Net-Net® 9000
ACLI Reference Guide
Release Version S-D7.1.0

Acme Packet, Inc.
100 Crosby Drive
Bedford, MA 01730 USA
t 781-328-4400
f 781-275-8800
www.acmepacket.com

Last Update: May 21, 2013
Document Number: 400-0076-71 Rev 2.10

Notices

Table of Contents

About this Guide

The *Net-Net 9000 ACLI Reference Guide* provides a comprehensive explanation of all commands and configuration parameters available to you in the Acme Command Line Interface (ACLI). This programming interface is used for configuring your Net-Net family of products. This document does not explain configurations and the logic involved in their creation.

Who is Acme Packet?

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

Established in August 2000 by networking industry veterans, Acme Packet is a public company traded on the NASDAQ and headquartered in Bedford, MA.

Document Organization

- About this Guide—This chapter.
- How to Use the ACLI—Explains how to use the ACLI, the CLI-based environment for configuring the Net-Net family of products.
- Commands A-M—Lists commands starting with A-M, their syntax, and their usage.
- Commands N-Z—Lists commands starting with N-Z, their syntax, and their usage.
- Configuration Elements A-M—Lists configuration elements starting with A-M, their syntax, and their usage. Subelements are listed directly after the element where they are located.
- Configuration Elements N-Z—Lists configuration elements starting with N-Z, their syntax, and their usage. Subelements are listed directly after the element where they are located.
- ACLI Command Summary—Lists all ACLI commands.
- ACLI Configuration Element Tree—Shows a graphical representation of all configuration elements and subelements in a tree-type format that reflects their hierarchical position in the ACLI.

Audience

This document is written for all users of the Net-Net SBC. Since the ACLI is one of the primary ways of configuring, monitoring, and maintaining your Net-Net SBC, this document lists the ACLI commands and their syntax.

Conventions

This section explains the documentation conventions used in this guide. Each of the following fields is used in the *Net-Net ACLI Reference Guide*.

The following are the fields associated with every command or configuration element in this guide. When no information is applicable, the field is simply omitted (this occurs mostly with the Notes field).

- **Description**—Describes each command, its purpose, and use.
- **Syntax**—Describes the proper syntax needed to execute the command. Syntax also includes syntax-specific explanation of the command.
- **Arguments**—Describes the argument place holders that are typed after a command. For commands only.
- **Parameters**—Describes the parameters available in a configuration element. For configuration elements only.
  - **Default**—Default value that populates this parameter when the configuration element is created.
  - **Values**—Valid values to enter for this parameter.
- **Notes**—Lists additional information not included in the above fields.
- **Mode**—Indicates whether the command is executed from User or Superuser mode.
- **Path**—Describes the ACLI path used to access the command.
- **Release**—Gives the original release version and the release last modified version for the command.

This guide uses the following callout conventions to simplify or explain the text.

Caution: This format is used to advise administrators and users that failure to take or avoid a specified action can result in loss of data or damage to the system.

Style

This guide uses the stylistic conventions identified within the following table to clarify and to distinguish specialized text from the main text.

Style	Definition
<Keypress or Keypress Combination>	Angle brackets distinguish a keypress or a keypress combination (e.g., <Tab>, <Ctrl-Alt-Delete>) from the text surrounding it.
`Code` or `Location`	Text in `Lucida Console` font identifies code or the location of an item (e.g., in a file or directory). You can identify it as the Lucida Console fixed-width font common in many terminal programs.
`user-entered-text`	Text in **`Lucida Console BOLD`** style depicts data that the user enters. You can identify it as the Lucida Console fixed-width font.
command	This style depicts a command or pre-determined text to be typed into the ACLI. You can identify it as text set in bold style.

Associated Documentation

The Net-Net SBC and Net-Net SBC OS Release 5.0 are supported by the documentation listed in the table below.

Document Number	Document Name	Description
400-0073-20	Net-Net 9200 Hardware Guide	Describes the hardware components of the Net-Net SBC, and provides removal and replacement procedures
400-0074-71	Net-Net 9000 Configuration Guide Release Version 7.1	Provides explanations of features and functions, and provides instructions for configuring your Net-Net SBC using the Acme Packet command-line interface
400-0077-71	Net-Net 9000 MIB Reference Guide Release Version 7.1	Provides information about the Net-Net SBC's MIB, trap, and alarm support
400-0078-71	Net-Net 9000 RADIUS Reference Guide Release Version 7.1	Provides information about the Net-Net SBC's RADIUS support, including Acme Packet VSAs

Document Number	Document Name	Description
400-0079-71	Net-Net 9000 Maintenance and Troubleshooting Guide Release Version 7.1	Provides information about viewing and interpreting Net-Net SBC statistics, as well as other maintenance information
400-0080-71	Net-Net 9000 Release Notes Release Version 7.1	Provides an overview of the Net-Net SBC hardware and the Net-Net SBC OS Release 5.0; includes caveats and limitations, and known issues with workarounds

Customer Questions, Comments, or Suggestions

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

Contact Us

Acme Packet
100 Crosby Drive
Bedford, MA 01730 USA
t 781 328 4400
f 781-275-8800
http://www.acmepacket.com

Document Revision History

This section provides a chronological overview of the changes made to this document starting with the first revision after the GA posting.

Date	Revision Number	Description
December 01, 2010	Revision 1.01	• Updates trap receiver configuration element
May 31, 2012	Revision 2.00	• Revises definition for register-contact-host (should be home-address, not home-proxy-address) for surrogate-agent • Adds Note for application-protocol: "If application-protocol is set to none, the destination-address and port will be used. Ensure that your destination-address is set to a non-default value (0.0.0.0.)" • Adds Note for customer-next-hop: "Even though the customer-next-hop field allows specification of a SAG or FQDN, the functionality will only support these values if they resolve to a single IP address. Multiple IP addresses, via SAG, NAPTR, SRV, or DNS record lookup, are not allowed." • Revises descriptive text for session-constraints, specifically, adds the second paragraph and Note • Adds Note for local-routing-config: "Entering XML comments on the same line as LRT XML data is not currently supported." • Adds disconnect-on-timeout and gate-spec-mask parameter definitions for ext-policy-server • Adds last sentence to definition for permit-on-reject for ext-policy-server • Adds additional information and Note for sustain-rate-window for session-agent • Adds Note for gateway (for host-route): "The gateway entered must already be defined as a gateway for an existing network interface." • Revises defintion for next-hop for local-policy->policy-attributes (as pertaining to SAGs) • Adds three values to comparison-type: refer-case-sensitive, refer-case-insensitive, and boolean (sip-manipulation, header-rules) • Revises the definition for ttr-no-response for session-agent • Revises the definition for time-to-resume for session-agent • Corrects the ACLI command for creating backups to **save backup <name>** • Changes the section title: backup-config to **save backup** • Changes the command: **backup-config** to **save backup** as listed in the ACLI Command Summary
May 21, 2013	Rev 2.10	• Removed READ-WRITE from access-mode in snmp-community

1 How to Use the ACLI

The ACLI

The ACLI is an administrative interface that communicates with other components of the Net-Net SBC. The ACLI is a single DOS-like, line-by-line entry interface.

The ACLI is modeled after industry standard CLIs. Users familiar with this type of interface should quickly become accustomed to the ACLI.

Using the ACLI

You can access the ACLI either through a direct console connection, a Telnet connection, or an SSH connection.

Local Console Access

Console access takes place via a serial connection to the console port directly on the Net-Net SBC chassis. When you are working with the Net-Net SBC at the console, the ACLI comes up automatically.

Accessing the ACLI through a console connection is the most secure method of connection, given that the physical location is itself secure.

Remote Telnet Access

Accessing the ACLI via Telnet gives you the flexibility to connect to your Net-Net SBC from a remote location. In addition, you can administer multiple Net-Net SBCs from a single location.

Caution: Security is a main issue of concern with a Telnet connection. If you elect to use a Telnet connection to configure your Net-Net SBC, be aware that Telnet connections are not secure. You should connect your Net-Net SBC's management interface to a secure administrative LAN.

Remote SSH Access

SSH provides strong authentication and secure communications over unsecure channels. Accessing the ACLI via an SSH connection gives you the flexibility to connect to your Net-Net SBC from a remote location over an insecure connection.

Exiting the ACLI

Typing **`exit`** at any ACLI prompt moves you to the next "higher" level in the ACLI. After exiting through enough ACLI levels you will eventually log yourself out of the system.

Navigation Tips

This section provides information about hotkeys used to navigate the ACLI. This information applies to both User mode and Superuser mode, although the specific commands available to those modes differ.

Hotkeys

Hotkeys can assist you in navigating and editing the ACLI, and they also allow you to scroll through a list of commands that you have recently executed. These hotkeys are similar to those found in many other CLIs. The following table lists ACLI hotkeys and a description of each.

Category	Hotkey	Description
General	<Ctrl-D>	Equivalent of the **done** command when used at the end of a command line. When used within a command line, this hotkey deletes the character at the cursor when it is used within the command line.
	<UParrow>	Scrolls forward through former commands.
	<DOWNarrow>	Scrolls backward through former commands.
	<Tab>	Completes a partially entered command or lists all options available if the characters entered match multiple commands. Executed at the beginning of the command line, this hotkey lists the configurable elements/parameters and available commands for that configuration level.
	!	Functions like the **done** command, but it is used at the end of a command line.
Context-Sensitive Help	?	Provides context-sensitive help. It functions both for ACLI commands and configuration elements.
Moving the Cursor	<Ctrl-B>	Moves the cursor back one character.
	<Esc-B>	Moves the cursor back one word.
	<Ctrl-F>	Moves the cursor forward one character.
	<Esc-F>	Moves the cursor forward one word.
	<Ctrl-A>	Moves the cursor to the beginning of the command line.
	<Ctrl-E>	Moves the cursor to the end of the command line.
	<Ctrl-L>	Redraws the screen.

Category	Hotkey	Description
Deleting Characters	<Delete>	Deletes the character at the cursor.
	<Backspace>	Deletes the characters behind the cursor.
	<Ctrl-D>	Deletes the character at the cursor when used from within the command line.
	<Ctrl-K>	Deletes all characters from the cursor to the end of the command line.
	<Ctrl-W>	Deletes the word before the cursor.
	<Esc-D>	Deletes the word after the cursor.
Displaying Previous Command Lines	<Ctrl-P>	Scrolls backward through the list of recently executed commands.
	<Ctrl-R>	Searches the command history for the character(s) you enter. These characters appear within single quotation marks (''). When you press <UParrow> and <DOWNarrow>, the ACLI scrolls through commands that match the character(s). Press <Enter> to use the command displayed on this line.

Command Abbreviation and Completion

This section describes how abridged commands can be used in the ACLI. Command completion can save you extra keystrokes and increase efficiency.

Command Abbreviation

Commands can be abbreviated to the minimum number of characters that identify a unique selection. For example, you may abbreviate the configure terminal command to "config t." You cannot abbreviate the command to "c t" because more than one command fits this criteria.

Tab Completion

When you do not supply enough characters to identify a single selection, you can press <Tab> to view a list of commands that begin with the character(s) you entered. After you press <Tab>, the ACLI returns you to the system prompt and reprints the character(s) you originally typed. This enables you to complete the command with the characters that uniquely identify the command that you need. You can continue this process until enough characters to identify a single command are entered.

```
ACMEPACKET# de<Tab>
debug                                delete
ACMEPACKET# debug
```

ACLI Menus

The ACLI provides menus for system commands and for configuration elements in the Net-Net SBC. To access these menus, enter a question mark (?) at the system prompt. This action displays the entire menu for the system command or configuration element.

Configuration Element and System Command Menus

Command menus and configuration element menus display similarly in the ACLI. The menus for each are divided into two columns. The first column lists all of the command and configuration elements available to a user working in this mode; the second column offers short explanations of each command or configuration element's purpose.

```
ACMEPACKET(configure)# system ?

system-config          configure system-wide settings
timezone               configure system timezone information
ntp                    configure ntp servers
phy-interface          configure physical interfaces
network-interface      configure layer3 network interfaces
host-route             configure host routes
system-access-list     configure system-access-list
capture-receiver       configure capture receivers
soap-config            configure soap settings
snmp-community         configure snmp communities
trap-receiver          configure trap receivers
collect                configure collect settings
license                configure licenses
exit                   return to previous menu
```

Context-Sensitive Help

In addition to the information that ACLI menus offer, context-sensitive help can assist you with navigation and configuration.

To use the context-sensitive help, enter the name of the command or field with which you require assistance, followed by a <Space> and then a question mark (?). The context-sensitive help information appears.

In general, context-sensitive help provides more detailed information than within ACLI menus. For system commands, it prompts you about the information you need to enter to execute a system command successfully. For configuration elements, it prompts you with a brief description of the field, as well as available values, ranges of values, and data types.

Context-Sensitive Help for System Commands

The ACLI's context-sensitive help feature displays information you need to complete system commands and the body of subcommands available for each system command. In the following example, the **reset** command menu appears.

Typing a **?** after a system command asks if the system requires further information to complete a specific command, the system responds that there are `no further known parameters` if there are no subcommands. Otherwise, the system responds with a list of available subcommands.

```
ACMEPACKET# reset ?

arp                         clear all ARP statistics
card                        Reset Cards, Cpus, and Cores
collection                  reset HDR collector to its boot state
h323                        reset H323 statistics
hip                         clear all HIP statistics
log                         start a new logfile, backing up old one
mbcd                        reset MBCD statistics
media                       clear media statistics
nat                         clear all NAT statistics
net-management-control  reset Network Management Control statistics
qos                         QOS Statistics and Errors are set to zero for NPU
session-agent               reset session-agent last registered
sip                         reset SIP statistics

ACMEPACKET# show version ?

<ENTER>  no further known parameters

ACMEPACKET# show version
```

Configuration Methods

This section describes how to configure the ACLI on the Net-Net SBC:

Configuring Using Line-by-Line Commands

Using line-by-line commands, you can target a specific field for editing. Line-by-line commands appear in the ACLI as their name suggests: each argument consists of a parameter followed by a valid value, both on one line.

At any time, you can access either the element menu or the context-sensitive help to guide you. In the following example, you enter values for three parameters, and then issue the show command to check your work. Finally, type **done** to save your configuration.

```
ACMEPACKET(trap-receiver)# ip-address 10.0.0.1
ACMEPACKET(trap-receiver)# filter-level major
ACMEPACKET(trap-receiver)# community-name acme
ACMEPACKET(trap-receiver)# show
trap-receiver
    ip-address              10.0.0.1
    filter-level            Major
    community-name          acme
```

```
        last-modified-date              2001-12-07 17:58:47
ACMEPACKET(trap-receiver)# done
```

Working with Configuration Elements

Data entry involves entering commands into the ACLI path that corresponds to the configuration you want to create, and then entering data in accordance with the required format.

Creating Configurations

Creating elements involves using the ACLI path to enter configurations.

```
ACMEPACKET(trap-receiver)# ip-address 10.0.0.1
ACMEPACKET(trap-receiver)# filter-level major
ACMEPACKET(trap-receiver)# community-name acme
ACMEPACKET(trap-receiver)# done
```

Saving Configurations

At all levels of the ACLI hierarchy, there are several methods of saving your settings and data.

- The `done` command.
- The hotkey <Ctrl-D>, which enters the done command in the command line and saves your information.

The `Save Changes y/n ? #` prompt appears when you exit a configuration element if you have not saved your changes using another method. This prompt only appears if you have changed old information and/or entered new information.

Using the Show Command and Saving Elements

We recommend that you view all of the information you have entered before carrying out the **done** command or another method of saving. Use the **show** command to review your configurations. Reviewing your settings will give you the opportunity to make any necessary changes before writing the information to the system database.

To view configuration information, type **show** when you are finished with a command.

The following example illustrates the use of the **show** command before executing the done command.

```
ACMEPACKET(media-profile)# show
media-profile
                name                    G723
                media-type              audio
                payload-type            4
                transport               RTP/AVP
                req-bandwidth           16
ACMEPACKET(media-profile)#
```

Using the Done Command to Save Elements

We strongly recommend that you save your configuration information as you work. This ensures that your configurations have been written to the system database.

Every menu contains the **done** command.

```
ACMEPACKET(snmp-community)# show
snmp-community
        community-name              Acme_Community
        access-mode                 READ-ONLY
        ip-addresses
                                    10.0.0.2
                                    10.0.0.3
                                    10.0.0.4
ACMEPACKET(snmp-community)# done
snmp-community
        community-name              Acme_Community
        access-mode                 READ-ONLY
        ip-addresses
                                    10.0.0.2
                                    10.0.0.3
                                    10.0.0.4
ACMEPACKET(snmp-community)#
```

Exiting and Saving Elements

When you use the **exit** command and have not already saved your changes, the ACLI produces the following message:

```
Save Changes y/n ? #
```

When this line appears, the ACLI is prompting you to save your configurations. This prompt only appears if you have changed old information or entered new information.

If you type anything other than a **y** in response to the `Save Changes y/n ? #` prompt, the system will interpret that character as a **no** response and will not save your work. You must type a **y** to save your work.

Editing Configurations

Editing individual configurations in the ACLI involves finding the element or field you need to update, entering the new information, and then saving the element. Besides configuring parameters with no value in them, you can also overwrite existing values.

To edit an element:

1. Enter the configuration path of the element for which you want to edit.
2. Use the **select** command to choose an element to update. A list of options appears when you press <Enter> at the key field prompt (e.g., <name:>).
3. Enter the number corresponding to the element you would like to update. If there are no elements configured, you will still be presented with the prompt, but no list will appear. When you press <Enter> at the key field prompt, you will be returned to the system prompt.

```
ACMEPACKET(phy-interface)# sel
<name>:
1: phyTEST
2: phyTEST-RIGHT
```

```
3: wancom0


selection: 3
ACMEPACKET(phy-interface)#
```

4. Edit the configuration element by re-entering any new changes.

```
ACMEPACKET(phy-interface)# wancom-health-score 55
```

5. Use the show command to be sure that your changes have been registered.

```
ACMEPACKET(phy-interface)# show
phy-interface
    name                    wancom0
    operation-type          Control
    port                    0
    slot                    0
    virtual-mac
    wancom-health-score     55
```

6. Use the **done** command to save your updates (any changed information).

You can also overwrite parameters by entering a new value after a previous value has been created.

Deleting Configurations

There are two methods of deleting configurations.

- You can delete the information for elements while you are still working with them.
- You can delete all configuration information for a previously configured element.

For either method, use the **no** command to clear configurations.

Only Multiple Instance Elements can be deleted from the system. Single Instance Elements can not be deleted; they can only be edited.

Deleting while Working with an Element

While you are configuring an element for the Net-Net SBC, you may accidentally enter incorrect information or make some other error. To correct these errors, use the **no** command to clear the system of the information you have entered.

Deleting an Existing Element

You can only delete individual configurations from within their ACLI path. Use the select command to choose the configuration element you want to delete.

To delete an existing element:

1. Enter the ALCI path to the element you wish to delete.
2. Enter the **no** command. After you do so the key field prompt (e.g., <name:>) appears with a list of the existing configured elements beneath it.

```
ACMEPACKET(media-profile)# no
<name>:
1: PCMU
2: G723
```

```
3: G729
```

3. Enter the number corresponding to the element you wish to delete.

```
selection:3
```

4. To confirm the deletion, use the **select** command to view the list of remaining elements.

```
ACMEPACKET(media-profile)# select
<name>:
1: PCMU
2: G723
```

ACLI Configuration Summaries

The ACLI offers several ways for you to view configuration summaries. While the most straightforward and commonly used method is the **show** command, the ACLI also provides summary information every time you execute the **done** command.

Viewing Summaries

The **show** command that appears for each ACLI configuration element allows you to view the configured information for a given element.

To view the settings for the media-profile element:

1. From the **media-profile**, use the **select** command. After you press <Enter>, the **<name>:** prompt and a list of configured media-profile elements appears.

```
ACMEPACKET(media-profile)# select
<name>:
1: PCMU
2: G723
3: G729
```

2. Select a key field by entering the number for the element you want to view.

```
selection:1
```

3. Type **show** followed by the name of the element you want to view.

```
(media-profile)# show pcmu
media-profile
    name                PCMU
    media-type          audio
    payload-type        0
    transport           RTP/AVP
    req-bandwidth       80
ACMEPACKET(media-profile)#
```

Data Entry

To enter data using the ACLI, your entries must conform to required field formats. In addition to describing these formats, this section provides information about preset values, default values, and error messages.

The final part of this section covers information about using quotation marks (**“”**) and parentheses (**()**) to enhance your data entry options and capabilities.

ACLI Field Formats

This section describes required data entry formats. You can learn the data type for a field by using the menu or the help function.

Boolean Format

Boolean entries take the form of either enabled or disabled. To choose one of these two values, type either **enabled** or **disabled**.

Carrier Format

Carrier entries can be from 1 to 24 characters in length and can consist of any alphabetical character (Aa-Zz), numerical character (0-9), punctuation mark (! ”$ % ^ & * ( ) + - = ‘ | { } [ ] @ / \ ‘ ~ , . _ : ;), or any combination of alphabetical characters, numerical characters, or punctuation marks. For example, both 1-0288 and acme_carrier are valid carrier field formats.

Date Format

Date entries must adhere to the ccYY-mM-dD format, where cc is the century, YY is the year, mM is the month, and dD is the day (e.g., 2005-06-10). The minimum entry requirement for date fields is YY-M-D.

The Net-Net SBC can assign the current century (cc) information, as well as leading zeroes for the month (m) and the day (d). Date fields must be entered in the valid format described above.

Day of Week Format

Day of week entries set any combination of day(s) of the week plus holidays that the `local-policy-attributes` can use for preference determination. The day of week field options are:

- U—Sunday
- M—Monday
- T—Tuesday
- W—Wednesday
- R—Thursday
- F—Friday
- S—Saturday
- H—Holiday

This field format cannot accept spaces. For example, U-S and M,W,F are valid day of week field entries.

Enumerated Format

Enumerated parameters allow you to choose from a preset list of values. To access the list of choices from within the ACLI, use the help function for the appropriate parameter.

Hostname (or FQDN) Format

Hostname (FQDN) entries consist of any number of Domain Labels, separated by periods, and one Top Label. The minimum field value is a single alphabetical character to indicate the top label value (e.g., c to indicate '.com').

All hostname fields support IPv4 addresses as well as hostnames.

For Example: In the hostname `acme-packet.domainlabel.example100.com`, acme-packet is a domain label, domainlabel is a domain label, example100 is a domain label, and com is the top label.

- domain label—acme-packet, domainlabel, example100
- top label—com

Note that each label is separated by a period.

The following describes hostname (FQDN) format label types:

- Domain Label—A domain label consists of any number or combination of alphabetical or numerical characters, or any number or combination of alphabetical or numerical characters separated by a dash (-). A dash must be surrounded on both sides by alphabetical or numerical characters, any number or combination. A dash can not immediately follow or precede a period . A domain label is not required in a hostname field value.
- Top Label—A top label is the last segment of the hostname. A top label must start with an alphabetical character; it cannot start with a numerical character or with a dash (-). After the first character, a top label can consist of any number, or combination of alphabetical or numerical characters or any number or combination of alphabetical or numerical characters separated by a dash. Similar to dashes in domain labels, a top label dash must be surrounded on both sides by alphabetical or numerical characters, any number or combination. A single alphabetical character is the minimum requirement for a hostname field value.

IP Address Format

IP address entries must follow the dotted decimal notation format and can only include numerical characters (0-9). Entries for an IP address field should be between 0.0.0.0 and 255.255.255.255.

Name Format

Name entries must start with either an underscore symbol (_) or an alphabetical character from A through Z (A-Za-z). After the first character, the field entry can contain any combination of alphabetical or numerical characters (0-9A-Za-z), as well as the period (.), the dash (-), and the underscore (_) (e.g., acmepacket_configuration). The total entry can be from 1 to 24 characters in length.

Number Format

Number entries (e.g., phone number digits without dashes, any address that is not a hostname, etc.) can be any numerical character (0-9) or alphabetical character from A through F (A-Fa-f) or any combination of numerical and alphabetical characters from A through F (0-9A-Fa-f) (e.g., 18005551212 or 18005552CAB). The minimum number of characters for a number entry is 1, and the maximum number is 32.

Text Format

Text entries (e.g., description fields) do not need to follow a particular format. Text fields can accommodate any combination of printable numerical and alphabetical

characters, spaces, and most symbols. Noted exceptions are the ampersand (&), the apostrophe (‘), and the less than symbol (<). Entries with spaces must be entered fully within quotation marks. For example, “This is the official Acme Packet Net-Net SBC configuration” is a valid text entry.

Time of Day Format

Time of day entries must include only numerical characters (0-9) and must follow the 4-digit military time format (e.g., 1400). Time of day entries set the time of day that attributes can be considered for preference determination. The minimum field value is 0000, and the maximum field value is 2400.

Preset Values

All configurations share one field: `last-modified-date`. This field value is set by the system database and cannot be altered. It displays the date and time of the last modified action. The system sets this value automatically.

Default Values

By default, the system populates some ACLI values with preset system values if you do not manually configure them.

Error Messages

The ACLI produces error messages when information cannot be saved or commands cannot be executed. These events may occur when there is a problem either with the command itself, the information entered, the format of the information entered, or with the system in general.

For example, if you enter several words for a description and you do not put the entry inside quotation marks, the ACLI will tell you that you have entered an invalid number of arguments. In the example below, a user entered a media-type field value of “audio visual,” but did not enclose the value in quotation marks (“”).

```
ACMEPACKET(media-profile)# media-type audio visual
invalid number of arguments
ACMEPACKET(media-profile)#
```

When the value does not conform to format requirements, the ACLI returns a message that you have made an invalid entry for a given field. In the example below, a user entered an invalid IP address.

```
ACMEPACKET(snmp-community)# ip-addresses (1877.5647.457.2 45.124
254.65.23)
invalid IP address
ACMEPACKET(snmp-community)#
```

Message	Description
error invalid data...	You have entered a value not permitted by the system. This error includes numeric values that exceed defined parameters and misspellings of specifically spelled values (such as “enabled” or “disabled”).
% command not found	You entered a command that is not valid. The command may be misspelled, or it may not exist where you are working.
invalid selection...	You have selected an item that does not exist in the system.

Message	Description
invalid number of arguments	You either have entered too many arguments (or commands) on one line or you may not have quotation marks (“”) around your multi-word entry.
error 500 saving ...	The system could not save the data you entered to the system database.

