NAT-ID=1 xop=80:1770 noQoS MP=
    I=1 <private=s1/p0:0>0.0.0.0:0,192.168.0.123:5060
    O=1 <private=s1/p0:0>0.0.0.0:0,0.0.0.0:0 SP=6000
UNTRUSTED NAT-ID=2 xop=80:1770 noQoS MP=
    I=2 <public=s0/p0:0>0.0.0.0:0,172.16.0.123:5060
    O=2 <public=s0/p0:0>0.0.0.0:0,0.0.0.0:0 SP=6000
UNTRUSTED NAT-ID=3 xop=80:1770 noQoS MP=
```

```
    I=3 <private=s1/p0:0>192.168.0.10:53,192.168.0.123:0
    O=3 <private=s1/p0:0>0.0.0.0:0,192.168.0.123:0 SP=6000
3 NAT-Flows
```

The following explains the show mbcd flows output in detail:



show mbcd realms

The **show mbcd realms** command displays steering ports and bandwidth usage for home, public, and private realms by using the **show mbcd realms** command.

For example:

```
ACMEPACKET# show mbcd realms
18:46:29-2819
             --- Steering Ports ---  ----------- Bandwidth Usage ----
------
Realm       Used   Free  No Ports    Flows Ingrss Egress  Total  Insuf BW
acme           0      0         0        0     0K     0K     0K         0
h323172        0  30001         0        0     0K     0K     0K         0
sip172         2  29999         0        0     0K     0K     0K         0
sip192         2  29999         0        0     0K     0K     0K         0
```

The information displayed includes the following:

- Used—Number of steering ports used
- Free—Number of free steering ports
- No Ports—Number of times that a steering port could not be allocated
- Flows—Number of established media flows
- Ingress—Amount of bandwidth being used for inbound flows
- Egress—Amount of bandwidth being used for outbound flows
- Total—Maximum bandwidth set for this realm
- Insuf BW—Number of times that a session was rejected due to insufficient bandwidth.

You can also add a configured realm name which to display specific information about by using the **show mbcd realms <realm-name>** command. This information is given for period and lifetime durations.

For example:

```
ACMEPACKET# show mbcd realms sip172
18:47:31-2881 Realm=sip172
                           -- Period -- -------- Lifetime --------
                  Active    High   Total      Total  PerMax    High
Ports Used             2       2      18         18      18       2
```

```
Free Ports          29999    30001    30017      30017    30017    30001
No Ports Avail          -        -        0          0        0        -
Ingress Band           0K       0K        0          0        0       0K
Egress Band            0K       0K        0          0        0       0K
BW Allocations          0        0        0          0        0        0
Band Not Avail          -        -        0          0        0        -
Total Bandwidth=0K

Steering Ports: 100% Success
```

The information displayed includes the following:

- Ports Used—Number of ports used
- Free Ports—Number of free ports
- No Ports Avail—Number of times no steering ports were available
- Ingress Band—Amount of bandwidth used for inbound flows
- Egress Band—Amount of bandwidth used for outbound flows
- BW Allocations—Number of times that bandwidth was allocated
- Band Not Avail—Number of times a session was rejected due to insufficient bandwidth

show mbcd rules-natalg

The **show mbcd rules-natalg** command displays the number of configured static flows. Because internally to the Net-Net 9200 a static flow is configured as a ALG NAT entry, they show up here. For example:

```
ACMEPACKET# show mbcd rules-natalg
NatAlg Rules: 0
```

show mbcd sessions-natalg

The **show mbcd sessions-natalg** command displays the number of static flow sessions, created as NAT ALG s, listed by protocol.

```
ACMEPACKET# show mbcd sessions-natalg
NatAlg UDP Sessions: 0
NatAlg TCP Sessions: 0
```

show mbcd forked-session

The show mbcd forked-session command takes a forked call ID argument. This command displays the forkedSession table with the ingress and egress resource table entries. For example:

```
ACMEPACKET# show mbcd forked-session
pmultiringcorrelator@192.168.200.139
ForkedSessionEntry: pmultiringcorrelator@192.168.200.139
InResourceTable :
ForkedSessionResourceEntry: net2001
maxbwallocated = 200
Flows :
Flow id = 65537 bw = 200 bwi = 200 bwe = 200
Flow id = 65539 bw = 200 bwi = 0 bwe = 0

ForkedSessionResourceEntry: net11
maxbwallocated = 200
Flows :
```

```
Flow id = 65538 bw = 200 bwi = 200 bwe = 200
Flow id = 65540 bw = 200 bwi = 0 bwe = 0

OutResourceTable :
ForkedSessionResourceEntry: net11
maxbwallocated = 200
Flows :
Flow id = 65537 bw = 200 bwi = 200 bwe = 200
Flow id = 65539 bw = 200 bwi = 0 bwe = 0

ForkedSessionResourceEntry: net2001
maxbwallocated = 200
Flows :
Flow id = 65538 bw = 200 bwi = 200 bwe = 200
Flow id = 65540 bw = 200 bwi = 0 bwe = 0
```

Note: Do not execute the **show mbcd forked-session** command on a loaded production system. The output's load on the Net-Net 9200 could interrupt call processing.

MBCD CPU Load Limiting

See MBCD Load Limiting (234) for a description on how to enable MBCD CPU load limiting.

SIP Session Management

You can query and view information about currently established SIP sessions. Because there can be a large number of sessions active at one time, the commands explained in this section may take several seconds to complete. This delay accommodates no net impact on active call processing. If the command requires many seconds to find a match, the system will display status messages to show progress.

All search terms in the following commands are implemented as substring filters. This means sessions matching any part of the string entered will be displayed (i.e., specifying the substring "168" will match sessions with "192.168.1.1" or "1.1.1.1:1680").

Note: The **show sip sessions <argument>** command described in this section should not be confused with the **show sip sessions** command, entered without any arguments, which displays cumulative counts of all SIP sessions active on the Net-Net 9200.

show sip sessions

The following commands must all begin with **show sip sessions**. All variations of the **show sip sessions** command display one or more SIP sessions entries. The

following is an example of such an output. After specifying the argument, enter a search term. The following is an sample output of a matching session.

```
------------------------------------------------------------
Session ID=0-000004 <ESTABLISHED=86398.474>
    ingress=private egress=public media=65537 lic (1 dialog)
    CallID=1-6818@192.168.1.211
    From=sipp <sip:sipp@192.168.1.211:5060>;tag=1
    To=sut <sip:service@192.168.1.85:5060>;tag=1
  Client Dialog ID=0-000007 <CONFIRMED>
   other=0-000006 ses=0-000004 media=65537 trans=UDP
    CallID=1-6818@192.168.1.211;realm=public
    Local=sipp <sip:sipp@192.168.1.211:5060>;tag=1;seq=1
    Remote=sut <sip:service@192.168.1.85:5060>;tag=1;seq=0
    RemoteTgt=<sip:192.168.200.211:5060;transport=UDP>;UDP
    LocalTgt=sip:sipp@192.168.200.85:5060
    branch=1elksi45l36g35o8r7gss35bv0
  Server Dialog ID=0-000006 <CONFIRMED>
   other=0-000007 ses=0-000004 media=65537 trans=UDP
    CallID=1-6818@192.168.1.211;realm=private
    Local=sut <sip:service@192.168.1.85:5060>;tag=1;seq=0
    Remote=sipp <sip:sipp@192.168.1.211:5060>;tag=1;seq=1
    RemoteTgt=sip:sipp@192.168.1.211:5060;UDP
    LocalTgt=<sip:192.168.1.85:5060;transport=UDP>
    branch=1ekv7h46rr4ckuvhq7d0ta9961
  Media ID=65537 <Talking|NONE>
    [private:65538]+a 192.168.1.211:6000<=192.168.1.235:10000
    [public:65537]+a 192.168.200.235:20000=>192.168.200.211:6000
  Forward codec audio/PCMU p='0' bw='0' fpp='0' param='ptime=10'
peakr='0' avgr='0' mbs='0' sdp-rl='0' sdp-bw='disabled' pref='65536'
  Reverse codec audio/PCMU p='0' bw='0' fpp='0' param='ptime=10'
peakr='0' avgr='0' mbs='0' sdp-rl='0' sdp-bw='disabled' pref='65536'
 Call Duration (in seconds): 1
------------------------------------------------------------
```

all

The **show sip sessions all** command displays all active sessions.

by-to

The **show sip sessions by-to** command requires a <username> argument and matches this username as a substring to anything found in the “To=” line, after the “=”. For example:

```
show sip sessions by-to <username>
```

by-from

The **show sip sessions by-from** command requires a <username> argument and matches this username as a substring to anything found in the “From=” line, after the “=”. For example:

```
show sip sessions by-from <username>
```

by-ip

The **show sip sessions by-ip** command requires an <IP> argument and matches this IP as a substring to anything found in the “RemoteTgt=” line, after the “=”. There can be multiple RemoteTgt lines for a session. For example:

```
show sip sessions by-ip <IP>
```

by-media

The **show sip sessions by-media** command requires a <media> argument and matches this text as a substring to anything found in the "MediaID=" section, after the "=". There multiple pieces of information in this section of a session's description, including transcoding information. For example:

```
show sip sessions by-media <media>
```

by-call-id

The **show sip sessions by-call-id** command requires a <call-id> argument and matches this call ID as a substring to anything found in the "CallID=" line, after the "=". There can be multiple CallID lines for a session. For example:

```
show sip sessions by-call-id <call-id>
```

by-agent

The **show sip sessions by-agent** command requires an <agent> argument and matches this agent as a substring to anything found in the "From=" or "To=" lines, after the "=" signs. For example:

```
show sip sessions by-agent <agent>
```

Session Agent Registration Management

The Net-Net SBC includes provisions to explicitly invalidate current registrations in certain instances with the **reset session-agent** command. If the registrar, configured as a session agent, goes out of service, the SBC can invalidate the current endpoint registrations to that session agent. Thus, after resetting the session agent, the Net-Net SBC acts as if the registrations have expired, and forces the endpoints to re-register with the registrar. The command is entered as follows:

```
reset session-agent <session-agent-name>
```

Short Duration Session Monitoring

A short duration sessions is defined as an answered session that has lasts only a short duration. If the number of short duration sessions received exceeds the configurable threshold within the configurable burst window, then an SNMP trap will be sent.

Short session statistics shows up in the **show sip realm** display.

Short Duration Session Trap

You can configure a number of short sessions that fall within a specific window of time that will set the apSysMgmtShortSessionExceedTrap.

ACLI Instructions and Examples

To configure short duration session monitoring:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ```

3. Type **session-router** and press <Enter>. You can now begin configuring the short duration session monitoring feature.

   ```
   ACMEPACKET(session-router)# session-router
   ACMEPACKET(session-router-config)#
   ```

4. **short-session-duration**—Enter the maximum length of time in seconds that defines a session as short duration. A value of 0 disables this feature.
5. **short-session-threshold**—Enter the number of active sessions, within the short duration window, that must occur to trigger the short session warning trap. A value of 0 disables this feature.
6. **short-session-window**—Enter the length of time in seconds that defines the burst window used to determine if a short session warning trap should be sent.
7. Save your work using the ACLI **done** command.

Clear SIP and H.323 Sessions

The Clear Sessions function gracefully terminates a group of SIP or H.323 sessions from the ACLI. IWF sessions are considered both SIP and H.323 and can be cleared from either SIP or H.323.

Clearing SIP Sessions

The Net-Net 9200 clears SIP sessions by sending BYE messages to the originator and terminator. SIP initial and early sessions are cleared by sending a CANCEL message to the terminator and an error response to the originator.

Only sessions created by INVITE messages may be cleared by this feature, thus subscriptions would not be affected. Sessions in TERMINATED state are not cleared.

Clearing H.323 Sessions

The Net-Net 9200 clears H.323 sessions by sending release messages with cmReasonTypeUndefinedReason, reason code 8 (Preemption) to endpoints when clearing them. The CDR terminate-cause for this action is "Admin-Reset"

Rate Limiting

As a single clear sessions command could potentially tear down thousands of sessions, the Net-Net SBC's provides a mechanism to moderate the tear down rate as the CPU load grows to high levels. At 0% CPU usage, clear session requests are sequentially performed every 1 ms. At 100% CPU usage, requests are sequentially performed every 500 ms. Clear request intervals are scaled upward as CPU load increases.

System State

In order to prevent the Net-Net SBC from creating new sessions as it clears existing sessions, you must set the application protocol of the calls you are canceling in an off-line state. While a protocol is offline, it will not accept new sessions, although administrative tasks may still be performed. When the system state is set to offline, sessions and new registrations are rejected with 503 (SIP) or cmReasonTypeNoBandwidth (H.323) reasons. Established sessions and registrations will be allowed to operate as normal while system state is offline. Omitting the protocol argument ([sip | h323]) puts both protocols in the specified mode. The syntax is as follows:

```
set system-state <online | offline> [h323 | sip]
```

For example:

```
set system-state offline sip
```

ACLI Instructions and Examples

The clear sessions command is used to gracefully terminate existing sessions. The syntax is as follows:

```
clear sessions <h323 | sip> <all | by-agent <SA-name> | by-call-id
<call-id> | by-ip <ip-addr> | by-user <username>>
```

- `<h323 | sip>` - Protocol of sessions to clear. For IWF session, choose one leg of the call to terminate first and use that leg's protocol.
- `all` - Clear all sessions for the protocol
- `by-agent` <**SA-name**> - Clear sessions originating or terminating from session-agent: <SA-name>
- `by-call-id` <call-id> - Clear session with call id: <call-id>
- `by-ip` <**ip-addr**> - Clear sessions originating or terminating from a client or server dialog URI IP address: <ip-addr> (found in the To:, From" or Contact: headers)
- `by-user` <**username**> - Clear sessions originating or terminating from client or server dialog URI username: <username> (found in the To:, From: or Contact: headers)

For example:

```
ACMEPACKET# clear sessions sip by-ip 192.168.44.55
```

Show sessions and show virtual-interfaces

The show sessions command allows you to determine the total sessions on the Net-Net 9200 over Period and Lifetime monitoring spans.

The show virtual-interfaces command shows the virtual interfaces for the Net-Net 9200 signaling services; for example, SIP-NAT external address, H.323 interface (stack) IP interface, and MGCP IP interface.

These two commands are useful for determining:

- Total sessions on the Net-Net 9200
- IP addresses in use by protocol

ACLI Instructions and Examples

Show sessions

To display sessions over a period or lifetime:

1. In either User or Superuser mode, type **show sessions** at the prompt.

```
ACMEPACKET# show sessions

ACMEPACKET > show sessions
Session Statistics            -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High

Total Sessions           0       -       -          0       -       -
SIP Sessions             0       0       0          0       0       0
H.323 calls              0       0       0          0       0       0

IWF Statistics                -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
```

Show virtual-interfaces

To display virtual interfaces for signaling serves:

1. In either User or Superuser mode, type **show virtual-interfaces** at the prompt.

```
ACMEPACKET# show virtual-interfaces
```

```
ACMEPACKET > show virtual-interfaces
intf phy-name vlan  ip-addr         realm     type
0/0  access   0     172.16.34.131   Realm172  sip-port
1/0  backbone 0     192.168.34.131  Realm192  sip-port
```

SIP Media and Transcoding Statistics

Media-processing statistics per SIP traffic is viewable with the **show sip codecs** command. This command displays statistics per realm and requires a realm argument.

Session Based Statistics

Three statistics are session based. They are the transcoded, transrated, and transparent counts.

- transcoded—counts of sessions that use the Net-Net 9200's TCUs to transcode between two or more codes.
- transrated—counts of sessions that use the Net-Net 9200's TCUs change the packetization interval among dialogs in the session.
- transparent—counts of sessions that require no TCU hardware intervention (all end-to-end media uses the same codec)

A value of "none" which is not counted in the statistics is set when there is no media at all or media is not yet negotiated. Sessions within the same realm are counted only once.

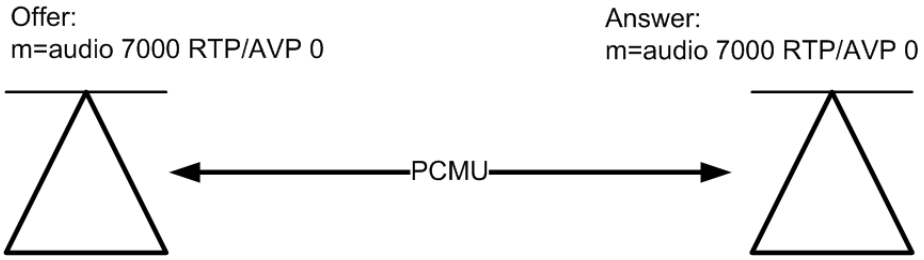
These are meter type counters, and thus have an "active" count as well as total lifetime values. The media-processing state of the session only can increase in precedence (highest=transcoded, transrated, transparent, lowest=none). Thus, if a session begins as transcoded, and then is re-negotiated to transparent later by a re-INVITE, it is still considered transcoded. However, if a session begins as transparent, it can go to transcoded by a re-INVITE. In such a case, the total counts for both transparent and transcoded would be incremented. If there are several media lines, the highest precedence is used for the session.

Flow Based Statistics

The remaining 16 lines of the **show sip codecs** command track the number of codecs in established sessions. Only the Recent-Total and other lifetime columns are populated; the Active and Recent High are not applicable. Theses counts represent each SDP m= line emanating in the queried realm. Refer to the following examples:

Example 1

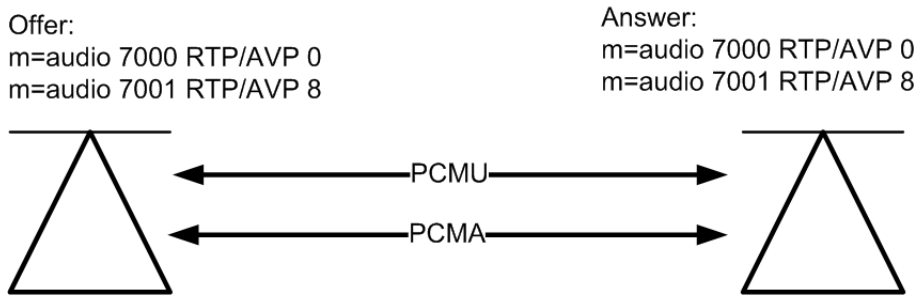
The following diagram shows an intra-realm session with one audio stream using the PCMU codec. Once the session is established, the PCMU count in the **show sip codecs** output is 2.



If the session originator and terminator in the previous diagram exist in two different realms, you must execute the **show sip codecs** command twice, once for each realm. A single PCMU count will be reflected in each respective query because only one m= line emanates from each realm.

Example 2

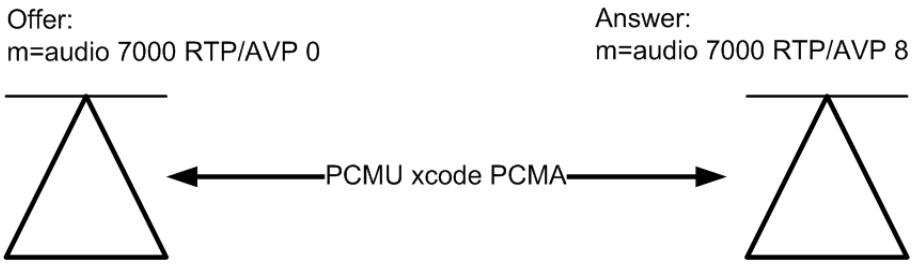
The following diagram shows an intra-realm session with two audio steams. Each stream uses a different codec. Once the session is established, the PCMU count in the **show sip codecs** output is 2, and the PCMA count is 2.



If the session originator and terminator in the previous diagram exist in two different realms, you must execute the **show sip codecs** command twice, once for each realm. A single PCMU count and a single PCMA count will be reflected in each respective query because two m= lines emanate from each realm.

Example 3

The following diagram shows an intra-realm transcoding scenario where the originator and terminator are using different audio codecs. The Net-Net 9200 is performing transcoding functions, which are invisible to the endpoints. Once the session is established, the PCMU count in the **show sip codecs** output is 1, and the PCMA count is 1.



If the session originator and terminator in the previous diagram exist in two different realms, you must execute the **show sip codecs** command twice, once for each realm.

A single PCMU count appears in one query and a single PCMA count appears in the other query because only one m= line emanate from each realm.

An example **show sip codecs** command follows:

```
ACMEPACKET# show sip codecs public
13:37:29-59 Codec statistics
                          ---- Recent ---- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
Transcoded               0       0       0          0       0       0
Transrated               0       0       0          0       0       0
Transparent              0       0       0          0       0       0
PCMU Count               -       -       0          0       0
PCMA Count               -       -       0          0       0
G722 Count               -       -       0          0       0
G723 Count               -       -       0          0       0
G726-16 Count            -       -       0          0       0
G726-24 Count            -       -       0          0       0
G726-32 Count            -       -       0          0       0
G726-40 Count            -       -       0          0       0
G728 Count               -       -       0          0       0
G729 Count               -       -       0          0       0
GSM Count                -       -       0          0       0
iLBC Count               -       -       0          0       0
H261 Count               -       -       0          0       0
H263 Count               -       -       0          0       0
T38 Count                -       -       0          0       0
Other Count              -       -       0          0       0
```

QOS Management

QoS Commands

The Net-Net 9200 includes several commands used to debug, validate, and monitor QoS statistic gathering.

show qos errors

The **show qos errors** command displays debug-level QoS exception statistics. For example:

```
ACMEPACKET# show qos errors

QOS Exception Statistics:

qos delete failed               0
qos_gimp0_err:                  0
qos_gimp1_err:                  0
qos bad control struct:         0
qos update bad handle:          0
qos get handle fail:            0
cross connect failure:          0
qos update - invalid handle:    0
qos add no handle avail:        0
qos free already err:           0
qos update pend err:            0
qos del handle release err:     0
```

```
qos update unsetpend err:        0
OFD table exception:             0
qos free queue empty:            0
qos no adjacent free entries:    0
Semaphore error on add:          0
Semaphore error on delete:       0
Semaphore error on show:         0
Semaphore error on isr:          0
Semaphore error on write:        0
```

show qos statistics

The **show qos statistics** command displays QoS processing statistics. For example:

```
ACMEPACKET# show qos statistics

QOS Processing Statistics:

qos adds received:               0
qos adds completed:              0
qos deletes received:            0
qos deletes completed:           0
```

show qos flow

The **show qos flow** command is used to view live QoS statistics about currently active calls. This command requires a flow ID argument in order to show the flow statistic for a specified call. The flow ID is a hexadecimal value given by the FPGA_handle field as displayed in the show nat by-index command.

Reset QoS Statistics

You can reset the accumulated QoS statistics with the **reset qos** command. For example:

```
ACMEPACKET# reset qos
```

Application Load Limiting

SIP Load Limiting

You can set load limiting for all SIP tasks using the **set sip limit** command. The SIP load limit default is 80%. A value of 0 disables the load limiting function. When load-limiting is triggered, the Net-Net 9200 rejects the computed percentage (100 minus the load-limit) of requests that are outside of a dialog. For example:

```
ACMEPACKET# set sip limit 75
```

SIP load limiting can also be configured upon boot within the sip-config. In the options parameter, add **load-limit=**<x>, where x = the load limit percentage.

MBCD Load Limiting

You can set load limiting for the MBCD task using the **set mbcd limit** command. The MBCD load limit default is 80%. A value of 0 disables the load limiting function. When load-limiting is triggered, the Net-Net 9200 rejects the computed percentage (100 minus the load-limit) of flow ADDs. For example:

```
ACMEPACKET# set mbcd limit 75
```

Media load limiting can also be configured upon boot within the media-manager. In the options parameter, add **media-load-limit=**<x>, where x = the load limit percentage.

NATM Load Limiting

You can set load limiting for the NATM task using the **set nat limit** command. When load-limiting is triggered, the Net-Net 9200 drops signaling packets. A value of 0 disables the load limiting function; the default is 80%.

Once NATM task limiting is enabled because of an overload condition, the Net-Net 9200's drop rate scales linearly from 0 to the nat drop rate value at 100% CPU. The NAT drop rate default is 20%. You can optionally set the NAT drop rate using the **set nat limit** command.

NAT load limiting is entered as:

```
ACMEPACKET# set nat limit <limit> [<nat drop rate>]
```

NAT load limiting can also be configured upon boot within the media-manager. In the options parameter, add **nat-load-limit=**<x>, where x = the load limit percentage. Add **nat-load-drop=**<x>, where x = the nat load drop rate.

> **Note:** natm statistics are absent from SPU2/NPU2-based systems for architectural reasons.

SFE Load Limiting

You can set load limiting for the SFE task using the **set sfe limit** command. When load-limiting is triggered, the Net-Net 9200 drops signaling packets. A value of 0 disables the load limiting function; the default is 95%.

Once SFE task limiting is enabled because of an overload condition, the Net-Net 9200's drop rate scales linearly from 0 to the sfe drop rate value at 100% CPU. The SFE drop rate default is 20%. You can optionally set the SFE drop rate using the **set sfe limit** command.

SFE load limiting is entered as:

```
ACMEPACKET# set sfe limit <limit> [<drop rate>]
```

SFE load limiting can also be configured upon boot within the media-manager. In the options parameter, add **sfe-load-limit=**<x>, where x = the load limit percentage. Add **sfe-load-drop=**<x>, where x = the SFE load drop rate.

H.323 Load Limiting

You can set load limiting for all H.323 tasks using the **set h323 limit** command. The H.323 load limit default is 80%. A value of 0 disables the load limiting function. When load-limiting is triggered, the Net-Net 9200 rejects the computed percentage (100 minus the load-limit) of requests. For example:

```
ACMEPACKET# set h323 limit 75
```

H.323 load limiting can also be configured upon boot within the h323-config. In the options parameter, add **load-limit=**<x>, where x = the load limit percentage.

Transcoding Management

The Net-Net 9200 includes several commands used to debug, validate, and monitor transcoding sessions.

Xcode Server Commands

One xcode server runs on each the TCU's four cores and is responsible for controlling sessions and resources on each TCM. The following show commands are used to query the xserver and display real time statistics. The **show xserv** command usage is as follows:

```
show xserv <xserv identified by core> [api-stats | sessstats <session>
| stats | sysinfo | dbginfo | devinfo <session> | dsp-events | dsp-
channel <device ID> <channel ID> | dsp-device <device ID> | dsp-status
<device ID>]
```

The location argument for the show xserv command works exclusively for: slots 4, 5, and 6; CPUs 0 and 1; cores 0 and 1.

show xserv stats

The **show xserv stats** command displays the 10 DSPs' loads on a TCM. The location argument you supply corresponds with an xserv that control a TCM. It also shows total sessions, created, located, free, allocated, and lost. For example:

```
ACMEPACKET# show xserv 4.0.0 stats

################## RESOURCE STATS ##########################

 Total Sessions Created = 1000
 Total Sessions Located = 1000
 Total Sessions FREE    = 0992
 Total Sessions ALLOC'd = 0008
 Total Sessions Lost    = 0000
 Current Device Loading:
    Device00: 00.00%
    Device01: 00.00%
    Device02: 01.00%
    Device03: 01.00%
    Device04: 01.00%
    Device05: 01.00%
    Device06: 01.00%
    Device07: 01.00%
    Device08: 01.00%
    Device09: 01.00%
 Max Device Loading:
    Device00: 00.00%
    Device01: 00.00%
    Device02: 01.00%
    Device03: 01.00%
    Device04: 01.00%
    Device05: 01.00%
    Device06: 01.00%
    Device07: 01.00%
    Device08: 01.00%
    Device09: 01.00%
```

show xserv api_stats

The **show xserv api_stats** command displays communication statistics about communication between xserver and xclient. For example:

```
ACMEPACKET# show xserv 4.0.0 api_stats

Xserv Msg/API Stats
===================
Total     Alloc's   Update's  Free's    Queries   Register  Heartbeat Dropped
=====     =======   ========  ======    =======   ========= ========= =======
104       8         0         0         3         0         92        0
```

show xserv audit-alloc

The **show xserv audit-alloc** displays session allocation information about the selected xserver's sessions. For example:

```
ACMEPACKET# show xserv 4.0.0 audit-alloc

################# RESOURCE AUDIT ALLOC ######################

Device: 0
Device: 1
Device: 2
Session idx: 0x0000          Session ID: 0x30000000 ALLOCATED
Device: 3
Session idx: 0x0000          Session ID: 0x40000000 ALLOCATED
Device: 4
Session idx: 0x0000          Session ID: 0x50000000 ALLOCATED
Device: 5
Session idx: 0x0000          Session ID: 0x60000000 ALLOCATED
Device: 6
Session idx: 0x0000          Session ID: 0x70000000 ALLOCATED
Device: 7
Session idx: 0x0000          Session ID: 0x80000000 ALLOCATED
Device: 8
Session idx: 0x0000          Session ID: 0x90000000 ALLOCATED
Device: 9
Session idx: 0x0000          Session ID: 0xa0000000 ALLOCATED

 Total Sessions Located = 1000
 Total Sessions ALLOCATED = 8000
```

show xserv audit-free

The **show xserv audit-free** displays session information about the selected xserver's free sessions.

show xserv audit-lost

The **show xserv audit-lost** displays information about lost sessions, those neither free nor allocated for a selected xserver's sessions. For example:

```
ACMEPACKET# show xserv 4.0.0 audit-lost

################# RESOURCE AUDIT LOST ######################

Device: 0
Device: 1
Device: 2
Device: 3
Device: 4
Device: 5
Device: 6
Device: 7
Device: 8
Device: 9
 Total Sessions Located = 1000

 Total Sessions LOST = 0000
```

show xserv audit-full

The **show xserv audit-full** command displays information about all session on a xserver. Use care in executing this command because the output of this command for a highly loaded xserver can span many screens.

show xserv api-stats

The **show xserv api-stats** command shows software/API information for an xserver application. For example:

```
ACMEPACKET# show xserv 4.0.0 api_stats

Xserv Msg/API Stats
====================
Total     Alloc's   Update's  Free's    Queries   Register  Heartbeat
Dropped
=====     =======   ========  ======    =======   ========= =========
=======
26344     5360      5041      4941      2         0         10994     0
```

show xserv dbginfo

The **show xserv dbginfo** displays debug information for various transcoding process counters.

```
ACMEPACKET# show xserv 4.0.0 dbginfo
GetDebugInfo
csmQStats:
    QgetCnt=00000000
    QputCnt=17560000
gtlQStats:
    QgetCnt=17560000
    QputCnt=00000000
TX pktStats:
    csmCnt_tx_csmwrite     =17540000
    csmCnt_tx_queueblock   =17540000
    csmCnt_tx_addblock     =17540000
    csmCnt_tx_sendblock    =17540000
    csmCnt_tx_Cmddosend    =17540000
    csmCnt_tx_Ackdosend    =75300000
    csmCnt_tx_sendto       =25080000

RX pktStats:
    csmCnt_rx_readPacket   =25080000
    csmCnt_rx_handlePacket =25080000
    csmCnt_rx_controlPacket=25070000
    csmCnt_rx_dataPacket   =00000000
    csmCnt_rx_noopPacket   =10000000
    csmCnt_rx_csmcallback  =17560000
    csmCnt_rx_msgQSend     =17560000
    csmCnt_rx_msgQReceive  =17560000
    csmCnt_rx_gtlreadcb    =17560000
    csmCnt_rx_response     =17550000
    csmCnt_rx_event        =10000000

GTL ethStats:
    mSentCount             =17540000
    mReSentCount           =00000000
    mAckableSentCount      =17540000
    mAckCount              =17540000
```

```
    mRecvCount             =75300000
    mDupRecvCount          =20000000
    mNoopCount             =00000000
    mLastSentCmdSeqNum     =10000000
    mLastRecvdAckSeqNum    =10000000
    mLastRecvdRespSeqNum   =30000000
    mLastSentAckSeqNum     =30000000
    mBlockWaitingForAck    =00000000
```

show xserv session

The **show xserv session** command displays the source and destination IP address and port associated with a transcoded call's NAT flow. This command requires a session ID argument and is entered in the form:

show xserv <slot.CPU.core> session <transcoding_sessionID>

For example:

```
ACMEPACKET# show xserv 4.0.0 session 0xa0000

        GetSessionInfo() for session: a0000

################# SESSION  a0000000 ##################

Channel 0:
   Conf ID    = 0xa0000000
   MSP device = 9
   MSP chan   = 10
   MSP conf   = 0
   SrcIP      = 0.0.0.0:0
   DstIP      = 0.0.0.0:0

Channel 1:
   Conf ID    = 0xa0000000
   MSP device = 9
   MSP chan   = 11
   MSP conf   = 0
   SrcIP      = 0.0.0.0:0
   DstIP      = 0.0.0.0:0
```

show xserv sessstats

The **show xserv sessstats** command displays session Ethernet statistics associated with a given session. It also displays transcoding information about the session. This command requires a session ID argument and is entered in the form:

show xserv <slot.CPU.core> sessstats <transcoding_sessionID>

For example:

```
ACMEPACKET# show xserv 4.0.0 sessstats 0xa0000

        GetSessionStats() for session: a0000

################# SESSION  0xa0000 ##################

Channel 0:
   MSP device   = 9
   MSP chan     = 10
   Src IP:Port          = 0.0.0.0:0
```

```
   Dst IP:Port          = 0.0.0.0:0
   Codec                = G711_ULAW_PCM
   RTP Payload Type     = 00
   RTP Pkt Interval     = 20 msec
   LL Trancoding        = DISABLED

MSP Counters:
   CallTimerSecs      0x4cd


   TXVoicePkts        0x00000000
   RXVoicePkts        0x00000000
   RXVoiceOctets      0x00000000

   TXCmfNoisePkts     0x00000000
   RXCmfNoisePkts     0x00000000

   TXSigPkts          0x00000000
   RXSigPkts          0x00000000

   BuffOvflowDiscard  0x00000000
   OutOfSeqPkts       0x00000000
   BadHeaderPkts      0x00000000
   LatePkts           0x00000000
   EarlyPkts          0x00000000
   LostPkts           0x00000000
   FormatRev          0x40000000
```

show xserv sysinfo

The **show xserv sysinfo** command displays a high level overview for the given xserver. For example:

```
ACMEPACKET# show xserv 4.0.0 sysinfo

-------------------------------------------
XSERVER System Info
-------------------------------------------
core ID         : 0
cpu  ID         : 0
slot ID         : 0
tile ID         : 0
numDevices      : 10
numTiles        : 1
sessions per DSP: 100
FAX      per DSP: 5
Initialized     : 1
Active DSP count: 10
Avail Sess count: 1000
Avail Fax  count: 50
Free  Sess count: 992
Free  Fax  count: 50
VAPI Initialized: 1
```

show xserv red-peers

The **show xserv red-peers** command displays redundancy information about this xserver's redundant peer on a separate TCU. For example:

```
ACMEPACKET# show xserv 4.0.0 red-peers

Redundancy Peer @ 169.254.165.0:8012 -------------------------
Status          : FOUND!
IP Port         : 169.254.165.0:8012
Object ID       : ObjectId [NONE:0]
Trans  ID       : 0
RedState (ours) : 1, ACTIVE
RedState (peer) : 0, INITIAL
Sync State      : 0, None
```

show xserv devinfo

The **show xserv dev-info** command shows device information for a supplied session running on a defined xserver application. You must supply a session ID for this show command. For example:

```
ACMEPACKET# show xserv 4.0.0 devinfo 0x10000
        GetDeviceInfo() for session: 10000
 GetDeviceInfo() stub
################## Device Stats  10000000 ##################

Device ID: 0:
    MSP device   = 0
****************** EMAC Stats *******************
    RxDroppedPkts      0x00000000
    RxPktErrors        0x00000000
****************** ETH Stats *******************
    TxFrames           0x7d76b500
    RxFrames           0x687b2f00
    TxVLANFrames       0x7ae83900
    RxVLANFrames       0x65ebac00
    RxBcastPkts        0x10700000
    RxERIFFrames       0x00000000
    UnknownBcstPkts    0x00000000
    UnknownPktType     0x00000000
****************** IP Stats *******************
    TxFrames           0x7ae83900
    RxFrames           0x65eca000
    FragPkts           0x00000000
    BadIPChecksum      0x00000000
    BadUDPChecksum     0x00000000
    UnknownProt        0x00000000
    UnknownIPAddr      0x9de30000
    UnknownPort        0x00000000
```

show xserv dsp-events

The **show xserv dsp-events** command views the DSP events trace per xserver's DSPs.

show xserv dsp-channel

The **show xserv dsp-channel** command shows information about a DSP devices selected channel on a given xserver. A DSP device ID and channel ID are required, in addition to specifying an Xserver. The command is entered as:

```
show xserver <core> dsp-channel <device ID> <channel ID>
```

For example:

```
ACMEPACKET# show xserv 4.0.0 dsp-channel 0 0
DSP Channel Info for Device=0 Channel=0
-------------------------------------------
DSP Device ID: 0
CHANNEL 0
-------------------------------------------
channel address      : 0xc2082a38
device address       : 0xc20829f0
callback function    : 0xc11a6588
request list         : 0xd5daecb0
connection ID        : 0x0
connection Type      : 2
connection State     : 3
connection Mode      : 0
MSP Channel ID       : 0
TDM timeslot         : 0
channel param pointer: 0xd5daf150
channel param[0]     : 0xd5daef80
channel param[1]     : 0xd5daf150
Message Index        : 8
Payload Type         : 0
Codec                : 0
```

show xserv dsp-device

The **show xserv dsp-device** command shows information about a DSP device on a given xserver. A DSP device ID is required, in addition to specifying an Xserver. For example:

```
ACMEPACKET# show xserv 4.0.0 dsp-device 0
Supervisor Channel Info for active DSP devices
-------------------------------------------
DSP Device ID: 0
CHANNEL SUPV
-------------------------------------------
channel address      : 0xc20b56bc
device address       : 0xc20829f0
callback function    : 0x0
request list         : 0xd5d3a130
connection ID        : 0x0
connection Type      : 0
connection State     : 0
connection Mode      : 0
MSP Channel ID       : 65535
TDM timeslot         : 0
channel param pointer: 0x0
Message Index        : 173
```

show xserv dsp-status

The **show xserv dsp-status** command shows information about the TCM's DSPs which a given xserver controls. A DSP device ID is required, in addition to specifying an Xserver. For example:

```
ACMEPACKET# show xserv 4.0.0 dsp-status 0

-------------------------------------------
DSP Hardware Device Status
```

```
-------------------------------------------
 ID  State   Mode   EthHdrSet
  0     4     1          0
  1     4     1          0
  2     4     1          0
  3     4     1          0
  4     4     1          0
  5     4     1          0
  6     4     1          0
  7     4     1          0
  8     4     1          0
  9     4     1          0
```

Xcode Client Commands

The xcode client communicates with the xcode server to request and set up transcoding sessions. The following show commands are used to query the xclient and display real time statistics. The **show xclient** command usage is as follows:

```
show xclient [api-stats | session-bitinfo | session-byid | session-
byipp | session-cache | sessions | status | xlist | xserv-lock]
```

show xclient status

The **show xclient status** command displays an overview of the xclient. Information displayed includes the xclient state, number of xservers the xclient connects to, and whether the xclient to xserver communication is synchronous (non-blocking) or asynchronous (blocking). For example:

```
ACMEPACKET# show xclient status
xclient state: Created
        xserver count: 8
        XClient->XServ msg state: ASYNC
        Total Sessions:             16
        Licensed AMR Sessions:      16 of 25
        Licensed AMR-WB Sessions:    0 of 50
        Licensed EVRC Sessions:      0 of 75
        Licensed EVRCB Sessions:     0 of 100
```

show xclient sessions

The **show xclient sessions** command displays the number and session ID of cached transcoding sessions. For example:

```
ACMEPACKET# show xclient sessions
Requesting xclient sessions table
Total Active Sessions:8
Session Id: 0x30000 * cached *
Session Id: 0x40000 * cached *
Session Id: 0x50000 * cached *
Session Id: 0x60000 * cached *
Session Id: 0x70000 * cached *
Session Id: 0x80000 * cached *
Session Id: 0x90000 * cached *
Session Id: 0xa0000 * cached *
```

show xclient xlist

The **show xclient xlist** displays the xservers connected to the xclient, and the xservers' internal IP address and status. For example:

```
ACMEPACKET# show xclient xlist
```

```
Requesting XClient's list of XServers:

  State  VA_addr              VC_addr              Slot   Id  Devices
  =====  ==================   ==================   ====   ==  ======-
Xserv_1: - Not Active/Lost HB.
XServ_2: 169.254.178.1:8012     169.254.164.1:8012     4     0   10
  HB_Found/Active
Xserv_3: - Not Active/Lost HB.
Xserv_4: - Not Active/Lost HB.
Xserv_5: - Not Active/Lost HB.
Xserv_6: - Not Active/Lost HB.
Xserv_7: - Not Active/Lost HB.
Xserv_8: - Not Active/Lost HB.
```

show xclient session-bitinfo

The **show xclient bit-info** command displays the session header for a given session. You must supply a session ID for this show command. It is entered as follows:

```
show xclient session-bitinfo <session-ID>
```

show xclient session-byid

The **show xclient session-byid** command shows session statistics for a supplied session. It is entered as follows:

```
show xclient session-byid <session-ID>
```

show xclient session-byipp

The **show xclient session-byipp** command shows session statistics for an endpoint's supplied IP address and port. It is entered as follows:

```
show xclient session-byipp <endpoint IP address> <port>
```

show xclient session-cache

The **show xclient session-cache** command displays the cached transcoding sessions. It is entered as follows:

```
show xclient session-cache
```

show xclient xserv-lock

The **show xclient xserv-lock** command shows if the xclient is forced to allocated resources to one xserver. For example:

```
ACMEPACKET# show xclient xserv-lock
xserv lock is not set
```

Realm Management

The following features are used for realm management.

Monthly Minutes-Based CAC Data

The Net-Net SBC's Call Admission Control (CAC) feature lets you configure the system to put time constraints on incoming networking calls. You can view current monthly minutes CAC data for a specified realm with the **show monthly-minutes** command. The usage is as follows:

```
show monthly-minutes <realm>
```

By not specifying a realm, data for all realms is displayed. The ACLI show monthly-minutes command displays the following information:

- How many minutes are configured for a realm
- How many of those are still available

- How many calls have been rejected due to exceeding the limit

For example:

```
ACMEPACKET# show monthly-minutes
Realm          MinutesAllowed  MinutesLeft       Minutes Exceed Rejects
------------    -------------  -----------        --------------------
                                                 Recent   Total  PerMax
private          0              0                   0         0       0
public           0              0                   0         0       0
```

Realm Specifics

You can display configuration information for configuration elements associated with a specific realm with the **show realm-specifics** command. The command's usage is as follows:

```
show realm-specifics <realm ID>
```

The information displayed includes the following configuration elements associated with the supplied realm:

- Realm configuration
- Steering pool
- Session agent
- Session translation
- Class policy
- Local policy (if the source realm or destination realm is defined)

H.323 Management

The Net-Net System provides numerous statistics and real-time operating parameters reflecting all aspects of its H.323 implementation.

H.323 Show Commands

H.323 processing spans several tasks on the Net-Net 9200. The following H.323 **show** commands display various details of SIP system functionality.

show h323 agentstats

The **show h323 agentstats** command displays H.323 session agent statistics. For example:

```
ACMEPACKET# show h323 agentstats


H323RasGk@1.4.1

15:22:06-33

                    ----- Inbound -----  ---- Outbound ----- -- Latency
--   Max

Session Agent      Active  Rate  ConEx  Active  Rate  ConEx    Avg
Max Burst

172.16.0.29      I    0  0.0     0    220  2.8     0  0.093  0.229   10
172.16.0.37      I    0  0.0     0      0  0.0     0  0.000  0.000    0
172.16.0.38      I    0  0.0     0      0  0.0     0  0.000  0.000    0
172.16.0.39      I    0  0.0     0      0  0.0     0  0.000  0.000    0
192.168.200.29   I  220  2.8     0      0  0.0     0  0.000  0.000    9
192.168.200.37   I    0  0.0     0      0  0.0     0  0.000  0.000    0
192.168.200.38   I    0  0.0     0      0  0.0     0  0.000  0.000    0
192.168.200.39   I    0  0.0     0      0  0.0     0  0.000  0.000    0
```

show h323 all

The **show h323 all** command displays all H.323 statistics stored on the Net-Net SBC. For example:

```
ACMEPACKET# show h323 all
14:27:42-349168 h323RasGk@0.4.1
H323 SESSIONS                      ---- Recent ---- -------- Lifetime -
-------
                         Active    High   Total     Total  PerMax    High
Total Sessions                0       0       0         0       0       0
Total Incoming  Sessions      0       0       0         0       0       0
Total Outgoing  Sessions      0       0       0         0       0       0
Total Connected Sessions      0       0       0         0       0       0
Total Incoming  Channels      0       0       0         0       0       0
Total Outgoing  Channels      0       0       0         0       0       0
Incoming  IWF Sessions        0       0       0         0       0       0
Outgoing  IWF Sessions        0       0       0         0       0       0
IWF Server Transactions       0       0       0         0       0       0
IWF Client Transactions       0       0       0         0       0       0

H323D Status     Current   Lifetime
Queued Messages        0          0
```

```
TPKT Channels          0          0
UDP Channels           0          0
AgentStats
No Session Agents
StackH323Stats
StackPvtStats
```

show h323 groupstats

The **show h323 groupstats** command displays H.323 session group statistics. For example:

```
ACMEPACKET# show h323 groupstats

H323RasGk@0.4.1
17:00:10-10

              ----- Inbound -----  ---- Outbound ----- -- Latency --  Max

SAG           Active  Rate  ConEx  Active  Rate  ConEx   Avg   Max Burst
H323Group        D    0   0.0     0    222  11.7     0  0.112  0.582    8
```

show h323 h323stats

The **show h323 h323stats** command displays H.323 message statistics. For example:

```
ACMEPACKET# show h323 h323stats
H323RasGk@1.4.1

STACK : h323172
H.225 : Sent    4       Recd    8       maxCPU  0
H245  : Msg     0       Ack     0       Rej     0       Rel     0
RAS   : Req    11       Ack    11       Rej     0       maxCPU  4

STACK : h323192
H.225 : Sent    0       Recd    0       maxCPU  0
H245  : Msg     0       Ack     0       Rej     0       Rel     0
RAS   : Req     0       Ack     0       Rej     0       maxCPU  0
```

show h323 load

The **show h323 load** command displays H.323 load limiting information. For example:

```
ACMEPACKET# show h323 load
H323RasGk@0.0.0
H323RasGk Load Limit is disabled
```

show h323 registrations

The **show h323 registrations** command displays H.323 endpoint registrations.

show h323 stackCallstats

The **show h323 stackCallstats** command displays H.323 stack call statistics. For example:

```
ACMEPACKET# show h323 stackCallstats

H323RasGk@0.4.1

STACK             Max       Active    Exceeded   InitFail   InFail
OutFail
h323172            0         0         0         0         0         0
h323192            1         0         0         0         1         0
```

show h323 stackDisconnectInstats

The **show h323 stackDisconnectInstats** command displays H.323 stack disconnect incall statistics. For example:

```
ACMEPACKET# show h323 stackDisconnectInstats

H323RasGk@0.4.1
STACK        Busy     Normal    Reject    Unreachable  Unknown   Local
h323172       0         0         0         0           0         0
h323192       0         0         0         0           0         1
```

show h323 stackDisconnectOutstats

The **show h323 stackDisconnectOutstats** command displays H.323 stack disconnect outcall statistics. For example:

```
ACMEPACKET# show h323 stackDisconnectOutstats

H323RasGk@0.4.1
STACK        Busy     Normal     Reject   Unreachable  Unknown   Local
h323172       0         0         0         0           0         0
h323192       0         0         0         0           0         1
```

show h323 stackPvtstats

The **show h323 stackPvtstats** command displays H.323 stack PVT statistics. For example:

```
ACMEPACKET# show h323 stackPvtstats

H323RasGk@1.4.1
STACK               Max        Current    maxUsed
h323172             115470     873        873
h323192             115470     873        873
```

show h323 status

The **show h323 status** command displays H.323 server statistics. For example:

```
ACMEPACKET# show h323 status
14:29:47-349292 h323RasGk@0.4.1
H323 SESSIONS                    ---- Recent ---- -------- Lifetime -
-------
                        Active    High   Total     Total  PerMax    High
Total Sessions               0       0      0         0       0       0
Total Incoming  Sessions      0       0      0         0       0       0
Total Outgoing  Sessions      0       0      0         0       0       0
Total Connected Sessions      0       0      0         0       0       0
Total Incoming  Channels      0       0      0         0       0       0
Total Outgoing  Channels      0       0      0         0       0       0
Incoming  IWF Sessions        0       0      0         0       0       0
```

```
Outgoing  IWF Sessions          0      0      0         0      0      0
IWF Server Transactions         0      0      0         0      0      0
IWF Client Transactions         0      0      0         0      0      0

H323D Status     Current   Lifetime
Queued Messages        0          0
TPKT Channels          0          0
UDP Channels           0          0
```

Resetting H.323 Statistics

You can reset the H.323 statistics counters on the Net-Net SBC by using the **reset h323** command.

```
ACMEPACKET# reset h323
```

H.323 CPU Load Limiting

See H.323 Load Limiting (235) for a description on how to enable H.323 CPU load limiting.

H.323 Stack Monitoring

The H.323 stack/interface configuration provides a way to set one of three alarm thresholds on a per-stack basis, based on the max-calls value. Upon a threshold being crossed the Net-Net SBC will trigger an alarm and an SNMP trap.

To prevent the alarm from firing continuously as call volume through the stack varies, each severity level has an has a reset value below the TCA you set. In addition, each threshold value resets when:

- An alarm with a higher severity is triggered, or
- The built-in reset value for the threshold level is 1% less than the parameter value

ACLI Instructions and Examples

This section shows you how to configure H.323 stack monitoring for one H.323 stack configuration. This example shows one instance of the alarm-threshold sub-configuration being established; remember that you can set three—critical, major, and minor. Simply repeat the configuration steps to add more severity levels.

To set up H.323 stack monitoring:

1. In Superuser mode, type **configure terminal** and press <Enter>.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)#
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)#
   ```

3. Type **h323** and press <Enter> to access the global H.323 configuration.

   ```
   ACMEPACKET(session-router)# h323
   ACMEPACKET(h323)#
   ```

4. Type **h323-stack** and press <Enter>. If you are adding H.323 stack monitoring to an existing H.323 stack configuration, then remember you must select the stack you want to edit.

   ```
   ACMEPACKET(h323)# h323-stack
   ACMEPACKET(h323-stack)#
   ```

5. Type **alarm-threshold** and press <Enter> to configure this feature.

```
ACMEPACKET(h323-stack)# alarm-threshold
ACMEPACKET(alarm-threshold)#
```

6. **severity**—Enter the type of severity level for the alarm you want to define. Choose from: **critical**, **major**, or **minor**. This value is required, and defaults to **minor**.
7. **value**—Enter the percentage of the number of calls defined in the **max-calls** parameter that triggers the alarm. For example, if you want to set a minor alarm to fire when the call rate through the stack reaches half the **max-calls** value, enter **50** (meaning 50%). The default value for this parameter is 0, which disables the alarm.

   Remember that if the number of calls falls to below 1% of the max-calls threshold you set, the clear trap fires.
8. Save your work.

For example:

```
alarm-threshold
           severity                    minor
           value                       50
alarm-threshold
           severity                    major
           value                       80
alarm-threshold
           severity                    critical
           value                       90
```

Management: ACLI

This section provides ACLI management information related to the H.323 stack monitoring feature.

Viewing the Number of Active Calls

You can see the number of active calls using the **show h323 stack call** command at either the User or Superuser prompt. As described in the Management: SNMP (251) section below, you can also access this information with an SNMP query.

Viewing Alarm Information

Two ACLI commands support this feature, and provide different information:

- **show alarms current**—This command shows alarm the most recently generated by an H.323 stack and the total number of stack monitoring alarms the Net-Net SBC has generated.
- **show h323 stack-alarms**—This command refers to specific stacks by stack name, and displays the alarm severity and current percentage of max-calls that triggered the alarm. The Net-Net SBC keeps track of how many alarms are raised by each stacks, and the severity of each of those alarms. When the alarm clears, the information relating to it is erased from the display.

```
ACMEPACKET# show h323 stack-alarms
Stack-Name          Alarm-Severity %Max-Call
external            minor                    50
internal            critical                   50
```

Management: SNMP

The ap-H323.mib MIB provides the information required to generate a trap and also includes a trap table of current call data for each stack so you can access it externally.

External Policy Servers Management

The Net-Net System provides numerous statistics and real-time operating parameters reflecting all aspects of its External Policy Servers and DIamaneter implementation.

Policy Server Show Commands

The following external policy server **show** commands display various details of external policy server system functionality.

show policy-server bandwidth

You can view external bandwidth manager statistics with the **show policy-server bandwidth** command. For example:

```
ACMEPACKET# show policy-server bandwidth
19:40:28-105 eps@0.1.0
Bandwidth Policy Server      ---- Recent ---- -------- Lifetime -------

                       Active    High   Total     Total  PerMax    High

Sockets                     1       1       1         1       1       1
Connections                 1       1       1         1       1       1
Client Transactions         0       0       0         0       0       0
  Reserve Requests Sent     -       -       0         0       0
  Update Requests Sent      -       -       0         0       0
  Remove Requests Sent      -       -       0         0       0
  Requests Re-Trans         -       -       0         0       0
  Install Resp Received     -       -       0         0       0
  Reject Resp Received      -       -       0         0       0
  Errors Received           -       -       0         0       0
  Transaction Timeouts      -       -       0         0       0
Server Transactions         0       0       0         0       0       0
  Requests Received         -       -       0         0       0
  Dup Req Received          -       -       0         0       0
  Success Resp Sent         -       -       0         0       0
  Error Resp Sent           -       -       0         0       0
  Requests Dropped          -       -       0         0       0
```

You may also add the standby argument to view external policy server statistics on the standby SPU. For example:

```
ACMEPACKET# show policy-server standby
14:11:41-2957 eps@1.1.0
Bandwidth Policy Server      ---- Recent ---- ------ Lifetime --------
                       Active    High   Total     Total  PerMax    High
Sockets                     0       0       0         0       0       0
Connections                 0       0       0         0       0       0
Client Transactions         0       0       0         0       0       0
  Reserve Requests Sent     -       -       0         0       0
```

```
  Update Requests Sent        -       -       0          0       0
  Remove Requests Sent        -       -       0          0       0
  Requests Re-Trans           -       -       0          0       0
  Install Resp Received       -       -       0          0       0
  Reject Resp Received        -       -       0          0       0
  Errors Received             -       -       0          0       0
  Transaction Timeouts        -       -       0          0       0
Server Transactions           0       0       0          0       0       0
  Requests Received           -       -       0          0       0
  Dup Req Received            -       -       0          0       0
  Success Resp Sent           -       -       0          0       0
  Error Resp Sent             -       -       0          0       0
  Requests Dropped            -       -       0          0       0
```

6 Security Management

The statistics and display commands described in this section are used for TLS and IPsec.

TLS Maintenance

The following commands are used for TLS maintenance and troubleshooting.

Viewing Certificates

You can view either a brief version or detailed information about the certificates. The show security certificates command has the following syntax

```
show security certificate [brief | details | list | pem]
```

show security certificate brief

Obtaining the brief version uses this syntax, and will appear like the following example:

```
ACMEPACKET# show security certificate brief acmepacket

certificate-record:acmepacket

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            02:13:02:50:00:84:00:71
        Issuer:
            C=US
            ST=California
            L=San Jose
            O=sipit
            OU=Sipit Test Certificate Authority
        Subject:
            C=US
            ST=MA
            L=Burlington
            O=Engineering
            CN=acme
```

show security certificate details

Obtaining the detailed version uses this syntax, and will appear like the following example:

```
ACMEPACKET#show security certificate details acmepacket

certificate-record:acmepacket

Certificate:
    Data:
```

```
Version: 3 (0x2)
Serial Number:
    02:13:02:50:00:84:00:71
Signature Algorithm: sha1WithRSAEncryption
Issuer:
    C=US
    ST=California
    L=San Jose
    O=sipit
    OU=Sipit Test Certificate Authority
Validity
    Not Before: Apr 13 21:37:43 2005 GMT
    Not After : Apr 12 21:37:43 2008 GMT
Subject:
    C=US
    ST=MA
    L=Burlington
    O=Engineering
    CN=acme
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS:pkumar
    X509v3 Basic Constraints:
        CA:FALSE
```

show security certificate list

The show security certificate list command lists all installed certificates. For example:

```
ACMEPACKET# show security certificate list
1: acmepacket
```

TLS Cache Statistics

You can view the number of entries in the TLS session cache, and then clear this cache as needed.

To view number of entries in the TLS session cache use the following command:

```
show security tls cache-count
```

To clear the entries in the TLS session cache use the following command:

```
security tls cache-clear
```

IPsec Maintenance

The following commands are used for IPsec maintenance and troubleshooting.

show security ipsec sad

This command shows the security association database entries which are programmed into the IPsec processor. In the case of manual keying, the entries should match that of the running configuration. This command is entered as:

```
show security ipsec sad [network-interface] <brief | verbose>
[selectors]
```

The [selectors] field allows you to specify which SA entries you would like to display according to the following table:

Selector	Description
<enter>	Display all entries
Direction	Direction (IN | OUT | BOTH), Default: BOTH
dst-addr-prefix	Destination address prefix, Default: match any
dst-port	Destination port, Default: match any
ipsec-protocol	IPsec protocol (AH | ESP | BOTH), Default: BOTH
Spi	security-policy-index, Default: match any
src-addr-prefix	Source address prefix, Default: match any
src-port	Source port, Default: match any
trans-proto	Transport protocol (UDP | TCP | | ICMP | ALL), Default: ALL

For example:

```
ACMEPACKET# show security ipsec sad M10 brief
IPSEC security-association-database for interface 'M10':

Total number of inbound SA records  : 1
Total number of outbound SA records : 1

Displaying SA's that match the following criteria -
   spi             : "any"
   direction       : both
   ipsec-proto     : "any"
   src-addr-prefix : "any"
   src-port        : "any"
   dst-addr-prefix : "any"
   dst-port        : "any"
   trans-proto     : ALL
   vlan-id         : "any"

Inbound, SPI: 257
        destination-address       : 192.168.1.2
        vlan-id                   : 0
        sal-mask                  : 3
        ipsec-proto               : ESP
        sad-index                 : 0
        encr-algo                 : aes-128-cbc
        auth-algo                 : hmac-sha1
        ipsec-mode    : transport
        match fields:
                src-ip            : 192.168.1.1
                dst-ip            : 192.168.1.2
                src-port          : 0
                dst-port          : 0
                vlan-id           : 0
                trans-proto       : ALL
        mask fields:
```

```
                src-ip           : 255.255.255.255
                dst-ip           : 255.255.255.255
                src-port         : 0
                dst-port         : 0
                vlan-id          : 0
                protocol         : 0

Outbound, SPI: 257
        source-address           : 192.168.1.2
        destination-address      : 192.168.1.1
        source-port              : 0
        destination-port         : 0
        trans-proto              : ALL
        vlan-id                  : 0
        sad-index                : 0
        encr-algo                : aes-128-cbc
        auth-algo                : hmac-sha1
        ipsec-mode    : transport
```

show security ipsec statistics sad

This command shows the security policy database entries which are programmed into the IPsec processor. This command is entered as:

```
show security ipsec spd [network-interface]
```

For example:

```
ACMEPACKET# show security ipsec spd M10
Inbound SPD records:
SPD Record, Priority: 0
        action                          : "ipsec"
        match fields:
                local-ip-addr           : 192.168.1.1
                remote-ip-addr          : 192.168.1.2
                local-port              : 0
                remote-port             : 0
                protocol                : "all"
                vlan-id                 : 0
        mask fields:
                local-ip-addr           : 255.255.255.255
                remote-ip-addr          : 255.255.255.255
                local-port              : "disabled"
                remote-port             : "disabled"
                protocol                : "disabled"
                vlan-id                 : 0


Outbound SPD records:
SPD Record, Priority: 0
        action                          : "ipsec"
        match fields:
                local-ip-addr           : 192.168.1.2
                remote-ip-addr          : 192.168.1.1
                local-port              : 0
                remote-port             : 0
                protocol                : "all"
```

```
        vlan-id                 : 0
    mask fields:
        local-ip-addr           : 255.255.255.255
        remote-ip-addr          : 255.255.255.255
        local-port              : "disabled"
        remote-port             : "disabled"
        protocol                : "disabled"
        vlan-id                 : 0
    fine-grained:
        valid                   : "enabled"
        local-ip-mask           : 255.255.255.255
        remote-ip-mask          : 255.255.255.255
        local-port-mask         : 0
        remote-port-mask        : 0
        vlan-id-mask            : 4096
        protocol                : "ALL"
```

Key Generation

The **generate-key** command generates keys for the supported encryption or authentication algorithms supported by the Net-Net SBC's IPsec implementation. The generate-key commands generate random values which are not stored on the Net-Net SBC, but are only displayed on the screen. This command is a convenient function for users who would like to randomly generate encryption and authentication keys. The generate-key usage is as follows:

```
seucurity generate-key [hmac-md5 | hmac-sha1 | aes-128 | aes-256 |
3des]
```

IPsec Hardware Statistics

You can query the IPsec processor for hardware identification or Ethernet counts.

show security ipsec statistics gmac

The **show security ipsec statistics gmac** command displays values for the GMAC interface on an IPsec phy card. You can display either all, or only error, receive, or transmit statistics. This command is entered as:

```
show security ipsec statistics gmac [network-interface] <enter | error
| rx | tx>
```

For example:

```
ACMEPACKET# show security ipsec statistics gmac M10
Host 0 Status:
        Receive Statistics:
                Total bytes             : 458422
                Total frames            : 1802
                Pause frames            : 0
                Frames < 64 bytes       : 403
                Frames 65-127 bytes     : 1053
                Frames 128-255 bytes    : 5
                Frames 256-511 bytes    : 0
                Frames 512-1024 bytes   : 4
                Frames 1024-1500 bytes  : 336
                Frames > 1500 bytes     : 1
        Transmit Statistics:
                Total bytes             : 1180666
```

```
                Total frames             : 8898
                Good frames              : 8898
                Pause frames             : 0
                Frames < 64 bytes        : 438
                Frames 65-127 bytes      : 7437
                Frames 128-255 bytes     : 726
                Frames 256-511 bytes     : 23
                Frames 512-1024 bytes    : 2
                Frames 1024-1500 bytes   : 272
                Frames > 1500 bytes      : 0
        Error Statistics:
                Underflow errors         : 0
                Collision errors         : 0
                Excessive collisions     : 0
                Carrier sense errors     : 0
                Excessive deferrals      : 0
                CRC errors               : 0
                Alignment errors         : 0
                < 64 bytes & CRC errors  : 0
                > 1518 bytes & CRC errors : 0
                Length errors            : 0
                FIFO overflows           : 0
                Watchdog errors          : 0
```

show security status

The **show security status** command displays whether a particular interface on a session-director is IPsec enabled. If so, the hardware status of the security processor will be displayed. This command is entered as:

```
show security status [slot] [port]
```

For example:

```
ACMEPACKET# show security status 1 0
Interface '1, 0' IPSEC hardware status:
  Structure version       = 2
  Payload length (words)  = 8
  Boot ROM code device ID = 0x0025
  Vendor ID               = 0x13a3
  Device ID               = 0x8450
  Hardware version        = 0x0000
  Subsystem type          = 0x00
  Software type           = 0x01
  Major software version  = 0x01
  Minor software version  = 0x02
  Memory config value     = 0x00000006
  System config register  = 0x00a40020
  System clock 2 register = 0x00009555
  Saved parity status     = 0x0000
  Current parity status   = 0x0002
  POST test number        = 0x00
  POST sub-test number    = 0x00
  POST test result        = 0x00
  SW major revision       = 0x01
  SW minor revision       = 0x02
  SW maintenance revision = 0x00
```

```
SW build number         = 0x09
```

Protected Password Configuration

In the Net-Net 9200's configuration files, sensitive data is encrypted with the fixed protected configuration password (PCP). The fixed password provides security and convenience when migrating configurations to different Net-Net 9200s. You can also change the PCP to a password of your own choosing for added security.

Protected Data

The following data within a Net-Net 9200 configuration is protected by the PCP:

1. Security certificate's private key in the certificate record. This information is imported from the ACLI or imported from a text file. Once imported it is not viewable from the ACLI.
2. IPsec authentication and encryption key in the security association. This information is entered in the security -> ipsec -> manual-security-association configuration element.
3. FTP credentials (login password) for Historical Data Reporting. This information is entered in the system ->collect -> push-receiver configuration element.
4. CDR push-receiver credential (FTP/SFTP login password)
5. LI X1 agent (auth-user and auth-password), SS8 (auth-serial-number)
6. SSH private key

Configuring the PCP

Use the set password config command to change the PCP. Initiating this command walks you through changing the PCP. Remember that your new PCP is subject to the Setting the Password Policy (136) you set. For example:

```
ACMEPACKET# set password config
-------------------------------------------------
WARNING:
Proceed with caution!
Changing the configuration password will result any
previous backup/archive configuration file unusable.
The process will also update and activate the
configuration once the password is updated
-------------------------------------------------
Are you sure [y/n]?: y
Enter old password:
verifying the input password...
password verified

verifying configuration with the password ...
7 cert-record verified
1 sec-assco verified
2 cdr push receiver verified
1 ssh-pub-key-record verified
x1 agent (agent1) credential verified
ss8 agent (ss8) credential verified
the configuration and the password are in sycnh (5)

Enter new password:
Enter password again:
```

```
7 cert-record updated
1 sec-assoc updated
2 cdr push-receiver updated
1 ssh-pu-key-record updated
x1 agent (agent1) credential updated
ss8 agent (ss8) credential updated
moving file /code/config/tmp/editing/dataDoc.gz ->
/code/config/dataDoc.gz
Save complete
configuration has been updated and saved(5)
configuration password changed on SPU 0
configuration password changed on SPU 1
extracting /code/config/dataDoc.gz
loading configuration caches
NPU0 configuration activated
NPU1 configuration activated
SPU0 configuration activated
SPU1 configuration activated
new configuration is activated
```

Note: In the previous display, lawful intercept cedential designations will not be shown unless LI admin password has been entered.