Special Entry Types: Quotation Marks and Parentheses

The ACLI uses certain syntax in order to increase ease of use.

- Quotation marks (**“”**)—The values inside quotation marks are read as being one argument; commonly used in text fields.
- Parentheses (**( )**)—The values inside parentheses are read as being multiple arguments for an element.

Entering Multiple Values for the Same Field

To enter multiple values for the same field, you can either use quotation marks (**“”**) or parentheses (**( )**) in order to express these values to the system. In a field that might contain multiple values, you must use either of these when you enter more than one value.

Your use of either of these methods signals to the system that it should read the data within the punctuation marks as multiple values. The following example shows how parentheses (**( )**) are used in an instance of the local-policy element.

In the example that follows, there are three entries for the to-address in the parentheses (**( )**).

*Note: If you enter multiple values within either quotation marks (**“”**) or parentheses (**( )**), be sure that the closing marks are made directly after the final value entered. Otherwise, the system will not read your data properly.*

```
ACMEPACKET(local-policy)# to-address (196.154.2.3 196.154.2.4 196.154.2.5)
ACMEPACKET(local-policy)# show
local-policy
    from-address
                                196.154.2.3
                                196.154.2.4
                                196.154.2.5
    to-address
    source-realm                *
    activate-time               N/A
    deactivate-time             N/A
    state                       enabled
    policy-priority             none
```

Entering Multi-Word Text Values

For many fields, you may want to enter a multi-word text value. This value may either be a series of descriptive words, a combination of words and numbers that identify a location, or a combination of words and numbers that identify a contact person.

To enter a multi-word text value, surround that value either with quotation marks (“”) or parentheses (()). Generally, quotation marks are most commonly used to configure text fields. The example below shows how quotation marks (“”) surround a multi-word value.

```
ACMEPACKET(session-router-config)# holidays
ACMEPACKET(session-router-holidays)# date 2008-01-01
ACMEPACKET(session-router-holidays)# description "new year's day"
ACMEPACKET(session-router-holidays)# done
    holiday
        date                2008-01-01
        description         new year's day
```

An Additional Note on Using Parentheses

Parentheses can be used in the ACLI to enter multiple arguments on the same line. A command line can contain any number of entries inside parentheses. Single parentheses (()) connote one list, nested parentheses ((())) connote a list within a list, and so forth.

Working with Options in Your Configuration

The ACLI **options** parameter is used to configure the Net-Net SBC to conform to non-standard or customer-specific behavior, and is found in the following configurations:

- Global SIP configuration
- SIP interfaces
- Global H.323 configuration
- H.323 interfaces (stacks)
- Global MGCP configuration
- Realm configurations
- Session agents

Depending on your network architecture, you might need to use only one option or you might need to configure multiple options in the same configuration. This section shows you how to add one option to a configuration, and how to add multiple options using a single command-line entry. Since it is easy to overwrite your options lists when you are editing them (adding or deleting options), this section also describes the two ACLI mechanisms that allow you to edit while preserving the options you want to keep.

Adding Options in a New Configuration

When adding options to a new, unconfigured element, you do not have to worry about overwriting a preexisting option list.

To add the option you want to configure:

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

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(terminal)#session-router
   ```

```
ACMEPACKET(session-router)#
```

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

```
ACMEPACKET(session-router)# sip-config
ACMEPACKET(sip-config)#
```

4. Type **options** at the prompt, followed by the name of the option you want to add, then press <Enter>.

```
ACMEPACKET(sip-config)# options max-udp-length=0
```

5. Type **show**, then <Enter> at the prompt to assure that the option you have added appears in the configuration.

```
ACMEPACKET(sip-config)# show
sip-config
        state                   enabled
        operation-mode          dialog
        dialog-transparency     enabled
        home-realm-id           public
        egress-realm-id
        nat-mode                None
        registrar-domain
        registrar-host
        registrar-port          0
        register-service-route  always
        init-timer              500
        max-timer               4000
        trans-expire            32
        invite-expire           180
        inactive-dynamic-conn   32
        userinfo-mode           none
        sip-message-len         0
        add-reason-header       disabled
        response-map
        local-response-map
        enforcement-profile
        extra-method-stats      disabled
        network-model
        rph-feature             disabled
        nsep-user-sessions-rate  0
        options                 max-udp-length=0
        last-modified-by
        last-modified-date      2006-04-24 17:55:05
```

You can enter multiple options on one command line. There are two ways of doing this. You can enter all of your options within a set of parentheses ( ), all separated from one another with a space. Or you can list them all on the command line with the word **add** in front of every option, and separated from one another with a space. Be aware that if you use the parentheses method, and you already have an existing options list configured, it will overwrite the entire list.

To add multiple options to a configuration in one command-line entry:

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

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(terminal)#session-router
   ACMEPACKET(session-router)#
   ```

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

   ```
   ACMEPACKET(session-router)#sip-config
   ACMEPACKET(sip-config)#
   ```

4. Type **options** at the prompt, followed by an open parentheses, the names of all the options you want to add separated by spaces, followed by a closed parentheses. Then press <Enter>.

   ```
   ACMEPACKET(sip-config)#options (max-udp-length=0 register-grace-timer=32 reinvite-trying)
   ```

Or you can type **options** at the prompt, followed by the list of options you want, each with the word **add** in front of it and all separated by spaces. Then press <Enter>.

```
ACMEPACKET(sip-config)# options add max-udp-length=0 add register-grace-timer=32 add reinvite-trying
```

5. Type **show**, then <Enter> at the prompt to assure that the options you have added appear in the configuration.

```
ACMEPACKET(sip-config)# show
sip-config
        state                   enabled
        operation-mode          dialog
        dialog-transparency     enabled
        home-realm-id           public
        egress-realm-id
        nat-mode                None
        registrar-domain
        registrar-host
        registrar-port          0
        register-service-route  always
        init-timer              500
        max-timer               4000
        trans-expire            32
        invite-expire           180
        inactive-dynamic-conn   32
        userinfo-mode           none
        sip-message-len         0
        add-reason-header       disabled
        response-map
        local-response-map
        enforcement-profile
        extra-method-stats      disabled
```

```
network-model
rph-feature                 disabled
nsep-user-sessions-rate     0
options                     max-udp-length=0
                            register-grace-timer=32
                            reinvite-trying
last-modified-by
last-modified-date          2006-04-24 17:55:05
```

Editing Options

When you are editing the options for an existing configuration, you should take care not to overwrite any existing options required to support the functionality you want to use. To help you, there are two commands for working with lists of options:

- Add—Used directly before the option you want to append when you type it into the command line, this mechanism allows you to add an option to a pre-existing list
- Delete—Used directly before the option you want to delete when you type it into the command line, this mechanism allows you to delete an option from a pre-existing list and leave the rest of the list intact

To append a new option to an existing options list:

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

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(terminal)#session-router
   ACMEPACKET(session-router)#
   ```

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

   ```
   ACMEPACKET(session-router)#sip-config
   ACMEPACKET(sip-config)#
   ```

4. Type **options** at the prompt, followed by a space, the word **add** and the name of the option you want to add, then press <Enter>.

   ```
   ACMEPACKET(sip-config)#options add max-udp-length=0
   ```

5. Type **show**, then <Enter> at the prompt to assure that the option(s) you have added appears in the configuration.

   ```
   ACMEPACKET(sip-config)# show
   sip-config
       state                   enabled
       operation-mode          dialog
       dialog-transparency     enabled
       home-realm-id           public
       egress-realm-id
       nat-mode                None
       registrar-domain
       registrar-host
       registrar-port          0
       register-service-route  always
   ```

```
init-timer                500
max-timer                 4000
trans-expire              32
invite-expire             180
inactive-dynamic-conn     32
userinfo-mode             none
sip-message-len           0
add-reason-header         disabled
response-map
local-response-map
enforcement-profile
extra-method-stats        disabled
network-model
rph-feature               disabled
nsep-user-sessions-rate   0
options                   max-udp-length=0
last-modified-by
last-modified-date        2006-04-24 17:55:05
```

You can also delete a single existing option from the options list without deleting the previously configured list:

To delete a single option from an existing options list:

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

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(terminal)#session-router
   ACMEPACKET(session-router)#
   ```

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

   ```
   ACMEPACKET(session-router)#sip-config
   ACMEPACKET(sip-config)#
   ```

4. Type **options** at the prompt, followed by a space, the word **delete**, and the name of the option you want to delete, then press <Enter>.

   ```
   ACMEPACKET(sip-config)#options delete max-udp-length=0
   ```

5. Type **show**, then <Enter> at the prompt to assure that the option you have deleted has been removed from the options list.

   ```
   ACMEPACKET(sip-config)# show
   sip-config
       state                 enabled
       operation-mode        dialog
       dialog-transparency   enabled
       home-realm-id         public
       egress-realm-id
       nat-mode              None
       registrar-domain
   ```

```
registrar-host
registrar-port                  0
register-service-route          always
init-timer                      500
max-timer                       4000
trans-expire                    32
invite-expire                   180
inactive-dynamic-conn           32
userinfo-mode                   none
sip-message-len                 0
add-reason-header               disabled
response-map
local-response-map
enforcement-profile
extra-method-stats              disabled
network-model
rph-feature                     disabled
nsep-user-sessions-rate         0
options                         -max-udp-length=0
last-modified-by
last-modified-date              2006-04-24 17:55:05
```

Just as you can add multiple options on one command-line, you can also delete multiple options using one command-line.

To delete multiple options from a configuration in one command-line entry:

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

   ```
   ACMEPACKET# configure terminal
   ```

2. Type **session-router** and press <Enter>.

   ```
   ACMEPACKET(terminal)#session-router
   ACMEPACKET(session-router)#
   ```

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

   ```
   ACMEPACKET(session-router)#sip-config
   ACMEPACKET(sip-config)#
   ```

4. Type **options** at the prompt, followed by the list of options you want to remove, each with the word **delete** in front of it and all separated by spaces. Then press <Enter>.

   ```
   ACMEPACKET(sip-config)#options delete max-udp-length=0 delete reinvite-trying
   ```

5. Type **show**, then <Enter> at the prompt to assure that the options you have deleted has been removed from the options list.

   ```
   ACMEPACKET(sip-config)# show
   sip-config
       state                       enabled
       operation-mode              dialog
       dialog-transparency         enabled
   ```

home-realm-id	public
egress-realm-id	
nat-mode	None
registrar-domain	
registrar-host	
registrar-port	0
register-service-route	always
init-timer	500
max-timer	4000
trans-expire	32
invite-expire	180
inactive-dynamic-conn	32
userinfo-mode	none
sip-message-len	0
add-reason-header	disabled
response-map	
local-response-map	
enforcement-profile	
extra-method-stats	disabled
network-model	
rph-feature	disabled
nsep-user-sessions-rate	0
options	register-grace-timer=32
last-modified-by	
last-modified-date	2006-04-24 17:55:05

Note: Enter data in options lists with care. If entered incorrectly, the entire options list could be overwritten.

2 ACLI Commands A - M

activate

The **activate config** command activates the current configuration on the Net-Net SBC and overwrites the pre-existing one to make it the running configuration. This command cannot be completed until the configuration has been saved.

Syntax `activate config`

Mode Superuser

Path Type **activate config** at the topmost ACLI prompt.

Release First appearance: 5.0

Example

```
ACMEPACKET# activate config
```

add

add arp

The **add arp** command manually adds ARP entries to the ARP table.

Syntax `add arp <slot> <port> <vlan> <ip> <mac>`

Arguments

<slot>	Select the media interface slot to which you are adding the ARP entry
Values	• 0—Bottom slot • 1—Top slot
<port>	Select the media interface port to which you are adding the ARP entry
Values	• 0—Leftmost port • 1—Second from left port • 2—Third from left port • 3—Rightmost port
<vlan>	Enter the VLAN identifierfor this ARP entry
<ip>	Enter the IP address you are adding in the IP Address format
<mac>	Enter the MAC address in hexadecimal notation

Mode Superuser

Path Type **add arp** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0

Notes Enter slot, port, vlan, IP address, and MAC address in the spaced format.

Example

```
ACMEPACKET# add arp 0 0 0 172.16.0.102 ab:cd:ef:01:23:14
```

check

check arp

The **check arp** command sends an ARP message to the specified IP address when the MAC address is not known, via a specific interface.

Syntax

```
check arp <slot> <port> <vlan> <ip>
```

Arguments

<slot>	Select the media interface slot you are checking
Values	• 0—Bottom slot • 1—Top slot
<port>	Select the media interface port you are checking
Values	• 0—Leftmost port • 1—Second from left port • 2—Third from left port • 3—Rightmost port
<vlan>	Enter the VLAN identifierthat you are checking
<ip>	Enter the IP address that you are checking

Mode Superuser

Path Type **check arp** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0

Notes Enter slot, port, vlan, and IP address in the spaced format.

Example

```
ACMEPACKET# check arp 0 0 0 172.16.0.102
```

save backup

Syntax

```
save backup <name-of-backup> [running | editing | saved]
```

The **save backup** command backs up the current flash memory configuration to the specified filename in the `/code/bkups` directory.

Arguments

<name-of-backup>	Enter the name of the backup configuration file
[running]	Backup the configuration from the running configuration cache. This is an optional argument.
[editing]	Backup the configuration from the editing configuration cache. This is an optional argument.
[saved]	Backup the last saved configuration. This is an optional argument.

Mode Superuser

Path Type **save backup** + arguments at the topmost ACLI prompt.

Notes If insufficient disk space is available, the Net-Net SBC will not complete the task.

Notes If neither [running] or [editing] is specified, the Net-Net SBC will backup the last saved configuration.

Example

```
ACMEPACKET# save backup FEB_BACKUP.gz running
```

clear

This command clears unwanted ACL statistics, alarms, and logs stored on the Net-Net SBC.

clear acl

Syntax

```
clear acl <denied | trusted> <all | index>
```

The **clear acl** command deletes ACL lists or entries.

Arguments

<denied>	Delete a denied entry or list
<trusted>	Delete a trusted entry or list
<all>	Delete all denied or trusted entries
<index>	Delete one denied or trusted entry

Example

```
ACMEPACKET# clear acl denied all
```

clear alarm

Syntax

```
clear alarm <alarm ID> <task ID> <severity>
```

The **clear alarm** command manually clears a specified alarm.

Arguments

<alarm id>	Enter a unique 32-bit integer that contains a 16-bit category name or number and a unique 16-bit identifier for the error or failure within that category. You can find the alarm ID by using the **show alarm** command. The alarm ID is the number listed in the first column of the display.
<task ID>	Enter the task ID of the task that sent the alarm.
<severity>	Select the severity of the alarm. The following are the levels of severity:
Values	• NONE • EMERGENCY • CRITICAL • MAJOR • MINOR • WARNING • NOTICE

Example

```
ACMEPACKET# clear alarm 65524 lcm@0.1.1 major
```

clear dns

Syntax

```
clear dns [realm] [type] [name] [all]
```

The **clear DNS** command removes one or more entries from the DNS cache.

Arguments

[realm]	Clear the cache of a particular realm. This is an optional argument.
[type]	Clear a certain type of entry from the cache of a DNS realm. This is an optional argument.
[name]	Clear a particular name from the cache of a DNS realm. This is an optional argument.
[all]	Clear all entries from the DNS cache

Example

```
ACMEPACKET# clear dns realm1 all
```

clear enum

Syntax

```
clear enum <enum-server> [number] [all]
```

The **clear enum** command removes one or more entries from the ENUM cache.

Arguments

<arguments>	The type of enum statistics you want to clear. The following are valid **clear enum** arguments:
Values	• enum-server—Clear the cache for the specified server • number—Clear the specified number from the cache. This is an optional argument • all—Clear all cache entries. This is an optional argument.

Example

```
ACMEPACKET# clear enum all
```

clear log

Syntax

```
clear log <task@location> [logfile | all]
```

The **clear log** command manually deletes all of a task's log files.

Arguments

<task@location>	Enter the location of the log you want to clear in the format of <task>@<slot>.<cpu>.<core>
<logfile>	Delete a specific trace log. This argument is optional. If no file name is specified, the entire task log is deleted.
<all>	Delete both a trace log and a task log by including the term `all` at the end of the command.

Example

```
ACMEPACKET# clear log lcm@0.1.1
```

clear lrt

Syntax

```
clear lrt <all | lrt-name> [number]
```

The **clear lrt** command clears the local cache for the named LRT table.

Arguments

<all>	Remove all cache entries for all servers
<lrt-name>	Remove all cache entries for a specific LRT table
[number] cache	Remove a specific cache entry by phone number from the local

Example

```
ACMEPACKET# clear lrt lrt-name lrt2
```

clear registration

Syntax

```
clear registration <protocol> [type]
```

The **clear registration** command allows you to clear the registration cache for a specified protocol.

Arguments

<sip> Clear the SIP registration cache. The following are the types of information for which you can clear:

Values
- all
- by-user <username | phone number>

<h323> Clear the H.323 registration cache. The following are the types of information for which you can query:

Values
- all
- by-alias <terminal Alias>

Example

```
ACMEPACKET# clear registration sip all
```

clear sessions

Syntax

```
clear sessions <h323 | sip> <all | by-agent | by-call-id | by-ip |
by-user>
```

The **clear session** command deletes SIP and H.323 sessions from the system.

Arguments

<h323> Clear H.323 sessions from the system.

<sip> Clear SIP sessions from the system.

Notes

For IWF session, choose one leg of the call to terminate first and use that leg's protocol.

<all> Clear all sessions for the specified protocol.

<by-agent> Clear sessions originating or terminating from a specified session agent.

Values
- SA-name—Enter the name of the session agent. This entry is required.

<by-call-id> Clear session from a specified call-id <call-id>.

Values
- call-id—Enter the call-id. This entry is required.

<by-ip> Clear sessions originating or terminating from a client or server dialog with a specified URI IP address.

Values
- ip-addr—Enter the IP address. This entry is required.

<by-user> Clear sessions originating or terminating from a client or server dialog with a specified URI username.

Values • user-name—Enter the user name. This entry is required.

Example `ACMEPACKET# clear sessions sip by-ip 192.168.44.55`

Mode Superuser

Path Type **clear** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0 / Most recent update: 7.1

configure

The **configure terminal** command enters you into the system level where you can create, view, edit, and delete the configuration elements and applications on your Net-Net SBC.

Syntax `configure terminal`

Mode Superuser

Path Type **configure terminal** at the topmost ACLI prompt.

Release First appearance: 5.0

Example `ACMEPACKET# configure terminal`

connect

The **connect console** command makes a console connection to anywhere. This can be useful for debugging purposes and also for viewing local logs. When you make an initial connection to the Net-Net SBC through the ACLI, by default you are automatically connected to the master core (CPU 0, Core 0) on the SPU.

Syntax `connect console <slot> <cpu> <core>`

Arguments

<slot> Select the slot number you want to connect to

Values 0 | 1 | 2 | 3 | 4 | 5 | 6

<cpu> Select the CPU number you want to connect to

Values 0 | 1 | 2 | 3 | 4

<core> Select the core number you want to connect to

Values 0 | 1

Mode User

Path Type **connect console** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0

Notes Enter slot, CPU, and core numbers in the spaced format.

Example **ACMEPACKET# connect console 3 1 1**

debug

This command debugs a specific task on the Net-Net SBC.

Syntax `debug <task@location> [log type]`

Arguments

<task@location>	Enter the name of the task you want to debug in the form of <name>@<card>.<cpu>.<core>
[log type]	Enter the specific type of log you want to enable. This is an optional argument.

Mode Superuser

Path Type **debug** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0

Notes Wildcards are allowed in the task/location argument.

Example **ACMEPACKET# debug lcm@0.1.1**

delete

The **delete** command deletes current or backup configurations or ARP table entries.

delete arp

Syntax `delete arp <slot> <port> <vlan> <ip>`

The **delete arp** command manually removes ARP entries from the ARP table.

Arguments

<slot>	Select the physical interface slot of the ARP entry you want to delete
Values	• 0—Bottom slot • 1—Top slot
<port>	Select the physical interface port of the ARP entry you want to delete
Values	• 0—Leftmost port • 1—Second from left port • 2—Third from left port • 3—Rightmost port

	<vlan>	Enter the VLAN identifier of the ARP entry you want to delete
	<ip-address>	Enter the IP address of the ARP entry you want to delete

Example ACMEPACKET# **delete arp 0 0 0 172.16.0.102**

delete backup

Syntax `delete backup <filename>`

The **delete backup** command deletes a saved configuration file from the Net-Net SBC's standard backup file directory (/code/bkups).

Arguments

<filename>	Enter the name of the backup file you want to delete

Example ACMEPACKET# **delete backup FEB_BACKUP.gz**

delete collection

Syntax

```
delete collection
```

The **delete collection** command deletes all collection data files residing on the Net-Net SBC.

Example

```
ACMEPACKET# delete collection
```

delete config

Syntax

```
delete config
```

The **delete config** command deletes the current configuration from the Net-Net SBC.

Example

```
ACMEPACKET# delete config
```

delete dump

Syntax

```
delete dump <type> <slot> [cpu] [core]
```

The **delete dump** command allows you to delete all dumps present on any SPU , for any card, cpu, or core.

Arguments

<type>	Select the type of entry you want to dump. The following are valid types:
Values	• arp—Delete ARP entries • backup—Delete backup from persistent memory • collection—Delete unpushed HDR collector files • config—Delete editing configurations • dump—Delete log dumps from flash • image—Delete images from flash
<slot>	Specify the slot whose log dumps you want to delete
[cpu]	Specify the CPU whose log dumps you want to delete. This is an optional argument.
[core]	Specify the core whose log dumps you want to delete. This is an optional argument.

Example

```
ACMEPACKET# delete dump 2
```

delete image

Syntax `delete image <image name> [SPU #]`

This command deletes images from the flash memory. Not specifying which SPU deletes an image from both.

Arguments

<image name>	Enter the name of the image you want to delete from flash memory
[SPU #]	Enter the specific SPU you want to delete an image from

Mode Superuser

Example `ACMEPACKET# delete image July_07.gz 0`

Path Type **delete** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0

dump

The **dump npu-stats** command dumps NPU debug information into a log file.

Syntax `dump npu-stats`

Mode Superuser

Path Type **dump npu-stats** at the topmost ACLI prompt.

Release First appearance: 5.0

Example `ACMEPACKET# dump npu-stats`

enable

The **enable** command changes the current ACLI session from User mode to Superuser mode.

Syntax `enable`

Mode User

Path Type **enable** at the topmost ACLI prompt.

Release First appearance: 5.0

Example `ACMEPACKET# enable`

exit

The **exit** command exits from the current command mode or configuration subsystem to the next higher level.

Syntax `exit`

Mode User

Path Type **exit** at any prompt.

Release First appearance: 5.0

Example

```
ACMEPACKET# exit
```

kill

The **kill** command terminates a Telnet or SSH session on the Net-Net SBC.

Syntax `kill <id>`

Arguments

`<id>`	Enter the index number of the Telnet or SSH session you want to terminate

Mode Superuser

Path Type **kill** + arguments at the Superuser prompt.

Release First appearance: 5.0

Notes You can use the **show users** command to view all active Telnet and SSH sessions and the index number associated with each session.

Example

```
ACMEPACKET# kill 4
```

3 ACLI Commands N - Z

nodebug

This command cancels the debug command and discontinues the log level for specified logs for particular system processes being set to DEBUG.

Syntax

```
nodebug <task@location>
```

Arguments

<task@location> Enter the name of the task being debugged that you want to cancel in the form of <task>@<card>.<cpu>.<core>

Mode

Superuser

Path

Type **nodebug** + arguments at the topmost ACLI prompt.

Release

First appearance: 5.0

Example

```
ACMEPACKET# nodebug sipc@0.0.0
```

ping

The **ping** command pings a remote IP address.

Syntax

```
ping <IP address> [network-interface-name:vlan] [source-address]
```

Arguments

<IP address> Enter the IP address of the host you want to ping

Mode

User

Path

Type **ping** + arguments at the topmost ACLI prompt.

Release

First appearance: 5.0

Notes

This command sends ICMP echo messages, and displays:

- Minimum round trip time (RTT)
- Maximum RTT
- Average RTT
- Number of packets transmitted
- Number of packets received
- Percentage of packets lost

The ping timeout is 64ms.

Example **ACMEPACKET# ping 192.168.0.96 private:0 192.168.0.80**

power

The **power** command turns the power on or off for each particular card manually through the ACLI.

Syntax `power <slot> <“on” | “off”>`

Arguments

<slot>	Enter the specified card whose power you want to turn on or off
<on>	Turn the power of a specified card on
<off>	Turn the power of a specified card off

Mode Superuser

Path Type **power** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0

Example **ACMEPACKET# power 0 on**

reboot

The **reboot** command reboots your Net-Net SBC.

Syntax `reboot [force]`

Arguments

[force]	Quicken the reboot process slightly by rebooting without having the Net-Net SBC prompt you for a confirmation. This is an optional argument.

Mode Superuser

Path Type **reboot** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0

Example **ACMEPACKET# reboot force**

reset

The **reset** command clears and resets statistic counters on the Net-Net SBC.

reset arp

Syntax

```
reset arp statistics
```

The **reset arp statistics** command clears ARP statistics that are saved in the system.

Example

```
ACMEPACKET# reset arp statistics
```

reset card

Syntax

```
reset card <"all" | location>
```

The **reset card** command clears accumulated information from a specified card, CPU, and core on the system.

Arguments

<all>	Reset all cards on the system
<location>	Clear a specified card or group of cards by entering <slot> <cpu> <core>. You can enter just <slot> or just <slot><cpu> for a broader group of cards.

Example

```
ACMEPACKET# reset card 0 0 0
```

reset collection

Syntax

```
reset collection
```

The **reset collection** command restarts the collection process on the Net-Net SBC to a state based on the running configuration.

Example

```
ACMEPACKET# reset collection
```

reset dns

Syntax

```
reset dns
```

The **reset dns** clears command DNS statistics.

Example

```
ACMEPACKET# reset dns
```

reset enum

Syntax

```
reset enum
```

The **reset enum** clears command DNS statistics.

Example

```
ACMEPACKET# reset enum
```

reset gateway

Syntax

```
reset gateway <primary | secondary> <location>
```

The **reset gateway** command allows you to switch between primary and secondary gateways on the Net-Net SBC.

Arguments

<primary>	Switch from the secondary gateway to the primary gateway
<secondary>	Switch from the primary gateway to the secondary gateway
<location>	Switch a gateway on a specified card or group of cards by entering <slot> <cpu> <core>. You can enter just <slot> or just <slot> <cpu> for a broader group of cards.

Example

```
ACMEPACKET# reset gateway secondary 0 0 0
```

reset h323

Syntax

```
reset h323
```

The **reset h323** command resets all H.323 statistics currently stored on the Net-Net SBC.

Example

```
ACMEPACKET# reset h323
```

reset hip

Syntax

```
reset hip statistics
```

The **reset hip statistics** command clears Host in Path (HIP) statistics on the system.

Example

```
ACMEPACKET# reset hip statistics
```

reset log

Syntax

```
reset log <task@location> [logfile | "all"]
```

The **reset log** command forces a log rotate, closing one log file and opening a new one.

Arguments

<task@location>	Enter the location of the log you want to rotate in the form of <task>@<card>.<cpu>.<core>
[logfile]	Rotate a trace log by including the filename. This is an optional argument.
[all]	Include the term `all` at the end of this command allows you to rotate both the trace log and the task log. This is an optional argument.

Example

```
ACMEPACKET# reset log sip@0.0.0 all
```

reset lrt

Syntax

```
reset lrt <local-route-config name>
```

The **reset lrt** command updates the named local route configuration.

Arguments

<local-route-config name>Enter the name of the local route table you want to reset.

Example

```
ACMEPACKET# reset lrt lrt2
```

reset mbcd

Syntax

```
reset mbcd
```

The **reset mbcd** command resets all MBCD statistics currently stored on the Net-Net SBC.

Example

```
ACMEPACKET# reset mbcd
```

reset media

Syntax

```
reset media <"gmac-statistics" | "host-statistics">
```

The **reset media** command clears accumulated media statistics on the system.

Arguments

<gmac-statistics>	Clear all of the Gigabit MAC interface statistics

<host-statistics> Clear all of the host packet statistics

Example ACMEPACKET# **reset media gmac-statistics**

reset nat

Syntax `reset nat statistics`

The **reset nat statistics** command clears all of the NAT statistics from the system.

Example ACMEPACKET# **reset nat statistics**

reset net-management-control

Syntax `reset net-management-control [rule-name]`

The **reset net-management-control** command resets all NMC statistics currently stored on the Net-Net SBC.

Arguments

[rule-name] Reset NMC statistics for a specified NMC rule. This argument is optional. The Net-Net SBC resets all NMC rules if no rule name is specified.

Example ACMEPACKET# **reset net-management-control**

reset qos

Syntax `reset qos`

The **reset qos** command clears all accumulated QOS statistics from the system.

Example ACMEPACKET# **reset qos**

reset session-agent

Syntax `reset session-agent <session agent ID>`

The **reset session-agent** command clears accumulated session-agent statistics from a specified session-agent.

Arguments <session agent ID> Enter the name of the session agent whose statistics you want to clear.

Example `ACMEPACKET# reset session-agent agent1`

reset sip

Syntax `reset sip`

The **reset sip** command resets all SIP statistics currently stored on the Net-Net SBC.

Example `ACMEPACKET# reset sip`

Mode Superuser

Path Type **reset** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0 / Most recent update: 7.1

restore

The **restore** command restores a previous or backup configuration.

Syntax `restore [backup <config filename> | previous | running | saved]`

Arguments

[backup]	Restore a backup configuration. You must enter the name of the backup configuration file.
[previous]	Restore the previously saved configuration
[saved]	Restore the configuration to the last running configuration.
[running]	Restore the last running configuration

Mode Superuser

Path Type **restore** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0 / Most recent update: 7.1

Example `ACMEPACKET# restore backup 01_July.gz`

save

The **save** command stores parameters that you've configured on the Net-Net SBC's memory.

Syntax `save <"config" | "backup">`

Arguments

<config>	Save the system configuration. You are informed when the process is complete.
<backup>	Add a name for the backup file to save the backup configuration

Mode Superuser

Path Type **save** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0

Example

```
ACMEPACKET# save config
```

security

The **security** command allows you to implement all certificate and security key commands.

security certificate

Syntax

```
security certificate <import | request | verify>
```

The **security** certificate command allows you to import certificates, create certificates, view the content of a certificate record, and verify the validity of a certificate.

Arguments

<import>	Import a specified type of certificate. The following are valid certificates:
Values	• pkcs12 <filename> <certificate-record-name> <password>—Import a certificate in pkcs12 format • pkcs7 <certificate-record-name> [filename]—Import a certificate in pkcs7 format • try-all <certificate-record-name> [filename]—Try importing both x509 and pkcs7 formats • x509 <certificate-record-name> [filename]—Import a certificate in password enhanced mail format
<request>	Generate a pkcs10 certificate request.
Values	• certificate-record-name—Enter the certificate record to generate a request for
<verify>	Verify a certificate record.
Values	• certificate-record-name—Enter the certificate record to verify

Example

```
ACMEPACKET# security certificate request acmepacket
```

security generate-key

Syntax

```
security generate-key <type>
```

The **security generate-key** command allows you to generate random security keys for the Net-Net SBC.

Arguments

<type>		Enter the type of security key you want to generate. The following are valid key types:
Values		• 3des—Generate a 3DES 192 bit, odd parity key • aes-128—Generate an AES 128 bit key • aes-256—Generate an AES 256 bit key • hmac-md5—Generate an HMAC MD5 secret • hmac-sha1—Generate an HMAC SHA1 secret

Example

```
ACMEPACKET# security generate-key hmac-md5
```

security ssh-pub-key

Syntax

```
security ssh-pub-key <delete | export | generate | import>
```

The **security ssh-pub-key** command allows you to delete, export, import and generate ssh public keys.

Arguments

<delete>		Remove a specified SSH public key.
Values		login-name—Delete SSH public key with specific login name. This entry is required.
<export>		Export a specified SSH public key.
Values		public-key—Display the specified public-key in RFC 4716 (SECSH) format. This entry is required.
<generate>		Generate an SSH public key.
Values		public-key—Generate a key pair for the specified public-key. This entry is required.
<import>		Import an SSH public key.
Values		• authorized-key—Import authorized key • known-host—Import known host key

Example

```
ACMEPACKET# ssh-pub-key import jdoe
```

security tls

Syntax `security tls clear-cache`

The **security tls clear-cache** command clears the entries in the TLS session cache.

Example `ACMEPACKET# security tls clear-cache`

Mode Superuser

Path Type **security** + arguments at the topmost prompt.

Release First appearance: 6.0

set

The **set** command manipulates certain Net-Net SBC settings in real-time, without reloading the full system configuration.

set alarm filter

Syntax `set alarm filter <task@location> <category> <time>`

Some error conditions continually send alarms to the Alarm Manager until the problem has been solved. To avoid having the alarm table overwhelmed by redundant messages from the Local Card Manager, you can set an alarm filter.

Arguments

<task@location>	Enter the specific task for which you want to set the alarm in the form of <task>@<card>.<cpu>.<core>
<category>	Select the category of alarm you want filtered
Values	• Hardware • System • Network • Media • Application • Configuration • All
<time>	Enter the time period, in milliseconds, of arrival in which redundant alarm messages are ignored, so the alarm table is not overwhelmed

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

set autofailover

Syntax `set autofailover <state>`

The **set autofailover** command enables or disables the system's ability to automatically switchover cards during failures.

Arguments

<state>	Enable or disable autofailover on your Net-Net SBC
Values	• Enable—Enable autofailover • Disable—Disable autofailover

Example

```
ACMEPACKET# set autofailover enable
```

set autoreset

Syntax

```
set autoreset <state>
```

The **set autoreset** command enables or disables the system's ability to reset cards during failures.

Arguments

<state>	Enable or disable autoreset on your Net-Net SBC
Values	• Enable—Enable autoreset • Disable—Disable autoreset

Example

```
ACMEPACKET# set autoreset enable
```

set bootparams

Syntax

```
set bootparams
```

Accesses and changes system boot parameters. Once you have made any necessary changes, the system informs you that your changes will not be implemented until you reboot the system.

Example

```
ACMEPACKET# set bootparams
```

set cfgchange-prompt

Syntax

```
set cfgchange-prompt <state>
```

Enable Net-Net 9200 to 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 for a configuration and return to Superuser mode, the system prefixes the ACLI prompt with two asterisks (**). When you have saved the configuration, but not yet activated it, the system prefixes the ACLI prompt with one asterisk (*).

Arguments

<state>	Enable or disable the CFG change prompt on the Net-Net SBC
Default	disabled
Values	enabled | disabled

Example

```
ACMEPACKET# set cfgchange-prompt enabled
**ACMEPACKET#
```

set ftp

Syntax

```
set ftp <state>
```

Set the state of FTP on the Net-Net SBC.

Arguments

<state>	Enable or disable FTP on the Net-Net SBC
Values	• enabled—Enable FTP • disabled—Disable FTP

Example

```
ACMEPACKET# set ftp enable
```

set log compression

Syntax

```
set log compression <state>
```

The **set log compression** command compresses archived logs for system tasks.

Arguments

<state>	Enable or disable log compression on your Net-Net SBC
Values	• Enabled—Enable log compression • Disabled—Disable log compression

Example

```
ACMEPACKET# set log compression enabled
```

set log echo

Syntax

```
set log echo <task@location> <message>
```

Adds a text message to a log file at any point. This can be very useful to note a point in the debugging process.

Arguments

<task@location>	Enter the task name and location in the form of <name>@<card>.<cpu>.<core>

	<message>	Enter the message being written to the task log. All following arguments go to the log and there is no need to include any parentheses ( ) or quotation marks " ".

Example ACMEPACKET# **set log echo lcm@0.0.0 BEGINNING BATCH TEST NOW**

set log level

Syntax `set log level <task@location> <log-level> [<type> | "all"]`

The **set log level** command changes the log level of a task from the command line without reloading the full system configuration.

Arguments

	<task@location>	Enter the task name you want to change in the form of <name>@<card>.<cpu>.<core>
	<log-level>	Select the log level you want the specified task set to. The following is a list of valid log levels:
	Values	• Critical • Major • Minor • Warning • Notice • Info • Trace • Debug
	[type]	Enter an argument for the task(s) to only output messages of the supplied log type to the given output location. By either entering `all` or by not supplying a type argument sets the level for all facility types. This argument is optional.
	Values	• Session • Media • SIP

Example ACMEPACKET# **set log level sip@0.0.0 warning media**

set log mode

Syntax `set log mode <task@location> <mode> [<type> | "all"]`

The **set log mode** command changes where a task's log files are output to, without reloading the full system configuration.

Arguments

	<task>	Enter the task name in the form of <name>@<card>.<cpu>.<core>

	<mode>	Select the log mode you want a task set to. The following is a list of valid log modes:
	Values	• Default—To the Log Manager only • Local—To task the local log file only • Remote—To the remote log server only • Both—To task both the local log file and the remote log server
	[type]	Enter an argument for the task(s) to only output messages of the supplied mode type to the given output location. By either entering **all** or by not supplying a facility argument sets the log mode for all facility types. This is an optional argument.
	Values	• Session • Media • SIP

Example ACMEPACKET# **set log mode sip@0.0.0 local session**

set log server

Syntax `set log server <task@location> <server> [<type> | “all”]`

The **set log server** command changes the server where a task’s log files are sent to, without reloading the full system configuration.

Arguments

	<task@location>	Enter the task name you want to change in the form of <name>@<card>.<cpu>.<core>
	<server>	Enter the IP address and port of the server. This value can be set to **disabled** to disable the log server for selected types.
	[type]	Enter an argument for the task(s) to only output messages of the supplied server type to the given process server. By either entering `all` or by not supplying a facility argument sets the server for all facility types. This is an optional argument.

Example ACMEPACKET# **set log server sip@0.0.0 192.168.0.10:2500 all**

set mbcd limit

Syntax `set mbcd limit <percentage>`

This command sets the MBCD load limit.

Arguments

	<percentage>	Set the MBCD load limit for the Net-Net SBC
	Values	Min: 0 / Max: 100

Example ACMEPACKET# set mbcd limit 50

set nat limit

Syntax `set nat limit <percentage>`

This command sets the NAT load limit.

Arguments

<percentage>	Set the MBCD load limit for the Net-Net SBC
Values	Min: 0 / Max: 100

Example ACMEPACKET# set nat limit 75

set password

Syntax `set password <config | login | enable | reset>`

This command changes your password for either the User mode or the Superuser mode.

Arguments

<config>	Set the configuration password
Values	• only—Set the password without updating the configuration • reset—Set the password back to the default value • verify—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.
<login>	Set the User mode password
<enable>	Set the Superuser mode password
<reset>	Reset passwords for both the User and Superuser to their original factory default

Example ACMEPACKET# set password login user1

set sfe limit

Syntax `set sfe limit <cpu-limit> <drop-limit>`

The set sfe limit command allows you to set the SFE load limits on the Net-Net SBC.

Arguments

<cpu-limit>	Enter the maximum CPU load limit, in percentage
Values	Min: 0 / Max: 100

	<drop-limit>	Enter the maximum percentage of packet drops
	Values	Min: 0 / Max: 100

Example **ACMEPACKET# set sfe limit cpu-limit 75 drop-limit 75**

set sip limit

Syntax `set sip limit <percentage>`

This command sets the SIP transport CPU load limit in percentage.

Arguments

	<percentage>	Enter the CPU load limit

Example **ACMEPACKET# set sip limit 80**

set system-state

Syntax `set system-state <state> [h323 | sip]`

The **set system-state** command sets the Net-Net SBC as either online or offline.

Arguments

	<state>	Select the system state.
	Values	• online—Enable online system state • offline—Emable offline system state
	[h323]	Specifies the state for H.323 sessions.
	[sip]	Specifies the state for SIP sessions.

Notes If h323 or sip is not specified, all protocols will be set.

The offline setting puts the Net-Net SBC into a state where it is powered on and available for administrative purposes, but does not accept calls. Existing calls in progress are not affected.

Example `ACMEPACKET# set system-state online h323`

set telnet

Syntax `set telnet <state>`

The **set telnet** command sets the state of telnet on the Net-Net SBC.

Arguments

	<state>	The state of telnet on the Net-Net SBC
	Values	• enable—Enable the telnet connection

• disable—Disable the telnet connection

Example ACMEPACKET# set telnet enable

set terminal

Syntax `set terminal <height | more | width>`

The **set terminal** command sets some of the terminal properties including the height, width, and the more prompt.

Arguments

<height>	Set the height of the terminal in number of rows
Default	24
Values	Min: 0 / Max: 1000
<more>	Enable or disable the more prompt. By default this feature is disabled.
Values	enabled | disabled
<width>	Set the width of the terminal in number of columns
Default	80
Values	Min: 10 / Max: 256

Example ACMEPACKET# set terminal height 50

Mode Superuser

Path Type **set** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0 / Most recent update: 7.1

show

The **show** command displays Net-Net SBC statistics, configurations, and other information. Many of the show commands display period and lifetime statistic counts.

show acl

Syntax `show acl <argument>`

The **show acl** command displays ACL entries in the ACL table for signaling and media interfaces.

Arguments

<argument>	The following is a list of valid **show acl** arguments:

Values

• Denied—Display a list of denied entries. Once an endpoint is added to the denied list, it appears in this command's output.
• Info—Display ACL table statistics. For each type of ACL entry, statistics are given for the number of active entries, % utilization of total entries, and max entries, as well as the count and percentage of CAM space used. The following is a list of ACL entry types:

–denied

–trusted

–media

–untrusted

• IP <IP address>—Filter an ACL search and check the ACL properties for a specific IP address. Enter the specific IP address you want to check at the end of the command.
• Trusted—Display a list of trusted ACL entries. Once an endpoint is added to the trusted list, it appears in this command's output.
• Untrusted—Display a list of untrusted ACL entries. Once an endpoint is added to the untrusted list, it appears in this command's output.
• Summary—Display a brief summary of all host ACL entries
• All—Display the information from all of the above show ACL commands along with a brief summary.

Example

```
ACMEPACKET# show acl trusted
```

show alarm

Syntax

```
show alarms <"current" | "filtered">
```

The **show alarm** command displays current alarms configured on the system.

Arguments

<current> Display a list of the current alarms configured on the Net-Net SBC

<filtered> Display the total number of instances of redundant alarms received from a specified LCM. Enter this argument followed by lcm@location.

Example

```
ACMEPACKET# show alarm filtered lcm@0.0.0
```

show amp

Syntax

```
show amp <task@location>
```

The **show amp** command displays AMP statistics for the various tasks on the Net-Net SBC. The following is a list of valid system tasks:

Arguments

<task@location> Enter the task you want to view in the form of <task>@<slot>.<cpu>.<core>. The following is a list of valid system tasks:

Values

- acli—Display Acme Command Line Interface AMP statistics
- arpm—Display ARP Manager AMP statistics
- auth—Display User Authentication AMP statistics
- broker—Display Broker Daemon AMP statistics
- cm—Display Card Manager AMP statistics
- collect—Display collector Daemon AMP statistics
- dnsres—Display Acme DNS Resolution Server AMP statistics
- ftpdalg—Display Acme FTP ALG Server AMP statistics
- h323gkgw—Display H.323 Gatekeeper/Gateway AMP statistics
- h323rasgk—Display H.323 RAS Gatekeeper AMP statistics
- ipc—Display AMP Send/Receive statistics
- lcm—Display Local Core Manager AMP statistics
- lem—Display Local Element Manager AMP statistics
- logman—Display Log Manager AMP statistics
- mbcd—Display MBCD AMP statistics
- msfe—Displays Management Socket Front End AMP statistic
- natm—Display NAT Manager AMP statistics
- npm—Displays NPM AMP statistics
- ntpd—Display network Time Daemon AMP statistics
- rasm—Display Radius Accounting System Manager AMP statistics
- secured—Displays Security Daemon AMP statistics
- sem—Display System Element Manager AMP statistics
- sfe—Display Socket Front End AMP statistics
- sipc—Display SIP Core AMP statistics
- sipls—Display SIP Location Server AMP statistics
- sipt—Display SIP Transport AMP statistics
- sm—Display System Manager AMP statistics
- snmpd—Display Simple Network Management Protocol AMP statistics
- soapd—Display SOAP Protocol Daemon AMP statistics
- sshd—Display SSH Daemon AMP statistics
- xserv—Display Transcoder Server AMP statistics

Example

```
ACMEPACKET# show amp broker@0.0.0
```

show arp

Syntax

```
show arp <argument>
```

This command displays ARP tables, ARP table statistics for network interfaces, and management routes.

<argument> Select the type of ARP statistics you want to view. The following are valid **show arp** arguments:

- info—Display the ARP table statistics including:
  - –Maximum number of entries
  - –Number of used entries
  - –Length of search key
  - –First search entry address
  - –Length of data entry
  - –First data entry address
  - –Enable aging
  - –Enable policing
- standby—Display standby ARP statistics stored on the Net-Net SBC
- statistics-all—Display all ARP statistics for all configured media interfaces.
- statistics-by-interface <slot> <port>—Display the counts and statistics for a specified network interface's ARP table. You must enter this command with the slot and port numbers:
  - –<slot>: 0, 1
  - –<port>: 0, 1, 2, 3
- table-all—Display the complete ARP table including:
  - –Interface (slot/port)
  - –VLAN
  - –IP address
  - –MAC address
  - –Time added to the table for each entry
  - –ARP table entry type
- table-by-interface <slot> <port>—Display the same information as the **show arp table-all** command for a specified network interface. You must enter this command with the slot and port numbers:
  - –<slot>
  - –: 0, 1
  - –<port>: 0, 1, 2, 3
- app-red-table—Display ARP redundancy table statistics

Example

```
ACMEPACKET# show arp table-by-interface 0 1
```

show auditlog

Syntax `show auditlog`

This command displays CLI audit trail files (cli.audit.log). If no arguments are specified, the system displays the file to which audits are currently bring written.

Example `ACMEPACKET# show auditlog`

show backups

Syntax `show backups`

The **show backups** command displays all configuration files in the Net-Net SBC's standard backup file directory.

Example `ACMEPACKET# show backups`

show bootparams

Syntax `show bootparams [ 0 | 1 ]`

The **show bootparams** command displays the system boot parameters. When this command is executed without specifying an SPU, boot parameters for the active SPU are displayed.

Arguments

[0 | 1]	Specify which SPU bootlines you want to view. This is an optional argument.

Example `ACMEPACKET# show bootparams 0`

show built-in-manipulations

Syntax `show built-in-sip-manipulations`

This command displays the name of all built-in SIP-manipulations and descriptions.

Example `ACMEPACKET# show built-in-sip-manipulations`

show cfgchange-prompt

Syntax `show cfgchange-prompt`

The **show cfgchange-prompt** command confirms the state of the version mismatch alert functionality.

Example

```
ACMEPACKET# show cfgchange-prompt
```

show clock

Syntax

```
show clock
```

The **show clock** command displays the current system UTC time and date.

Example

```
ACMEPACKET# show clock
```

show collection

Syntax

```
show collection
```

The **show collection** command displays the status of HDR collection groups and push receivers.

Example

```
ACMEPACKET# show collection
```

show config

Syntax

```
show config <element> [element-id] [“short”] [inventory]
```

The **show config** command displays system configurations.

Arguments

<element> — Select the type of configuration element you want to see. If multiple instances of a configuration element are configured, the Net-Net SBC OS displays all elements. The following is a list of valid configurations:

Values

- system-config—Display the system-config configuration
- timezone—Display system timezone information
- ntp—Display the ntp-config configurations
- phy-interface—Display all physical interfaces
- network-interface—Display all network interfaces
- host-route—Display all host-route configurations
- system-access-list—Display the system-access-list configuration
- capture-receiver—Display capture receiver configuration settings
- soap-config—Display soap-config settings
- snmp-community—Display all snmp-community configurations
- trap-receiver—Display all trap-receiver configurations

- collect—Display collect configurations
- authentication—Display the authentication configuration
- password-policy—Display password-policy configuration settings
- manual-security-association—Display the manual-security-association configuration
- security-policy—Display the security-policy configuration
- certificate—Display certificate configuration settings
- tls-profile—Display the tls-profile configuration
- tls-global—Display the tls-config settings
- public-key—Display public keys
- media-manager—Display the media-manager configuration
- realm-config—Display all realm configurations
- static-flow—Display all static-flow configurations
- steering-pool—Display all steering-pool configurations
- dns-config—Display the dns-config settings
- media-policy—Display all media-policy configurations
- transcoding-policy—Display transcoding policies
- realm-group—Display realm groups
- ext-policy-server—Display external policy servers
- access-control—Display the access control configuration
- net-management-control—Display network management control configuration settings
- account-config—Display the account-config configuration
- local-policy—Display all local-policy configurations
- sip-config—Display all sip-config configurations
- session-agent—Display all session-agent configurations
- session-group—Display all session-group configurations
- sip-feature—Display all sip-feature configurations
- sip-interface—Display all sip-interface configurations
- sip-nat—Display all sip-nat configurations
- media-profile—Display all media-profile configurations
- class-policy—Display all class-policy configurations
- rph-policy—Display RPH policy configuration settings
- rph-profile—Display RPH profile configuration settings
- sip-manipulation—Display the sip manipulation configuration
- session-translation—Display all session-translation configurations
- translation-rules—Display all translation-rules configurations
- sip-response-map—Display sip response maps
- sip-profile—Display SIP profiles
- surrogate-agent—Display surrogate agent configuration settings
- enforcement-profile—Display enforcement profile configuration settings
- session-constraints—Display session constraint configuration settings
- enum-config—Display ENUM server configuration settings
- local-routing-config—Display local routing configurations
- h323-config—Display the h323-config settings
- h323-stack—Display h323-stack configurations
- iwf-config—Display the iwf-config settings

• session-router—Display the session-router configuration
• network-parameters—Display the network-parameters configuration
• sip-q850-map—Display the sip-q850-map configuration
• q850-sip-map—Display the q850-sip-map configuration
• sip-isup-profile—Show the sip-isup-profile configurations

[element-id] Specify a unique element name when multiple instances of a configuration element are configured to view the output for just that specified element. This is an optional argument.

[short] Display an abbreviated output of any **show config** command.

[inventory] Display an inventory of configuration elements.

Example ACMEPACKET# **show config media-policy short**

show cpu

Syntax `show cpu <summary | location | active | standby [“all”]>`

Display all running tasks and their CPU usage on a specified core.

Arguments

<summary> Display a summary of all CPUs

<location> Enter the location of the CPU core in the format of `<slot>.<cpu>.<core>`

<active> Display a summary of active CPUs

<standby> Display a summary of standby CPUs

<all> Display all tasks for the specified core rather than just the top 15. This is an optional argument that works with the **location** argument.

This command along with location displays the following information:

- Task Name—Name of the Net-Net SBC 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 in hours, minutes, and seconds
- Avg—Displays percentage of CPU usage since the Net-Net SBC was last rebooted
- Now—Task’s CPU usage in the last second

Example ACMEPACKET# **show cpu 0.0.0**

show directory

Syntax

```
show directory <path>
```

The **show directory** command allows you to view directories and files on the Net-Net SBC. You can type show directory without any arguments to view all volumes on the Net-Net SBC.

Arguments

<path> Enter the absolute path of the file directory with a forward slash preceding the path name.

[none] Enter the command without any arguments to view all top-level directories.

[*] Enter the command followed by "*" to display all top-level directories and their contents.

Example

```
ACMEPACKET# show directory /pcmia
```

show dns

Syntax

```
show dns <argument>
```

Display DNS statistics stored on the Net-Net SBC.

Arguments

<argument> The DNS statistics you want to view

Values

- Sockets—Display DNS sockets
- Realm—Display DNS statistics for a specified realm. Enter this argument followed by the realm name.
- Server—Display DNS Resolution Server statistics
- cache <realm> [type] [name] [all]—Display the contents of the DNS cache

–realm—The realm on which you want to query

–type—The DNS query type. A, SRV, or NAPTR.

–name—The DNS name to look up

–all—Display all entries

- lookup <realm> <type> <name>—Display the results of a DNS lookup for a number within the DNS cache

–realm—The realm on which you want to query

–type—The DNS query type. A, SRV, or NAPTR.