Verifying the PCP

You can verify that a password is correct for a configuration before you change the PCP with the **set password config verify** <password> command. If the password you entered matches the active configuration's password, a confirmation message is printed at the ACLI.

Migrating a PCP-Protected Configuration

This section provides with instructions for how to move your configuration file from one Net-Net SBC to another. Additional checking has been added to the verification and activation processes. To describe how to migrate a configuration, this section uses the designations Net-Net SBC1 and Net-Net SBC2, where:

- Net-Net SBC1 has the configuration you want to move
- Net-Net SBC2 is the system to which you want to migrate the configuration from Net-Net SBC1

To migrate a configuration from Net-Net SBC1 (where the password configuration has been set) to Net-Net SBC2:

1. Confirm that you know the protected configuration password for Net-Net SBC1's configuration.
2. Backup the configuration file on Net-Net SBC1 using the **save backup** command as explained in the Backup File Management (275) section.
3. Backup the configuration file on Net-Net SBC2 using the save backup command.
4. Download the configuration file on Net-Net SBC1 using an FTP or SCP client.
5. Upload the configuration file to Net-Net SBC2 using an FTP or SCP client.
6. Delete the old configuration file on Net-Net SBC2 using the **delete configuration** command.

7. Use the **set password config verify** to ensure that the PCP password for this moved configuration is correct before activating it.

   ```
   ACMEPACKET# set password config verify
   Enter old password:
   ```

8. Use the **set password config** command to change the configuration password on Net-Net SBC2 to that of the password that protected the Net-Net SBC1's configuration. See Configuring the PCP (259).
9. Restore the configuration file on Net-Net SBC2 using the **restore backup** command as explained in the Backup File Management (275) section.
10. Activate the configuration on Net-Net SBC2.

SSH Public Key Support

SSHv2 Public Key Authentication

The Net-Net SBC supports importing, generating, viewing, and deleting public keys used for authentication of SSHv2 sessions from administrative remote users.

Importing an SSH Host Key

Importing a host key requires access to the SFTP server or servers. Access is generally most easily accomplished with a terminal emulation program such as PuTTY, SecureCRT, or TeraTerm.

To import an SSHv2 host key:

1. Access the SSH file system on a configured SFTP server using a terminal emulation program.
2. Copy the server's base64 encoded public file, including the Begin and End markers as specified by RFC 4716, *The Secure Shell (SSH) Public Key File Format*.

   For OpenSSH implementations, host files are generally found at */etc/ssh/ssh_host_dsa_key.pub*, or *etc/ssh/sss_host_rsa.pub*. Other SSH implementations can differ.
3. Use the **security ssh-pub-key import known-host <name>** command (where **<name>** is an alias or handle assigned to the imported host key, generally the server name or a description of the server function) to import the host key to the SBC.
4. Paste the public key with the bracketing Begin and End markers at the cursor point.
5. Enter a semi-colon (;) to signal the end of the imported host key.
6. Save and activate the configuration.

The entire import sequence is shown below.

```
ACMEPACKET# security ssh-pub-key import known-host fedallah
IMPORTANT:
        Please paste ssh public key in the format defined in rfc4716.
        Terminate the key with ";" to exit.......

---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted from OpenSSH by klee@acme54"
AAAAB3NzaC1yc2EAAAABIwAAAQEA7OBf08jJe7MSMgerjDTgZpbPblrX4n17LQJgPC7clL
cDGEtKSiVt5MjcSav3v6AEN2pYZihOxd2Zzismpoo019kkJ56s/IjGstEzqXMKHKUr9mBV
qvqIEOTqbowEi5sz2AP31GUjQTCKZRF1XOQx8A44vHZCum93/jfNRsnWQ1mhHmaZMmT2LS
hOr4J/Nlp+vpsvpdrolV6Ftz5eiVfgocxrDrjNcVtsAMyLBpDdL6e9XebQzGSS92TPuKP/
yqzLJ2G5NVFhxdw5i+FvdHz1vBdvB505y2QPj/iz1u3TA/3O7tyntBOb7beDyIrg64Azc8
G7E3AGiH49LnBtlQf/aw==
---- END SSH2 PUBLIC KEY ----
:
 SSH public key imported successfully....
 WARNING: Configuration changed, run "save-config" command to save it
 and run "activate-config" to activate the changes
 ACMEPACKET# save config
 checking configuration
 ------------------------------------------------------------------------
 ...
 ...
 ...
 ------------------------------------------------------------------------
 Save-Config received, processing.
 waiting for request to finish
 Request to 'SAVE-CONFIG' has Finished,
 Save complete
 Currently active and saved configurations do not match!
 To sync & activate, run 'activate-config' or 'reboot activate'.
 ACMEPACKET# activate config
 Activate-Config received, processing.
 waiting for request to finish
 SD is not QOS-capable
 Request to 'ACTIVATE-CONFIG' has Finished,
 Activate Complete
 ACMEPACKET#
```

Importing an SSH Public Key

Prior to using SSH public key-based authentication you must import a copy of the public key of each user who will authenticate using this method. The public key identifies the user as a trusted entity when the Acme Packet Net-Net SBC performs authentication.

During the SSH login, the user presents its public key to the SBC. Upon receiving the offered public key, the SBC validates it against the previously obtained trusted copy of the key to identify and authenticate the user.

Importing a public key requires access to the device on which the public key was generated, or on which it is currently stored with its associated private key. Access is generally attained with a terminal emulation program such as PuTTY, SecureCRT, or TeraTerm.

To import a public key:

1. Access the system from which the public key will be obtained using a terminal emulation program.
2. Copy the base64 encoded public key, including the Begin and End markers as specified by RFC 4716, *The Secure Shell (SSH) Public Key File Format*.
3. Use the **security ssh-pub-key import authorized-key <name>** command (where **<name>** is an alias or handle assigned to the imported public key, often the user's name) to import the public key to the SBC. For example:

   ```
   ACMEPACKET# security ssh-pub-key import authorized-key key1
   ```

   Use the optional **<"admin">** argument to import a public key who will be authorized for admin privileges. For example:

   ```
   ACMEPACKET# security ssh-pub-key import authorized-key key1 admin
   ```
4. Paste the public key with the bracketing Begin and End markers at the cursor point.
5. Enter a semi-colon (;) to signal the end of the imported host key.
6. Save and activate the configuration.

   The entire import sequence is shown below.

```
ACMEPACKET# security ssh-pub-key import authorized-key Matilda
admin


IMPORTANT:
        Please paste ssh public key in the format defined in rfc4716.
        Terminate the key with ";" to exit.......

---- BEGIN SSH2 PUBLIC KEY ----
Comment: "1024-bit RSA, converted from OpenSSH by abhat@acme74"
AAAAB3NzaC1yc2EAAAABIwAAAIEAxcYTV595VqdHy12P+mIZBlpeOZx9sX/mSAFihDJYdL
qJIWdiZuSmny8HZIxTIC6na62iD25mlEdyLhlYOuknkYBCU7UsLwmx4dLDyHTbrQHz3b1q
3Tb8auz97/J1p4pw39PT42CoRODzPBrXJV+OglNE/83C1y0SSJ8BjC9LEwE=
---- END SSH2 PUBLIC KEY ----:
 SSH public key imported successfully....
 WARNING: Configuration changed, run "save-config" command to save it
 and run "activate-config" to activate the changes
 ACMEPACKET# save config
 checking configuration
 ------------------------------------------------------------------------
 ...
 ...
 ...
 ------------------------------------------------------------------------
 Save-Config received, processing.
 waiting for request to finish
 Request to 'SAVE-CONFIG' has Finished,
 Save complete
 Currently active and saved configurations do not match!
 To sync & activate, run 'activate-config' or 'reboot activate'.
 ACMEPACKET# activate config
 Activate-Config received, processing.
 waiting for request to finish
 SD is not QOS-capable
 Request to 'ACTIVATE-CONFIG' has Finished,
 Activate Complete
 ACMEPACKET#
```

Generating an SSH Key Pair

To generate an SSH key pair you must initially configure a public key record which will serve as a container for the generated key pair.

To configure a public key record:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)#
```

2. Type **security** and press <Enter>.

```
ACMEPACKET(configure)# security
ACMEPACKET(security)#
```

3. Type **public-key** and press <Enter>. The system prompt changes to let you know that you can begin configuring individual parameters.

```
ACMEPACKET(security)# public-key
ACMEPACKET(public-key)#
```

4. **name**—Enter the name of this public key.

```
ACMEPACKET(public-key)# name tashtego
```

5. **type**—Select the type of key you want to create. Valid values are **rsa** and **dsa**. The default value is **rsa.**
6. **size**—Enter the size of the key you are creating. Valid key sizes are **512**, **1024**, or **2048**. The default value is **1024**.
7. Save and activate the configuration.

To generate an SSH key pair:

1. Enter the **security ssh-pub-key generate** command along with the name of the public key you created in the previous step as follows.

```
ACMEPACKET# security ssh-pub-key generate tashtego
Please wait...
public-key 'tashtego' (RFC 4716/SECSH format):
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "1024-bit rsa"
AAAAB3NzaC1yc2EAAAABIwAAAIEArZEP1/WiYsdGd/Pi8V6pnSwV4cVG4U+jV
OwiSwNJCC9Nk82/FKYleLZevy9D3lrZ8ytvu+sCYy0fNk4nwvz20c2N+r86kD
ru88JkUqpelJDx1AR718Icpr7ZaAx2L+e7cpyRSXCgbQR7rXu2H3bp9Jc0VhR
2fmkclmrGAIr7Gnc=
---- END SSH2 PUBLIC KEY ----

SSH public-key pair generated successfully....

WARNING: Configuration changed, run "save config" command to
save it and run "activate config" to activate the changes
ACMEPACKET#
```

2. Copy the base64-encoded public key. Copy the public key including the bracketing Begin and End markers. Shortly you will paste the public key to one or more SFTP servers.
3. Save and activate the configuration.

Copying a Client Key or an SSH or SFTP Server

Copying the client public key to the SFTP server requires server access generally using a terminal emulation program such as PuTTY, SecureCRT, or TeraTerm.

1. Use a terminal emulation program to access the SSH file system on a configured SFTP server.
2. Copy the client key to the SFTP server.

   On OpenSSH implementations, public keys are usually stored in the *~/.ssh/authorized_keys* file. Each line this file (1) is empty, (2) starts with a pound(#) character (indicating a comment), or (3) contains a single public key.

   Refer to the sshd manual pages for additional information regarding file format.

   Use a text editor such as *vi* or *emacs* to open the file and paste the public key to the tail of the *authorized_keys* file.

For SSH implementations other than OpenSSH, consult the system administrator for file structure details.

Viewing SSH Imported Keys

You can use the **show security ssh-pub-key** command to display information about SSH keys imported to the SBC with the **ssh-pub-key** command; you cannot display information about keys generated by the **ssh-pub-key** command. You can view either a brief version of detailed information about the certificates.

Viewing a Brief SSH Imported Key Version

When you use the **show security ssh-pub-key brief [name]** command, the following information is displayed:

- login-name—Contains the name assigned to the RSA or DSA public key when it was first imported
- finger-print—Contains the output of an MD5 hash computed across the base64-encoded public key
- finger-print-raw—Contains the output of an MD5 hash computed across the binary form of the public key

To view the brief version for all imported SSH public keys:

```
ACMEPACKET# show security ssh-pub-key brief
login-name:
    acme74
finger-print:
    51:2f:f1:dd:79:9e:64:85:6f:22:3d:fe:99:1f:c8:21
finger-print-raw:
    0a:ba:d8:ef:bb:b4:41:d0:dd:42:b0:6f:6b:50:97:31

login-name:
    fedallah
finger-print:
    c4:a0:eb:79:5b:19:01:f1:9c:50:b3:6a:6a:7c:63:d5
finger-print-raw:
    ac:27:58:14:a9:7e:83:fd:61:c0:5c:c8:ef:78:e0:9c
ACMEPACKET#
```

To view the brief version for a specified imported SSH public key:

```
ACMEPACKET# show security ssh-pub-key brief fedallah
login-name:
fedallah
finger-print:
    c4:a0:eb:79:5b:19:01:f1:9c:50:b3:6a:6a:7c:63:d5
finger-print-raw:
    ac:27:58:14:a9:7e:83:fd:61:c0:5c:c8:ef:78:e0:9c
```

```
ACMEPACKET#
```

Viewing a Detailed SSH Imported Key Version

When you use the **show security ssh-pub-key detail <name>** command, the following information is displayed:

For an RSA key:

- host-name—Contains the name assigned to the RSA key when it was first imported
- finger-print—Contains the output of an MD5 hash computed across the base64-encoded RSA public key
- finger-print-raw—Contains the output of an MD5 hash computed across the binary form of the RSA public key
- public key—Contains the base64-encoded RSA key
- modulus—Contains the hexadecimal modulus (256) of the RSA key
- exponent—Contains an integer value that is used during the RSA key generation algorithm. Commonly used values are 17 and 65537. A prime exponent greater than 2 is generally used for more efficient key generation.

For a DSA key:

- host name—Contains the name assigned to the DSA public key when it was first imported
- comment—Contains any comments associated with the DSA key
- finger-print—Contains the output of an MD5 hash computed across the base64-encoded DSA public key
- finger-print-raw—Contains the output of an MD5 hash computed across the binary form of the DSA public key
- public key—Contains the base64 encoded DSA key
- p—Contains the first of two prime numbers used for key generation
- q—Contains the second of two prime numbers used for key generation
- g—Contains an integer that together with p and q are the inputs to the DSA key generation algorithm

To view the detailed version for a specific RSA key:

```
ACMEPACKET# show security ssh-pub-key detail fedallah
host-name:
    fedallah
comment:
    "2048-bit RSA, converted from OpenSSH by klee@acme54"
finger-print:
    c4:a0:eb:79:5b:19:01:f1:9c:50:b3:6a:6a:7c:63:d5
finger-print-raw:
    ac:27:58:14:a9:7e:83:fd:61:c0:5c:c8:ef:78:e0:9c
pub-key:

AAAAB3NzaC1yc2EAAAABIwAAAQEA7OBf08jJe7MSMgerjDTgZpbPblrX4n17LQJgP
C7clLcDGEtKSiVt5MjcSav3v6AEN2pYZihOxd2Zzismpoo019kkJ56s/IjGstEzqX
MKHKUr9mBVqvqIEOTqbowEi5sz2AP31GUjQTCKZRF1XOQx8A44vHZCum93/jfNRsn
WQ1mhHmaZMmT2LShOr4J/Nlp+vpsvpdrolV6Ftz5eiVfgocxrDrjNcVtsAMyLBpDd
L6e9XebQzGSS92TPuKP/yqzLJ2G5NVFhxdw5i+FvdHz1vBdvB505y2QPj/iz1u3TA
/3O7tyntBOb7beDyIrg64Azc8G7E3AGiH49LnBtlQf/aw==
```

```
modulus: (256)
ECE05FD3C8C97BB3123207AB8C34E06696CF6E5AD7E27D7B2D02603C2EDC94B70
3184B4A4A256DE4C8DC49ABF7BFA004376A5866284EC5DD99CE2B26A68A34D7D9
24279EACFC88C6B2D133A9730A1CA52BF66055AAFA8810E4EA6E8C048B9B33D80
3F7D4652341308A6511755CE431F00E38BC7642BA6F77FE37CD46C9D64359A11E
66993264F62D284EAF827F365A7EBE9B2FA5DAE8955E85B73E5E8957E0A1CC6B0
EB8CD715B6C00CC8B0690DD2FA7BD5DE6D0CC6492F764CFB8A3FFCAACCB2761B9
355161C5DC398BE16F747CF5BC176F079D39CB640F8FF8B3D6EDD303FDCEEEDCA
7B4139BEDB783C88AE0EB803373C1BB137006887E3D2E706D9507FF6B
exponent: (1)
23

ACMEPACKET#
```

To view the detailed version for a specific DSA key:

```
ACMEPACKET# show security ssh-pub-key detail acme74
host-name:
    acme74
comment:
    DSA Public Key
finger-print:
    51:2f:f1:dd:79:9e:64:85:6f:22:3d:fe:99:1f:c8:21
finger-print-raw:
    0a:ba:d8:ef:bb:b4:41:d0:dd:42:b0:6f:6b:50:97:31
pub-key:

AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXx
bETW6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T
6JYrdHYI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAA
AFQDb8D5cvwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPg
gA4pfdtW9vGfJ0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2
AWQ2dsknf+i/FAAvioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJ
mJ80qadxTRHtUAAACBAN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQ
eSXG1vO+JsvphVMBJc9HSn24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3
VVmxHLmxnAz643WK42Z7dLM5sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV

p: (128)
F63C64E1D8DB2152240E97602F47470347C5A7A1BF1E70389D2BCD9773A12397C
5B1135BA4E81EFF03D5427FCFECC7A3D162928E57C9B6670C86810C7B5B950F98
A7B4ADC7296D1E75C5D582DF283D46E13E8962B747608D783A6D5E83D7B836709
195E6AAA193C5DD419F6626BA6D7AC64D07F7809AB67BB622B24FE017ED55
q: (20)
DBF03E5CBF01D64D90CF7D7D03DACF5177B341BD
g: (128)
94DF76F816FB0F828B624DC8C116D76E5C177643E0800E297DDB56F6F19F274FD
11DDF8D8C1E1EA350FED1D8B1EAD5F060637B3CA4B947F1573CDC311CF6A9723F
6E2F5267D80590D9DB249DFFA2FC5000BE2A143E499D31CD33B96A12384B12361
543B57DD676F55C19C06AF5C7ADCEBB4E2963A8709989F34A9A7714D11ED5
pub_key: (128)
DEC263E28ABF5807A51CC5C1D426EC72BD6DBD4B028D8AC1AA179DA74581EA6D3
4141E4971B5BCEF89B2FA6154C04973D1D29F6E1562D62DB0CBBBE2A5EF8988F3
895B9C58A8E32846F5D63BAA9C5D060E50775559B11CB9B19C0CFAE3758AE3667
B74B339B18DBDA2E7B3BF85F3D8FB8C721E5518F3FE083AB308CE25A16815

ACMEPACKET#
```

To view the detailed version for all SSH imported keys:

```
ACMEPACKET# show security ssh-pub-key detail
```

```
...
...
...
ACMEPACKET#
```

Deleting a Public Key Record

This section shows you how to delete a public key record. Note that this process requires you to save and activate your configuration.

To delete an SSHv2 public key record:

1. In Superuser mode, type the command **security ssh-public-key delete**, then a <Space> and the login-name (found in both brief and detail **show security public-key** commands) corresponding to the public key you want to delete.

   The Net-Net SBC confirms you have successfully deleted the key, and then reminds you to save your configuration.

   After you complete this procedure, you can confirm the public key has been deleted by using either of the show security **ssh-pub-key** commands.

   ```
   ACMEPACKET# security ssh-pub-key delete jdoe
   SSH public key deleted successfully....
   WARNING: Configuration changed, run "save-config" command.

   ACMEPACKET# security ssh-pub-key delete jdoe
   record (jdoe) does not exist
   ```

2. Save and activate your configuration.

TACAC+s Management

The **show tacacs+** command can take the **servers** or **statistics** argument**.**

show tacacs+ servers

The **show tacacs+ servers** command displays all TACACS+ server available. The output lists each server by IP address, the server's configuration state (enabled/disabled) and AAA status (Active, Standby, Out of service).

```
ACMEPACKET# show tacacs+ servers
TACACS+ Server       Config State            AAA Status
---------------      ------------            -----------
172.0.0.200:49          disabled
172.30.0.7:49           disabled
172.30.0.54:49          enabled         Active
172.30.200.1:49         enabled         Standby
```

show tacacs+ statistics

The **show tacacs+ statistics** command displays overall requests and response statistics for each TACACS+ server including:

- number of ACLI commands sent for TAGACS+ accounting
- number of successful TACACS+ authentications
- number of failed TACACS+ authentications
- number of successful TACACS+ authorizations
- number of failed TACACS+ authentications
- the IP address of the TACACS+ daemon used for the last transaction

```
ACMEPACKET# show tacacs+ statistics
```

```
Server: 172.30.0.54:49
Tacacs+ Statistics           ---- Lifetime ----
                           Recent      Total  PerMax
Authentication Success          2          2       2
Authentication Failure          0          0       0
Authorization Success           0          0       0
Authorization Failure           0          0       0
Accounting Success              0          0       0
Accounting Failure              0          0       0
Last transaction: 2011-11-24 02:06:08.181
-------------------------------------------------
Server: 172.30.200.1:49
Tacacs+ Statistics           ---- Lifetime ----
                           Recent      Total  PerMax
Authentication Success          0          0       0
Authentication Failure          0          0       0
Authorization Success           2          2       2
Authorization Failure           0          0       0
Accounting Success              0          0       0
Accounting Failure              0          0       0
Last transaction: 2011-11-24 02:06:09.264
-------------------------------------------------
Last transaction server: 172.30.200.1:49
```

TACACS+ Logging

All messages between the Net-Net SBC and the TACACS+ daemon are logged in a cleartext format, allowing an *admin* user to view all data exchange, except for password information.

7 Configuration Management

System Configuration Process

Net-Net 9200 Configuration

There are three steps you must follow to proceed from setting a configuration parameter to enabling the Net-Net OS to use the changed parameter.

1. While you are in configuration mode, use the **done** command to save your work. This command saves all changes you've made in a configuration element to memory.
2. Once you are satisfied with your edits, save all of them to the current configuration space with the **save config** command. This creates a configuration file that is persistent across reboot.

   In addition, a copy of the previously saved configuration is maintained and labeled as the previous configuration version.
3. Finally, execute the **activate config** command to make the Net-Net 9200 go "live" using the configuration. This is called the running configuration, reflecting the running state of the Net-Net SD.

Configuration Process

The following example walks through configuring one configuration element (ntp), saving the configuration, and then activating the configuration.

To set a configuration element, create a current configuration, and execute the running configuration:

1. Set all the necessary parameters on the SD. Each time you complete configuring a full configuration element, type **done** to save that element.