–name—The DNS name to look up

- query—Perform a DNS lookup directly to the DNS server, without looking in the local cache in the DNS cache

–realm—The realm on which you want to query

–type—The DNS query type. A, SRV, or NAPTR

–name—The DNS name to look up

• sip—Display SIP DNS statistics

Example ACMEPACKET# **show dns target**

show dumps

Syntax `show dumps <slot> [cpu] [core]`

The **show dumps** command lists all dumps present on any SPU present, for any card, cpu, or core.

Arguments

<slot>	Specify the slot whose log dumps you want to view
[cpu]	Specify the CPU whose log dumps you want to view. This is an optional argument.
[core]	Specify the core whose log dumps you want to view. This is an optional argument.

Example ACMEPACKET# **show dumps 2 0 1**

show enum

Syntax `show enum <arguments>`

The **show enum** command displays Net-Net SBC ENUM statistics.

Arguments

<arguments>	The type of enum statistics you want to view. The following are valid **show enum** arguments:
Values	• cache <enum-server> [number] [all]—The **show enum cache** command displays the contents of the ENUM cache
	–enum-server—Choose the cache statistics for the given ENUM server
	–number—Display cache statistics for that phone number on the entered enum server. This is an optional argument.
	–all—Display all cache entries. This is an optional argument.
	• lookup <enum-server> [number]—The **show enum lookup** command displays the results of an ENUM lookup for a number within the cache
	–enum-server—Choose the lookup statistics for the given ENUM server
	–number—Display lookup statistics for the specified phone number on the entered enum server. This is an optional argument.

• query [enum-server] [number]—The **show enum query** command performs an ENUM lookup directly to the ENUM server

–enum-server—Select the server you want to query

–number—Enter the queried number. This is an optional argument.

• server <enum-server>—The **show enum server** command displays a specific ENUM server's statistics

–enum-server—Enter the server whose statistics you want to view

• stats—The **show enum stats** command displays statistics for the ENUM configuration.

Example `ACMEPACKET# show cache server1 all`

show features

Syntax `show features`

The **show features** command displays the currently allowed features and sessions that are licensed on your Net-Net SBC.

Example `ACMEPACKET# show features`

show ftp

Syntax `show ftp`

The **show ftp** command displays the state of the FTP feature on the Net-Net SBC.

Example `ACMEPACKET# show ftp`

show h323

Syntax `show h323 <argument>`

The **show h323** command allows you to view H.323 statistics saved on the Net-Net SBC.

Arguments

<argument> — The following is a list of valid show h323 arguments:

Values

- agentstats—Display H.323 session agent statistics
- all—Display all H.323 statistics
- groupstats—Display H.323 session group statistics
- h323stats—Display H.323 message statistics

• load—Display H.323 load limiting information
• registrations—Display H.323 endpoint registrations
• stackcallstats—Display H.323 stack call statistics
• stackdisconnectinstats—Display H.323 stack disconnect incall statistics
• stackdisconnectoutstats—Display H.323 stack disconnect outcall statistics
• stackpvtstats—Display H.323 stack PVT statistics
• status—Display H.323 server statisticsstack call—Display active H.323 calls
• stack-alarms—Display stacks by stack name, and display the alarm severity and current percentage of max-calls that triggered the alarm.

Example

```
ACMEPACKET# show h323 all
```

show health

```
show health [slot] [CPU] [core]
```

The **show health** command displays the Net-Net SBC's health score. To view the health of a particular card, include the slot number.

Arguments

[slot]	Enter the specified card whose health you want to view
[CPU]	All alarms for the specified CPU are displayed
[core]	All alarms for the specified core are displayed

Example

```
ACMEPACKET# show health 0
```

show hip

Syntax

```
show hip <argument>
```

The **show hip** command displays information about your Net-Net SBC's HIP statistics.

Arguments

<argument>	Enter the type of HIP statistics you want to view
Values	• Statistics-all—Display receive and transmit statistics for all services that reach the host, from all network interfaces, as well as overall HIP statistics • Statistics-by-interface <slot> <port>—Display HIP statistics for a specified network interface –slot—0, 1 –port—0, 1, 2, 3 • Interfaces—Display statistics for configured HIP interfaces

Example

```
ACMEPACKET# show hip statistics-by-interface 0 1
```

show i2c

Syntax

`show i2c [slot]`

The **show i2c** command displays the operating information for all devices that are connected to the I^2C management bus. This command is the primary means of displaying all environmental chassis conditions. By entering the **show i2c** command without any argument, the Net-Net SBC OS will display all I^2C devices.

Arguments

[slot]	Display I^2C properties for a specified slot. This is an optional argument.

Example

```
ACMEPACKET# show i2c 0
```

show images

Syntax

`show images [SPU #]`

This command displays the images stored on either both SPUs or a specified SPU.

Arguments

[SPU #]	Specify the SPU whose images you want to view

Example

```
ACMEPACKET# show images 0
```

show interfaces

Syntax

`show interfaces`

The **show interfaces** command displays statistics for physical, network, and media interfaces.

Example

```
ACMEPACKET# show interfaces
```

show ip

Syntax

`show ip <connections | statistics>`

The **show ip** command displays all TCP and UDP connections and statistics.

Arguments

<connections>	Display all TCP and UPD connections on the Net-Net SBC
<statistics>	Display a list of IP statistics stored on the Net-Net SBC

Example

```
ACMEPACKET# show ip connections
```

show log

Syntax

```
show log <argument> <task@location> [<type> | “all”]
```

Displays the current state of a task’s logging configuration.

Arguments

<argument>	Enter the type of log statistics you want to view. The following is a list of valid log arguments:
Values	• Level—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. • Mode—View the output mode for a supplied task. You can also specify a facility argument. • Server—View the configured Process log server for a supplied task. You can also specify a facility argument. • Compression—Check whether system log files are compressed or not. This argument does not need to be followed with <task@location> and <type> arguments since it reflects a global system setting.
<task@location>	Enter the task and location of the log files you are viewing in the form of <task>@<slot>.<cpu>.<core>
<type>	Specify the type of log file you want to view
Values	• Session • Media • SIP
[all]	View all log file types

Example

```
ACMEPACKET# show log mode sipc@0.0.0 session
```

show lrt cache

Syntax

```
show lrt cache <local-route-config name> <telephone number>
```

The show LRT cache command performs a test LRT cache lookup on the supplied phone number.

Arguments

<local-route-config name>Enter the name of the local route configuration you want to view

<telephone number>Enter the phone number whose statistics you want to view

Example

```
ACMEPACKET# show lrt cache lrtable 16172830971
```

show lrt route-entry

Syntax

```
show lrt route-entry <local-route-config name> <telephone number>
```

The show LRT route-entry command displays a route-entry in the LRT cache for a supplied phone number. This command performs a lookup directly from the LRT file, the route list does not need to be loaded into memory for a positive match on a phone number.

Arguments

<local-route-config name>Enter the name of the local route configuration you want to view

<telephone number>Enter the phone number whose statistics you want to view

Example

```
ACMEPACKET# show lrt route-entry lrtable 16172830971
```

show lrt stats

Syntax

```
show lrt stats [local-route-config name]
```

The show lrt stats command is used to display the statistics corresponding to a specified local LRT route table lookup or to all LRT lookups in aggregate

Arguments

[local-route-config name]Enter the name of the specific LRT you want to look up

Example

```
ACMEPACKET# show lrt stats lrtable
```

show manifest

Syntax

```
show manifest
```

The **show manifest** command displays application tasks, their location, and internal address and port used for communication.

Example

```
ACMEPACKET# show manifest
```

show mbcd

Syntax

```
show mbcd <argument>
```

The **show mbcd** command displays MBCD statistics.

Arguments

<argument>	Select the type of MBCD statistics you want to view.
Values	• all—Display all MBCD statistics • client—Display MBCD Client statistics

- server—Display MBCD Server statistics
- nat—Display MBCD NAT Table statistics
- acl—Display MBCD Access Control statistics
- errors—Display MBCD Error statistics
- add—Display MBCD Add statistics
- modify—Display MBCD Modify statistics
- subtract—Display MBCD Subtract statistics
- notify—Display MBCD Notify statistics
- flows—Display active MBCD flows
- cams—Display active MBCD NAT flows
- rules-natalg—Display active MBCD Nat Alg Rules
- sessions-natalg—Display active MBCD Nat Alg Sessions
- standby—Display standby MBCD statistics
- load—Display media load limiting statistics
- stun—Display MBCD STUN statistics
- realms—Display steering ports and bandwidth usage for home, public, and private realms. The following is a list of statistics displayed when you enter this command:

  –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

- realms <realm-name>—Display mbcd realm statistics for a given realm; given for period and lifetime durations. The following is a list of statistics displayed when you enter this command:

  –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
- forked-session—Display bandwidth constraints for forked sessions.

Example ACMEPACKET# **show mbcd errors**

show media

Syntax `show media <argument>`

The **show media** command displays media statistics.

Arguments

<argument> — Enter the type of media you want to view. The following is a list of valid **show media** arguments:

Values

- Network—Display network interfaces configured for media
- Classify <slot> <port>—Display Network Processor packet classification statistics

  –slot—0, 1

  –port—0, 1, 2, 3
- Host-statistics <slot> <port>—Display host packet statistics

  –slot—0, 1

  –port—0, 1, 2, 3
- Gmac-statistics <slot> <port>—Display Gigabit MAC interface statistics

  –slot—0, 1

  –port—0, 1, 2, 3
- Phy-statistics <slot> <port>—Display physical interface statistics

  –slot—0, 1

  –port—0, 1, 2, 3
- Frame-statistics—Display Traffic Manager Control packet statistics

Example ACMEPACKET# **show media host-statistics 0 1**

show monthly-minutes

Syntax `show monthly-minutes <realm-id>`

Display the monthly minutes for a specified realm.

Arguments

<realm-id> — Enter the specific realm whose monthly minutes you want to view

Example ACMEPACKET# **show monthly-minutes realm1**

show msfe

Syntax

`show msfe <argument>`

This **show msfe** command displays mSFE statistics on the Net-Net SBC.

Arguments

<argument> The type of MSFE statistics you want to view

Values

- Clients—Display MSFE client information
- load—Display SFE load information
- Pending—Display MSFE pending open requests
- Sockets <"total"> <"full"><"listen"> <handle>—Display MSFE socket information

–<total>—Display summary counters

–<full>—Display full information for all sockets

–<listen>—Display UDP sockets and TCP listen sockets info

–<handle>—Display information about a specified socket. Entries should be in the form of <slot> : <client IPPort>

- Summary—Display MSFE summary statistics including the following:

–Handles

–Slow Path Transmit Port

–Server State

–UDP Sockets

–TCP Listen Sockets

–TCP Inbound Connection s

–TCP Outbound Connections

–TCP Timers

–Total Active Clients

Example

```
ACMEPACKET# show msfe sockets full
```

show nat

Syntax

`show nat <argument>`

The **show nat** command displays NAT table information and statistics.

Arguments

<argument> Enter the type of NAT statistics you want to view.

Values

- by-addr<ip>— Display NAT statistics for a specified IP address. Enter the IP address in the form x.x.x.x.
- by-index—Display a specified range of entries in the NAT table.

–Min: 1 / Max: 63488

• host—Display NAT host path statistics
• in-tabular—Display a specified range of entries in the NAT table display in the table form.

–Min: 1 / Max: 63488

• info—Display general NAT table information used for quick viewing of a Net-Net SBC's overall NAT functions. Output includes the following:

–Maximum number of entries

–Number of used entries

–Length of search key

–First search entry address

–Length of data entry

–First data entry address

–Enable aging

–Enable policing

–Flow ID list size

–Number of used flows

–Number of free flows

• load—Display NAT load limiting information
• standby—Display standby NAT statistics stored on the Net-Net SBC
• statistics—Display all NAT table statistics including API and CAM statistics
• table<by-dest-addr><by-dest-port><by-src-addr><by-src-port><tabular>—The **show nat table** command expands on the **show nat in-tabular** command by displaying the written-out protocol and weight of each NAT entry.

–<by-dest-addr>—Search for entries in the nat table by specifying destination address

–<by-dest-port>—Search for entries in the nat table by specifying destination port

–<by-src-addr>—Search for entries in the nat table by specifying source address

–<by-src-port>—Search for entries in the nat table by specifying source port

–<tabular>—Search for entries in the nat table by entry range in tabular form

Example

```
ACMEPACKET# show nat statistics
```

show net-management-control

Syntax

```
show net-management-control [rule-name]
```

This command displays the Net-Net SBC's NMC statistics for either all NMC rules or a specified rule.

Arguments

[rule-name]	Display NMC statistics for a specified NMC rule. This argument is optional. The Net-Net SBC displays all NMC rules if you do not include a rule name.

Example

```
ACMEPACKET# show net-management-control
```

show npu

Syntax

```
show npu <argument>
```

This command displays NPU system statistics stored on the Net-Net SBC.

Arguments

<argument>	Enter the type of NPU statistics you want to view. Some of these arguments require you to specify the slot and port numbers you are checking. The following is a list of valid **show npu** arguments:
Values	• Phy-port <slot> <port>—Display the port configuration on the phy side of the DX240 –slot—0, 1 –port—0, 1, 2, 3 • Gmac-port <slot> <port>—Display the port configuration on the GMAC side of the DX240 –slot—0, 1 –port—0, 1, 2, 3 • Phy-stats <slot> <port>—Display Ethernet statistics on the phy side of the DX240 –slot—0, 1 –port—0, 1, 2, 3 • Gmac-stats <slot> <port>—Display statistics on the GMAC side of the DX240 –slot—0, 1 –port—0, 1, 2, 3 • Cpu-stats—Display NPU DX240 CPU port stats • Phy-registers <slot> <port>—Display 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. Entering this command without specifying the slot and port numbers gives you the statistics for port 0 by default.

–slot—0, 1

–port—0, 1, 2, 3

• Interrupts—Display the contents of the interrupt registers on the NPU's DX240
• Registers—Display four key register contents for each of the DX240's ports
• hm—Display NPU Health Monitor statistics

Example `ACMEPACKET# show npu phy-port 0 1`

show ntp

Syntax `show ntp <server | status>`

This command displays current NTP information on the Net-Net SBC.

Arguments

<server>	Display information regarding the configured server
<status>	Display information regarding the status of the daemon

Example `ACMEPACKET# show ntp server`

show packet-trace

Syntax `show packet-trace`

Displays statistics for packet traces initiated on the Net-Net SBC.

`ACMEPACKET# show packet-trace`

show policy-server

Syntax `show policy-server <bandwidth | standby>`

The show policy-server command allows you to view CAC statistics.

Arguments

<bandwidth>	Display external bandwidth manager statistics
<standby>	Display external policy server statistics on the standby SPU

Example `ACMEPACKET# show policy-server bandwidth`

show qos

Syntax

`show qos <argument>`

The **show qos** command displays the Net-Net SBC's Quality of Service statistics.

Arguments

<argument> — Enter the type of QOS statistics you want to view.

Values

- Statistics—Show QOS statistics including the following:
  - –qos adds received
  - –qos adds completed
  - –qos deletes received
  - –qos deletes completed
- Errors—Show QOS errors
- Flow <flow id>—Show QOS flow statistics. You must supply a flow id when using this command.

Example

```
ACMEPACKET# show qos errors
```

show radius

Syntax

`show radius <argument>`

This command displays system radius statistics.

Arguments

<argument> — Enter the type of RADIUS statistics you want to view. The following is a list of valid RADIUS arguments:

- Accounting—Display accounting statistics. The accounting information can be narrowed down even further using the following optional arguments:
  - –slot—Send the command to a specified slot
  - –red—Show redundancy information
  - –ver—Display the verbose output
- Authentication—Show authentication statistics for primary and secondary RADIUS servers, including: server IP address and port; round trip time; information about failed and successful requisitions/authentications; number of rejections; number of challenges; number of time-outs, number of retransmissions
- cdr—Display current CDR files

Example

```
ACMEPACKET# show radius authentication
```

show rdp

Syntax

```
show rdp <location> [<argument>]
```

The **show rdp** command displays the Net-Net SBC's internal network links.

Arguments

<location> — Enter the location of the RDP statistics you are checking in the form of <slot> <cpu> <core>

[argument] — Enter the type of RDP statistics you want to view. This is an optional argument. Not specifying an argument presents a quick summary and current links. The following is a list of valid **show rdp** arguments:

Values

- All—Display the RDP stack information for a given CPU/core, as well as all connections on a specified core and statistics for that connection
- Links [peer]—Display the RDP link information from a supplied CPU/core to all external sockets within the chassis
- Linkstats[peer]—Display the RDP link information from a supplied CPU/core to all external sockets within the chassis. Using this argument includes the same **show rdp links** output plus additional statistics.
- Serv [taskname]—Display the RDP server socket information from a supplied CPU/core to all external sockets within the chassis. You have the option to specify a task name at the end of this command to filter for a supplied task.
- Servstats [taskname]—Display the same output as the **show rdp serv** command, as well as some additional information.
- Conn [taskname]—Display the RDP connection information between tasks running on a supplied CPU/core to all external sockets within the chassis. You have the option to specify a task name at the end of this command to filter for a supplied task.
- Connstats [taskname]—Display the same output as the **show rdp conn** command, as well as some additional information.

Example

```
ACMEPACKET# show rdp 0 0 0 links
```

show realm-specifics

Syntax

```
show realm-specifics <realm-id>
```

Display all realm-specific configurations based on a specified realm ID.

<realm-id> — Specify the realm-id whose realm-specific configurations you want to view

Example ACMEPACKET# **show realm-specifics realm1**

show redundancy

Syntax `show redundancy <argument>`

The **show redundancy** command displays the Net-Net SBC's redundancy statistics.

Arguments

<argument> Enter the type of redundancy statistics you want to view. The following is a list of valid **show redundancy** statistics:

Values
- Cache—Display SIP-LS redundancy statistics
- Configuration—Display configuration redundancy statistics
- Core—Display SIP-CORE redundancy statistics
- MBCD—Display MBCD redundancy statistics
- Transport—Display SIP-T redundancy statistics
- SFE—Display SFE redundancy statistics
- ARP—Display ARP redundancy statistics
- Xserv—Display XSERV redundancy statistics
- Standby—Display standby redundancy statistics
- auth—Display AUTH redundancy statistics
- collect—Display HDR collector redundancy statistics
- pkt-trace—Display packet trace redundancy statistics
- rasm—Display RASM redundancy statistics
- soapd—Display SOAP redundancy statistics
- snmpd—Display SNMP redundancy statistics

Example ACMEPACKET# **show redundancy core**

show registration h323

Syntax `show registration h323 <by-alias> [brief | detailed] [to-file]`

The **show registration h323** command displays detailed information regarding the registration cache.

Arguments

<by-alias <endpoint>>—Display registration cache information by a registered alias.

Values endpoint—Specify the endpoint or the alias whose registration cache information you want to view. This value can be wildcarded.

[brief]—Display a brief command output. This is the default output if the option is omitted.

[detail]—Display the complete registration cache that is available for a specified endpoint or IP address.

Notes

Use of a wildcard value is not allowed for this option.

[to-file]—Display all output from the show registration h323 commands to a file located on the local flash file system instead of to the ACLI.

Example

```
ACMEPACKET# show registration h323 by-alias * to-file /ramdrv/output.txt
```

show registration sip

Syntax

```
show registration sip <by-realm | by-registrar | by-route | by-
user> [brief | detailed | extended] [to-file]
```

The **show registration sip** command displays detailed information regarding the registration cache.

Arguments

There are five ways to view registration cache information. The following are valid arguments:

<by-realm <realm>>—Display information for calls that have registered through a specified ingress realm

realm—Enter the realm whose registration cache information you want to view. This value can be wildcarded.

<by-registrar <IP address>>—Display information for calls that use a specific registrar

Values IP address—Enter the IP address of the registrar whose registration cache information you want to view. This value can be wildcarded.

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

Values IP address—Enter the IP address whose registration cache information you want to view. This value can be wildcarded.

<by-user <endpoint>>—Display registration cache information for a specific endpoint

Values endpoint—Specify the endpoint whose registration cache information you want to view. This value can be wildcarded.

[brief]—Display a brief command output. This is the default output if the option is omitted.

[extend]—Display an extended command output.

[detail]—Display the complete registration cache that is available for a specified endpoint or IP address.

Notes

Use of a wildcard value is not allowed for this option.

[to-file]—Display all output from the show registration sip commands to a file located on the local flash file system instead of to the ACLI.

Example ACMEPACKET# **show registration sip by-user * to-file /ramdrv/output.txt**

show routes

Syntax `show routes`

The **show routes** command displays the current system routing table. This table displays the following information:

- Destination
- TOS
- Gateway
- Flags
- Reference count
- Use
- Interface
- Protocol information

Example ACMEPACKET# **show routes**

show route-stats

Syntax `show route-stats`

The **show route-stats** command displays routing statistics including bad routing redirects, dynamically created routes, new gateway due to redirects, destinations found unreachable, and use of a wildcard route.

Example ACMEPACKET# **show route-stats**

show running-config

`show running-config <element> [element-id] [“short”] [inventory]`

Display statistics about the Net-Net SBC’s running configurations.

Arguments

<element> — Enter the type of running configuration element you want to view. If multiple instances of a configuration element are configured, the Net-Net SBC OS displays all elements. The following is a list of valid running configurations:

Values
- system-config—Display the system-config configuration
- timezone—Display system timezone information
- ntp—Display the ntp-config configurations
- phy-interface—Display all physical interfaces

- network-interface—Display all network interfaces
- host-route—Display all host-route configurations
- system-access-list—Display the system-access-list configuration
- capture-receiver—Display capture receiver configuration settings
- soap-config—Display soap-config settings
- snmp-community—Display all snmp-community configurations
- trap-receiver—Display all trap-receiver configurations
- collect—Display collect configurations
- authentication—Display the authentication configuration
- password-policy—Display password-policy configuration settings
- manual-security-association—Display the manual-security-association configuration
- security-policy—Display the security-policy configuration
- certificate—Display certificate configuration settings
- tls-profile—Display the tls-profile configuration
- tls-global—Display the tls-config settings
- public-key—Display public keys
- media-manager—Display the media-manager configuration
- realm-config—Display all realm configurations
- static-flow—Display all static-flow configurations
- steering-pool—Display all steering-pool configurations
- dns-config—Display the dns-config settings
- media-policy—Display all media-policy configurations
- transcoding-policy—Display transcoding policies
- realm-group—Display realm groups
- ext-policy-server—Display external policy servers
- access-control—Display the access control configuration
- net-management-control—Display network management control configuration settings
- account-config—Display the account-config configuration
- local-policy—Display all local-policy configurations
- sip-config—Display all sip-config configurations
- session-agent—Display all session-agent configurations
- session-group—Display all session-group configurations
- sip-feature—Display all sip-feature configurations
- sip-interface—Display all sip-interface configurations
- sip-nat—Display all sip-nat configurations
- media-profile—Display all media-profile configurations
- class-policy—Display all class-policy configurations
- rph-policy—Display RPH policy configuration settings
- rph-profile—Display RPH profile configuration settings
- sip-manipulation—Display the sip manipulation configuration
- session-translation—Display all session-translation configurations
- translation-rules—Display all translation-rules configurations
- sip-response-map—Display sip response maps
- sip-profile—Display SIP profiles

• surrogate-agent—Display surrogate agent configuration settings
• enforcement-profile—Display enforcement profile configuration settings
• session-constraints—Display session constraint configuration settings
• enum-config—Display ENUM server configuration settings
• local-routing-config—Display local routing configurations
• h323-config—Display the h323-config settings
• h323-stack—Display h323-stack configurations
• iwf-config—Display the iwf-config settings
• session-router—Display the session-router configuration
• network-parameters—Display the network-parameters configuration
• sip-q850-map—Display the sip-q850-map configuration
• q850-sip-map—Display the q850-sip-map configuration
• sip-isup-profile—Show the sip-isup-profile configurations

[element-id] Specify a unique element name when multiple instances of a running configuration element are configured to view the output for just that specified element

[short] Display an abbreviated output of any **show running-config** command

[inventory] Display an inventory of configuration elements.

Example

```
ACMEPACKET# show running-config sip-interface
```

show security

Syntax

```
show security <certificate | ipsec | status | tls cache-count>
```

The **show security** command displays security information on the Net-Net SBC.

Arguments

<certificate> Display certificate record information

Values

• brief <certificate-record-name>—View a brief description of the specified certificate
• details <certificate-record-name>—View a detailed description of the specified certificate
• list—View a list of certificate records
• pem <certificate-record-name>—View a specified certificate in password enhanced mail format

<ipsec> Display IPSec information

Values

• sad [network-interface] <brief | verbose> [selectors]—Display security-association database entries. The following is a list of valid selectors:

–direction—Select by direction

	–dst-addr-prefix—Select by remote IP address prefix –dst-port—Select by destination port –ipsec-protocol—Select by IPSec protocol –spi—Select by security-policy-index –src-addr-prefix—Select by source IP address prefix –src-port—Select by source port –trans-protocol—Select by transport protocol • spd—Display security-policy database entries • statistics—Display interface and security-association statistics –gmac—View GMAC statistics –sad—View security-association statistics
<status>	Display interface hardware status. You have the option to specify the slot and port whose security status you want to view.
Values	• slot • port
<tls cache-count>	Displays the number of entries in the TLS session cache
<ssh-pub-key>	Displays public key record information including login name, fingerprint, fingerprint raw, comment (detailed view only), and public key (detailed view only).
Values	• brief—View a brief display • detail—View a detailed display

Example

```
ACMEPACKET# show security status 0 1
```

show sessions

Syntax

```
show sessions <argument>
```

The **show sessions** command allows you to determine the aggregate sessions for SIP and H.323 on the Net-Net 9200 over Period and Lifetime monitoring spans.

Notes

The Session Statistics are shown for the Period and Lifetime monitoring spans:

–Total sessions—The aggregation of all current active subscriber sessions (H.323 call/SIP session) and is the total session count against the capacity license.

–SIP Sessions—The total current active SIP sessions

–H.323 Calls—The total current active H.323 calls

Notes

The IWF Statistics are shown for the Period and Lifetime monitoring spans:

–H.323 to SIP Calls—The calls that come in H.323 and go out SIP Note that these calls are included in "H.323 Calls" in the Sessions Statistics.

–SIP to H.323 Calls—The calls that come in SIP and go out H.323. Note that these calls are included in "SIP Sessions" in the Session Statistics.

show sfe

Syntax

```
show sfe <argument>
```

The **show sfe** command displays the system's SFE statistics.

Arguments

<argument> Enter the type of SFE statistics you want to view

Values

- Clients—Display SFE client information
- load—Display SFE load information
- Pending—Display SFE pending open requests
- Sockets <"total"> <"full"><"listen"> <handle>—Display SFE socket information

–<total>—Display summary counters

–<full>—Display full information for all sockets

–<listen>—Display UDP sockets and TCP listen sockets info

–<handle>—Display information about a specified socket. Entries should be in the form of <slot> : <client IPPort>

- Summary—Display SFE summary statistics including the following:

–Handles

–Slow Path Transmit Port

–Server State

–UDP Sockets

–TCP Listen Sockets

–TCP Inbound Connection s

–TCP Outbound Connections

–TCP Timers

–Total Active Clients

Example

```
ACMEPACKET# show sfe summary
```

show sip

Syntax

```
show sip <argument>
```

Displays the system's SIP statistics.

Arguments

<argument>

Enter the sip statistics you want to view. The following is a list of valid **show sip** arguments:

Values

• ACK—Display statistics related to incoming SIP ACK messages. The following are the statistics displayed by the **show sip ack** command:

–ACK Requests—Number of ACK requests received

–Retransmissions—Number of retransmissions

–Duplicate Response—Number of duplicate responses

–Transaction Timeouts—Number of transaction timeouts

–Avg Latency—Average latency for packets traveling to and from each session agent

–Max Latency—Maximum latency for packets traveling to and from each session agent

• ACL <realm>—Display SIP Access Control List statistics

–Total Entries—Total ACL entries, including both trusted and blocked

–Trusted—Number of trusted ACL entries

–Blocked—Number of denied ACL entries

–ACL Requests—Number of ACL Requests

–Bad Messages—Number of bad messages

–Promotions—Number of times an entry was promoted to trusted

–Demotions—Number of times an entry was demoted to untrusted

• Agents [ip-address][method]—Display statistics related to defined SIP session agents. Entering this command without any arguments list all SIP session agents. By adding the IP address or hostname of a session agent as well as a specified method at the end of the command, you can display statistics for that specific session agent and method.
• All—Display all SIP statistics
• b2bua—Display statistics related to the SIP Back To Back User Agent task. The SIP B2B UA manages all SIP sessions and dialogs in addition to implementing the Back-to-Back User Agent functionality for SIP. The following are the statistics displayed by the **show sip b2bua** command:

–Dialogs—Number of dialogs

–Sessions—Number of sessions

–CallID Map—Number of Call ID maps

–Pending Requests—Number of pending requests

–Missing Dialog—Dialog could not be found for an in-dialog request or response

–Expired Sessions—Number of expired sessions

–Multiple OK Drops—Number of multiple OK drops

–Multiple OK Terms—Number of multiple OK terms

–Media Failure Drops—Number of media failure drops

–Non-ACK 2xx Drops—Number of non-ACK 2xx drops

–Transaction Errors—Number of transaction errors

–Application Errors—Number of application errors

• BYE—Display statistics related to incoming SIP BYE messages. The following are the statistics displayed by the **show sip ack** command:

–BYE Requests—Number of BYE requests received

–Retransmissions—Number of BYE retransmissions

–200 OK—The number of "200 OK" messages sent in response to a BYE message

–Duplicate Response—Number of duplicate responses

–Transaction Timeouts—Number of transaction timeouts

–Avg Latency—Average latency for packets traveling to and from each session agent

–Max Latency—Maximum latency for packets traveling to and from each session agent

• Cache—Display statistics for the SIP Registration Cache. The following are the statistics displayed by the **show sip cache** command:

–Cached Entries—Number of cached entries

–Local Entries—Number of local entries

–Free Map Ports—Number of free map ports

–Used Map Ports—Number of used map ports

–Transactions—Number of transactions

–Forwards—Number of forwards

–Refreshes—Number of refreshes

–Rejects—Number of rejects

–Timeouts—Number of timeouts

–Fwd Postponed—Number of postponed forwards

–Fwd Rejects—Number of rejected forwards

–Refr Extension—Number of refreshed extensions

–Refresh Extended— Number of extended refreshes

–Reg Cache Hits—Number of successful registration cache lookups

–Reg Cache Misses—Number of failed registration cache lookups

–Route to Registrar—Number of registrations forwarded to the registrar

–Reg w/o Contacts—Number of registrations made without contacts

–Out of Map Ports—Number of times the system ran out of map ports

–Transaction Errors—Number of transaction errors

–Application Errors—Number of application errors

• Cancel—Display statistics related to incoming SIP cancel messages. The following are the statistics displayed by the **show sip cancel** command:

–CANCEL Requests—Number of CANCEL requests received

–Retransmissions—Number of retransmissions

–200 OK—The number of "200 OK" messages sent in response to a CANCEL message

–Duplicate Response—Number of duplicate responses

–Transaction Timeouts—Number of transaction timeouts

–Avg Latency—Average latency for packets traveling to and from each session agent

–Max Latency—Maximum latency for packets traveling to and from each session agent

• Client—Display statistics for SIP client events when the Net-Net SBC is acting as a SIP client in its B2BUA role. Period and lifetime monitoring spans are displayed. The following are statistics displayed by the **show sip client** command:

–Initial—State before a request is sent out

–Trying—Number of times the *trying* state was entered due to the receipt of a request

–Calling—Number of times that the *calling* state was entered due to the receipt of an INVITE request

–Proceeding—Number of times that the *proceeding* state was entered due to the receipt of a provisional response while in the *calling* state

–Cancelled—Number of cancelled calls

–Established—Number of situations in which the client receives a 2xx response to an INVITE

–Completed—Number of times that the *completed* state was entered due to the receipt of a 300 to 699 status code when either in the *calling* or *proceeding* state

–Confirmed—Number of confirmed calls

–Terminated—Number of times that the *terminated* state was entered due to the receipt of a 2xx message.

• codecs <realm-id>—Display SIP realm codec statistics for a specified realm

• Core—Display statistics related to the SIP Core task. This is where the SIP Proxy function is carried out and where requests are forwarded to one or more next hop target destinations. The following are the statistics displayed by the **show sip core** command:

–Response Contacts—Number of response contacts

–Forwarded Requests—Number of forwarded requests

–Saved Contexts—Number of saved contexts the SD found

–Challenge Found—Number of saved contexts found for requests with credentials

–Challenge Not Found—Number of requests with credentials with no saved context found

–Challenge Dropped—Number of saved contexts for which no subsequent request with credentials was received

–Overload Rejects—Number of rejections due to overload

–DNS Errors—Number of DNS errors

–No Target/Route—Number of requests addressed to the SD that did not match local policy or registration cache entry.

–Transaction Errors—Number of transaction errors

–Application Errors—Number of application errors

• Endpoint—Display registration information for a supplied endpoint.
• Errors—Display SIP error statistics on the Net-Net 9000
• Info—Display statistics related to incoming SIP INFO messages
• Interface [interface-id][method]—Display SIP interface statistics. By adding the optional interface-id and method arguments you can narrow the display to view just the interface and method you want to view.
• Invite—Display statistics related to incoming SIP invite messages. The following are the statistics displayed by the **show sip invite** command:

–INVITE Requests—Number of INVITE requests received

–Retransmissions—Number of retransmissions

–100 Trying—The number of “100 Trying” messages sent in response to an INVITE message

–180 Ringing—Number of “180 Ringing” messages sent in response to an INVITE message

–200 OK—The number of “200 OK” messages sent in response to an INVITE message

–Response Retrans—Number of response retransmissions

–Transaction Timeouts—Number of transaction timeouts

–Avg Latency—Average latency for packets traveling to and from each session agent

–Max Latency—Maximum latency for packets traveling to and from each session agent

• ip-cac <IP address>—Display CAC parameters for an IP address
• Load—Display the SIP transport task’s current load

• Media—Display statistics related to SIP media sessions. The following are the statistics displayed by the **show sip media** command:

–Media Sessions—Number of media sessions

–Media Pending—Number of pending media sessions

–SDP Offer Errors—Number of SDP offer errors

–SDP Answer Errors—Number of SDP answer errors

–Drop Media Errors—Number of drop media errors

–Invalid SDP—Number of invalid SDP messages

–Media Exp Events—Number of media flows dropped because they exceed the subsq-guard-timer flow guard, as defined in the media-manager config

–Early Media Exps—Number of media flows dropped because they exceeded the initial-guard-timer flow guard, as defined in the media-manager config

–Exp Media Drops—Number of media flows dropped because they exceeded the flow-time-limit allowed for a media flow, as defined in the media-manager config

–Transaction Errors—Number of transaction errors

–Application Errors—Number of application errors

• Message—Display statistics related to incoming SIP MESSAGE messages
• Notify—Display statistics related to incoming SIP NOTIFY messages
• Nsep [<rvalue> | all]—Display NS/EP RPH statistics
• Options—Display statistics related to incoming SIP OPTIONS messages
• Other—Display statistics related to unknown incoming SIP method statistics
• Policy—Display statistics related to the local policy lookups. The following are the statistics displayed by the **show sip policy** command:

–Local Policy Lookups—Number of local policy lookups

–Local Policy Hits—Number of local policy hits

–Local Policy Misses—Number of local policy misses

–Local Policy Drops—Number of local policy drops

–Agent Group Hits—Number of agent group hits

–Agent Group Misses—Number of agent group misses

–No Routes Found—Number of times no routes were found after the local policy lookup

–Next Hop OOS—Number of times the designated next hop was out of service

–Anonymous Source—Number of requests rejected because they came from an anonymous endpoint based on the allow-anonymous mode for the ingress sip-port

–Invalid Trunk Group—Number of times an invalid trunk group was used

–Inb SA Constraints—Number of times inbound SA constraints were exceeded

–Outb SA Constraints—Number of times outbound SA constraints were exceeded

–Inb REG SA Constraints—Number of inbound requests rejected due to registration constraints being exceeded

–Outb REG SA Constraints—Number of outbound requests rejected due to registration constraints being exceeded

–Overload Rejects—Number of rejections due to overload

• Prack—Display statistics related to incoming SIP PRACK messages
• Publish—Display statistics related to incoming SIP PUBLISH messages
• Realms [realm-id][method]—Display SIP realm statistics. By adding the optional realm-id and method arguments, you can narrow the display to include only the realm and methods you want to view.
• Refer—Display statistics related to incoming SIP REFER messages
• Register—Display statistics related to incoming SIP register messages. The following are the statistics displayed by the **show sip register** command:

–REGISTER Requests—Number of REGISTER requests received

–Retransmissions—Number of retransmissions

–200 OK—The number of "200 OK" messages sent in response to a REGISTER message

–Duplicate Response—Number of duplicate responses

–Transaction Timeouts—Number of transaction timeouts

–Avg Latency—Average latency for packets traveling to and from each session agent

–Max Latency—Maximum latency for packets traveling to and from each session agent

• Server—Display statistics for SIP server events when the Net-Net SBC is acting as a SIP server in its B2BUA role. Period and lifetime monitoring spans for SIP server transactions are given. The following are the statistics displayed by the **show sip server** command:

–Initial—State of the server after a request is received

–Trying—Number of times the "100 Trying" message has been sent

–Calling—Number of times the *calling* state was entered due to the receipt of an INVITE request

–Proceeding—Number of times a server transaction has been constructed for a request

–Cancelled—Number of INVITE transactions for which the Net-Net SBC receives a CANCEL

–Established—Situation in which the server sends a 2xx response to an INVITE

–Completed—Number of times that the server has received a 300 to 699 status code

–Confirmed—Number of times an ACK was received while the server was in the completed state

–Terminated—Number of times the server has received a 2xx response or has never received an ACKI while in the completed state

• sessions [argument]—Displays SIP session statistics. Not entering an argument with this command gives you a summary of all session information stored on the Net-Net SBC. The following is a list of optional **show sip sessions** arguments:

–<all>—Display details for all active sessions

–<by-to><username>—Display information for all sessions matching the SIP "To:" field

–<by-from><username>—Display information for all sessions matching the SIP "From:" field

–<by-ip><IP address>—Display information for all sessions matching either the client or server dialog "RemoteTgt" field

–<by-call-id><call-id>—Display all sessions matching the specified call ID

–<by-media><media>—Display information for all sessions matching any of the media strings contained in the display, including any media IP, port, or codec type

–<by-agent><agent>—Display all the sessions matching either the "To" of "From" session agent name or IP

–The following are the statistics displayed by the **show sip sessions** command:

–*Sessions:*

–Initial—Number of initial sessions

–Early—Number of early sessions

–Established—Number of established sessions

–Terminated—Number of terminated sessions

–*Dialogs:*

–None—Number of dialogs in the process of being created

–Early—Number of early dialogs

–Confirmed—Number of confirmed dialogs

–Terminated—Number of terminated dialogs

• Sockets—Display network connections and message counts on the Net-Net SBC. The following are statistics displayed by the **show sip sockets** command:

–Handle—Index number of an open SIP socket

–Socket—Open socket defined by its protocol, hardware interface, IP address, and port

–MsgRcvd—Number of messages received

–MsgSent—Number of messages sent

–Errors—Number of errors

• Standby <statistic>—Display a specified SIP statistic for the standby card on the Net-Net 9000

–ack

–acl

–agents

–all

–b2bua

–bye

–cache

–cancel

–client

–core

–endpoint

–errors

–info

–invite

–load

–media

–message

–notify

–options

–other

–policy

–prack

–publish

–realms

–refer

–register

–server

–sessions

–sockets

–subscribe

–transport

–update

• Subscribe—Display statistics related to incoming SIP SUBSCRIBE messages
• Transport—Display statistics related to the SIP transport application (sipt). The following are the statistics displayed by the **show sip transport** command:

–Server Trans—Number of server transactions

–Client Trans—Number of client transactions

–Context IDs—Number of context IDs

–Sockets—Number of sockets

–Overload Rejects—Number of rejections due to overload

–Suppressed Retransmit—Number of suppressions due to retransmission

–Response Retransmit—Number of responses due to retransmission

–Req Dropped—Number of dropped requests

–Invalid Requests—Number of invalid requests

–Invalid Responses—Number of invalid responses

–Invalid Messages—Number of invalid messages

–Transaction Errors—Number of transaction errors

–Application Errors—Number of application errors

• Update—Display statistics related to incoming SIP UPDATE messages
• Forked—Display SIP Forked sessions statistics

–Total Sessions

–Total Sessions Rejected

Example

```
ACMEPACKET# show sip sessions
```

show snmp

Syntax

```
show snmp <argument>
```

The **show snmp** command displays SNMP system statistics stored on the Net-Net SBC.

Arguments

<argument>	Enter the type of SNMP statistics you want to view

Values	• Communities—Display SNMP community information including community name, IP addresses, total requests in, and total requests out • Trap-receivers—Display SNMP trap-receiver information including trap-community, filter, level, IP addresses, and total traps out • All—Display both community and trap-receiver SNMP information	

Example **ACMEPACKET# show snmp trap-receivers**

show snr

Syntax `show snr <argument>`

The **show snr** command displays System Name Registry information.

Arguments

<argument>	Enter the type of SNR statistics you want to view	
Values	• Core—Display SNR database contents • Relay—Display SNR relay counters	

Example **ACMEPACKET# show snr core**

show space

Syntax `show space <argument>`

The show space command allows you to view volumes and free disk space.

Arguments

<code>	Display space available on the flash drive.
<pcmcia>	Display space available on the compact flash module.
<ramdrv>	Display space available on the RAM drive.

Example **ACMEPACKET# show space pcmcia**

show ssh

Syntax `show ssh`

The **show ssh** command displays the Net-Net SBC's SSH statistics.

Example **ACMEPACKET# show ssh**

show status

Syntax

```
show status [<slot> [<cpu> [<core>]]]
```

The **show status** command lists all 19 possible feature and interface cards, power supplies, and fan trays. For each of these components, Type, State, HA role, environmental conditions, and a memory usage summary are given. To narrow down the output, you can include the specific card, CPU, and core you want to view to get more detailed information.

Arguments

<slot>	Enter the slot whose status you want to view
<cpu>	Enter the CPU whose status you want to view
<core>	Enter the core whose status you want to view

Example

```
ACMEPACKET# show status 0 1 0
```

show support-info

Syntax

```
show support-info [custom | standard | config | media | signaling]
```

This command gathers a set of information commonly requested by the Acme Packet TAC when troubleshooting customers.

Arguments

[custom] Display information in the `/code/supportinfo.cmds` file to determine what commands should be encompassed. If the file does not exist, then the system notifies you.

[standard] Display information for all commands the **show support-info** command encompasses.

[media] Execute command and write only the show media commands to the support-info.log file.

[signaling] Execute command and write all but the show media commands to the support-info.log.file.

[config] Display "show running-config" output appended to the support-info command output.

Example

```
ACMEPACKET# show support-info standard
```

show switch

Syntax

```
show switch <slot> <argument> [port]
```

The **show switch** command displays the internal BCM56K SPU switch statistics.

Arguments

	<slot>	Enter the slot number the BCM56K switch is connected to
	<argument>	The following is a list of valid **show switch** arguments:
	Values	• Portstate—Display the state of each port on the specified switch • Portstats—Display the statistics for each port on the specified switch • Linkstate—Display the link state for each port on the specified switch • 12table—Display the Layer 2, Ethernet table on the specified switch
	[port]	Filter for a specified port. This is an optional argument.

Example

```
ACMEPACKET# show switch 0 portstats 1
```

show system

Syntax

```
show system
```

Display all system statistics including the following:

- System Uptime
- Temperature Status
- Voltage Status
- Fan Status
- CPU Status
- Memory Status
- State of the system based on the latest setting of the set system-state command

Example

```
ACMEPACKET# show system
```

show task

Syntax

```
show task <task>
```

Display system task statistics. The following is a list of valid arguments:

Arguments

	<task>	Enter the system task you want to view. The following is a list of valid system tasks for this command:
	Values	• acli—Display Acme Command Line Interface task statistics • active—Display a summary of active application tasks • arpm—Display ARP manager task statistics • auth—Display User Authentication task statistics • broker—Display Broker Daemon task statistics

- cm—Display Card Manager task statistics
- collect—Display collector daemon task statistics
- dnsres—Display Acme DNS Resolution Server task statistics
- ftpdalg—Display Acme FTP ALG Server task statistics
- h323gkgw—Display H.323 Gatekeeper/Gateway task statistics
- h323rasgk—Display H.323 RAS Gatekeeper task statistics
- lcm—Display Local Core Manager task statistics
- lem—Display Local Element Manager task statistics
- logman—Display Acmelog Log Manager task statistics
- mbcd—Display MBCD task statistics
- msfe—Display Management Socket Front End task statistics
- natm—Display NAT manager task statistics
- npm—Display NPM task statistics
- ntpd—Display Network Time Daemon task statistics
- rasm—Display Radius Accounting System Manager task statistics
- secured—Display Security Daemon task statistics
- sem—Display System Element Manager task statistics
- sfe—Display Socket Front End task statistics
- sipc—Display SIP Core task statistics
- sipls—Display SIP Location server task statistics
- sipt—Display SIP Transport task statistics
- sm—Display System Manager task statistics
- snmpd—Display Simple Network Management Protocol task statistics
- soapd—Display SOAP Protocol Daemon task statistics
- sshd—Display SSH Daemon task statistics
- standby—Display a summary of standby application tasks
- xserv—Display transcoder server task statistics

Example

```
ACMEPACKET# show task lcm
```

show tcu

Syntax

```
show tcu <argument> <slot>
```

The **show tcu** command displays statistics related to the transcoding unit.

Arguments

<flair> Display FLAIR statistics of a certain TCU

<gbe><tcm ID> Display GBE statistics of a certain TCM

Values <tcm ID>— 0-3

<ibx> <tcm ID> <port>Display IBX statistics of a certain TCU

Values
- <tcm ID>— 0-3
- <port>

–DSP: 0-9

–DBG: 15

–FLAIR: 25

	–BCM1250: 26
<tcm>	Display TCM statistics of a certain TCU
<hm>	Display health monitor statistics of a particular TCU
<slot>	Enter the slot in which you want to view transcoding statistics

Example ACMEPACKET# show gbe flair 1 5

show telnet

Syntax `show telnet`

The **show telnet** command displays the status of the telnet feature on the Net-Net SBC.

Example ACMEPACKET# show telnet

show terminal

Syntax `show terminal`

The **show terminal** command displays the status of the terminal features including the terminal height, width, and more prompt.

Example ACMEPACKET# show terminal

show uptime

Syntax `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.

Example ACMEPACKET# show uptime

show users

Syntax `show users <extended>`

The **show users** command displays all users currently logged into the Net-Net SBC by index number. The following information for each session is also displayed:

- Remote IP address for Telnet or SSH connections
- ID Number
- Duration of the connection

- Type of connection, whether console, telnet, ssh, ftp, or sftp
- State—login state of the connection:
  - user — indicates that the user is logged on, but does not have administrative privileges.
  - priv — indicates the user has have administrative privileges such as the ability to change the configuration or otherwise administer the Net-Net SBC.
  - login — indicates that the session is presenting a log on prompt.
  - A trailing 'C' after the state indicates that user is in configuration mode.
  - A trailing '*' after the state indicates the session issuing the show command.
  - A trailing '!' after the state indicates the session is unresponsive.
  - A trailing '^' after the state indicates the session is dead and must be manually removed from the list.
- Redirect—a console session may be redirected to an internal core. This appears as: <slot>.<cpu>.<core> to which the session is directed.
- FTP sessions
- SFTP sessions

<extended> The extended arguments adds the following columns to the base show users output.

–slot.cpu.core—The core that this session exists on.

–local-address—The local, external IP address on this Net-Net SBC.

show version

Syntax

```
show version <"software" | "hardware" | "all"> [location]
```

The **show version** command displays the OS version currently running on the hardware, as well as the current configuration version and the running configuration version. By not entering an argument you get the same output as you do using the <software> argument.

<software> Display statistics having to do with the software version you are running including:

–Software version

–Software build date

–Current config version

–Running config version

<hardware> Display statistics having to do with the hardware you are running the Net-Net SBC on. Include the location in the form of <slot.>.<cpu>.<core> with this command. The output includes the following:

–Type
–Part Number
–Serial Number
–Func Rev
–Artwk Rev
–Boot Loader Rev

<all> Display both software and hardware statistics

Example **ACMEPACKET# show version**

show virtual-interfaces

Syntax `show virtual-interfaces`

This command displays virtual interfaces for the Net-Net 9200 signaling services.

Example **ACMEPACKET# show virtual-interfaces**

show xclient

Syntax `show xclient <argument>`

The **show xclient** command displays xclient statistics.

Arguments

<argument> Enter the type of xclient statistics you want to view

Values
- <api-stats>—Display XServ API statistics
- <session-all>—Display information about all XClient sessions
- <session-cache>—Display session IDs that have been cached
- <session-byattr> <attribute>—Display xclient sessions for a specified attribute
- <status>—Display the XClient status
- <xlist>—Display a list of XServers for the XClient
- <xserv-lock>—Display the XServ that currently has session allocates locked to it
- <session-bitinfo> <session id>—Display the breakdown of bits of an xclient session
- <session-byid> <ip addr><port>—Display session information and statistics based on the port number and IP address
- <session-byipp> <session-id>—Display session information and statistics based on session ID

Example **ACMEPACKET# show xclient xserv-lock**

show xserv

Syntax

```
show xserv <location> <argument>
```

Arguments

<location> — Enter the location of the xserver whose statistics you want to view

Values
- slot—4-6
- CPU—0-1
- core—0-1

<argument> — Enter the type of xserv statistics you want to view.

Values
- stats—Display the 10 DSPs' loads on a TCM. The location argument you supply corresponds with an xserv that control a TCM.
- api_stats—Display communication statistics about communication between xserver and xclient.
- audit-alloc—Display session allocation information about the selected xserver's sessions.
- audit-free—Display session information about the selected xserver's free sessions.
- audit-lost—Display information about lost sessions, those neither free nor allocated for a selected xserver's sessions.
- audit-full—Display information about all session on a xserver.
- dbginfo—Display debug information for various transcoding process counters.
- session <transcoding_sessionid>—Display 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 at the end of the full command.
- sessstats <transcoding_sessionid>—Display 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 at the end of the full command.
- sysinfo—Display a high level overview for the given xserver
- red-peers—Display redundancy information about this xserver's redundant peer on a separate TCU
- devinfo—Display the SMP device information
- dsp-channel—Display the DSP channel state information
- dsp-device—Display the DSP device state information
- dsp-status—Display the DSP device status
- load—Display the current loading
- red-debug—Display the TCU HA redundancy debug information
- red-flowguard—Display the TCU flow guard information
- red-mode—Display the TCU HA control mask
- red-object-by-ipdest—Display the TCU HA redundancy IP destination state information
- red-object-by-ipsrc—Display the TCU HA redundancy IP source state information

• red-object-by-sessid—Display the TCU HA redundancy session ID state information
• red-resync—Display the TCU HA redundancy RESYNC history
• red-table-addstate—Display the TCU HA redundancy objects in the ADD state
• red-table-codectype—Display the TCU redundancy objects that match the codec type
• red-table-full—Display the TCU HA redundancy object table
• red-table-modstate—Display the TCU HA redundancy objects in the MOD state
• red-transactions—Display the TCU HA redundancy recent transaction log for sync responses

Example `ACMEPACKET# show xserv 5 0 1 session 0xa0000`

Mode User

Path Type **show** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0 / Most recent update: 7.1

start

The **start** command allows you to manually start tasks on the Net-Net SBC.

start collection

The **start collection** command starts the HDR collection process on either all groups or a specified group.

Syntax

```
start collection <group>
```

Arguments

<group> Enter the specified group on which you want to start collection. The following are valid groups:

Values
• all
• card
• core
• fan
• interface
• session-realm
• sip-acl
• sip-b2bua
• sip-client
• sip-core
• sip-errors
• sip-media
• sip-policy
• sip-register
• sip-server
• sip-sessions

- sip-transport
- system
- temperature
- enum-stats
- eps-bw
- h323-stats
- sip-invite
- space

Release First appearance: 5.1 / Most recent update: 7.1

Example

```
ACMEPACKET# start collection temperature
```

start packet-trace

The **start packet-trace** command starts packet tracing on the Net-Net SBC. Once the trace is initiated, the Net-Net SBC duplicates all packets sent to and from the endpoint identified by the IP address that is sent or received on the specified Net-Net SBC network interface.