```
ACMEPACKET(ntp)# server 10.10.10.15
ACMEPACKET(ntp)# done
ntp
        server                          10.10.10.15
        last-modified-date              2000-01-01 19:15:21
```

2. When all configuration elements are set, back out of configuration tree to the topmost ACLI level at the superuser prompt.

```
ACMEPACKET(ntp)# exit
ACMEPACKET(system)# exit
ACMEPACKET(terminal)# exit
ACMEPACKET#
```

3. Save all configurations to the current configuration by using the **save config** command.

```
ACMEPACKET# save config
copying file /code/config/dataDoc.gz -> /code/config/dataDoc_299.gz
copying file /code/config/tmp/editing/dataDoc.gz ->
/code/config/dataDoc.gz
```

```
Save complete
```

4. Set the Net-Net SD to enact the current configuration into the running state by using the **activate config** command. This will make the current configuration the running configuration.

```
ACMEPACKET# activate config
Activate Complete
```

Configuration Versions

The Net-Net SD maintains counts of the running configuration version and current configuration version. It can be helpful to know when the running and current configurations are out of sync.

No matter how many times you increment the current configuration by executing the save config command, once you execute the activate config command, the current and running configuration versions will be identical.

To check the version of each configuration:

1. Type **show version software** at a command prompt to display the version number of the current configuration.

```
ACMEPACKET# show version software
  NN9200 Software Version:      5.0.0 Beta Workspace (Build 01)
  NN9200 Software Build Date:   07/07/07
  Built in /home/NEOBETA on acme29

   Current config version:      301
   Running config version:      300
```

Deleting Configurations

You can completely delete the data in the current configuration with two commands. This can be useful if you want to reconfigure your Net-Net SD starting with a blank configuration.

To delete the running and current configuration:

1. Type **delete config** at a superuser command prompt. You will be prompted to confirm that you want to complete this task.

```
ACMEPACKET# delete config
```

2. Save and activate the cleared configuration with the **save config** and **activate config** commands.

   Note: There is no confirmation for this command.

Displaying Configurations

The Net-Net OS can display the current and running configurations to the screen. These commands are used to inspect how the Net-Net system is configured.

Configuration Show Commands

The Net-Net system provides a flexible means for displaying the system configurations with the show command.

```
ACMEPACKET# show [config | running-config] [<configuration element>
<element identifier>] [<“short”>]
```

Basic Show Configuration Usage

The **show config** command displays the current configuration, while the **show running-config** command displays the running configuration. The output of these commands might span several screens.

Show Configuration by Element

Both the **show config** and the **show running-config** commands let you include a configuration element name as an argument to view only instances for that configuration element. The valid configuration elements you can use as an argument are:

- access-control
- account-config
- authentication
- class-policy
- collect
- enforcement-profile
- host-route
- local-policy
- media-manager
- media-policy
- media-profile
- net-management-control
- network-interface
- ntp
- password-policy
- phy-interface
- realm-config
- session-agent
- session-constraints
- session-group
- session-translation
- sip-config
- sip-feature
- sip-interface
- sip-manipulation
- sip-nat
- sip-response-map
- snmp-community
- soap-config
- static-flow
- steering-pool
- surrogate-agent

- system-config
- timezone
- transcoding-policy
- translation-rules
- trap-receiver

If multiple instances of a configuration element are configured, the Net-Net OS will display all elements. In the following example, the two phy-interface instances, private and public, are displayed.

```
ACMEPACKET# show config phy-interface
phy-interface
        name                            private
        operation-type                  Media
        slot                            1
        port                            0
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode
        speed
        virtual-mac
        last-modified-date              3000-05-23 17:31:11
phy-interface
        name                            public
        operation-type                  Media
        slot                            0
        port                            0
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode
        speed
        virtual-mac
        last-modified-date              2000-05-23 17:31:26
```

Configuration Element Identifier

To view a specific instance of a configuration element, you must include the element identifier argument in the **show config** command. The element identifier is usually the *name* parameter of that configuration element. In the following example, only the phy-interface configuration element named *public* is displayed:

```
ACMEPACKET# show config phy-interface public
phy-interface
        name                            public
        operation-type                  Media
        slot                            0
        port                            0
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode
        speed
        virtual-mac
```

Configuration Summary

By adding the **short** argument to the end of any **show config** or **show running-config** command, the Net-Net system will display an abbreviated output. The short

argument forces the Net-Net OS to display only those parameters that have changed from the defaults. In the following example, parameters which have not been altered from default, duplex-mode and speed, are omitted:

```
ACMEPACKET# show config phy-interface short
phy-interface
        name                            private
        operation-type                  Media
        slot                            1
        admin-state                     enabled
        auto-negotiation                enabled
```

Backup File Management

The Net-Net OS saves the full system configuration to a single backup file. You can perform a limited set of actions on backup files, such as saving, backing up, listing, deleting, and restoring the files back to the full system configuration. All backup files are compressed using gzip compression to save disk space.

Acme Packet suggests that you back up properly functioning configurations on your Net-Net system before making any new major configuration changes. The backup configurations are crucial to have when configuration changes do not function as anticipated and a rollback must be applied immediately. Backups are created as gzipped files in a .gz format. They are stored in the `/code/bkups` directory on the Net-Net 9200.

Creating Backups

To create a backup file:

1. In the ACLI at the superuser prompt, enter the **save backup** command followed by a descriptive filename for the backup you are creating. You do not need to add a file extension.

```
ACMEPACKET# save backup 01_July

task done
ACMEPACKET#
```

Listing Backups

Listing backups is the process of viewing all files in the Net-Net system's standard backup file directory.

To display backup files:

1. In the ACLI at the superuser prompt, enter the **show backup** command. A list of available backup files from the `/code/bkups` directory is displayed on the screen.

```
ACMEPACKET# show backup
test.gz
bmc_pbrb_20120.gz
bmc_snb_20120.gz
test34.gz
normal.gz
01_July.gz
```

Restoring Backups

Restoring a backup writes a backup file's contents to the current configuration.

To restore a backup configuration:

1. In the ACLI at the superuser prompt, enter the **restore backup** command followed by a backup filename. You must explicitly name the backup file you wish to restore, including the file extension.

   ```
   ACMEPACKET# restore backup 01_July.gz
   Need to perform 'save config' and 'activate config' for changes to take effect
   ACMEPACKET#
   ```

   You must still save and activate the configuration to apply the backup configuration.

You can also restore the last saved confguration with the restore previous command.

To restore the last saved configuration:

1. In the ACLI at the superuser prompt, enter the **restore previous** command followed by a backup filename. You must explicitly name the backup file you wish to restore, including the file extension.

   ```
   ACMEPACKET# restore previous
   Restoring previous configuration dataDoc_001.gz
   Need to perform 'save config' and 'activate config' for changes to take effect
   ```

   You must still save and activate the configuration to apply the backup configuration.

Deleting Backups

Deleting backups deletes a specified backup file from the Net-Net 9200's standard backup file directory.

1. In the ACLI at the superuser prompt, enter the **delete backup** command, followed by the backup file you wish to delete. You must explicitly name the backup file you wish to restore, including the file extension

   ```
   ACMEPACKET# delete backup FEB_BACKUP.gz
   ACMEPACKET#
   ```

   There is no confirmation warning before executing this command.

Checking Free Space

You can see how much space is available and how much space is currently in use on the code flash.

show space

The **show space** command is used to view the amount of flash file space in use and the amount remaining. This command reports flash space on both SPU 0 and SPU 1. For example:

```
ACMEPACKET# show space
Slot 0 filesystem: 215339008/249675776 bytes (86%) remaining
Slot 1 filesystem: 178262016/249675776 bytes (71%) remaining
```

You can also see how much space is available on a CF card plugged into an MIU's PCMCIA slot with the **show space pcmcia** command. For example:

```
ACMEPACKET# show space pcmcia

/sys: 19695716352/19695749120 bytes (99%) remaining
/local: 19693335040/19693367808 bytes (99%) remaining
/logs: 19693335040/19693367808 bytes (99%) remaining
```

```
/misc: 19693335040/19693367808 bytes (99%) remaining
ACMEPACKET#
```

Configuration Inventory Method

The following commands have been enhanced to provide more control when working with configurations:

- backup config
- restore
- show configuration
- show running-config

Backing Up Configurations

You can now specify which configuration you want to back up: the **running** configuration or the **editing** configuration. If you execute the backup config command without specifying a configuration type, the Net-Net SBC backs up the last saved configuration by default.

ACLI Instructions and Examples

In this sample, the editing configuration is being backed up.

To back up the editing or running configuration:

1. In Superuser mode, type **save backup** followed by a <Space>, the name of the backup file followed by a <Space>, and the word **editing**. Then press <Enter>.

   If you want to back up the running configuration, you simply type **running** instead of **editing**.

   ```
   ACMEPACKET# save backup 06092008_E.gz editing
   task done
   ACMEPACKET#
   ```

Restoring Configurations

You can restore the last running or the last saved configurations to use as the editing configuration. You use the **saved** or **running** argument with the ACLI **restore** command.

The two kinds of configurations are defined as follows:

- last running—Last copy of the configuration loaded from persistent storage to become the running configuration on the system using the ACLI **activate config** command
- last saved—Last copy of the configuration committed from the editing state to persistent storage on the system using the ACLI **save config** command

These two configurations might represent the same file, which is true when a configuration has been saved and activated. They might also represent different configurations, as is the case when a configuration has been saved but not activated.

Remember to type save-config to make the newly-restored last saved config persistent after a reboot, if it has not been activated.

ACLI Instructions and Examples

In this sample, the last running configuration is being restored.

To restore the last running or last saved configurations:

1. In Superuser mode, type **restore** followed by the word **running**. Then press <Enter>. This restores the last running configuration. For example:

```
ACMEPACKET# restore running
task done
ACMEPACKET#
```

To restore the last saved configuration, refer to the following example:

```
ACMEPACKET# restore saved
task done
ACMEPACKET#
```

Configuration Inventory

You can obtain inventory information using updated ACLI commands. The ACLI commands **show config** and **show running-config** commands accept an inventory argument. When you use the inventory argument, the system tells you the number of each type of configurations (elements) exist in the configuration.

The Net-Net SBC updates the inventories at these times:

- System boot
- Back-up configuration restoration
- Configuration activation
- Addition or deletion of a configuration element to the editing configuration

When there are no elements, the Net-Net SBC reports the number as zero.

Note that the Net-Net SBC does not compare the contents of these elements, and only top-level elements appear in the count.

ACLI Instructions and Examples

To see the inventory for configuration elements on your Net-Net SBC, simply add the inventory argument to either the **show config** or **show running-config** ACLI command. The example in this section shows you information for **show configuration**.

To see the configuration inventory for show configuration:

1. At the system prompt, type **show configuration inventory** and then press <Enter>.

```
ACMEPACKET# show configuration inventory
Current Editing Configuration Inventory:
Element:                 Count:
------------------------ -------
access-control           0
account-config           1
auth-config              0
capture-receiver         0
certificate-record       0
class-policy             0
dns-config               0
enforcement-profile      0
enum-config              0
ext-policy-server        0
h323-config              0
h323-stack               0
host-route               1
```

```
iwf-config                0
lawful-intercept          0
local-policy              1
manual-security-association1
media-manager-config      0
media-policy              0
media-profile             0
net-management-control    0
network-interface         2
network-parameters        0
ntp-config                0
password-policy           0
phy-interface             2
public-key                0
q850-sip-map              0
realm-config              1
realm-group               0
rph-policy                0
rph-profile               0
security-policy           0
session-agent             1
session-constraints       0
session-group             0
session-router            1
session-translation       0
sip-config                1
sip-feature               0
sip-interface             1
sip-isup-profile          0
sip-manipulation          0
sip-nat-config            0
sip-q850-map              0
sip-response-map          0
snmp-community            1
soap-config               0
static-flow               0
steering-pool             1
surrogate-agent           0
system-access-list        0
system-config             1
timezone                  0
tls-global                0
tls-profile               0
transcoding-config        0
translation-rules         0
trap-receiver             2

Total:                    19
```

Standard XML Config File Format

The functionality described in this section is of interest only to those users running software version D700m3p3 and D710A5 or later who want to downgrade to an earlier release. Other users can safely ignore this section.

Configuration files, referred to as *config* files, are stored in XML format. Releases prior to D700m3p3 and D710A5 saved certain special characters in a non-standard XML format. From releases D700m3p3 and D710A5 and forward, these characters have been saved in formats compliant with current W3C XML standards. Character formats are shown below.

Character	Standard XML D720f1	Non-Standard XML Pre D700m3p3 and D710A5
ASCII hard tab	&#xp;	value 0x9
ASCII line feed
value0xA
ASCII carriage return
value0xD
Ampersand	&	&
Less than	<	<
Greater than	>	>
Double quote	"	“
Single quote	'	‘

By default *config* files are now saved using standard XML coding. Consequently pre-D700m3p3 and D710A5 software images are unable to parse such *config* files, complicating the software downgrade process.

To address these complications, the **save-config** and **backup-config** ACLI commands has been enhanced to allow the saving of *config* files and backup configuration files in either standard XML or legacy, non-standard XML format.

save-config ACLI Command

By default, *config* files are saved in standard XML format that is non-parsable by a pre-D700m3p3 and D710A5 software images.

```
ACMEPACKET# save config
checking configuration
-----------------------------------------------------------------------
Results of config verification:
2 configuration warnings
Run 'verify config' for more details
-----------------------------------------------------------------------
Save Config received, processing.
waiting for request to finish
Request to 'SAVE CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
ACMEPACKET# verify-config
-----------------------------------------------------------------------
WARNING: security-policy [SP] local-ip-addr-match has 0.0.0.0. This is
an acceptable configuration if intended.
WARNING: security-policy [SP] remote-ip-addr-match has 0.0.0.0. This
is an acceptable configuration if intended.
-----------------------------------------------------------------------
Total:
```

```
2 warnings

ACMEPACKET#
```

save config, when used in conjunction with the **standard** argument saves *config* files in standard XML format that is non-parsable by pre-D700m3p3 and D710A5 software images.

```
ACMEPACKET# save config standard
checking configuration
------------------------------------------------------------------------
Results of config verification:
2 configuration warnings
Run 'verify-config' for more details
------------------------------------------------------------------------
Save-Config received, processing.
waiting for request to finish
Request to 'SAve conFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
ACMEPACKET# verify-config
------------------------------------------------------------------------
WARNING: security-policy [SP] local-ip-addr-match has 0.0.0.0. This is
an acceptable configuration if intended.
WARNING: security-policy [SP] remote-ip-addr-match has 0.0.0.0. This
is an acceptable configuration if intended.
------------------------------------------------------------------------
Total:
2 warnings
ACMEPACKET#
```

save config, when used in conjunction with the **non-standard** argument saves *config* files in legacy XML format that is parsable by pre-D700m3p3 and D710A5 software images.

```
ACMEPACKET# save config non-standard
checking configuration
------------------------------------------------------------------------
Results of config verification:
2 configuration warnings
Run 'verify-config' for more details
------------------------------------------------------------------------
Save Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
ACMEPACKET# verify-config
------------------------------------------------------------------------
WARNING: security-policy [SP] local-ip-addr-match has 0.0.0.0. This is
an acceptable configuration if intended.
WARNING: security-policy [SP] remote-ip-addr-match has 0.0.0.0. This
is an acceptable configuration if intended.
------------------------------------------------------------------------
Total:
```

```
2 warnings
ACMEPACKET#
```

save backup ACLI Command

By default, backup *config* files are saved in standard XML format that is non-parsable by pre-D700m3p3 and D710A5 software images.

```
ACMEPACKET# save backup testBU
task done
ACMEPACKET#
```

save backup <*filename*> **standard** also saves backup *config* files in standard XML format that is non-parsable by pre-D700m3p3 and D710A5 software images.

```
ACMEPACKET# save backup standardBU standard
task done
ACMEPACKET#
```

save backup<*filename*> **non-standard** saves backup *config* files in legacy XML format that is parsable by pre-D700m3p3 and D710A5 software images.

```
ACMEPACKET# save backup nonStandardBU non-standard
task done
ACMEPACKET#
```

Note: The **standard** and **non-standard** optional arguments are not supported by the **save config** <*filename*> **saved** command, which takes the last saved version of *config* (whatever the XML format), and saves a copy of that file as the backup.

Verify Configuration

The **verify config** command checks the consistency of configuration elements that make up the current configuration and should be carried out prior to activating a configuration on the Net-Net SBC.

When the **verify config** command is run, anything configured that is inconsistent produces either an error or a warning message. An error message lets the user know that there is something wrong in the configuration that will affect the way Net-Net SBC runs. A warning message lets the user know that there is something wrong in the configuration, but it will not affect the way the Net-Net SBC runs. The following is an example of the verify config output:

```
ACMEPACKET# verify config
-------------------------------------------------------------------------
-----------
ERROR: network-interface [private:0] has reference to phy-interface
[private] which does not exist
ERROR: network-interface [public:0] has reference to phy-interface
[public] which does not exist
ERROR: sip-nat [northside] is missing home-address entry
ERROR: sip-nat [northside] is missing ext-proxy-address entry
WARNING: sip-config has nat-mode set to [None], but there are
configured sip-nat objects
ERROR: sip-nat [northside] does not have a sip-interface
ERROR: access-control [172.30.12.12; 0.0.0.0; northside] has reference
to realm-id [northside] which does not exist
```

```
------------------------------------------------------------------------
-----------
Total:
6 errors
1 warning
```

Every time a user executes the **save config** command, **verify config** is automatically run. If any configuration problems are found, you receive a message pointing to the number of errors found during the saving, along with a recommendation to run the **verify config** command to view the errors fully. The following is an example of the **save config** verification output:

```
ACMEPACKET# save config
------------------------------------------------------------------------
Results of config verification:
   6 configuration errors
   1 configuration warning
Run 'verify config' for more details
------------------------------------------------------------------------
-----------
moving file /code/config/tmp/editing/dataDoc.gz ->
/code/config/dataDoc.gz
Save complete
```

Verifying Address Duplication

The **verify-config** command, entered either directly or via the **save-config** command, checks for address duplication for a given network-interface within a configuration. Addresses are checked for duplication based on the following criteria:

- All UDP, TCP, and TFTP addresses are checked against other UDP, TCP, and TFTP addresses respectively within the same port range

The following tables display the entire list of addresses which are checked for duplication, the network-interface or realm which they are checked against, and the port range:

Network-Interface

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
ip-address	Unknown	itself	0	0
ftp-address	Unknown	itself	0	0
snmp-address	Unknown	itself	0	0
telnet-address	Unknown	itself	0	0
dns-ip-primary	Unknown	itself	0	0
dns-ip-backup1	Unknown	itself	0	0
dns-ip-backup2	Unknown	itself	0	0
hip-ip-address	Unknown	itself	0	0
icmp-address	Unknown	itself	0	0

Steering-Pool

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
ip-address	UDP	network-interface or realm-id	start-port	end-port

SIP-Interface

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
sip-port address	transport-protocol (UDP or TCP)	realm-id	sip-port port	0
sip-port address	UDP if transport-protocol is UDP	realm-id	port-map-start	port-map-end

H323-Stack

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
local-ip	TCP	realm-id	q031-port	0
local-ip	TCP	realm-id	q931-start-port	q931-start-port + q931-number-ports - 1
local-ip	TCP	realm-id	dynamic-start-port	dynamic-start-port + dynamic-number-port - 1
local-ip	UDP	realm-id	ras-port	0
gatekeeper	Unknown	realm-id	0	0
alternate-protocol	UDP	realm-id	it's port	0

* If an **h323-stack**'s **q931-port** (TCP) parameter is configured with **a** value of 1720, there is an address duplication exception. This configured port can exist within two port map ranges; the value of **q931-start-port** and its entire port range, and the value of **dynamic-start-port** and its entire port range.

Local-Policy>Local-Policy-Attributes

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
next-hop	Unknown	realm	0	0

Session-Agent

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
ip-address	UDP or TCP	realm-id	port	0
host-name (If different from ip-address)	UDP or TCP	realm-id	port	0
ip-address	UDP or TCP	egress-realm-id if no realm-id or different from it	port	0
host-name (If different from ip-address)	UDP or TCP	egress-realm-id if no realm-id or different from it	port	0

Capture-Receiver

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
address	Unknown	network-interface	0	0

Realm-Config

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
stun-server-ip	UDP	network-interfaces	stun-server-port	0
stun-server-ip	UDP	network-interfaces	stun-changed-port	0
stun-changed-ip	UDP	network-interfaces	stun-server-port	0
stun-changed-ip	UDP	network-interfaces	stun-changed-port	0

Verify-Config Errors and Warnings

The following tables list every error and warning the **verify config** command produces for each configuration element:

Access-Control

Error Text	Reason for Error
WARNING: access-control [id] has unsupported application-protocol [x]	Unsupported protocols [x]
ERROR: access-control [id] has reference to realm-id [xyz] which does not exist	Realm was not found in realm table

Account-Config

Error Text	Reason for Error
ERROR: account-config is enabled, but there are no account servers configured	State is enabled, file-output is disabled and there are not servers
WARNING: account-config is enabled, there are no account-servers configured, but ftp-push is disabled	State and file-output are enabled, there are not account servers and ftp-push is disabled
WARNING: account-config is enabled, account-servers are configured, file-output is disabled, but ftp-push is enabled	State and ftp-push are enabled, account servers are configured, file-output is disabled
ERROR : account-config is enabled, ftp-push is enabled, but there is no ftp-address entered or push-receiver configured	State and ftp-push are enabled, but there is no ftp-address or push-receiver configured
ERROR: account-config has reference to push-receiver [xyz] which can not get password	Password failed decryption
ERROR: account-config has reference to push-receiver [xyz] which does not have remote-path set	Push-receiver has no remote-path set
ERROR: account-config has reference to push-receiver [xyz] which does not have username set	Push-receiver has no username set
ERROR: account-config has reference to push-receiver [xyz] which does not have password set for protocol FTP	Push-receiver has no password set for FTP
WARNING: account-config has reference to push-receiver [xyz] with a public key set, but protocol is set to FTP	Push-receiver has set public key, but protocol is FTP
ERROR: account-config has reference to push-receiver [xyz] which does not have password or public key set for protocol SFTP	Push-receiver has no password or public key set for SFTP
ERROR: account-config has push-receiver [xyz] with reference to public-key [zyx] which does not exist	Public key was not found in public key table
ERROR: account-config has account-server [IP:Port] with empty secret	Account-server [IP:Port] has empty secret field

Auth-config

Error Text	Reason for Error
ERROR: auth-config has specified unsupported protocol [x] for type [y]	Unsupported protocols for given type
ERROR: auth-config has no configured active radius servers for authentication type [x]	No configured active radius for given type

Capture-Receiver

Error Text	Reason for Error
ERROR: capture-receiver [id] has reference to network-interface [xyz] which does not exist	Network-interface was not found in network-interface table

Certificate-Record

Error Text	Reason for Error
ERROR: certificate-record [id] is not trusted and will not be loaded	Certificate record is not trusted
ERROR: certificate-record [id] cannot extract private key	Certificate record failed to extract the private key
ERROR: certificate-record [id] cannot convert PKCS7 string to structure	Failure to convert PKCS7 record to the structure

Class-Policy

Error Text	Reason for Error
ERROR: class-policy [id] has reference to the media-policy [xyz] which does not exist	Media-policy [xyz] was not found in the media-policy table

Collect

Error text	Reason for error
ERROR: collect has sample-interval [x] greater than push-interval [y]	sample-interval greater than push-interval
ERROR: collect has start-time [x] greater than end-time [y]	start-time greater than end-time
ERROR: collect has group [xyz] with sample-interval [x] greater than collection push-interval [y]	group [xyz] has incorrect sample interval
ERROR: collect has group [xyz] with start-time [x] greater than end-time [y]	group [xyz] has incorrect sample interval
ERROR: collect has no push-receivers defined	no push-receivers defined
ERROR: collect has reference to push-receiver [xyz] which does not have user-name set	no user-name set
ERROR: collect has reference to push-receiver [xyz] which does not have password set	no password set
ERROR: collect has reference to push-receiver [xyz] which does not have address set	no address set
ERROR: collect has reference to push-receiver [xyz] which does not have data-store set	no data-store set

DNS-Config

Error text	Reason for error
ERROR: dns-config [id] is missing client-realm entry	missing client realm
ERROR: dns-config [id] has reference to client-realm [xyz] which does not exist	realm was not found in the realm-config table

Error text	Reason for error
ERROR: dns-config [id] has reference to client-address [xyz] which is not local to client-realm [zxy]	address was not found in the NI of the realm-config
ERROR: dns-config [id] does not have any server-dns-attributes	server-dns-attributes are missing
ERROR: dns-config [id] is missing server-realm entry	realm entry is missing (source address is empty)
ERROR: dns-config [id] is missing server-realm entry for source-address [x]	realm entry is missing (source address is not empty)
ERROR: dns-config [id] has reference to server-realm [xyz] which does not exist	realm was not found in the realm-config table
ERROR: dns-config [id] has reference to source-address [xyz] which is not local to server-realm [zxy]	address was not found in the NI of the realm-config

ENUM-Config

Error Text	Reason for Error
ERROR: enum-config [id] is missing realm-id entry	Missing realm
ERROR: enum-config [id] has reference to the realm-id [xyz] which does not exist	Realm [xyz] was not found in realm-config table
ERROR: enum-config [id] has no enum-servers	List of ENUM servers is empty

Ext-Policy-Server

Error Text	Reason for Error
ERROR: ext-policy-server [id] is missing realm entry	Missing realm
ERROR: ext-policy-server [id] address is not valid	Invalid address entry
ERROR: ext-policy-server [id] has reference to protocol [xyz] which is not valid	Invalid protocol entry
ERROR: ext-policy-server [id] has reference to realm [xyz] which does not exist	Realm was not found in the realm-config table
ERROR: ext-policy-server [id] does not have valid operation type	has invalid protocol

H323-Stack

Error Text	Reason for Error
ERROR: h323-stack [id] has no realm-id	Missing realm entry
ERROR: h323-stack [id] has reference to the realm-id [xyz] which does not exist	Realm was not found in the realm-config table
ERROR: h323-stack [id] is missing local-ip address entry	Missing address entry
WARNING : h323-stack [id] has reference to media-profile [xyz] which does not exist	Media profile was not found in media profile table
ERROR: h323-stack [id] has reference to the assoc-stack [xyz] which does not exist	Stack name was not found in the h323-stack table

Host-Route

Error Text	Reason for Error
WARNING: host-route [id] has reference to gateway [xyz] which does not exist in any network-interface	gateway entry was not found in any network-interface object

IWF-Config

Error Text	Reason for Error
WARNING: iwf-config has reference to media-profile [xyz] which does not exist	media profile was not found in media profile table

Local-Policy

Error Text	Reason for Error
ERROR: local-policy [id] has reference to source-realm [xyz] which does not exist	Source-realm [xyz] was not found in realm-config table
WARNING: local-policy [id] has no policy-attributes set	No policy-attributes set
ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to realm [xyz] which does not exist	Realm [xyz] was not found in realm-config table
ERROR: local-policy-attribute [id1] from local-policy [id2] is missing next-hop entry	Next-hop is missing for given attribute
ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which is invalid	Invalid value for the next-hop
ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which does not exist	Value for the next-hop was not found (either from enum-config, or lrt-config, or session-group)
WARNING: local-policy-attribute [id] from local-policy [di] has reference to media-policy [xyz] which does not exist	Media-policy [xyz] was not found in media-policy table

Local-Routing-Config

Error Text	Reason for Error
ERROR: local-routing-config [id] has reference to the file-name [xyz] which does not exist	specified file is missing from /boot/code/lrt folder

Manual-security-association

Error text	Reason for error
ERROR: manual-security-association[id] is missing network-interface entry	missing network-interface entry
ERROR: security-association [id] has reference to network-interface [xyz] which does not exist	network-interface was not found in NI table
ERROR: manual-security-association [id] has invalid local-ip-addr	invalid local-ip-addr entry
ERROR: manual-security-association [id] has invalid remote-ip-addr	invalid remote-ip-addr
ERROR: manual-security-association [id] Unable to decrypt auth-key from configuration. This configuration may not have been saved using this systems configuration password	failed to decrypt auth-key
ERROR: manual-security-association [id] has auth-algo [hmac-md5] with an auth-key of invalid length, must be 32 hex characters long	invalid length of the auth-key for auth-algo [hmac-md5]
ERROR: manual-security-association [id] has auth-algo [hmac-sha1] with an auth-key of invalid length, must be 40 hex characters long	invalid length of the auth-key for auth-algo [hmac-sha1]
ERROR: manual-security-association [id] Unable to decrypt encr-key from configuration. This configuration may not have been saved using this systems configuration password	failed to decrypt encr-key
ERROR: manual-security-association [id] has encr-algo [xyz] with an encr-key of invalid length, must be 64 bits (odd parity in hex)	invalid encr-key length for given algorithm
ERROR: manual-security-association [id] has encr-algo [xyz] with an encr-key of invalid length, must be 192 bits (odd parity in hex)	invalid encr-key length for given algorithm
ERROR: manual-security-association [id] has encr-algo [xyz] with an encr-key of invalid length, must be 128 bits (odd parity in hex)	invalid encr-key length for given algorithm
ERROR: manual-security-association [id] has encr-algo [xyz] with an encr-key of invalid length, must be 256 bits (odd parity in hex)	invalid encr-key length for given algorithm
ERROR: manual-security-association [id] has invalid aes-ctr-nonce (must be non-zero value) for encr-algo [xyz]	has invalid aes-ctr-nonce for given algorithm

Error text	Reason for error
ERROR: manual-security-association [id] has invalid tunnel-mode local-ip-addr (will be set to inner local-ip-address)	invalid tunnel-mode local-ip-addr
ERROR: manual-security-association [id] has invalid tunnel-mode remote-ip-addr (will be set to inner remote-ip-address)	invalid tunnel-mode remote-ip-addr

Network-Interface

Error Text	Reason for Error
ERROR: network-interface [id] has reference to phy-interface [xyz] which does not exist	Phy-interface [xyz] was not found in phy-interface table
ERROR: network-interface [id] has reference to DNS address, but dns-domain is empty	Dns-domain is empty. Word “address” will be plural “addresses” if there are more DNS addresses entered
ERROR: network-interface [id] has reference to DNS address, but ip-address is empty	Ip-address is empty. Word “address” will be plural “addresses” if there are more DNS addresses entered

Phy-Interface

Error Text	Reason for Error
ERROR: phy-interface [id] has invalid operation-type value [x]	Operation-type value is invalid
ERROR: phy-interface [id] of type [x] with port [y] and slot [z] has invalid name	If type is MAINTENANCE or CONTROL name has to start with either “eth” or “wancom”
ERROR: phy-interface [id] of type [x] has duplicated port [y] and slot [z] values with phy-interface [di]	Port and slot values are duplicated with another phy-interface

Public-Key

Error Text	Reason for Error
ERROR: public-key [id] has not generated public/private key pair	No public/private key generated
ERROR: public-key [id] has empty private key	empty private key
ERROR: public-key [id] cannot extract private key	Cannot extract private key

Realm-Config

Error text	Reason for error
ERROR: realm-config [id] has reference to ext-policy-svr [xyz] which does not exist	missing external BW manager
ERROR: realm-config [id] is missing entry for network-interface	missing Network Interface
ERROR: realm-config [id] has reference to network-interface [xyz] which does not exist	network interface was not found in network-interface table
ERROR: realm-config [id] has reference to media-policy [xyz] which does not exist	media-policy was not found in media-policy table
ERROR: realm-config [id] has reference to class-profile [xyz] which does not exist	class-profile was not found in class-profile table
ERROR: realm-config [id] has reference to in-translationid [xyz] which does not exist	in-translationid was not found in session translation table
ERROR: realm-config [id] has reference to out-translationid [xyz] which does not exist	out-translationid was not found in session translation table
ERROR: realm-config [id] has reference to enforcement-profile [xyz] which does not exist	enforcement-profile was not found in enforcement-profile table
ERROR: realm-config [id] has reference to session-constraints [xyz] which does not exist	session-constraints was not found in session-constraints table
ERROR: realm-config [id] has reference sip-profile [xyz] which does not exist	sip-profile was not found sip-profile table
ERROR: realm-config [id] has reference sip-isup-profile [xyz] which does not exist	sip-profile was not found sip- isup-profile table
ERROR: realm-config [id] has reference transcoding-policy [xyz] which does not exist	transcoding-policy was not found transcoding-policy table
ERROR: realm-config [id] has identical stun-server-port and stun-changed port [x]	Stun-server-ip is identical to stun-changed-ip, when stun is enabled.
ERROR: realm-config [id] has identical stun-server-ip and stun-changed-ip [x]	Stun-server-port is identical to stun-changed-port, when stun is enabled.
ERROR: realm-config [id] has reference to dns-realm [xyz] which does not exist	dns-realm doesn't exist in the realm table
WARNING: realm-config [id] has reference to itself as a parent (parent-realm value ignored)	realm name and parent name are the same
ERROR: realm-config [id] has reference to parent-realm [xyz] which does not exist	parent realm doesn't exist in the realm table
ERROR: realm-config [id] with parent-realm [xyz] are part of circular nested realms	realm and its parent realm are part of the closed loop where they referring back to them selves
ERROR: realm-config [id] has reference to in-manipulationid [xyz] which does not exist	in-manipulationid was not found in manipulation table
ERROR: realm-config [id] has reference to out-manipulationid [xyz] which does not exist	out-manipulationid was not found in manipulation table

Realm-Group

ERROR: realm-group [id] has reference to source-realm [xyz] which does not exist	Realm was not found in realm-config table
ERROR: realm-group [id] has reference to destination-realm [xyz] which does not exist	Realm was not found in realm-config table

Security-Policy

Error Text	Reason for Error
ERROR: security-policy [id] has invalid local-ip-addr	Empty local-ip-addr-match
ERROR: security-policy [id] has invalid remote-ip-addr	empty remote-ip-addr
ERROR: security-policy [id] is missing network-interface entry	missing network-interface entry
ERROR: security-policy [id] has reference to network-interface [xyz] which does not exist	network-interface was not found in NI table
ERROR: security-policy [id] priority [xyz] is identical to security-policy [id2] priority	priority duplication

Session-Agent

Error text	Reason for error
ERROR: session-agent [id] has reference to realm-id [xyz] which does not exist	realm was not found in realm table
ERROR: session-agent [id] has reference to in-translationid [xyz] which does not exist	translation id was not found in translation table
ERROR: session-agent [id] has reference to out-translationid [xyz] which does not exist	translation id was not found in translation table
ERROR: session-agent [id] has reference to in-manipulationid [xyz] which does not exist	manipulation id was not found in manipulation table
ERROR: session-agent [id] has reference to out-manipulationid [xyz] which does not exist	manipulation id was not found in manipulation table
ERROR: session-agent [id] has reference to enforcement-profile [xyz] which does not exist	enforcement-profile was not found in enforcement-profile table
ERROR: session-agent [id] has reference to response-map [xyz] which does not exist	response-map was not found in response map table
ERROR: session-agent [id] has reference to local-response-map [xyz] which does not exist	response-map was not found in response map table
ERROR: session-agent [id] has reference sip-profile [xyz] which does not exist	sip-profile was not found in sip-profile table
ERROR: session-agent [id] has reference sip-isup-profile [xyz] which does not exist	sip-isup-profile was not found in sip-isup-profile table

Session-Group

Error Text	Reason for Error
ERROR: session-group [id] has reference to session-agent [xyz] which does not exist	Session agent was not found in the session agent table

Session-Translation

Error Text	Reason for Error
ERROR: session-translation [id] has reference to rules-called [xyz] which does not exist	Translation rule was not found in the translation rule table
ERROR: session-translations [id] has reference to rules-calling [xyz] which does not exist	Translation rule was not found in the translation rule table

SIP-Config

Error text	Reason for error
ERROR: sip-config has reference to home-realm-id [xyz] which does not exist	realm was not found in the realm-config table
ERROR: sip-config has reference to egress-realm-id [xyz] which does not exist	realm was not found in the realm-config table
ERROR: sip-config has reference to enforcement-profile [xyz] which does not exist	enforcement profile was not found in enforcement profile table
WARNING: sip-config is missing home-realm-id for SIP-NAT, defaults to [$INTERNAL$]	missing home-realm-id, defaulted to sip-internal-realm
WARNING: sip-config home-realm-id [xyz] does not have a sip-interface	sip-interface missing for the home realm
WARNING: sip-config has nat-mode set to [None], but there are configured sip-nat objects	nat-mode needs to be set to either Public or Private if there are sip-nat object in the configuration
ERROR: sip-config object is disabled	sip-config is disabled, but there are configured sip-interface objects
ERROR: sip-config [id] has reference to response-map [xyz] which does not exist	response-map was not found in response map table
ERROR: sip-config [id] has reference to local-response-map [xyz] which does not exist	response-map was not found in response map table

SIP-Interface

Error text	Reason for error
ERROR: sip-interface [id] is missing realm-id entry	missing realm
ERROR: sip-interface [id] has reference to realm-id [xyz] which does not exist	realm was not found in realm-config table

Error text	Reason for error
ERROR: sip-interface [id] has reference to in-manipulationid [xyz] which does not exist	in-mainpulationid was not found in manipulation table
ERROR: sip-interface [id] has reference to out-manipulationid [xyz] which does not exist	out-mainpulationid was not found in manipulation table
ERROR: sip-interface [id] has reference to enforcement-profile [xyz] which does not exist	enforcement profile was not found in enforcement profile table
ERROR: sip-interface [id] has reference to response-map [xyz] which does not exist	response-map was not found in response-map table
ERROR: sip-interface [id] has reference to local-response-map [xyz] which does not exist	local-response-map was not found in response-map table
ERROR: sip-interface [id] has reference to constraint-name [xyz] which does not exist	constraint-name was not found in session constraint table
ERROR: sip-interface [id] has no sip-ports	sip-ports are missing
ERROR: sip-interface [id] with sip-port [id2] is missing tls-profile entry	sip-port missing tls-profile entry when protocol is TLS or DTLS
ERROR: sip-interface [id] with sip-port [id2] has reference to tls-profile [xyz] which does not exist	tls-profile was not found in TLS profile table (only valid for protocols TLS or DTLS)
ERROR: sip-interface [id] with sip-port [id2] has reference to ims-aka-profile [xyz] which does not exist	ims-aka-profile was not found in Ims-Aka-Profile table (valid for protocols other than TLS or DTLS)
WARNING: sip-interface [id] has no sip-ports, using SIP-NAT external-address	no sip-ports so SIP-NAT external-address is used
WARNING: sip-interface [id] has no valid sip-ports, using SIP-NAT external-address	no valid sip-ports so SIP-NAT external-address is used
ERROR: sip-interface [id] has reference sip-profile [xyz] which does not exist	sip-profile was not found in sip-profile table
ERROR: sip-interface [id] has reference sip-isup-profile [xyz] which does not exist	sip-isup-profile was not found in sip-isup-profile table

SIP-Manipulation

Error text	Reason for error
ERROR: %SIP_MANIP% is missing name	name missing from the object
WARNING: %SIP_MANIP% has name which contains invalid characters	name has invalid characters
ERROR: %SIP_MANIP% has invalid reject status code	invalid reject status code
ERROR: %SIP_MANIP% is missing new-value entry	missing new-value entry
ERROR: %SIP_MANIP% has new-value that refers to itself from sip-manipulation [xyz]	sip-manipulation calling itself in a loop
ERROR: %SIP_MANIP% is missing mime-header-name	missing mime-header-name
ERROR: %SIP_MANIP% is missing content-type	missing content-type

Error text	Reason for error
ERROR: %SIP_MANIP% has sub-rule with invalid type	sub-rule with invalid type
ERROR: %SIP_MANIP% is missing parameter-name	missing parameter-name
ERROR: %SIP_MANIP% has invalid type	invalid type
ERROR: %SIP_MANIP% is missing header-name	missing header-name
ERROR: %SIP_MANIP% has sub-rule with invalid type	sub-rule with invalid type
ERROR: sip-manipulation requires a name	name missing
ERROR: sip-manipulation [xyz] name overlaps with built-in-sip-manipulation name	name overlaps with built-in-sip-manipulation name
ERROR: sip-manipulation [xyz] has no header-rules defined	no header-rules defined

In order to cover all the possible cases for each entry %SIP_MANIP% was used instead of the actual path for the individual errors and warnings. At this time the path could have two or three levels of depth with each level separated with "from" string as shown below:

```
- header-rule [hr-name] from sip-manipulation [test]
- element-rule [ser-name] from header-rule [hr-name] from sip-
manipulation [test]
```

In the case of missing name for the object only CLI name will be show for any error or warning as shown below:

```
ERROR: header-rule from sip-manipulation [test] is missing name
```

SIP-NAT

Error Text	Reason for Error
ERROR: sip-nat [id] is missing home-address entry	Missing home-address
ERROR: sip-nat [id] has invalid home-address [x] entry	Invalid home-address entry
ERROR: sip-nat [id] is missing ext-address entry	Missing ext-address
ERROR: sip-nat [id] has invalid ext-address [x] entry	Invalid ext-address entry
ERROR: sip-nat [id] is missing ext-proxy-address entry	Missing ext-proxy-address
ERROR: sip-nat [id] has invalid ext-proxy-address [x] entry	Invalid ext-proxy-address entry
ERROR: sip-nat [id] is missing user-nat-tag entry	Missing user-nat-tag
ERROR: sip-nat [id] is missing host-nat-tag entry	Missing host-nat-tag
ERROR: sip-nat [id] is missing domain-suffix entry	Missing domain-suffix
ERROR: sip-nat [id] is missing realm-id entry	Missing realm entry
ERROR: sip-nat [id] does not match sip-interface realm [xyz]	Sip-interface name was not found in realm table
ERROR: sip-nat [id] does not have a sip-interface	Sip-interface is missing
WARNING: sip-nat [id] has same user-nat-tag as sip-nat [di]	Duplicated user-nat-tag

Error Text	Reason for Error
WARNING: sip-nat [id] has same host-nat-tag as sip-nat [di]	Duplicated host-nat-tag
WARNING: sip-nat [id] has ext-address [x] which is different from sip-interface [di] sip-port address [y]	Sip-nat ext-address needs to be the same as sip-port address
ERROR: sip-nat [id] has same home-address [x] as sip-nat [di]	Duplicated home-address
WARNING: sip-nat [id] checking is aborted because home-realm is missing or invalid	sip-nats are configured, but home realm in sip-config is missing
WARNING: sip-nat [id] checking is aborted because home-realm sip-port is invalid	associated sip-interface has no sip-ports and sip-nat is missing home-address entry

Static-Flow

Error Text	Reason for Error
ERROR: static-flow [id] is missing in-realm-id entry	Missing in-realm-id
ERROR: static-flow [id] has reference to in-realm-id [xyz] which does not exist	Realm was not found in the realm-config table
ERROR: static-flow [id] is missing out-realm-id entry	Missing out-realm-id
ERROR: static-flow [id] has reference to out-realm-id [xyz] which does not exist	Realm was not found in the realm-config table
ERROR: ext-policy-server [id] has illegal protocol value [xyz] for TFTP ALG	Invalid protocol entry
ERROR: ext-policy-server [id] has illegal protocol value [xyz] for NAPT ALG	Invalid protocol entry

Steering-Pool

Error Text	Reason for Error
ERROR: steering-pool [id] has invalid start-port [x]	Invalid start-port value (smaller than 1025)
ERROR: steering-pool [id] has start-port [x] greater than end-port [y]	Start-port value is greater than end-port value
ERROR: steering-pool [id] is missing realm entry	Missing realm entry
ERROR: steering-pool [id] has reference to realm [xyz] which does not exist	Realm [xyz] was not found in realm-config table
ERROR: steering-pool [id] has reference to network-interface [xyz] which does not exist	Network-interface [xyz] was not found in NI table

Surrogate-Agent

Error Text	Reason for Error
ERROR: surrogate-agent [id] is missing realm entry	Missing realm entry
ERROR: surrogate-agent [id] has reference to realm [xyz] which does not exist	Realm was not found in the realm-config table
ERROR: surrogate-agent [id] is missing customer-next-hop entry	Missing customer-next-hop entry
ERROR: surrogate-agent [id] is missing register-contact-user entry	Missing register-contact-user entry
ERROR: surrogate-agent [id] is missing register-contact-host entry	Missing register-contact-host entry

TLS-Profile

Error text	Reason for error
ERROR: tls-profile [id] is missing end-entity-certificate entry	missing end-entity-certificate entry
ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not have any certificates	end-entity-certificate entry missing certificate or certificate-record is part of config, but record was not imported to the SD
ERROR: tls-profile [id] has end-entity-certificate [xyz] which has an end entry certificate, but the private key is invalid.	bad private key for the cert-record
ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not exist	certificate record was not found in cert-record table
ERROR: tls-profile [id] found an entry in the trusted-ca-certificates with zero length	found an empty trusted-ca-record in the list
ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] which does not have any certificates	trusted-ca-records entry missing certificate
ERROR: tls-profile [id] has no trusted-ca- certificates, but mutual-authentication is enabled	no trusted certificates, but enabled mutual-authentication

8 Upgrade Management

Overview

You can upgrade your Net-Net 9200 software so that there is no impact or interruption to service.

Net-Net OS S-D7.1.0 Upgrade Prerequisites

Caution: The bootloader MUST be upgraded to bootloader package SWR-0012-00r2p03.tar prior to loading any Net-Net OS version S-D7.1.0 image/baseline of nnSD710b4 or later on the Net-Net 9000. This bootloader is backward compatible to all D600, D700, D710b3 or earlier images.

SWR-0012-00r2p08.tar is the recommended bootloader for Version S-D7.2.0.

After upgrading the bootloader, on the next reboot the new bootloader will be running. This can be verified with the **show version hardware** command.

Caution: It is advised to upload NN9200 Diagnostic Image SWR-0016-00, Rev 2.05 (filename: nnD_diags205.tar) or greater to the Net-Net 9200's **/code/images** directory before upgrading the bootloader. Older diagnostics images will not work with the 09/27/2010 bootloader.

Automatic Online Upgrade

System upgrades are the process of loading a new OS image on the Net-Net 9200. You can load either a newer (upgrade) or older (downgrade) version of the Net-Net OS compared to what is currently running on your system. This section uses the term upgrade interchangeably for an upgrade or downgrade. Bootloader images can be found on the Acme Packet Support Portal.

When upgrading the Net-Net 9200, the upgrade manager determines if the incoming OS is compatible with the existing OS, hardware, and bootloader. The upgrade manager then precedes or halts the upgrade based on the comparison.

System upgrade can be performed without interrupting service. This feature is referred to as an online software upgrade and can only be performed on a Net-Net 9200 with redundant hardware.

Upgrade Overview

During an upgrade, the SPU you initiate the upgrade from goes out of service and reboots with the new image. Before the reboot, you will be prompted to reconnect to the other SPU/MIU and continue guiding the upgrade to completion.

Upgrading from a remote (Telnet or SSH) session is not necessary but is advised because during the upgrade the system displays status messages on the console, which can interfere with your ability to clearly read instructional text. Monitoring console output on both active and standby SPU/MIUs is essential to observe and visually log the system during upgrades.

The upgrade manager guides you through the complete process, offering you the opportunity to confirm and proceed, or halt roll back the upgrade at the following key points.

- After the first reset
- After the first switchover
- After the second reset

At the completion of the upgrade, you can choose to commit, or rollback the upgrade. Committing the upgrade completes the upgrade process, leaving the system running a new image. Rolling back the upgrade reverts the system to its pre-upgrade state.

After the system has been upgraded, the SPUs, NPUs, and TCUs will have switched roles, relative to their pre-upgrade state.

Upgrade Path

To perform an online software upgrade to a newer or older release, your Net-Net 9200 must be running a version that is compatible with the release you are upgrading or downgrading to. This upgrade requirement is known as the roll-through. Roll-through releases are often used as a bridge when upgrading between major OS releases. If you are not running a compatible version, you must first upgrade your system to a valid roll-through.

Please contact TAC to confirm compatibility between your target upgrade software release and your current release.

> **Note:** You can still upgrade from any image to any other image with an offline upgrade or by changing the boot parameters and rebooting, but this action results in a system-wide loss of service.

Online vs. Offline

You can perform an online upgrade or an offline upgrade.

- Online upgrade—the system remains in service during the procedure with no loss of connected calls and minimal disruption of calls in transient states.
- Offline upgrade—the system performs a hard reset of all cards, resulting in the loss of any and all traffic present.

Both the online and offline upgrades are invoked similarly. After the upgrade begins, the ACLI informs you if the system is sufficiently redundant to perform an online OS upgrade. If the Net-Net 9200 is redundant, you can choose either an online or offline upgrade. If the Net-Net 9200 is insufficiently redundant, you can only perform an offline upgrade.

A Net-Net 9200 is considered redundant if each SPU/MIU pair, NPU, or TCU has at least one standby. NIUs are not reset in the OS upgrade process and thus need not be redundant.

Duration

The time needed to complete an OS upgrade depends on:

- Whether the upgrade is online or offline
- Whether an image is located on the Flash RAM, or is downloaded from the network
- The type of image downloaded
- The types of processing units (cards) present

The following times should only be used as an estimate:

- Download a system image: ~3 minutes
- Perform online upgrade with 7 cards: ~15 minutes
- Perform offline upgrade: ~ system reset time

Note: The download duration must be added to the upgrade time. If the image booted from the network, just the upgrade time can be used as an estimate.

Net-Net 9200 Software Upgrade

This section describes how to perform the upgrade procedure.

Virtual Management Interface

To simplify the upgrade, configure the Net-Net 9200's bootparams with a virtual management interface. A virtual management interface is a single IP address that connects you to the active SPU/MIU. To configure and view the virtual management interface's IP address, view the final section of a show bootparams system query. For example:

```
ACMEPACKET# show bootparams

 Boot parameters stored on ACTIVE SPU :

--- Slot 0 Boot Parameters ---
<...>
--- Slot 1 Boot Parameters ---
<...>
--- Virtual Management Interface Parameters ---

Interface IP Address: 172.30.92.96
Gateway IP Address:   172.30.0.1
ACMEPACKET#
```

The virtual management interface IP address follows the active SPU/MIU after a switchover by binding to the active SPU/MIU's MAC address. This means that you can open a remote ACLI session to this address to initiate the upgrade, and when the SPU/MIU pair switches over and you are disconnected from the Net-Net 9200,

you can open a new remote ACLI session to the same address to continue the upgrade.

Netmask Requirement

If you configure a virtual management interface on your Net-Net 9200, and you wish to specify the netmask for the management IP addresses:

- You must explicitly configure the netmask for MIU0's IP address (inet on ethernet), MIU1's IP address (inet on ethernet), and the virtual management IP address (inet on ethernet).

- These three IP addresses must exist within the same network and use the name bitmask.

```
ACMEPACKET# set bootparams

Please specify boot parameters for Slot 0 :

'.' = clear field;  '-' = go to previous field;  ^D = quit

boot device          : eth2
processor number     : 0
host name            : nethost
file name            : /tftpboot/nnSD700m6p1.tar
inet on ethernet (e) : 172.30.251.55:ffff0000
inet on backplane (b):
host inet (h)        : 172.30.0.125
gateway inet (g)     : 172.30.0.1
user (u)             : abcftp
ftp password (pw) (blank = use rsh): abcftp
flags (f)            : 0x0
target name (tn)     : ACMEPACKET
startup script (s)   :
other (o)            :

Please specify boot parameters for Slot 1 :

'.' = clear field;  '-' = go to previous field;  ^D = quit

boot device          : eth2
processor number     : 0
host name            : nethost
file name            : /tftpboot/nnSD700m6p1.tar
inet on ethernet (e) : 172.30.251.54:ffff0000
inet on backplane (b):
host inet (h)        : 172.30.0.125
gateway inet (g)     : 172.30.0.1
user (u)             : abcftp
ftp password (pw) (blank = use rsh): abcftp
flags (f)            : 0x0

target name (tn)     : ACMEPACKET
startup script (s)   :
other (o)            :

Please specify virtual management IP parameters :

'.' = clear field;  '-' = go to previous field;  ^D = quit

inet on ethernet (e) : 172.30.251.54:ffff0000
gateway inet (g)     : 172.30.0.1

Boot parameters have been updated and will take effect on the next reboot.
```

Note: The above bootparameters are applicable for an SPU 1. SPU 2-based systems use a bootdevice of eth0.

File Location Prerequisites

The previously-booted image file, i.e., the image file currently running, must remain present in its original boot location until the upgrade is complete.

Upgrade from Flash

If the previously-booted image file was on the Net-Net SBC's flash, it must remain at the original path with the original filename until the upgrade has successfully completed.

In addition, the image file must also exist on the other SPU at the same path and with the same filename. By convention, you should ensure that the target image file is available on both SPUs in the same absolute location too. For example, if you are upgrading from nnSD700m2.tar to nnSD700m3.tar from flash:

```
SPU0:       /boot/nnSD700m3.tar
            /boot/nnSD700m2.tar

SPU1:       /boot/nnSD700m3.tar
            /boot/nnSD700m2.tar
```

Note: When uploading image files to the Net-Net SBC's SPUs, be sure to connect directly to SPU0 and SPU1 using their individual static IP addresses and not the virtual management IP address.

Upgrade from Network

If the Net-Net SBC was previously-booted from an FTP server, you must ensure that the booted image file remains available at the same network location from where it was originally booted.

For example, if the system's currently booted image is nnSD700m2.tar located on 192.168.20.22 in the /bootimages directory, the same named file must be available at the same address and path when performing an upgrade to later image file, regardless of where the target image file is located.

Process Overview

The following list outlines the major steps that make up an online upgrade.

- Determine if the system can accommodate online upgrade based on redundancy configuration
- Retrieve and validate new OS compatibility with hardware, bootloader, and current running version
- Load new software onto standby cards by resetting them
- Verify upgraded cards are stable and healthy in standby roles
- Switchover to newly upgraded cards
- Load new software only previously -active cards by resetting
- Verify upgraded cards are in a healthy standby state
- Perform third TCU upgrade if applicable
- Commit the upgrade

Upgrade Procedure Command Syntax

To begin an online upgrade, configure the Net-Net 9200 to upgrade from either:

- local flash OS image file
- FTP server based OS image file

If you are upgrading from an FTP server, you can choose to boot directly from the downloaded image file or to save the image file first to local flash storage, then boot from there. By downloading to flash first, the OS image file remains locally available after the Net-Net 9200 is rebooted.

You can specify a path in the image file name if the image file is not located in the FTP account's root location.

The **upgrade os** command syntax is as follows:

```
upgrade os <file name> [<FTP server IP> <username> <password>] <flash
| network>
```

Boot From Local Image File

To upgrade from an OS image file located on the local file system:

You must specify the full path to the image file name. For example, if the OS image file exists on the active SPUs' `/code/images` directory, use the following syntax to start the upgrade:

```
ACMEPACKET# upgrade os /code/images/nnD600m4.tar
```

This syntax upgrades the OS software to the image contained in the file `/code/images/nnD600m4.tar`.

Continue to the Redundancy Check (306) section.

Boot From FTP Server

To upgrade from an OS image file located on an FTP server:

1. If the OS image is on a remote FTP server and you want the Net-Net 9200 to boot directly from that system, use the following syntax to start the upgrade.

   ```
   ACMEPACKET#  upgrade os nnD600m4.tar 172.30.0.2 user password network
   ```

   Continue to the Redundancy Check (306) section.

Download and Boot From Remote Image File

You can download an OS image in advance of the upgrade, and optionally postpone the upgrade until a suitable time without network dependency. If you direct the upgrade manager to download the OS image file from a network server, you can specify to download the file to the local file system. Image files are downloaded to both SPUs' `/code/images` directory. When fully retrieved, the system then boots from this locally stored file.

To download OS image file located on an FTP server to both SPUs and boot from there:

To download an OS image from a remote FTP server and then boot from it locally, use the following syntax:

```
ACMEPACKET# upgrade os nnD600m4.tar 172.30.0.2 username password flash
Preparing for upgrade ...

System is fully redundant and ready for upgrade.

Starting download ...
UPGRADE: Download has started, please stand by...
SPU1 : '+'
SPU0 : '*'
+++***+++***+++******+++***++++++***++++****+++***+++***+++***+++******++++++***+
***+++***+++****+++++++++++++++++
Download finished.

Keep system in service during upgrade [y/n]?: n

 * * * Continuing this upgrade will INTERRUPT SERVICE.

Continue with OFFLINE upgrade [y/n]?: n
Upgrade cancelled.
ACMEPACKET#
```

Note: As the file is downloading, hash marks are printed on the screen in the form of *'s and +s. The *'s indicate a portion of the file being written to the active SPU and the +'s indicate the file as written to the standby SPU. If this succeeds, the OS image is written to both the active and standby SPUs' file systems.

Continue to the Redundancy Check (306) section.

Redundancy Check

After instructing the Net-Net 9200 to begin an OS upgrade, the system indicates whether or not it is sufficiently redundant to perform an online upgrade without an interruption in service. A Net-Net 9200 is considered redundant if each active processor unit (front panel card) has at least one standby.

```
ACMEPACKET# upgrade os nnD600m4.tar 172.30.0.2 username password network

Preparing for upgrade ...

System is fully redundant and ready for upgrade.
```

If the hardware cannot support a live upgrade, the user will be warned of an interruption.

```
ACMEPACKET# upgrade os nnD600m4.tar 172.30.0.2 username password network

Preparing for upgrade ...


 *** System is NOT redundant. ***
There will be a LOSS OF SERVICE for this upgrade.
```

After you configure the Net-Net 9200 with an OS image boot location (and optionally download it to the local file system), and you have chosen either an online or offline upgrade, you are prompted to begin the upgrade.

Note: Minimize network traffic during an online upgrade.

Caution: An offline upgrade is service-interrupting and fails all traffic currently flowing over the Net-Net 9200.

Offline Upgrade

To perform an offline upgrade on a redundant system, reply **N** <enter> to the prompt that questions if you want to perform an online upgrade. The system will offer to perform an offline upgrade at the next prompt.

```
ACMEPACKET# upgrade os /code/images/nnD600m4.tar

Preparing for upgrade ...

System is fully redundant and ready for upgrade.


Keep system in service during upgrade [y/n]?: n

 * * * Continuing this upgrade will INTERRUPT SERVICE.

Continue with OFFLINE upgrade [y/n]?: y
Upgrade in place, ready to reboot!
```

Online Upgrade

To perform an online upgrade on a redundant system, reply **Y** <enter> to the prompt that questions if you want to perform an online upgrade. The Net-Net 9200 will begin the upgrade process immediately.

```
System is fully redundant and ready for upgrade.


Keep system in service during upgrade [y/n]?: y
UPGRADE: Loading current release information...
UPGRADE: Exploding new OS tarball...
UPGRADE: Upgrade files in place...
UPGRADE: Ready to load version D6.0.0m4 04/01/09
UPGRADE: Performing first reset of standby cards...
UPGRADE: Parsing new manifest
UPGRADE: Recieved info for new task eps.
UPGRADE: Virtual reset complete.
UPGRADE: Verifying running version on cardset 0x4a

Standby upgrade complete. Ready to perform first switchover.
```

First Switchover

The upgrade begins after you choose either an online or offline upgrade. The ACLI displays all upgrade messages with the `UPGRADE:` or `DOWNGRADE:` prefix. These messages inform you of the upgrade's progress and prompt you for required action. In addition, the active SPU's console session can be monitored for general system output as the system transitions through the phases of a full upgrade (switchovers, resets, etc.).

The first upgrade milestone is after the standby cards reboot with the new image. Type **y** <enter> at this point to continue. For example:

```
...
UPGRADE: Ready to load version D6.0.0m4 04/01/09
UPGRADE: Performing first reset of standby cards...
UPGRADE: Parsing new manifest
UPGRADE: Recieved info for new task eps.
UPGRADE: Virtual reset complete.
UPGRADE: Verifying running version on cardset 0x4a

Standby upgrade complete. Ready to perform first switchover.

Continue [y/n]?: y
continuing...
UPGRADE: Synchronizing peer Upgrade Manager...
UPGRADE: Synchronizing SNR database with peer...
UPGRADE: Starting switchover....
UPGRADE: Switching over TCU in slot 4 by resetting...
```

The Upgrade Manager pauses at certain milestones to prompt you for confirmation that the system is stable and to allow the upgrade to continue. Answering **No** to any of the Continue prompts starts an OS rollback. The **upgrade cancel** command will rollback any upgrade in progress if the ACLI is not waiting for a response or prompting you for a response. Use <`CTRL + C`> to break and then use the **upgrade cancel** command.

> **Note:** The `UPGRADE:` or `DOWNGRADE:` prompts change to `ROLLBACK:` once a rollback has been initiated.

When the SPU/MIU that you initiate the upgrade from is ready to reboot with the new OS image, the ACLI alerts you must re-login to the other SPU/MIU to continue

the upgrade process. If you are connected to a virtual management IP, you will be disconnected due to the changeover.

```
UPGRADE: Synchronizing peer Upgrade Manager...
UPGRADE: Starting switchover....
UPGRADE: Switching over TCU in slot 4 by resetting...
UPGRADE: Slot 4 has transitioned to the STANDBY state...
UPGRADE: Initiating switchover of slot 2 to standby...
UPGRADE: Slot 2 has transitioned to the STANDBY state...
UPGRADE: Initiating switchover of slot 0 to standby...
UPGRADE:

 *** You are connected to an SPU which is about to become STANDBY.
 *** Please log in to the MIU in slot 1
     and type 'upgrade resume' to continue the upgrade.
```

Shortly after the last line is printed to the ACLI, if you are connected through a virtual management IP address, this Telnet or SSH session is terminated by the Net-Net 9200 and the SPU reboots.

Second SPU Connection

Connect to the active SPU/MIU using either the virtual management IP address or the static IP address for the appropriate SPU. Log in to the Net-Net 9200 and enter superuser mode. At this point, type **upgrade resume** <enter> to continue the upgrade. The Net-Net 9200 prompts you to continue with the upgrade. Type **y <enter>**, and the upgrade continues. For example:

```
Running acliT1
Password:
ACMEPACKET> en
Password:

ACMEPACKET# upgrade resume
UPGRADE: Resuming in-progress os upgrade from state WAIT_RESUME_ACTIVE [OS]

Switchover complete. Ready to perform second virtual upgrade.

Continue [y/n]?: y
continuing...

UPGRADE: Exploding OS tarball...
UPGRADE: Upgrade files in place...
UPGRADE: Continuing upgrade to version D6.0.0m4 04/01/09...
UPGRADE: Resetting standby cards.
UPGRADE: Parsing new manifest
UPGRADE: Virtual reset complete.
UPGRADE: Verifying running version on cardset 0x15
```

Upgrade Completion

After the upgrade completes, you are prompted to commit the upgrade.

Type **y** <enter> and the ACLI prints messages confirming the final cleanup on the screen. At this point you have completed the online upgrade.

```
UPGRADE: Verifying running version on cardset 0x15
UPGRADE: Starting switchover....
UPGRADE: Switching over TCU in slot 5 by resetting...
UPGRADE: Last TCU switch over complete.
UPGRADE: Resetting last TCU ...
UPGRADE: Last TCU reset complete.
UPGRADE: Verifying running version on cardset 0x7f
Upgrade complete. Ready to commit.
Continue [y/n]?: y
continuing...
UPGRADE: Committing OS upgrade ...
UPGRADE: OS upgrade successfully committed.
UPGRADE: Upgrade complete.
Upgrade finished successfully.
ACMEPACKET#
```

A Net-Net 9200 should never be left with more than one OS version running across all cards. After each card reset, and before each switchover, the Net-Net 9200 checks that all active images are the expected version. If there is a version mismatch, the upgrade manager will rollback the upgrade. If you find that mixed OS versions exist on complimentary cards when an upgrade is not in progress, then you must reset any cards that are not running the version specified in the bootparams. Redundancy allows this without interruption. Use the **show version software all** command to confirm like OS versions on all cards. Use the **upgrade status** command to see if an upgrade is in progress.

Canceling an Upgrade

Canceling an upgrade stops the upgrade in progress and begins a rollback to the previous version. The rollback resembles an upgrade but the process functions roughly in reverse and results in the entire system running the original release.

To cancel an upgrade, break out of the upgrade process using <ctrl> + C. Then issue the **upgrade cancel** command. Do not use this command unless the system is stable (i.e., not resetting or switching over). All cards should be in either active or standby state only.

Upgrade Cancellation Warning

Issuing **upgrade cancel** while an upgrade is already being canceled, results in the upgrade process halting, leaving the system in an undefined state. This should only be used to regain control of an unstable system, i.e. to reset cards by hand. If this

command is issued during a rollback, a warning will be issued and the user must confirm the desire to abort the rollback. For example:

```
ACMEPACKET# upgrade cancel

 *** WARNING :

 *** You are about to ABORT this rollback.

 *** This will leave the system in an undetermined state,
 *** which may require manual intervention to correct.
 *** Choose 'y' to continue with abort, 'n' to allow rollback to finish.


Continue [y/n]?: y
continuing...
```

Choosing **n** to this prompt results in the 'upgrade cancel' command returning without interrupting the rollback. If the rollback is aborted, the following message advises the user to manually check and possibly manually restore the proper running versions to all cards:

```
ROLLBACK:

 *** Rollback ABORTED !!
 *** Note that all cards may not be running the correct software version.
 *** Use 'show version software all' to determine which cards to reset.


ACMEPACKET#
```

Upgrade Support Tools

The following tools can aid you in the upgrade process.

Useful ACLI Commands

The following ACLI commands are useful during the upgrade procedure.

- **show version software**—Displays running version information on all or specified processor units (cards) in the system. In the case of an aborted or failed upgrade, the show version command can determine which cards have and have not been upgraded.

  ```
  show version software [slot # | all]
  ```

- **show version hardware** <slot #>—Displays installed hardware part numbers for system or an individual card. Use this command to query your system and determine hardware / software compatibility before beginning an upgrade. Please contact TAC for hardware / software compatibility.
- **switchover**—Swaps activity state of a specified card with its redundant card.