Syntax

```
start packet-trace <network-interface> <ip-address> [local-port]
[remote-port]
```

Arguments

<network-interface>	Enter the name of the network interface on the Net-Net SBC from which you want to start tracing packets; this value can be entered as either a name alone or as a name and subport identifier value (name:subportid)
<ip-address>	Enter the IP address of the endpoint to and from which the Net-Net SBC will mirror calls
[local-port]	Enter the Layer 4 port number on which the Net-Net SBC receives and from which it sends. This is an optional parameter.
[remote-port]	Enter the Layer 4 port to which the Net-Net SBC sends and from which it receives. This is an optional parameter.

Mode Superuser

Path Type **start** + arguments at the topmost prompt.

Release First appearance: 5.1

Example

```
ACMEPACKET# start packet-trace core:0 192.168.10.99 5060 5060
```

stop

The **start** command allows you to manually stop tasks on the Net-Net SBC.

stop collection

The **stop** command stops the HDR collection process on either all groups or a specified group.

Syntax

```
stop collection <group>
```

Arguments

<group>	Enter the specified group on which you want to stop collection. The following are valid groups:
Values	• all • card • core • fan • interface • session-realm • sip-acl

- sip-b2bua
- sip-client
- sip-core
- sip-errors
- sip-media
- sip-policy
- sip-register
- sip-server
- sip-sessions
- sip-transport
- system
- temperature
- eps-bw
- h323-stats
- space

Example **ACMEPACKET# stop collection sip-core**

stop packet-trace

Manually stop packet tracing on the Net-Net SBC. With this command you can either stop an individual packet trace or use the "all" argument to stop all packet traces that the Net-Net SBC is currently conducting.

Syntax

```
stop packet-trace <network-interface> <ip-address> [local-port]
[remote-port] [all]
```

Arguments

<network-interface>	Enter the name of the network interface on the Net-Net SBC from which you want to stop tracing packets; this value can be entered as either a name alone or as a name and subport identifier value (name:subportid)
<ip-address>	Enter the IP address of the endpoint to and from which the Net-Net SBC will mirror calls
[local-port]	Enter the Layer 4 port number on which the Net-Net SBC receives and from which it sends. This is an optional parameter.
[remote-port]	Enter the Layer 4 port to which the Net-Net SBC sends and from which it receives. This is an optional parameter.
[all]	Stop all packet traces the Net-Net SBC is currently conducting.

Mode Superuser

Path Type **stop** + arguments at the topmost ACLI prompt.

Release First appearance: 5.1

Example **ACMEPACKET# stop packet-trace all**

switchover

The **switchover** command forces the Net-Net SBC cards to switchover.

Syntax

```
switchover <slot> <role>
```

Arguments

	<slot>	Enter the slot number of the card you want to switch
	<role>	Select the new role for the card to assume
	Values	• Active • Standby

Mode Superuser

Path Type **switchover** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0

Example

```
ACMEPACKET# switchover 0 standby
```

tail

This command tails logs to the console.

Syntax

```
tail <task@location> [proto file] [“start” | “stop”]
```

	<task@location>	Enter the name of the task you want to tail in the form of <task>@<card>.<cpu>.<core>
	[proto file]	Enter the type of tracing log file you want to tail in relation to the specified task@location. This is an optional argument.
	[start]	Begin the tailing of the logfile. This is an optional argument
	[stop]	Stop the tailing of the logfile

Mode User

Path Type **tail** + arguments at the topmost ACLI prompt.

Release First appearance: 5.0

Example

```
ACMEPACKET# tail sm@0.0.0 sm.log stop
```

test pattern-rule

Syntax

```
test pattern-rule
```

The **test pattern-rule** command allows you to test header manipulation pattern rules for expression validation.

Arguments

<expression> Enter the regular expression that you want to test. The Net-Net SBC informs you whether or not there is a match.

<string> Enter the string against which you want to compare the regular expression

<show> View the test pattern you entered, whether there was a match, and if so, the number of matches

<exit> End the test

Mode User

Path Type **test pattern-rule** + arguments at the topmost ACLI prompt.

Release First appearance: 7.1

Example

```
ACMEPACKET# test-pattern-rule expression '.*;tgid=(.+).*'
```

test sip-manipulations

Syntax

```
test sip-manipulations
```

The **test sip-manipulations** command allows you test the outcome of your SIP manipulation and header rules without sending real traffic through the Net-Net SBC. The parameters of this command are mapped to test the parameters that exist in sip-interface, realm-config and session-agent (the logical remote entities at which manipulation would occur). Once a test scenario has been configured, you can execute commands for the test. Below are the configurable parameters for the command, followed by the test sip-manipulations commands.

Parameters

debugging—Enable this parameter to display SIP manipulation logging on the screen as the manipulation takes place.

Default disabled

Values enabled | disabled

direction—Enter the direction of the SIP message.

Default out

Values in | out

load-sip-message—Enter the SIP message to be parsed.

Default This tool uses a default SIP message if one is not specified.

Values Cut and paste a SIP message from sipmsg.log or another source.

Notes

Type <Ctrl-D> to stop the SIP text message collection and parse it.

local-ip—Enter the IP address and port for local IP.

Default 192.168.1.60:5060

manipulation-pattern—Enter the regular expression used in $MANIP_PATTERN.

Default \,+

manipulation-string—Enter the manipulation string used in $MANIP_STRING.

remote-ip—Enter the IP address and port for remote IP

Default 192.168.1.61:5060

sip-manipulation—Enter the name of the SIP manipulation pattern to be tested.

tgrp-context—Enter the trunk group context used in $TRUNK_GROUP_CONTEXT.

test sip-manipulations>display-sip-message

Syntax `display-sip-message`

Display the entered SIP message.

Example ACMEPACKET<test sip-manipulations># **display-sip-message**

test sip-manipulations>execute

Syntax `execute`

Execute a test for the referenced sip-manipulation against the SIP message.

Example ACMEPACKET<test sip-manipulations># **execute**

test sip-manipulations>refresh-manipulations

Syntax `refresh-manipulations`

Reload any newly configured SIP manipulations.

Example ACMEPACKET<test sip-manipulations># **refresh-manipulations**

test sip-manipulations>reset

Syntax `reset`

Reset all parameters, including the SIP message, back to their default values.

Example ACMEPACKET<test sip-manipulations># **reset**

test sip-manipulations>show

Syntax `show`

Show selected objected.

Example ACMEPACKET<test sip-manipulations># **show**

Mode Super User

Path Type **test sip-manipulations** + arguments at the topmost ACLI prompt.

Release First appearance: 7.1

upgrade

Upgrade or downgrade the system release that you are running on the Net-Net 9000.

upgrade cancel

Syntax `upgrade cancel`

The **upgrade cancel** command cancels an upgrade that is currently in progress.

Example ACMEPACKET# **upgrade cancel**

upgrade resume

Syntax `upgrade resume`

The **upgrade resume** command resumes an upgrade that is currently in progress.

Example ACMEPACKET# **upgrade resume**

upgrade status

Syntax `upgrade status`

The **upgrade status** command displays the status of an upgrade that is currently in progress.

Example `ACMEPACKET# upgrade status`

upgrade type

Syntax `<type> <file> [ <tftp-ip> <username> <password>]`

The **upgrade type** command upgrades a particular type of system on the Net-Net SBC.

Arguments

<type>	Select the type of file you want to upgrade. The following are valid options:
Values	• os—Upgrade the operating system
<file>	Enter the name of the file you want to upgrade
[tftp-ip]	Enter the TFTP IP address. This is an optional argument.
[username]	Enter the username. This is an optional argument.
[password]	Enter the password. This is an optional argument.

Example `ACMEPACKET# upgrade os nnD5xx.tar 172.30.0.2 user password`

Mode Superuser

Path Type **upgrade** + arguments at the topmost ACLI prompt.

Release First appearance: 5.1

verify config

Syntax `verify config`

The verify config command checks the consistency of configuration elements in the editing configuration to ensure that parameters are valid before activation.

Mode Superuser

Path Type **verify config** at the topmost ACLI prompt.

Release First appearance: 7.1

Example `ACMEPACKET# verify config`

4 Configuration Elements A-M

access-control

The **access-control** configuration element is used to manually create static ACLs for the host path in the Net-Net SBC.

Syntax

```
access-control <realm-id | description | destination-address |
source-address | application-protocol | transport-protocol |
access | average-rate-limit | trust-level | invalid-signal-
threshold | maximum-signal-threshold | untrusted-signal-threshold
| deny-period | nat-trust-threshold | minimum-reserve-bandwidth |
select | no | show | done | exit>
```

Parameters

realm-id—Enter the ingress realm of traffic destined to host to apply this ACL

description—Provide a brief description of this **access-control** configuration. This is an optional parameter.

source-address—Enter the source address, net mask, port number, and port mask to specify traffic matching for this ACL. Not specifying a port mask implies an exact source port. Not specifying an address mask implies an exact IP address. This parameter is entered in the following format:

```
<ip-address>[/<num-bits>][:<port>][/<port-bits>]
```

Default 0.0.0.0

destination-address—Enter the destination address, net mask, port number, and port mask to specify traffic matching for this ACL. Not specifying a port mask implies an exact source port. Not specifying an address mask implies an exact IP address. If `application-protocol` is not NONE the destination field will be ignored. This parameter is entered in the following format:

```
<ip-address>[/<num-bits>][:<port>][/<port-bits>]
```

Default 0.0.0.0

application-protocol—Select the application-layer protocol configured for this ACL entry

Values SIP | H.323 | NONE

> ***Note: If application-protocol is set to none, the destination-address and port will be used. Ensure that your destination-address is set to a non-default value (0.0.0.0.)***

transport-protocol—Select the transport-layer protocol configured for this ACL entry

Default ALL

Values
- TCP
- UDP
- ICMP
- ALL

access—Select the access control type for this entry

Default permit

Values
- Permit—Put the entry in trusted or untrusted list depending on the **trust-level** parameter. This gets promoted and demoted according to the trust level configured for the host.
- Deny—Put this entry in deny list

average-rate-limit—Enter the sustained rate in bytes per second for host path traffic from a trusted source within the realm. A value of 0 disables the policing.

Default 0

Values Min: 0 / Max: 999999999

trust-level—Select the trust level for the host

Default None

Values
- None—Host always remains untrusted
- Low—Host can get demoted to deny
- Medium—Host can get demoted to untrusted
- High—Host always remains trusted

invalid-signal-threshold—Enter the rate of invalid signaling messages per second to be exceeded within the tolerance-window that causes a demotion event. This parameter is only valid when **trust-level** is configured as low or medium. A value of 0 disables the threshold.

Default 0

Values Min: 0 / Max: 999999999

maximum-signal-threshold—Enter the maximum number of signaling messages that a master host can send within the tolerance-window. The host will be demoted if the Net-Net SBC receives messages more than the configured number. This parameter is only valid when **trust-level** is configured low or medium. A value of 0 disables the threshold.

Default 0

Values Min:0 / Max: 999999999

untrusted-signal-threshold—Enter the maximum number of signaling messages from untrusted sources allowed within the tolerance window

Default 0

Values Min:0 / Max: 999999999

deny-period—Enter the time period in seconds a denoted entry is blocked by this ACL. The host is taken out of deny-list after this time period elapses.

Default 30

Values Min: 0 / Max: 999999999

nat-trust-threshold—Enter the number of individual devices behind the NAT that must be in the denied list before all the devices behind the NAT have their trust level

set to denied. The default value of 0 means that the dynamic demotion feature is disabled.

Default 0

Values Min: 0 / Max: 65535

minimum-reserve-bandwidth—Enter the minimum reserved bandwidth you want for the session agent, and that triggers the creation of a separate pipe for it. This parameter is only valid when the trust level is set to high. A value of zero disables this feature.

Default 0

Values Min: 0 / Max: 999999999

Path **access-control** is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > access-control**.

Release First appearance: 5.0

Notes This is a multiple instance configuration element.

account-config

The **account-config** configuration element establishes where accounting messages are sent.

Syntax

```
account-config <hostname | port | strategy | state | max-msg-
delay | max-wait-failover | trans-at-close | generate-start |
generate-interim | | intermediate-period | file-output | file-
path | max-file-size | max-files | file-rotate-time | ftp-push |
ftp-address | ftp-port | ftp-user | ftp-password | ftp-remote-
path | ftp-strategy | ftp-max-wait-failover | prevent-duplicate-
attrs | vsa-id-range | account-servers | push-receiver | temp-
remote-file | file-seq-number | file-compression | file-
decompression | select | no | show | done | exit>
```

Parameters

hostname—Enter the hostname of this Net-Net SBC. The accounting configuration will not work properly unless this is set to "localhost".

Default Localhost name

port—Enter the UDP port number from which RADIUS messages are sent

Default 1813

Values Min: 1025 / Max: 65535

strategy—Select the strategy used to select the current accounting server

Default Hunt

Values
- Hunt—Select accounting servers in the order in which they are listed
- Failover—Use the first and subsequent servers in the accounting server list until a failure is received from that server

• RoundRobin—Select accounting server in order of the server list, distributing the selection of each accounting server evenly over time
• FastestRTT—Select accounting server with the fastest RTT observed during transactions with the servers
• FewestPending—Select accounting server with the fewest number of unacknowledged accounting messages

state—Enable or disable the accounting system

Default enabled

Values enabled | disabled

max-msg-delay—Enter the time in seconds the Net-Net SBC continues to send each accounting message

Default 60

Values Min: 0 / Max: 999999999

max-wait-failover—Enter the number of accounting messages held in the message waiting queue before a failover situation status is enacted

Default 100

Values Min: 1/ Max: 4096

trans-at-close—Enable or disable the Net-Net SBC's transmission of accounting message information only at the close of a session. Disabled sets the Net-Net SBC to transmit accounting information at the start of a session (Start), during the session (Interim), and at the close of a session (Stop).

Default disabled

Values enabled | disabled

generate-start—Select the type of SIP event that triggers the Net-Net SBC to transmit a RADIUS Start message

Default OK

Values
• None—RADIUS Start message is not generated.
• Invite—RADIUS Start message is generated once a SIP session INVITE is received.
• OK—RADIUS Start message is generated an OK message in response to an INVITE is received.

generate-interim—Select the type of SIP event(s) that cause the Net-Net SBC to transmit a RADIUS Interim message. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Default Reinvite-Response

Values [add | delete] <type> [<type>...]

intermediate-period—Enter the periodic interim record interval in seconds

Default 0

Values Min: 0 / Max: 999999999

file-output—Enable or disable the output of comma-delimited CDRs

Default disabled

Values enabled | disabled

file-path—Enter the path in which to save the comma-delimited CDR file. Most common settings for this parameter are /ramdrv or /ramdrv/logs directories. You cannot set this parameter to the /code or /boot directories.

max-file-size—Set the maximum file size in bytes for each CDR file

Default 1000000

Values Min: 1000000 / Max: 2000000000

max-files—Set the maximum number of files to store on the Net-Net SBC

Default 5

Values Min: 1 / Max: 4096

file-rotate-time—Set the time in minutes that the Net-Net SBC rotates the CDR files; the Net-Net SBC will overwrite the oldest file first

Default 0

Values Min: 2 / Max: 4096

ftp-push—Enable or disable the FTP push feature

Default disabled

Values enabled | disabled

ftp-address—Enter the IP address for the FTP server used with the FTP push feature

ftp-port—Set the TCP port on the FTP server to use with the FTP push feature

Default 21

Values Min: 1025 / Max: 65535

ftp-user—Enter the username the Net-Net SBC will use to log in to the FTP server

ftp-password—Enter the password the Net-Net SBC will use to log in to the FTP server

ftp-remote-path—Enter the file path the Net-Net SBC will use to work in on the FTP server

ftp-strategy—Set the strategy you want the Net-Net SBC to use when selecting from multiple push receivers

Default hunt

Values
- hunt—The Net-Net SBC selects the push receiver from the available list according to the priority level
- failover—The Net-Net SBC selects the push receiver based on priority level and continues to use that same push receiver until it fails over

• roundrobin—The Net-Net SBC selects push receivers systematically one after another, balancing the load among all responsive push receivers
• fastestrtt—The Net-Net SBC selects the push receiver based on best average throughput. For this situation, throughput is the number of bytes transferred divided by the response time. The system uses a running average of the five most recent throughput values to accommodate for network load fluctuations

ftp-max-wait-failover—Enter the amount of time in seconds to wait before the Net-Net SBC declares a push receiver to have failed over

Default 60

Values Min: 1 / Max: 4096

prevent-duplicate-attrs—Enable or disable the prevention of duplicate accounting attributes

Default disabled

Values enabled | disabled

vsa-id-range—Enter the range of accounting attributes to include in CDRs. A blank field means this feature is turned off and all attributes are included.

account-server—Access the account-server subelement

push-receiver—Access the **push-receiver** subelement

file-seq-number—Enable to include sequence numbers in CDR file names.

Default disabled

Values enabled | disabled

file-compression—Enable or disable compression of CDR files; when enabled, comma-delimited CDR files are zipped on the backup device to maximize storage space.

Default disabled

Values enabled | disabled

file-decompression—Enable or disable decompression of CDR files; when enabled, .gz files are decompressed before transmission to the remote server.

Default disabled

Values enabled | disabled

Path **account-config** is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > account-config**.

Release First appearance: 5.0 / Most recent update: 7.1

Notes This is a single instance configuration element.

account-config > account-server

The **account-server** configuration subelement stores the accounting server information for the account-config.

Syntax

```
account-server <hostname | port | state | min-round-trip | max-
inactivity | restart-delay | bundle-vsa | secret | NAS-ID |
priority | select | no | show | done | exit>
```

Parameters

hostname—Enter the hostname of the accounting server. Entries are in FQDN or IP Address Format.

port—Enter the UDP port number associated with the accounting server

Default 1813

Values Min: 1025 / Max: 65535

state—Enable or disable this accounting server

Default enabled

Values enabled | disabled

min-round-trip—Enter the time in milliseconds of the minimum RTT for an accounting message for use with the Fastest RTT strategy method

Default 10

Values Min: 10 / Max: 5000

max-inactivity—Enter the maximum time in seconds the Net-Net SBC waits when accounting messages are pending without a response before this account server is set as inactive for its failover scheme

Default 60

Values Min: 1 / Max: 300

restart-delay—Enter the time in seconds the Net-Net SBC waits after declaring an accounting server inactive before resending an accounting message to that same accounting server

Default 30

Values Min: 1 / Max: 300

bundle-vsa—Enable or disable the accounting server's bundling of VSAs within RADIUS accounting messages

Default enabled

Values enabled | disabled

secret—Enter the secret passed from the accounting server to the client server. Entries in this field must follow the Text Format.

NAS-ID—Enter the value the accounting server uses to identify the Net-Net SBC so messages can be transmitted. Entries in this field must follow the Text Format.

priority—Enter the number corresponding to the priority for this account server to have in relation to the other account servers to which you send traffic.

Default 0 (no set priority)

Values Min: 0 / Max: 999999999

origin-realm—

Path **account-server** is a subelement of the account-config element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > account-config > account-server**.

Release First appearance: 5.0 / Most recent update: 7.1

Notes This list can contain as many accounting servers as necessary. By default, this list remains empty. RADIUS will not work unless an account server is configured. This is a multiple instance configuration element.

account-config>push-receiver

You can configure CDR push receivers for use with the local file storage and FTP push feature.

Syntax

```
push-receiver <server | port | admin-state | remote-path |
filename-prefix | priority | protocol | username | password |
public-key | temp-remote-file | select | no | show | done | exit>
```

Parameters

server—Enter the IP address of the FTP/SFTP server to which you want the Net-Net SBC to push CDR files

Default 0.0.0.0

port—Enter the port number on the FTP/SFTP server. **The Net-Net SBC will send CDR files to this port on the designated FTP/SFTP server**

Default 21

Values Min: 1 / Max: 65535

admin-state—Set the state of this FTP/SFTP push receiver to enabled if you want the Net-Net SBC to send CDR files to it

Default enabled

Values enabled | disabled

remote-path—Enter the remote pathname to which you want CDR files to be sent on the push receiver. CDR files will be placed in this location on the FTP/SFTP server

filename-prefix—Enter the filename prefix to prepend to the CDR files the Net-Net SBC sends to the push receiver. The Net-Net SBC does not rename local files.

priority—Enter a number 0 through 4 to set the priority of this push receiver in relation to the others you configure on the system. The highest priority—and the push receiver the system will use first—is 0. The lowest priority—and the push receiver the system will use last—is 4.

Default 4

Values Min: 0 (highest) / Max: 4 (lowest)

protocol—Select the transport protocol you want to use for this push receiver. If you define this push receiver as an SFTP, you need to enter the public-key information in the appropriate parameter in this configuration subelement.

Default ftp

Values ftp | sftp

username—Enter the username the Net-Net SBC is to use when connecting to their push receiver

password—Enter the password corresponding to the username of this push receiver

public-key—Enter the public key profile to use for authentication when you have defined this as an SFTP push receiver. If you define this as an SFTP push receiver but do not set the public-key value, the Net-Net SBC will use password authentication.

temp-remote-file—Enable to upload CDR CSV files initially with a tmp-prefix and then rename the file after successful upload.

Default disabled

Values enabled | disabled

Path

push-receiver is a subelement under the **account-config** element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > account-config > push-receiver**.

Release

First appearance: D7.0 / Most recent update: 7.1

RTC Status

Supported

authentication

The **authentication** configuration element is used for configuring an authentication profile

Syntax

```
authentication <source-port | type | protocol | radius-servers |
allow-local-authorization | login-as-admin | select | no | show |
done>
```

Parameters

source-port—Enter the port number of the Net-Net SBC you want the message sent to the RADIUS server

Default 1812

Values 1645 | 1812

type—Select the type of user authentication you want to use on the Net-Net SBC

Default local

Values local | radius

protocol—Set the protocol type you want to use with your RADIUS server(s) if you are using the RADIUS user authentication

Default pap

Values pap | chap | mschapv2

radius-servers—Enter the radius-servers subelement

allow-local-authorization—Set this parameter to enabled if you want the Net-Net SBC to authorize users to enter Superuser (administrative) mode locally even when your RADIUS server does not return the ACME_USER_CLASS VSA or the Cisco-AVPair VSA.

Default disabled

Values enabled | disabled

login-as-admin—Enable this parameter if you want users to be logged automatically in Superuser (administrative) mode

Default disabled

Values enabled | disabled

Path

authentication is an element under the security path. The full path from the topmost ACLI prompt is: **configure terminal > security> authentication.**

Release

First appearance: 5.0

authentication>radius-servers

The **radius-servers** subelement defines and configures the RADIUS servers that the Net-Net SBC communicates with.

Syntax

```
radius-servers <address | port | state | secret | nas-id | retry-
limit | retry-time | maximum-sessions | class | dead-time |
authentication-methods | select | no | show | done>
```

Parameters

address—Enter the remote IP address for the RADIUS server

port—Enter the port number for the RADIUS server

Default 1812

Values 1645 | 1812

state—Enable or disable the the ability to authenticate users on the RADIUS server.

Default enabled

Values enabled | disabled

secret—Set the password for the RADIUS server and the Net-Net SBC to share. This password is transmitted between the two when the request for authentication is initiated; this ensures that the RADIUS server is communicating with the correct client.

nas-id—Set the NAS ID for the RADIUS server

retry-limit—Enter the number of times that you want the Net-Net SBC to try connecting to the RADIUS server

Default 3

Values Min: 1 / Max: 5

retry-time—Enter the amount of time (in seconds) that you want the Net-Net SBC to wait before connecting to the RADIUS server

Default 5

Values Min: 5 / Max: 10

maximum-sessions—Enter the maximum number of outstanding sessions for the RADIUS server

Default 255

Values Min: 1 / Max: 255

class—Select either primary or secondary for the class of this RADIUS server. The Net-Net SBC tries to initiate contact with primary RADIUS servers first, and then tries the secondary servers if it cannot reach any of the primary ones.

Default Primary

Values Primary | Secondary

dead-time—Enter the amount of time (in seconds) before the Net-Net SBC retries a RADIUS server that it has designated as dead because that server did not respond within the maximum number of retries

Default 10

Values Min: 10 / Max: 10000

authentication-methods—Select the authentication method you want the Net-Net SBC to use with this RADIUS server

This parameter has a specific relationship to the global protocol parameter for the authentication configuration, and you should exercise care when setting it. If the authentication method that you set for the RADIUS server does not match the global authentication protocol, then the RADIUS server is not used. The Net-Net SBC simply overlooks it and does not send authentication requests to it. To enable use of the server, change the global authentication protocol so that it matches.

Default all

Values all | pap | chap | mschapv2

Path **radius-server** is a subelement of the authentication element. The full path from the topmost ACLI prompt is: **configure terminal > security > authentication > radius-servers**.

Release First appearance: 5.0

capture-receiver

The **capture-receiver** configuration element allows you to configure packet tracing functionality on your Net-Net SBC.

Syntax

```
capture-receiver <state | ip-address | network-interface | select
| no | show | done | exit>
```

Parameters

state—Enable or disable the use of the trace server to which you want to send the mirrored packets for calls you are packet tracing.

Default disabled

Values enabled | disabled

ip-address—Enter the IP address of the trace server

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`.

Default :0

Path **capture-receiver** is an element of the system path. The full path from the topmost ACLI prompt is: **configure-terminal > system > capture-receiver**.

Release First appearance: 5.1

certificate

This configuration element configures certificate records for TLS support

Syntax

```
certificate <name | country | state | locality | organization |
unit | common-name | key-size | alternate-name | select | no |
show | done | exit>
```

Parameters

name—Enter the name of the certificate record. This is a required parameter.

country—Enter the name of the country

Default US

state—Enter the name of the state for the country

Default MA

locality—Enter the name of the locality for the state.

Default Burlington

organization—Enter the name of the organization holding the certificate

Default Engineering

unit—Enter the name of the unit holding the certificate within the organization

common-name—Enter the common name for the certificate record

key-size—Enter the size of the key for the certificate

Default 1024

Values 512 | 1024 |2048

alternate-name—Enter the alternate name of the certificate holder

Path

certificate is an element of the **security** path. The full path from the topmost ACLI prompt is: **configure terminal > security > certificate**.

Release

First appearance: 6.0

RTC Status

Supported

certificate-record

This configuration element configures certificate records for TLS support

Syntax

```
certificate <name | country | state | locality | organization |
unit | common-name | key-size | alternate-name | select | no |
show | done | exit>
```

Parameters

name—Enter the name of the certificate record. This is a required parameter.

country—Enter the name of the country

Default US

state—Enter the name of the state for the country

Default MA

locality—Enter the name of the locality for the state.

Default Burlington

organization—Enter the name of the organization holding the certificate

Default Engineering

unit—Enter the name of the unit holding the certificate within the organization

common-name—Enter the common name for the certificate record

key-size—Enter the size of the key for the certificate

Default 1024

Values 512 | 1024 |2048

alternate-name—Enter the alternate name of the certificate holder

key-usage-list—Enter the usage extensions you want to use with this certificate record. This parameter can be configured with multiple values, and its default is a combination.

Default digitalSignature and keyEncipherment

Values
- digitalSignature
- nonRepudiation
- keyEncipherment
- dataEncipherment
- keyAgreement
- encipherOnly
- decipherOnly

extended-key-usage-list—Enter the extended key usage extensions you want to use with this certificate record.

Default serverAuth

Values
- serverAuth
- clientAuth

Path

certificate is an element of the **security** path. The full path from the topmost ACLI prompt is: **configure terminal > security > certificate**-record.

Release

First appearance: 6.0 / Most recent update: D7.0

RTC Status Supported

class-profile

The **class-profile** configuration element lets you access the **class-policy** configuration element for creating classification policies for ToS marking for SIP and/or RTP.

Syntax

```
class-profile <class-policy | exit>
```

Parameters

class-policy—Enter the class-policy subelement

Path

class-profile is an element under the session-router path. The full path from the topmost prompt is: **configure terminal > session-router > class-profile.**

Release

First appearance: 5.0

class-profile > class-policy

The **class-policy** configuration subelement lets you create classification policies that are used to create a ToS marking on outgoing traffic based upon a matching **media-policy** and destination address.

Syntax

```
class-policy <profile-name | to-address | media-policy | select |
no | show | done | exit>
```

Parameters

profile-name—Enter the classification profile name

to-address—List the addresses to match for when determining when to apply this class-policy. Addresses can take the following forms:

- `+<number>`—Indicates an E164 address
- `<number>`—Indicates a default session router address type
- `[<host>.]<domain>`—Indicates a host or domain address

Excluding keywords **`add`** and **`delete`** when a list is already configured replaces the entire list.

Values [add | delete] <address> [<address>...]

media-policy—Enter the media-policy used for this class-policy

Path

class-policy is a subelement under the session-router path. The full path from the topmost prompt is: **configure terminal > session-router > class-profile > class-policy.**

Release

First appearance: 5.0

collect

The **collect** configuration element allows you to configure general collection commands for data collection on the Net-Net SBC.

Syntax

```
collect <boot-state | sample-interval | push-interval | start-
time | end-time | push-receiver | group-settings | push-success-
trap-stats | select | no | show | done | exit>
```

Parameters

boot-state—Enable or disable group collection on reboot

Default disabled

Values enabled | disabled

sample-interval—Enter the data collection sampling interval, in minutes

Default 5

Values Min: 1 / Max: 120

push-interval—Enter the data collecting push interval, in minutes

Default 15

Values Min: 1 / Max: 120

start-time—Enter the date and time to start data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hours; m=minutes; s=seconds).

Default now

end-time—Enter the date and time to stop data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hours; m=minutes; s=seconds)

Default never

push-receiver—Access the **push-receiver** subelement

group-settings—Access the **group-settings** subelement

push-success-trap-enabled-state—Enable or disable collector push success trap

Default disabled

Values enabled | disabled

Path

collect is an element of the system path. The full path from the topmost ACLI prompt is: **configure-terminal > system > collect**.

Release

First appearance: 5.1

collect>group-settings

The **group-settings** subelement allows you to configure and modify collection parameters for specific groups.

Syntax

```
group-settings <group-name | boot-state | sample-interval |
start-time | end-time | select | no | show | done | exit>
```

Parameters

group-name—Enter the name of the object the configuration parameters are for. There can only be one group.

Default system

Values
- all
- card
- core
- fan
- h323-stats
- interface
- mgcp-ACL
- mgcp-media-events,
- mgcp-oper
- mgcp-state
- mgcp-trans
- session-agent
- session-realm
- sip-ACL
- sip-client
- sip-errors
- sip-policy
- sip-server
- sip-sessions
- sip-b2bua
- sip-transport
- sip-core
- sip-media
- sip-register
- system
- temperature
- voltage
- eps-bw

boot-state—Enable or disable data collection for this group.

Default disabled

Values enabled | disabled

sample-interval—Enter the group data collection sampling interval, in minutes

Default 1

Values Min: 1 / Max: 120

start-time—Enter the date and time to start group data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hours; m=minutes; s=seconds)

Default now

end-time—Enter the date and time to stop group data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hours; m=minutes; s=seconds)

Default never

Path **group-settings** is a subelement of the system>collect path. The full path from the topmost ACLI prompt is: **configure-terminal > system > collect > group-settings**.

Release First appearance: 5.1 / Most recent update: 7.1

collect>push-receiver

The **push-receiver** subelement allows you to configure the Net-Net SBC to push collected data to a specified node.

Syntax

```
push-receiver <address | user-name | password | data-store |
protocol | select | no | show | done | exit>
```

Parameters

address—Enter the sIP address to which the Net-Net SBC pushes collected data

user-name—Enter the login user name for the specified server used when pushing collected data

password—Enter the login password for the specified server used when pushing collected data

data-store—Enter a directory on the specified server in which to put collected data

protocol—Enter the protocol you want to use for HDR collection record files

Default FTP

Values FTP | SFTP

Path **push-receiver** is a subelement of the system>collect path. The full path from the topmost ACLI prompt is: **configure-terminal > system > collect > push-receiver**.

Release First appearance: 5.1

dns-config

The **dns-config** configuration element configures the DNS-ALG on a per client-realm basis.

Syntax

```
dns-config <client-realm | description | client-address-list |
server-dns-attributes | select | no | show | done | exit>
```

client-realm—Enter the realm from which DNS queries are received. This value must be the name of a configured realm.

description—Enter a brief description of the dns-alg configuration element.

client-address-list—Enter the IP client-realm address(es) from which the Net-Net SBC can receive DNS queries. This is a required field.

server-dns-attributes—Enter the **server-dns-attributes** subelement.

Path **dns-config** is an element under the media-manager path. The full path from the topmost ACLI prompt is: configure-terminal > media-manager > dns-config.

Release First appearance: 6.0

RTC Status Supported

Notes This is a multiple instance configuration element.

dns-config>server-dns-attributes

The **server-dns-attributes** subelement configures DNS servers.

Syntax

```
server-dns-attributes <server-realm | domain-suffix | server-
address-list | source-address | source-port | transaction-timeout
| address-translation | select | no | show | done | exit>
```

server-realm—Enter the realm from which DNS responses are sent. This value must be the name of a configured realm and is a required parameter.

domain-suffix—Enter the domain suffix for which this DNS server attribute list is used. This field is required and can start with an asterisk or a period.

server-address-list—Enter a list of DNS server IP addresses used for the specified domains. This field is required and can include multiple entries.

source-address—Enter the source IP address from which the ALG sends queries to the DNS server (i.e., a layer 3/layer 4 source address). This is a required field.

source-port—Enter the DUP port number from which the ALG sense queries to the DNS server (i.e., layer 3/layer 4 source address). This is a required value.

Default 53

Values Min: 1025 / Max: 65535

transaction-timeout—Enter the number of seconds that the ALG maintains information to map a DNS server response to the appropriate client request. This is a required value.

Default 10

Values Min: 0 / Max: 999999999

address-translation—Access the address-translation subelement.

Path **server-dns-attributes** is a subelement under the **dns-config** element. The full path from the topmost ACLI prompt is: **configure-terminal > media-manager > dns-config > server-dns-attributes**.

Release First appearance: 6.0

RTC Status Supported

Notes This is a multiple instance configuration element.

dns-config>server-dns-attributes>address translation

The **address-translation** subelement sets the list of IP address translations and determines how the NAT function for this feature occurs. Multiple entries in this field allow one DNS-ALG network entity to service multiple Net-Net SBCs or multiple sets of addresses.

Syntax

```
address-translation <server-prefix | client-prefix | select | no
| show | done | exit>
```

server-prefix—Enter the address/prefix returned by the DNS server. The server-prefix is an IP address and number of bits in slash notation.

client-prefix—Enter the address/prefix to which a response is returned. The client-prefix is an IP address and number of bits in slash notation.

Path

address-translation is a sub-subelement of the **dns-config>server-dns-attributes** subelement. The full path from the topmost ACLI is: **configure-terminal > media-manager > dns-config > server-dns-attributes > address translation**.

Release

First appearance: 6.0

RTC Status

Supported

Notes

Values specified for the number of bits dictates how much of the IP address will be matched. If the number of bits remains unspecified, then the Net-Net SBC will use all 32 bits for matching. Setting the bits portion after the slash to 0 is the same as omitting it. This is a multiple instance configuration element.

enforcement-profile

The **enforcement-profile** configuration element sets groups of SIP methods to apply in the global SIP configuration, a SIP interface, a SIP session agent, or a realm.

Syntax

```
enforcement-profile <name | allowed-methods | sdp-address-check |
subscribe-event | select | no | show | done | exit>
```

Parameters

name—Enter the name of the ENUM configuration

allowed-methods—Select a list of SIP methods that you want to allow in this set. Any other text you enter for this parameter becomes a new method that the Net-Net SBC will not block, so be sure that you type the standard methods correctly or you could accidently block several messages. The messages ACK, BYE, and CANCEL are automatically unblocked. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Default none

Values

- invite
- register
- prack
- options
- info
- subscribe
- notify
- refer
- update
- message
- publish

sdp-address-check—Enable or disable SDP address checking on the Net-Net SBC

Default disabled

Values enabled | disabled

subscribe-event—Enter the subscribe-event configuration subelement

Path **enforcement-profile** is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure-terminal > session-router > enforcement-profile**.

Release First appearance: 5.1

enforcement-profile>subscribe-event

The **subscribe-event** subelement defines subscription event limits for SIP per-user dialogs.

Syntax

```
subscribe-event <event-type | max-subscriptions | select | no |
show | done | exit>
```

Parameters

event-type—Enter the SIP subscription event type for which you want to set up limits. You can also wildcard this value (meaning that this limit is applied to all event types except the others specifically configured in this enforcement profile). To use the wildcard, enter an asterisk (*****) for the parameter value.

max-subscriptions—Enter the maximum number of subscriptions allowed to a user for the SIP subscription event type you entered in the **event-type** parameter. When no value is entered for this parameter there is no limit.

Default 0

Values Min: 0 / Max: 65535

Path

subscribe-event is a subelement under the **enforcement-profile** element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > enforcement-profile > subscribe-event**.

Release

First appearance: D6.0

RTC Status

Supported

enum-config

The **enum-config** is used to configure ENUM functionality on your Net-Net SBC.

Syntax

```
enum-config <name | top-level-domain | realm-id | enum-servers |
timeout | cache-inactivity-timer | lookup-length | max-response-
size | query-method | health-query-number | health-query-interval
| failover-to | cache-addl-records | include-source-info | select
| no | show | done>
```

Parameters

name—Enter the name of the ENUM configuration

top-level-domain—Enter the domain extension used to query the ENUM servers for this configuration. The query name is a concatenation of the number and the domain.

realm-id—Enter the realm-id is used to determine on which network interface to issue an ENUM query

enum-servers—Enter the name of an ENUM server and its corresponding redundant servers to be queried. In a query, separate each server address with a space and enclose list within parentheses.

timeout—Enter the total time, in seconds, that should elapse before a query sent to a server (and its retransmissions) will timeout. If the first query times out, the next server is queried and the same timeout is applied. This process continues until all

the servers in the list have timed out or one of the servers responds. The retransmission of ENUM queries is controlled by three timers:

Values
- Init-timer—The initial retransmission interval. The minimum value allowed for this timer is 250 milliseconds.
- Max-timer—The maximum retransmission interval. The interval is doubled after every retransmission. If the resulting retransmission interval is greater than the value of max-timer, it is set to the max-timer value.
- Expire-timer—The query expiration timer. If a response is not received for a query and its retransmissions within this interval, the server will be considered non-responsive and the next server in the list will be tried.

cache-inactivity-timer—Enter the time interval, in seconds, after which you want cache entries created by ENUM requests deleted, if inactive for this interval. If the cache entry gets a hit, the timer restarts and the algorithm is continued until the cache entry reaches its actual time to live.

Default 3600

Values Min: 0 / Max: 999999999

lookup-length—Specify the length of the ENUM query, starting from the most significant bit

Default 0

Values Min: 0 / Max: 255

max-response-size—Specify the EDNS0 capability for UDP ENUM responses larger than 512 bytes.

Default 512

Values Min: 512 / Max: 65535

query-method—Enter the ENUM query distribution strategy

Default hunt

Values hunt | round-robin

health-query-number—Enter the phone number for the ENUM server health query; when this parameter is blank the feature is disabled.

health-query-interval—Enter the interval in seconds at which you want to query ENUM server health.

Default 0

Values Min: 0 / Max: 65535 (seconds)

failover-to—Enter the name of the **enum-config** to which you want to failover.

cache-addl-records—Set this parameter to **enabled** to add additional records received in an ENUM query to the local DNS cache.

Default enabled

Values enabled | disabled

include-source-info—Set this parameter to enabled to send source URI information to the ENUM server with any ENUM queries.

Default disabled

Values enabled | disabled

service-type—Enter the ENUM service types you want supported in this ENUM configuration seperated by a comma.

Default E2U+sip, sip+E2U

Values Possible ENUM service types are outlined in RFCs 2916 and 3721

Path **enum-config** is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure-terminal > session-router > enum-config**.

Release First appearance: 5.1 / Most recent update: 7.1

ext-policy-server

The **ext-policy-server** is used for configuring RACF or CLF functionality on the Net-Net SBC.

Syntax

```
ext-policy-server <name | state | operation-type | protocol |
address | port | realm | permit-conn-down | asynchronous-mode |
product-name | application-mode | application-id | framed-ip-
addr-encoding | dest-realm-format | ingress-realm-location |
domain-name-suffix | gate-spec-mask | allow-svr-proxy | options |
watchdog-ka-timer | service-class-options | reserve-incomplete |
permit-on-reject | disconnect-on-timeout | select | no | show |
done | exit>
```

Parameters

name—Enter the name for this external bandwidth manager instance. This parameter is used to identify the PDP that will be used in each Realm configuration.

state—Enable or disable this **ext-policy-server** configuration to run this CAC

Default enabled

Values enabled | disabled

operation-type—Select whether or not this external policy server performs bandwidth management functionality or is disabled

Default disabled

Values
- disabled—This parameter is disabled
- bandwidth-mgmt—The Net-Net SBC communicates with a CLF to obtain location string

protocol—Select the external policy server communication protocol

Default C-SOAP

Values
- **COPS**—Standard COPS implementation. COPS client type is 0x7929 for CLF, and 0x7926 for PDP/RACF usage as defined in the operation-type parameter
- **A-COPS**—Vendor specific protocol. COPS client type is 0x4AC0 for admission-control operation-type
- **SOAP**—Not used

• **DIAMETER**—Connects the Net-Net SBC to the policy-server

address—Enter the IP Address of the external PDP

port—Enter the port number the diameter connection connects to on the PDP. The standard port for COPS is 3288.

Default 80

Values Min: 0 / Max: 65535

realm—Enter the name of the Realm in which this Net-Net SBC defines the PDP to exist. This is not necessarily the Realm where the Net-Net SBC performs admission control.

permit-conn-down—Enable or disable this external policy server configuration to permit new calls into the network when the policy server connection is down

Default disabled

Values enabled | disabled

asynchronous-mode—Enable this external policy server to run in asynchronous mode.

Default disabled

Values enabled | disabled

product-name—Enter the vendor-assigned name for the RACF

application-mode—Enter the type of interface you want to use

Default none

Values Rq | Rx | Gq | e3

application-id—Enter a numeric application ID that describes the interface used to communicate with the RACF

Default 0

Values Min: 0 / Max: 999999999

framed-ip-addr-encoding—Enter the format of the Frame-IP-Address (AVP 8) value when this external policy server is configured for Diameter messages.

Default octet-string

Values
- octet-string:Example: 192.168.10.1
- ascii-string:Example: 0xC0A80A01

dest-realm-format—Enter the format you want to use for the Destination-Realm AVP.

Default user-with-realm

Values
- user-only
- user-with-realm
- realm-only

ingress-realm-location—Not used

domain-name-suffix—Enter the suffix you want to use for Origin-Realm and Origin-Host AVPs that have a payload string constructed as a domain name Your

value can be any string, to which the Net-Net SBC will prepend with a dot if you do not include one.

Default .com

gate-spec-mask—With this parameter, you can configure the Net-Net SBC to use a mask comprised entirely of zeros (0). The default value is 255. This parameter sets the value to use for the COPs pkt-mm-3 interface. This interface maintains a persistent TCP connection to the external policy server, even without repsonses to requests for bandwidth. This permits calls to traverse the Net-Net SBC even though the external policy server either fails to respond, or rejects the session.

Default 255

Values Min: 0 / Max: 255

allow-svr-proxy—Enable or disable the Net-Net SBC to include the proxy bit in the header. The presence of the proxy bit allows the Net-Net SBC to tell the external policy server whether it wants the main server to handle the Diameter message, or if it is okay to proxy it to another server on the network (disabled).

Default enabled

Values enabled | disabled

options—Select optional features or parameters. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <options> [<option>...]

watchdog-ka-timer—Not used

service-class-options—Not used

reserve-incomplete—The parameter allows the SBC to make admission requests before learning all the details of the flows and devices (e.g., not knowing the final UDP port numbers for the RTP media streams until after the RTP has begun). The orig-realm-only is used for asymetrically qualified policy server requests.

Default enabled

Values enabled | disabled | orig-realm-only

permit-on-reject—Set this parameter to **enabled** to allow rejected calls to proceed as if they were allowed. When **enabled**, the Net-Net SBC forwards the session on at a "best-effort". Leave this parameter set to **disabled** (default), if you want the Net-Net SBC to deny the session on attempts to revert to the previously-requested bandwidth.

Default disabled

Values enabled | disabled

disconnect-on-timeout—Leave this parameter set to enabled (default) so the Net-Net SBC maintains its TCP connection to the external policy server regardless of the upstream issues between policy servers (PS) and cable modem termination systems (CMTSs). When you disable this setting, the Net-Net SBC sends Gate-Set and Gate-Delete messages in response to the PS's timeouts and guards against impact to the TCP connection between the Net-Net SBC and the PS.

Default disabled

Values enabled | disabled

srv-selection-strategy—Select the strategy used to select an external policy server from the cluster. Failover is the only parameter currently supported.

Default Failover

Values Failover

cache-dest-host—Set this parameter to **enabled** for the Net-Net SBC to cache and send Destination-Host AVP value from PS Origin Host AVP.

Default disabled

Values enabled | disabled

max-connections—Set the number of servers to maintain in an external server cluster.

Default 1

Values Min: 1 | Max: 20

max-timeouts—Set the number of request timeouts before the Net-Net SBC sets the external policy server to inactive.

Default 0

Values Min: 0 | Max: 200

Path **ext-policy-server** is an element under the **media-manager** path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > ext-policy-server**.

Release First appearance: D7.0 / Most recent update: 7.1

RTC Status Supported

h323-config

The **h323-config** element is the top level of the H.323 configuration, and it contains H.323 parameters that apply globally.

Syntax

```
h323-config <state | log-level | response-tmo | connect-tmo |
alternate-routing | codec-fallback | enum-sag-match | switchover-
mode | red-cpu-limit | red-max-media | red-load-max-media |
options | h323-stack | select | no | show | done | exit>
```

Parameters

state—Enable or disable H.323 functionality

Default enabled

Values enabled | disabled

log-level—Select the log level for monitoring H.323 application stack functionality. This value can also override the H.323-specific **task-logging**, but only when the value set here is more verbose than the value set in the **system-config > task-logging** configuration element for either rasgk or gwgk tasks.

Default NOTICE

Values
- EMERGENCY
- CRITICAL

- MAJOR
- MINOR
- WARNING
- NOTICE
- INFO
- TRACE
- DEBUG

response-tmo—Set the number of seconds the Net-Net SBC waits between sending a SETUP message and receiving no response before the call is torn down

Default 4

Values Min: 1 / Max: 999999999

connect-tmo—Set the number of seconds the Net-Net SBC waits between sending a SETUP message and failing to receive a CONNECT message before the call is torn down. If the Net-Net SBC receives a PROCEEDING or ALERT message from the endpoint, it will tear down the session after this timer elapses if a CONNECT message is not received.

Default 32

Values Min: 0 / Max: 999999999

alternate-routing—Select whether to use alternate routing or not

Default proxy

Values
- proxy—The Net-Net SBC sends a release complete message back to the caller
- recur—The Net-Net SBC performs alternate routing

codec-fallback—Enable or disable slow start to fast start codec negotiation

Default disabled

Values enabled | disabled

enum-sag-match—Enable or disable the Net-Net SBC performing matching against the hostnames in ENUM/LRT lookup responses and session agent groups. If there is a match, the Net-Net SBC uses the matching SAG for routing. If no match is found, normal ENUM/LRT routing proceeds.

Default disabled

Values enabled | disabled

switchover-mode—Set the SPU switchover mode for H.323 calls

Default none

Values
- none—Switchover, immediately terminating all H.323 calls
- drop-media—Switchover and drop H.323 calls gracefully
- stop-cdr—Switchover, do not force any calls to terminate, send STOP CDRs when calls are terminated by UAs
- drop-stop—Switchover, gracefully terminate media streams, send respective STOP CDRs

red-cpu-limit—Set the maximum number of media streams to drop during a 10-second drop interval

Default 30

Values Min: 1 / Max: 99

red-max-media—Set the maximum number of media streams to drop during a 10-second drop interval

Default 15

Values Min: 0 / Max: 100

red-load-max-media—Set the number of media streams to drop during a 10-second drop interval after the **red-cpu-limit** has been exceeded

Default 3

Values Min: 0 / Max: 100

options—Select optional features or parameters. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <options> [<option>...]

h323-stack—Enter the **h323-stack** configuration subelement.

Path

h323-config is an element of the **session-router** path. The full path from the topmost ACLI is: **configure terminal > session-router > h323-config**.

Release

First appearance: 6.0

RTC Status

Supported

h323-stack

The **h323-stack** configuration element allows you to configure H.323 stacks on the Net-Net SBC.

Syntax

```
h323-stack <name | description | state | isgateway | realm-id |
assoc-stack | local-ip | max-calls | max-channels | registration-
ttl | terminal-alias | ras-port | auto-gk-discovery | multicast |
gatekeeper | gk-identifier | alternate-transport | q931-port |
q931-max-calls | h245-tunneling | fs-in-first-msg | call-start-
fast | call-start-slow | media-profiles | prefixes | process-
registration | allow-anonymous | options | proxy-mode | h245-
stage | q931-start-port | q931-number-ports | dynamic-start-port
| dynamic-number-ports | filename | tcp-keepalive | alarm-
threshold | select | no | show | done | exit>
```

Parameters

name—Enter the name of the H.323 stack. This value is required and must be unique.

description—Provide a brief description of this **h323-stack** configuration. This is an optional parameter.

state—Enable or disable this H.323 stack

Default enabled

Values enabled | disabled

isgateway—Enable or disable H.323 stack functionality as a Gateway. When this field is set to enabled, the H.323 stack runs as a Gateway. When this field is set to disabled, the H.323 stack runs as a Gatekeeper proxy.

Default enabled

Values enabled | disabled

realm-id—Enter the realm served by this H.323 stack. This value must be a valid identifier for a realm configuration.

assoc-stack—Enter the name of associated outbound H.323 stack for this h323-stack instance. If not configured, the Net-Net SBC will use policy-based stack selection based on a local policy (configured in the local-policy element). If you wish to use static stack select, then each configured h323-stack subelement must have an associated outbound stack. This parameter must correspond to a valid name field value in another instance of the h323-stack subelement.

local-ip—Enter the IP address H.323 stack uses when opening sockets. This field value is the default H.323 stack address.

Default 0.0.0.0

max-calls—Enter the maximum number of calls allowed for the network associated with this H.323 stack

Default 200

Values Min: 0 / Max: 999999999

max-channels—Enter the maximum number of concurrent channels (or pathways used between nodes) allowed for each call associated with this H.323 stack

Default 6

Values Min: 0 / Max: 999999999

registration-ttl—Enter the TTL, in seconds, before a registration becomes invalid. During the initial registration process, after a registration is confirmed, the TTL value set by the Gatekeeper in the RCF message will override this field value. This field is only applicable when the h323-stack: isgateway field is set to enabled.

Default 120

Values Min: 0 / Max: 999999999

terminal-alias—Enter a list of alias addresses that identify the H.323 stack terminal. This field value must be entered as a space-separated type=value string. This field is only applicable when the isgateway field is set to enabled.

ras-port—Select a listening port number for RAS requests. When this field value is 0, H.323 stack uses port assigned by the operating system and not the well-known port 1719.

Default 1719

Values Min: 1025 / Max: 65535

auto-gk-discovery—Enable or disable Automatic Gatekeeper discovery feature upon start-up. This field is applicable only when h323-stack:isgateway field is enabled.

Default disabled

Values enabled | disabled

multicast—Enter the multicast address and port of the RAS Multicast IP Group used for automatic gatekeeper discovery. In order to clear this field, you must enter an empty string by typing a space.

Default 0.0.0.0

gatekeeper—Enter the IP address and RAS port of the Gatekeeper. In order to clear this field, you must enter an empty string.

Default 0.0.0.0

gk-identifier—Enter the gatekeeper identifier with which the H.323 stack registers

alternate-transport—Enter the alternate transport addresses and ports. If this field is left empty, the H.323 stack will not listen for incoming Annex E requests.

q931-port—Enter the Q.931 call signaling port. This is the port for the h323-stack:local-ip address set above.

Default 1720

Values Min: 0 / Max: 999999999

q931-max-calls—Set the maximum number of concurrent, active calls allowed on the Net-Net SBC. If this field value is exceeded, the H.323 stack returns a state of "busy."