  ```
  switchover <slot #> [active | standby]
  ```

- **show health**—Displays the health score and status of all installed cards on the Net-Net 9200. To view the health of a particular card, include the slot number.

After printing the system health to the ACLI, the show health command also displays a redundancy history (not shown below). For example:

```
ACMEPACKET# show health

  Slot            Type            Health Score    Role
  0               SPU0            100             ACTIVE
  1               SPU1            100             STANDBY
  2               NPU0            100             ACTIVE
  3               NPU1            100             STANDBY
  4               TCU0            100             ACTIVE
  5               TCU1            100             STANDBY
  6               TCU2            50              ACTIVE
  7               MIU0            100             ACTIVE
  8               MIU1            100             STANDBY
  9               PHY0            100             ACTIVE
  10              PHY1            Not Installed
  11              PHY2            Not Installed
  12              PHY3            Not Installed
  13              FANCTRL 0       100             ACTIVE
  14              FANCTRL 1       100             ACTIVE
  15              POWER0          100             ACTIVE
  16              POWER1          100             ACTIVE
  17              POWER2          100             ACTIVE
  18              POWER3          Not Installed

                                Redundancy Event List
```

Local File Space

If there is insufficient storage space for the OS image on either SPU, the system displays a warning message on the ACLI. In this event, you can only upgrade the system without copying the file locally, i.e., upgrade from FTP server.

If a like-named file already exists, you will be prompted to accept overwriting it with the new download. To free local file system disk space, use the following commands:

- **show images**—Lists image files located in the /code/images directory on SPU0 and SPU1.

  ```
  ACMEPACKET# show images
  Images stored on SPU 0:
            nnD600m3p3.tar               3693560 bytes
  Images stored on SPU 1:
            nnD600m3p3.tar               3693560 bytes
  ```

- **delete image**—Deletes a selected image file from the /code/images directory on a specified SPU.

  ```
  delete image image_name [SPU number]
  ```

  For example:

  ```
  ACMEPACKET#delete image nnD600m3p3.tar 0
  ```

Upgrade Commands

This section defines ACLI commands used for upgrade.

- **upgrade status**—Shows the upgrade manager's current state: what type of upgrade is in progress, what stage it is in.

- **upgrade cancel**—Cancels an upgrade in progress by starting a rollback. Do not use this command unless the system is stable (i.e., not resetting or switching over). All cards should be in either active or standby state only.
- **upgrade resume**—Resumes an upgrade in progress. The ACLI might prompt you to continuing waiting or will repeat the last question if still pending.

Suspending Upgrade Output

The upgrade process continues separately from the ACLI session and command that is directing it.

You can exit the upgrade command's output without terminating the upgrade by typing <ctrl> + **c**. This allows you to use the current ACLI session to inspect the system's state, run a new command, or resume the upgrade.

You can then issue the **upgrade resume** command from the ACLI to continue where you left off. If the upgrade manager is waiting for user input, the question is reprinted on the terminal upon resuming the upgrade. If the upgrade manager is processing, and not waiting for user input, then resuming the ACLI session displays any progress messages.

Net-Net 9200 Bootloader Upgrade

Upgrading a bootloader is the process of updating the flash memory with the executable code that each CPU uses to boot when the system is powered on.

You can load either a newer (upgrade) or older (downgrade) version of the bootloader compared to the version currently running on your system. This section uses the term upgrade interchangeably for an upgrade or downgrade.

The upgrade manager validates hardware compatibility between the bootloader package and the current hardware. It then precedes or halts the upgrade based on the comparison.

Bootloader upgrades can be performed without interrupting service. Redundant cards do not need to be present for a bootloader upgrade. However, after cards are inserted into the system, you may need to perform a bootloader upgrade again for these new cards.

Bootloader Upgrade Precautions

Because a failed bootloader upgrade might render the Net-Net 9200 unbootable, special precautions must be taken when upgrading.

- The Net-Net 9200 disables HA switchovers when upgrading the bootloader. Therefore, ensure that the environmental and network conditions are minimized so that switchover-inducing-events do not occur.
- Perform all upgrades during low traffic periods.
- Ensure that both power supplies are powered by individual, backed-up circuits.

Duration

The time needed to complete an bootloader upgrade varies based on the number of cards that are present. The following times should only be used as an estimate:

- Download a bootloader package: ~10 seconds
- Perform upgrade with 7 cards: ~ 2 minutes

Bootloader File Location

The Net-Net 9200 can upgrade the bootloader from either a locally stored bootloader package or a bootloader package located on an FTP server.

On Local Filesystem

Use an FTP client to upload the bootloader package file in the Net-Net 9200's `/code/images` directory.

Note: Upload the bootloader package file to both SPUs.

On FTP Server

When the bootloader package file is booted from the FTP server, it is first downloaded to the active SPUs' `/code/images` directory. The ACLI will notify you if there is insufficient storage space on the active SPU for the bootloader package file.

```
Not enough space to copy release to flash.
You may need to make space using the 'show|delete images' commands.
```

The Net-Net 9200 then aborts the bootloader upgrade. You must free disk space by deleting files to continue. See the Backup File Management (275) section for how to fix this. If a like-named file already exists, you will be prompted to accept overwriting it with the new download.

Process Overview

The following list outlines the major steps that make up an online upgrade.

- Configure system to install bootloader from local filesystem or from FTP Server
- Commit bootloader upgrade

Upgrade Procedure Command Syntax

This section explains how to perform the bootloader upgrade procedure. Use the **upgrade bl** command to start the bootloader upgrade process. The **upgrade bl** command is entered as follows:

```
upgrade bl <filename> <card> [<IP address> <username> <password>]
```

- filename—bootloader package path and filename.
- card— **all** - upgrade all cards | **0**-**6** - specific processor card to upgrade

When upgrading the bootloader from file on an FTP server, you must supply the following additional credentials:

- ip address—IP address of FTP server
- username—username for FTP server
- password—password for FTP server

Upgrade Bootloader From Local File

To upgrade the bootloader from a local booloader package file:

1. At the superuser prompt, type the command using the following syntax to begin bootloader upgrade from a local bootloader package file. You must specify the absolute path on the Net-Net 9200's flash RAM in the **upgrade bl** command:

   ```
   ACMEPACKET# upgrade bl /code/images/SWR-0012-00r2p01.tar all
   ```

```
Preparing for upgrade ...


***** WARNING: Do NOT powerdown, remove, or reset any card   *****
```

Continue to the Commit Bootloader Upgrade (315) section of the documentation.

Upgrade Bootloader From FTP Server

To upgrade the bootloader from a booloader package file on an FTP server:

1. At the superuser prompt, type the command using the following prototype to begin bootloader upgrade from a local bootloader package file. You must specify the absolute path on the Net-Net 9200's flash RAM in the **upgrade bl** command:

```
ACMEPACKET# # upgrade bl SWR-0012-00r2p01.tar all 172.30.0.34 username
password

Preparing for upgrade ...

Starting download ...
SPU1 : '*'

*...*
...
Download finished.

***** WARNING: Do NOT powerdown, remove, or reset any card   *****
```

Continue to the Commit Bootloader Upgrade (315) section of the documentation.

Commit Bootloader Upgrade

To commit the bootloader upgrade:

1. Type **y** <enter> to confirm that you want to begin the update process. From this point you may NOT remove power from the system.

```
Continue [y/n]?: y
slot 0 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 1 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 2 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 3 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 4 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 5 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
slot 6 bootloader part# 00-0040-xx rev 1.09 upgrade to 2.01
.................
Slot 5 successfully upgraded.
.
Slot 6 successfully upgraded.

Slot 1 successfully upgraded.
.
Slot 2 successfully upgraded.
.
Slot 4 successfully upgraded.
.
Slot 3 successfully upgraded.
```

```
....
Slot 0 successfully upgraded.

Upgrade Completed.
```

Verify the Bootloader Upgrade

After each CPU's bootloader is successfully upgraded, the device's revision number is updated too. Each card's functional revision is updated by appending an **A** to the functional revision number. This A designation is not viewable from older versions of the Net-Net software.

You can verify the upgrade by using the **show version hardware** <card> command. This command displays the bootloader that the Net-Net 9200 is currently booted with, i.e., the current runtime. The bootloader is indicated by date. For example, you can query card 0, SPU0. Observe the bootloader revision date for each CPU's core 0:

```
ACMEPACKET# show version hardware 0


Slot   Cpu    Core   Boot Loader Rev CPLD1 Rev   CPLD2 Rev   Memory Size
0      0      0      09/10/2008      0.3.2       0.0.8       1024MB
0      0      1      N/A             0.3.2       0.0.8       1024MB
0      1      0      09/10/2008      N/A         N/A         1024MB
0      1      1      N/A             N/A         N/A         1024MB
0      2      0      09/10/2008      N/A         N/A         1024MB
0      2      1      N/A             N/A         N/A         1024MB
0      3      0      09/10/2008      N/A         N/A         1024MB
0      3      1      N/A             N/A         N/A         1024MB
0      4      0      09/10/2008      N/A         N/A         1024MB
0      4      1      N/A             N/A         N/A         1024MB
```

You can view more information by using the **show version hardware** command for the whole system. This show command displays which bootloader, by version will be used to boot the Net-Net 9200 on next reboot (or restart).

When you upgrade the bootloader, the version number for the xx-xx40-xx device will change, but the date in the **show version hardware** command only changes after the system has been rebooted.

Notice the xxx-xx40-xx programmable device is at a higher revision than before the upgrade.

```
ACMEPACKET# show version hardware

Type    Part Number     Serial Number   Func Rev  Artwk Rev
----    -----------     -------------   --------  ---------
SPU0    002-0507-50     060712001671      4.11A     4.00

Programmable Devices:
        ---------------------
        1. 004-0025-xx Rev:             4.00
        2. 004-0028-xx Rev:             1.10
        3. 004-0029-xx Rev:             1.04
        4. 004-0030-xx Rev:             1.01
        5. 004-0031-xx Rev:             1.00
        6. 004-0040-xx Rev:             2.01
```

TCU/TCM Upgrade

Hardware Upgrade Recommendation

When planning to upgrade transcoding hardware (TCUs and TCMs) in your Net-Net 9200 system, you should bias your equipment allocation toward 3 TCUs with fewer TCMs rather than 2 TCUs and maximized TCMs.

This recommendation enables hitless upgrades for future increases in channel density.

Single to Double Active TCU Upgrade

Upgrading from a single active TCU configuration to a double active TCU configuration is not dynamically supported by the Net-Net 9200 and requires a reboot. The general procedure is:

1. Remove the blank TCU panel from the Net-Net 9200 System Chassis.
2. Insert the new TCU into the system.
3. Wait until the TCU is recognized and settles to the "OOS" state by using the **show status** command.
4. Set the system-config configuration element's **tcu-double-active** parameter to **enabled.**
5. Reboot the system.

   Note: See the Net-Net 9200 TCM Installation Guide (401-0106-00) for all prerequisites, requirements and procedures for this maintenance.

Offline Transcoding Hardware Maintenance

Removing TCMs from an TCUs is not a hitless procedure. To efficiently remove TCMs from a system, you should drain active traffic from the system and re-route it through an alternate Net-Net system if possible.

Hitless TCM Upgrades

Adding TCMs to existing TCUs can be preformed without affecting existing service. This is considered a hitless upgrade. The following overview lists how to perform a TCM upgrade with no impact to active transcoded sessions.

Note: Fan packs and power supply listing in show status commands are removed for brevity.

Definitions

- 1+1 Redundancy: 1 Active TCU with 1 Standby TCU that can assume all transcoding traffic in the event of a failure.
- 2+1 Redundancy: 2 Active TCUs with 1 Standby TCU that can assume up to half the transcoding traffic in the event of a failure.

Please have the Net-Net 9200 TCM Installation Guide (401-0106-00) on hand for reference and additional procedural explanations.

Upgrade Procedure: 1+1 Redundancy

1. Identify the standby TCU by using the **show status** command.

```
ACMEPACKET# show status

Slot   Type      State           Role          Temperature CPU       Memory
  0    SPU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  1    SPU1      Not Installed
  2    NPU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  3    NPU1      CARD RUNNING    STANDBY       Normal      Normal    Normal
  4    TCU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  5    TCU1      CARD RUNNING    STANDBY       Normal      Normal    Normal
  6    TCU2      Not Installed
  7    MIU0      CARD RUNNING    ACTIVE        Normal      N/A       N/A
  8    MIU1      Not Installed
  9    PHY0      CARD RUNNING    ACTIVE        Normal      N/A       N/A
  10   PHY1      UNCONFIGURED    UNASSIGNED    Normal      N/A       N/A
  11   PHY2      Not Installed
  12   PHY3      Not Installed
```

Note that TCU0 in slot 4 is the Active TCU, while TCU1 in slot 5 is in standby role.

Verify that the expected number of TCMs are present on the active TCU with the show xclient xlist command. The following screen shot shows two active xservers, which control 2 TCMs, on the active TCU.

```
ACMEPACKET# show xclient xlist
Requesting XClient's list of XServers:
VA_addr               VC_addr               Slot    Id   DSPs   #Sess  Cache
==================    ==================    ====    ==   ====   =====  =====
XServ_1: 169.254.178.0:8012 169.254.164.0:8012 4       0    10     15     4
XServ_2: 169.254.178.1:8012 169.254.164.1:8012 4       0    10     14     4
Xserv_3: -
Xserv_4: -
Xserv_5: -
Xserv_6: -
Xserv_7: -
Xserv_8: -
ACMEPACKET#
```

Verify 2 TCMs are present on the standby TCU with the **show xserv 5.0.0 sysinfo** and **show xserv 5.0.1 sysinfo** commands. In the following screen shot,

the TCU in location A is present. The following screen shot omits querying TCM B, **show xserv 5.0.0 sysinfo**, which would be preformed in this procedure.

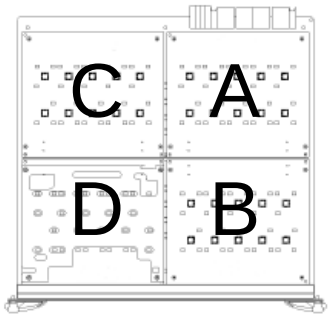
```
ACMEPACKET# show xserv 5.0.1 sysinfo
System not initialized for an active context.
Displaying STANDBY system information:
-------------------------------------------
XSERVER System Info for Context #0
-------------------------------------------
core ID         : 0
cpu  ID         : 0
slot ID         : 0
tile ID         : 2
numDevices      : 10
numTiles        : 1
sessions per DSP: 100
FAX      per DSP: 5
Initialized     : 1
Active DSP count: 10
Avail Sess count: 1000
Avail Fax  count: 50
Free  Sess count: 985
Free  Fax  count: 50
VAPI Initialized: 1
-------------------------------------------
XSERVER System Info for Context #1
-------------------------------------------
core ID         : 0
cpu  ID         : 0
slot ID         : 0
tile ID         : 2
numDevices      : 10
numTiles        : 1
sessions per DSP: 100
FAX      per DSP: 5
Initialized     : 1
Active DSP count: 10
Avail Sess count: 1000
Avail Fax  count: 50
Free  Sess count: 1000
Free  Fax  count: 50
VAPI Initialized: 1
```

When querying the standby TCU to ascertain which TCMs are present, use the **show xserv x.x.x sysinfo** command. Each time you execute this command for an xserver on a standby TCM, two contexts will be reported. The following table lists the core-to-TCM mapping:

Core to query	Tile ID reported in software	Physical TCM location
x.0.0	0	C
x.0.1	2	A

Core to query	Tile ID reported in software	Physical TCM location
x.1.0	1	D
x.1.1	3	B

The following image shows physical TCM location relative to the TCU:



2. Remove the standby TCU from the Net-Net 9200. In the following **show status** screen shot, note that TCU1 in Slot 5 has been removed.

```
ACMEPACKET# show status

Slot   Type      State           Role          Temperature CPU       Memory
  0    SPU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  1    SPU1      Not Installed
  2    NPU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  3    NPU1      CARD RUNNING    STANDBY       Normal      Normal    Normal
  4    TCU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  5    TCU1      Not Installed
  6    TCU2      Not Installed
  7    MIU0      CARD RUNNING    ACTIVE        Normal      N/A       N/A
  8    MIU1      Not Installed
  9    PHY0      CARD RUNNING    ACTIVE        Normal      N/A       N/A
  10   PHY1      UNCONFIGURED    UNASSIGNED    Normal      N/A       N/A
  11   PHY2      Not Installed
  12   PHY3      Not Installed
```

3. Add new TCMs to the TCU you removed from the Net-Net 9200 chassis by following the procedure in the TCM Installation section of the Net-Net 9200 TCM Installation Guide.

Caution: You must adhere to the mandatory TCM installation order illustrated on page 9 of the Net-Net 9200 TCM Installation Guide.

4. Reinsert the upgraded TCU by following the procedure in the TCU Replacement section of the Net-Net 9200 TCM Installation Guide.

5. Execute the show status command to confirm that the upgraded TCU has progressed through the normal progression of states until it reaches “CARD

RUNNING" state in the STANDBY role. This can take several minutes depending on the number of transcoded sessions that must be replicated across the redundant card. For example:

```
ACMEPACKET# show status

Slot   Type      State           Role          Temperature CPU       Memory
  0    SPU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  1    SPU1      Not Installed
  2    NPU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  3    NPU1      CARD RUNNING    STANDBY       Normal      Normal    Normal
  4    TCU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  5    TCU1      CARD RUNNING    STANDBY       Normal      Normal    Normal
  6    TCU2      Not Installed
  7    MIU0      CARD RUNNING    ACTIVE        Normal      N/A       N/A
  8    MIU1      Not Installed
  9    PHY0      CARD RUNNING    ACTIVE        Normal      N/A       N/A
  10   PHY1      UNCONFIGURED    UNASSIGNED    Normal      N/A       N/A
  11   PHY2      Not Installed
  12   PHY3      Not Installed
```

6. Execute the **show xserv 5.x.x sysinfo** command, described in Step 3, to confirm that all new TCMs have are operating correctly.

7. Remove the active TCU, TCU0 in Slot 4. This forces TCU1 to become active and assume all transcoding traffic.

```
ACMEPACKET# [RM: SPU Slot=0] - TCU in Slot 5 Assuming Active Role
[SM: Slot=0] - Got ACTIVE COMPLETE from CM cm@5.0.0
[RM: SPU Slot=0] - TCU Slot 5 has transitioned to ACTIVE

ACMEPACKET# show status

Slot   Type      State           Role          Temperature CPU       Memory
  0    SPU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  1    SPU1      Not Installed
  2    NPU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  3    NPU1      CARD RUNNING    STANDBY       Normal      Normal    Normal
  4    TCU0      Not Installed
  5    TCU1      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  6    TCU2      Not Installed
  7    MIU0      CARD RUNNING    ACTIVE        Normal      N/A       N/A
  8    MIU1      Not Installed
  9    PHY0      CARD RUNNING    ACTIVE        Normal      N/A       N/A
  10   PHY1      UNCONFIGURED    UNASSIGNED    Normal      N/A       N/A
  11   PHY2      Not Installed
  12   PHY3      Not Installed
```

8. Add new TCMs to the TCU you removed from the Net-Net 9200 chassis by following the procedure in the TCM Installation section of the Net-Net 9200 TCM Installation Guide.

Caution: The TCMs on each card must be placed in the SAME physical locations for all TCUs for redundancy. All TCUs in the system must have the SAME number of TCMs.

9. Reinsert the upgraded TCU by following the procedure in the TCU Replacement section of the Net-Net 9200 TCM Installation Guide. The following appears as the card boots and assumes operation:

```
ACMEPACKET# [SM: Slot=0] - Got READY from CM cm@4.0.0
Card in Slot 4 Transitioning to Standby Role
[SM: Slot=0] - Got STANDBY COMPLETE from CM cm@4.0.0
[RM: SPU Slot=0] - TCU Slot 4 has transitioned to STANDBY
```

10. Execute the show status command to confirm that the upgraded TCU has progressed through the normal progression of states until it reaches "CARD RUNNING" state in the STANDBY role. This can take several minutes depending on the number of transcoded sessions that must be replicated across the redundant card. For example:

```
ACMEPACKET# show status

Slot   Type      State           Role          Temperature CPU       Memory
  0    SPU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  1    SPU1      Not Installed
  2    NPU0      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  3    NPU1      CARD RUNNING    STANDBY       Normal      Normal    Normal
  4    TCU0      CARD RUNNING    STANDBY       Normal      Normal    Normal
  5    TCU1      CARD RUNNING    ACTIVE        Normal      Normal    Normal
  6    TCU2      Not Installed
  7    MIU0      CARD RUNNING    ACTIVE        Normal      N/A       N/A
  8    MIU1      Not Installed
  9    PHY0      CARD RUNNING    ACTIVE        Normal      N/A       N/A
  10   PHY1      UNCONFIGURED    UNASSIGNED    Normal      N/A       N/A
  11   PHY2      Not Installed
  12   PHY3      Not Installed
```

11. Execute the **show xserv 4.x.x sysinfo** command, described in Step 3, to confirm that all new TCMs have are operating correctly.

Upgrade Procedure: 2+1 Redundancy

This abbreviated procedure is for upgrading TCUs running in a 2+1 configuration. Please reread the previous section for background about this procedure.

1. Remove the standby TCU from the Net-Net 9200.
2. Add TCMs to the TCU according to the Net-Net 9200 TCM Installation Guide
3. Replace the upgraded TCU in the Net-Net 9200.
4. Execute the **show xserv x.x.x sysinfo** command to confirm that all new TCMs are operating correctly.

5. Choose the second TCU to upgrade.
6. Ensure that each TCU's State is "Card Running" in either ACTIVE or STANDBY role.
7. Remove the second TCU from the Net-Net 9200.
8. Add TCMs to the TCU according to the Net-Net 9200 TCM Installation Guide
9. Replace the upgraded TCU in the Net-Net 9200.
10. Execute the **show xserv x.x.x sysinfo** command to confirm that all new TCMs are operating correctly.
11. Ensure that each TCU's State is "Card Running" in either ACTIVE or STANDBY role.
12. Remove the third, upgraded TCU from the Net-Net 9200.
13. Add TCMs to the TCU according to the Net-Net 9200 TCM Installation Guide
14. Replace the upgraded TCU in the Net-Net 9200.
15. Execute the **show xserv x.x.x sysinfo** command to confirm that all new TCMs are operating correctly.

9 Index

A

B

C

D

E

F

G

H

I

L

M

N

P

Q

R

S

T

U