Default 200

Values Min: 0 / Max: 999999999

h245-tunneling—Enable or disable H.245 tunneling supported by this H.323 stack

Default disabled

Values enabled | disabled

fs-in-first-msg—Enable or disable Fast Start fields sent in the first message in response to a SETUP message that contains Fast Start fields

Default disabled

Values enabled | disabled

call-start-fast—Enable or disable conversion of an incoming Slow Start call into a Fast Start call. This H.323 stack must be the outgoing stack for conversion to work. If this field is set to disabled, the outgoing call will be setup with the same starting mode as the incoming call. This parameter must take the opposite value as the call-start-slow parameter.

Default enabled

Values enabled | disabled

call-start-slow—Enable or disable conversion of an incoming Fast Start call into a Slow Start call. This H.323 stack must be the outgoing stack for this conversion to work. If this field is set to disabled, the outgoing call will be set up to have the same starting mode as the incoming call. This parameter must take the opposite value as the call-start-fast parameter.

Default disabled

Values enabled | disabled

media-profiles—Enter a list of media profile names used for the logical channels of the outgoing call. These names are configured in the media-profile element. The media-profiles field value must correspond to a valid name field entry in a media-profile element that has already been configured.

prefixes—Enter a list of supported prefixes for this particular H.323 stack

process-registration—Enable or disable registration request processing for this H.323 stack. The Net-Net SBC will process any RRQs that arrive on this H.323 stack if enabled. Net-Net SBC does not acknowledge any requests and drops all RRQs if disabled.

Default disabled

Values enabled | disabled

allow-anonymous—Enter the admission control of anonymous connections accepted and processed by this H.323 stack

Default all

Values
- all
- agents-only
- realm-prefix
- registered
- register-prefix

options—Select optional features or parameters. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <options> [<option>...]

proxy-mode—Select the proxy functionality for signaling only operation

Values H225 | H245

h245-stage—Select the H.245 state at which the Net-Net SBC allows either of the following:

- Transfer of the H.245 address to the remote side of the call
- Acting on the H.245 address sent by the remote side

Default connect

Values
- setup
- proceeding
- alerting
- connect
- early
- facility
- noh245
- dynamic

q931-start-port—Set the starting port number for Q931 port range used for Q.931 call signalling

Default 0 (resets and disables the port range)

Values Min: 2000 / Max: 19999

q931-number-ports—Set the number of ports in Q.931 port range used for the H.323 registration proxy feature

Default 0

Values Min: 0 / Max: 17999

dynamic-start-port—Set the starting port number for Q.931 port range used for the H.323 registration proxy feature

Default 0 (resets and disables the port range)

Values Min: 2000 / Max: 19999

dynamic-number-ports—Enter the number of ports in port range used for dynamic TCP connections in the H.323 registration proxy feature

Default 0

Values Min: 0 / Max: 17999

filename—Enter the name of the configuration file used to override the default configuration. H.323 stack configuration is read from the file specified by this field value. The configuration file does not override manually configured values; the configuration uses the values you have configured plus the information that resides in the file. This file resides in <default-dir>/H323CfgFile, where <defaultdir> is usually /ramdrv.

tcp-keepalive—Enable or disable TCP keepalive processing on the call-signaling port

Default disabled

Values enabled | disabled

alarm-threshold—Access the alarm-threshold subelement.

Path **h323-stack** is a subelement of the **h323-config** configuration element. The full path from the topmost ACLI is: **configure terminal > session-router > h323-config** > **h323-stack**.

Release First appearance: 6.0 / Most recent update: 7.1

RTC Status Supported

h323-stack>alarm-threshold

The **alarm-threshold** subelement allows you to set a threshold for sending an alarm when the Net-Net SBC approaches the **max-calls** limit.

Syntax

```
alarm-threshold <severity | value | select | no | show | done |
exit>
```

Parameters

severity—Enter the level of alarm to be configured per port.

Default minor

Values minor | major | critical

value—Set the percentage of the value defined in the **max-calls** parameter to determine when the Net-Net SBC issues an alarm.

Default 0

Values Min: 0 | Max: 100

Path **alarm-threshold** is a subelement of the **h323-stack** configuration element. The full path from the topmost ACLI is: **configure terminal > session-router > h323-config** > **h323-stack>alarm-threshold**.

Release First appearance: D 7.1.0

RTC Status Supported

host-route

The **host-route** configuration element lets you create and modify host routes on the Net-Net SBC.

Syntax

```
host-route <address | mask | gateway | description | select | no |
show | done | exit>
```

Parameters

address—Enter the address of the host

mask—Enter the network mask for a route

gateway—Enter the gateway address for the host

> *Note: The gateway entered must already be defined as a gateway for an existing network interface.*

description—Provide a brief description of this **host-route** configuration. This is an optional parameter.

Path **host-route** is an element under the system path. The full path from the topmost prompt is: **configure terminal > system > host-route**.

Release First appearance: 5.0

ipsec

The **ipsec** configuration element allows you to configure security policies and security associations on your Net-Net SBC.

Syntax

```
ipsec <security-policy | security-association | exit>
```

Parameters

security-policy—Enter the **security-policy** configuration subelement

manual-security-association—Enter the **manual-security-association** subelement

Path **ipsec** is an element of the **security** path. The full path from the topmost ACLI prompt is: **configure terminal > security > ipsec**.

Release First appearance: 6.0

RTC Status Supported

ipsec>manual-security-association

The **manual-security-association** subelement is where you manually configure a security association on the Net-Net SBC.

Syntax

```
manual-security-association <name | network-interface | direction
| local-ip-addr | remote-ip-addr | in-local-ip-mask | in-remote-
ip-mask | in-vlan-id-mask | local-port | remote-port | trans-
protocol | spi | ipsec-mode | auth-algo | auth-key | encr-algo |
encr-key | aes-ctr-nonce | local-ip-addr | remote-ip-addr |
select | no | show | done | exit>
```

Parameters

name—Enter the name for this security policy

spi—Enter the security parameter index

Default 256

Values Min: 256 / Max: 2302

network-interface—Enter the network interface and VLAN where this security association applies in the form of: **`interface_name:VLAN`**

local-ip-addr—Enter the source IP address to match

Default 0.0.0.0

remote-ip-addr—Enter the destination IP address to match

Default 0.0.0.0

local-port—Enter the source port to match. A value of 0 disables this selector.

Default 0 (disabled)

Values Min: 0 / Max: 65535

remote-port—Enter the destination port to match. A value of 0 disables this selector.

Default 0 (disabled)

Values Min: / Max: 65535

trans-protocol—Enter the transport protocol to match

Default all

Values
- udp
- tcp
- icmp
- all

ipsec-protocol—Select the IPSec protocol you want to use for this security association

Default esp

Values
- esp
- ah

direction—Enter the direction of traffic this security policy can apply to

Default both

Values
- in—This security policy is valid for inbound traffic
- out—This security policy is valid for outbound traffic
- both—This security policy is valid for inbound and outbound traffic

ipsec-mode—Enter the IPSec mode of this SA

Default transport

Values
- tunnel
- transport

auth-algo—Enter the IPSec authentication algorithm for this SA

Default null

Values
- hmac-md5
- hmac-sha1
- null

encr-algo—Enter the IPSec encryption algorithm for this SA

Default null

Values
- des
- 3des
- aes-128-cbc
- aes-256-cbc
- aes-128-ctr
- aes-256-ctr
- null

auth-key—Enter the authentication key for the previously chosen authentication algorithm for this SA

encr-key—Enter the encryption key for the previously chosen encryption algorithm for this SA

aes-ctr-nonce—Enter the AES nonce. This parameter applies only when your encryption algorithm is either aes-128-ctr or aes-256-ctr.

Default 0

tunnel-mode—Enter the **tunnel-mode** subelement

Path

manual-security-association is a subelement under the **ipsec** element. The full path from the topmost ACLI prompt is: **configure terminal > security > ipsec > manual-security-association**.

Release

First appearance: 6.0

RTC Status

Supported

ipsec>manual-security-association>tunnel-mode

This configuration element allows you to configure the addresses in the security association. These addresses represent the external, public addresses of the termination points for the IPSEC tunnel.

Syntax

```
tunnel-mode <local-ip-addr | remote-ip-addr | select | no | show | done | exit>
```

local-ip-addr—Enter the local IP address for this security association

Default 0.0.0.0

remote-ip-addr—Enter the remote IP address for this security association

Default 0.0.0.0

Path

tunnel-mode is a subelement under the **ipsec>manual-security-association** subelement. The full path from the topmost ACLI prompt is: **configure terminal > security > ipsec > manual-security-association > tunnel-mode.**

Release

First appearance: 6.0

RTC Status

Supported

ipsec>security-policy

The **security-policy** configuration element allows you to configure IPSec security policies on your Net-Net SBC.

Syntax

```
security-policy <name | network-interface | priority | action | direction | local-ip-addr-match | remote-ip-addr-match | local-port-match | remote-port-match | trans-protocol-match | local-ip-mask | remote-ip-mask | outbound-sa-fine-grained-mask | select | no | show | done | exit>
```

Parameters

name—Enter the name for this security policy

priority—Set the priority number of this security policy

Default 0

Values Min: 0 / Max: 254

network-interface—Enter the network interface and VLAN where this security policy applies in the form: **`interface_name:VLAN`**

local-ip-addr-match—Enter the local IP address to match traffic selectors for this security policy

Default 0.0.0.0

remote-ip-addr-match—Enter the remote IP address to match traffic selectors for this security policy

Default 0.0.0.0

local-ip-mask—Enter the local IP address mask in dotted-decimal notation

Default 255.255.255.255

remote-ip-mask—Enter the remote IP address mask in dotted-decimal notation

Default 255.255.255.255

local-port-match—Enter the local port to match traffic selectors for this security policy

Default 0

Values Min: 0 / Max: 65535

remote-port-match—Enter the remote port to match traffic selectors for this security policy

Default 0

Values Min: 0 / Max: 65535

trans-protocol-match—Enter the transport protocol to match

Default all

Values
- udp
- tcp
- icmp
- all

direction—Set the direction of traffic this security policy can apply to

Default both

Values
- in
- out
- both

action—Enter the action the Net-Net SBC should take when this policy matches outbound IPSec traffic.

Default ipsec

Values
- ipsec—Continue processing as IPSec traffic
- allow—Forward the traffic without any security processing
- discard—Discard the traffic

outbound-sa-fine-grained-mask—Enter the **outbound-sa-fine-grained-mask** subelement

Path **security-policy** is a subelement under the **ipsec** element. The full path from the topmost ACLI prompt is: **configure terminal > security > ipsec > security-policy**.

Release First appearance: 6.0

RTC Status Supported

ipsec>security-policy>outbound-sa-fine-grained-mask

This configuration element allows you to configure a fine grained security policy.

Syntax

```
outbound-sa-fine-grained-mask <local-ip-mask | remote-ip-mask |
local-port-mask| remote-port-mask| vlan-id-mask | trans-protocol-
mask | select | no | show | done | exit>
```

Parameters

local-ip-mask—Enter the fine-grained source IP address mask to apply to outbound IP packets for SA matching. Values must be entered in dotted-decimal notation.

Default 255.255.255.255

remote-ip-mask—Enter the fine-grained destination IP address mask to apply to outbound IP packets for SA matching. Values must be entered in dotted-decimal notation.

Default 255.255.255.255

local-port-mask—Enter the local port mask for this security policy

Default 0

Values Min: 0 / Max: 65535

remote-port-mask—Enter the remote port mask for this security policy

Default 0

Values Min: 0 / Max: 65535

vlan-id-mask—Enter the VLAN ID mask

Default 0x000

Values 0x000 (disabled) - 0xFFF

trans-protocol-mask—Enter the transport protocol mask for this security policy

Default 0

Values Min: 0 / Max: 255

Path

outbound-sa-fine-grained-mask is a subelement under the **ipsec>security-policy** subelement. The full path from the topmost ACLI prompt is: **configure terminal > security > ipsec > security-policy > outbound-sa-fine-grained-mask**.

Release

First appearance: 6.0

RTC Status

Supported

iwf-config

The **iwf-config** element enables the H.323—SIP interworking (IWF) and provides a list of media profiles to use when IWF translations occur.

Syntax

```
iwf-config <state | add-reason-hdr | no-sdp-in-invite | media-
profiles | select | no | show | done | exit>
```

Parameters

state—Enable or disable the Net-Net SBC's IWF functionality

Default disabled

Values enabled | disabled

add-reason-hdr—Enable or disable adding the Reason header to IWF calls

Default disabled

Values enabled | disabled

slow-start-no-sdp-in-invite—Enable or disable sending an SDP offer in the SIP INVITE for an IWF call originating in H.323 slow start

Default disabled

Values enabled | disabled

media-profiles—Set the default media SDP profiles that the Net-Net SBC uses for Slow Start IWF calls. This field does not have a relationship with the media-profiles found in the h323-stack configuration subelement, as the values configured there affect calls that take place entirely in H.323. This list must be populated with SDP codec names.

Values

- PCMU
- PCMA
- G722
- G723
- G726-32
- G728
- G729
- H261
- H263

Path

iwf-config is an element under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > iwf-config**.

Release

First appearance: 6.0

RTC Status

Supported

Notes

This is a single instance configuration element.

license

The **license** configuration element is used for adding feature licenses.

Syntax

```
license <add | no | show | exit>
```

Parameters

add—Add a license by entering a key obtained from Acme Packet support

no—Delete a license. You are prompted to choose which license for deletion.

Path

license is an element under the system-config path. The full path from the topmost ACLI prompt is: **configure terminal > system > license**.

Release

First appearance: 5.0

local-policy

The **local-policy** configuration element determines where session signaling messages are routed and/or forwarded.

Syntax

```
local-policy <from-address | to-address | source-realm |
activate-time | deactivate-time | state | policy-priority |
description | policy-attributes | select | no | show | done |
exit>
```

Parameters

from-address—Enter the source IP address for the local-policy element. At least one address must be set within this list, but it can include as many addresses as necessary. Addresses can take the following forms:

- `+<number>`—Indicates an E164 address
- `<number>`—Indicates a default session router address type
- `[<host>.]<domain>`—Indicates a host or domain address

Excluding keywords **`add`** and **`delete`** when a list is already configured replaces the entire list.

Values [add | delete] <address> [<address>...]

to-address—Enter the destination IP address for the local-policy element. At least one address must be set within this list, but it can include as many addresses as necessary. Addresses can take the following forms:

- `+<number>`—Indicates an E164 address
- `<number>`—Indicates a default session router address type
- `[<host>.]<domain>`—Indicates a host or domain address

Excluding keywords **`add`** and **`delete`** when a list is already configured replaces the entire list.

Values [add | delete] <address> [<address>...]

source-realm—Enter the realms used to determine how to route traffic. This list identifies incoming traffic on a realm and is used for routing by ingress realm via the

local policy element. Source-realm entries must be a valid realm. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Default *

Values [add | delete] <name> [<name>...]

activate-time—Enter the time when selected local-policy becomes valid

```
activate-time yyyy-mm-dd hh:mm:ss.zzz
```

y=year; m=month; d=day h=hour (24-hour clock) m=minute; s=second; z=millisecond

deactivate-time—Enter the time when selected local-policy becomes invalid

```
deactivate-time yyyy-mm-dd hh:mm:ss.zzz
```

y=year; m=month; d=day h=hour (24-hour clock) m=minute; s=second; z=millisecond

state—Enable or disable the local-policy element

Default enabled

Values enabled | disabled

policy-priority—Set the priority for this local policy

Default none

Values
- none
- normal
- non-urgent
- urgent
- emergency

description—Provide a brief description of this **local-policy** configuration. This is an optional parameter.

policy-attributes—Access the policy-attributes subelement

Path **local-policy** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > local-policy**.

Release First appearance: 5.0

Notes This is a multiple instance configuration element.

local-policy > policy-attributes

The **policy-attributes** subelement in conjunction with local-policy make routing decisions for the session based on the next-hop field value.

Syntax

```
local-policy <from-address | to-address | source-realm |
activate-time | deactivate-time | state | policy-priority |
description | policy-attributes | lookup | next-key | select | no
| show | done | exit>
```

Parameters

next-hop—Enter the next signaling host IP address or FQDN. This parameter must correspond to a valid hostname value in a configured session agent or to a valid group-name value in a configured session agent group. You can use the following as next-hops:

- IPv4 address or IPv6 address of a specific endpoint
- Hostname or IPv4 address or IPv6 address of a configured session agent
- Group name of a configured session agent group

The group name of a configured session agent group must be prefixed with SAG:

For example:

- policy-attribute: next-hop SAG:appserver
- policy-attribute: next-hop lrt:routetable
- policy-attribute: next-hop enum:lerg

realm—Enter the egress realm, or the realm of the next hop. If traffic is routed using the local policy, and the selected route entry identifies an egress realm, then this realm field value will take precedence. This value must be a valid entry in a realm configuration.

action—Set to redirect if you want to send a REDIRECT message back to the calling party with the resolved next hop in the Contact.

Default none

Values
- None—No specific action requested
- Replace-uri—To replace the Request-URI with the next hop
- Redirect—To send a 305 redirect response with this next hop as contact

terminate-recursion—Enable or disable the termination of route recursion with this next hop

Default disabled

Values enabled | disabled

carrier—Enter the carrier for this local-policy. Carrier names are arbitrary names used to affect the routing of SIP signaling messages based on their being specified in the local-policy, session-agent, and the sip-config. These carrier names are global in scope, especially if they are exchanged in TRIP.

start-time—Enter the time of day these policy attributes are considered for preference determination

Default 0000

Values Min: 0000 / Max: 2400

end-time—Enter the time of day these policy attributes cease to be considered for preference determination.

Default 2400

Values Min: 0000 / Max: 2400

days-of-week—Enter the combination of days of the week plus holidays that policy attributes can be considered for preference determination. A holiday entry coincides with a configured holiday. At least one day or holiday must be specified in this field.

Default U-S

Values
- U—Sunday
- M—Monday
- T—Tuesday
- W—Wednesday
- R—Thursday
- F—Friday
- S—Saturday
- H—Holiday

cost—Enter the cost configured for local policy to rank policy attributes. This field represents the cost of a route relative to other routes reaching the same destination address.

Default 0

Values Min: 0 / Max: 999999999

state—Enable or disable consideration of these policy attributes as part of the local-policy element

Default enabled

Values enabled | disabled

app-protocol—Select the signaling protocol used when sending messages to the configured next-hop. When the Net-Net SBC receives an ingress signaling message and uses local policy to determine the message's destination, it will interwork the signaling between protocols if the signaling type does not match the value configured in the app-protocol field.

Values SIP | H.323 | NONE

media-profiles—Enter the names of media-profile elements related to the policy attribute. Media profiles define a set of media formats that the Net-Net SBC can recognize in SDP. This list does not have to be configured. However, if this list is configured, there can be as many entries within it as necessary. Excluding keywords **`add`** and **`delete`** when a list is already configured replaces the entire list.

[add | delete] <name> [<name>...]

Values
- PCMU
- PCMA
- G722
- G723
- G726-32

- G728
- G729
- H261
- H263

methods—Enter the SIP methods you want to use for matching this set of policy attributes. When this parameter is left empty (the default behavior), SIP methods will not be taken into consideration for routing based on this set of policy attributes.

lookup—Enable multistage local policy routing, or leave the parameter at the default **single** for single stage local policy routing.

Default single

Values single | multi

next-key—Select the key to use for the next stage of local policy look-up.

Default None

Values $TO | $FROM | $PAI

Path

policy-attributes is a subelement under the local-policy element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > local-policy > policy-attributes**.

Release

First appearance: 5.0 / Most recent update: 7.1

Notes

You must select a local-policy element to which you want to add policy attributes before you enter those elements. If you do not select a local-policy element prior to entering configurations for the policy attributes, your information will be lost. This is a multiple instance configuration element.

local-routing-config

The **local-routing-config** element allows you to configure the name for the local route table, the filename you want to give the database corresponding to this table, and the prefix length to be used for lookup.

Note: Entering XML comments on the same line as LRT XML data is not currently supported.

Syntax

```
local-routing-config <name | file-name | prefix-length | select |
no | show | done | exit>
```

Parameters

name—Enter the name (a unique identifier) for the local route table; this name is used for reference in the local policy attributes when to specify that local routing should be used

file-name—Enter the name for the file from which the database corresponding to this local route table will be created. You should use the `.gz` format, and the file should be placed in the `/code/lrt/` directory.

prefix-length—Enter the number of significant digits/bits to used for lookup and cache storage

Default 0

Values Min: 0 / Max: 999999999

Path **local-routing-config** is an element under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > local-routing-config**.

Release First appearance: D7.0

Notes This is a multiple instance configuration element.

media-manager-config

This **media-manager-config** element defines parameters used in the media steering functions performed by the Net-Net SBC including the flow timers.

Syntax

```
media-manager <state | latching | flow-time-limit | initial-
guard-timer | subsq-guard-timer | tcp-flow-time-limit | tcp-
initial-guard-timer | tcp-subsq-guard-timer | tcp-number-of-
ports-per-flow | hnt-rtcp | max-signaling-bandwidth | max-
untrusted-signaling | min-untrusted-signaling | options |
tolerance-window | rtcp-rate-limit | anonymous-sdp | arp-msg-
bandwidth | rfc2833-timestamp | default-2833-duration | rfc2833-
end-pkts-only-for-non-sig | translate-non-rfc2833-event |
translate-non-inband-event | max-trusted-allocation | deny-
allocation | dnsalg-server-failover | select | no | show | done |
exit>
```

Parameters

state—Enable or disable the media management functionality

Default enabled

Values enabled | disabled

latching—Enable or disable the Net-Net SBC obtaining the source of the first packet received for a dynamic flow. This parameter is only applicable to dynamic flows. If packet source is unresolved, but Net-Net SBC expects a packet, it will use newly arrived packet's source address if latching is enabled. All subsequent packets for the dynamic flow must come from the "latched" source address; otherwise, the packets are dropped.

Default enabled

Values enabled | disabled

flow-time-limit—Enter the total time limit in seconds for the flow. The Net-Net SBC notifies the signaling application when this time limit is exceeded. This field is only applicable to dynamic flows. A value of 0 seconds disables this function and allows the flow to continue indefinitely.

Default 86400

Values Min: 0 / Max: 999999999

initial-guard-timer—Enter the time in seconds allowed to elapse before the first packet of a flow arrives. If the first packet does not arrive within this time limit, the Net-Net SBC notifies the signaling application. This field is only applicable to dynamic flows. A value of 0 seconds indicates that no flow guard processing is required for the flow and disables this function.

Default 300

Values Min: 0 / Max: 999999999

subsq-guard-timer—Enter the maximum time in seconds allowed to elapse between packets in a flow. The Net-Net SBC notifies the signaling application if this timer is exceeded. This field is only applicable to dynamic flows. A field value of zero seconds means that no flow guard processing is required for the flow and disables this function.

Default 300

Values Min: 0 / Max: 999999999

tcp-flow-time-limit—Enter the maximum time in seconds that a media-over-TCP flow can last

Default 86400

Values Min: 0 / Max: 999999999

tcp-initial-guard-timer—Enter the maximum time in seconds allowed to elapse between the initial SYN packet and the next packet in a media-over-TCP flow

Default 300

Values Min: 0 / Max: 999999999

tcp-subsq-guard-timer—Enter the maximum time in seconds allowed to elapse between all subsequent sequential media-over-TCP packets

Default 300

Values Min: 0 / Max: 999999999

tcp-number-of-ports-per-flow—Enter the number of ports, inclusive of the server port, to use for media over TCP. The total number of supported flows is this value minus one.

Default 2

Values Min: 0 / Max: 999999999

hnt-rtcp—Enable or disable the support of RTCP when the Net-Net SBC performs HNT. If disabled, the Net-Net SBC will only do RTP for endpoints behind a NAT. If enabled, the Net-Net SBC will add a separate CAM entry for the RTCP flow so that it can send the RTCP back to the endpoint behind the NAT.

Default disabled

Values enabled | disabled

max-signaling-bandwidth—Enter the maximum signaling bandwidth allowed to the host-path in bytes per second

Default 10000000

Values Min: 71000; Max: 10000000

max-untrusted-signaling—Set the percentage of signaling bandwidth that can be used by untrusted hosts

Default 100

Values Min: 1 / Max: 100

min-untrusted-signaling—Set the percentage of signaling bandwidth guaranteed for untrusted hosts

Default 30

Values Min: 1 / Max: 100

tolerance-window—Enter the tolerance window size in seconds used to measure host access limits

Default 30

Values Min: 0 / Max: 999999999

rtcp-rate-limit—Enter the maximum speed in bytes per second for RTCP traffic

Default 0

Values Min: 0 / Max: 125000000

anonymous-sdp—Enable or disable anonymous username and session name fields in SDP

Default disabled

Values enabled | disabled

arp-msg-bandwidth—Enter the maximum ARP packet rate in bytes per second

Default 32000

Values Min: 2000 / Max: 200000

fragment-msg-bandwidth—Maximum bandwidth for fragmented IP packet queue. A value of 0 disables the unique fragmented IP packet queue and forces the Net-Net SBC to share media policing between fragmented and untrusted packets.

Default 0

Values 0 or Min: 32000 / Max: 10000000

rfc2833-timestamp—Enable or disable use of a timestamp value calculated using the actual time elapsed since the last RTP packet for H.245 to 2833 DTMF interworking

Default disabled

Values enabled | disabled

default-2833-duration—Enter the time in milliseconds for the Net-Net SBC to use when receiving an alphanumeric UII or SIP INFO with no specified duration.

Values Min: 50 / Max: 5000

rfc2833-end-pkts-only-for-non-sig—Enable this parameter if you want only the last three end 2833 packets used for non-signaled digit events. Disable this parameter if you want the entire start-interim-end RFC 2833 packet sequence for non-signaled digit events

Default enabled

Values enabled | disabled

translate-non-rfc2833-event—Enable or disable the Net-Net SBC's ability to translate non-rfc2833 events

Default disabled

Values enabled | disabled

translate-non-inband-event—Enable or disable the translation of UII/INFO Events into inband if possible

Default disabled

Values enabled | disabled

max-trusted-allocation—Enter the maximum number of trusted entries the CAM can hold

Default 120000

Values Min: 0 / Max: 180000 (16000 for 64K CAM)

deny-allocation—Enter the maximum number of denied entries the CAM can hold

Default 32000

Values Min: 0 / Max: 32000 (14000 for 64K CAM)

dnsalg-server-failover—Enable DNS queries to be sent to the next configured server - even when contacting the Net-Net SBC's DNS ALG on a single IP address.

Default disabled

Values enabled | disabled

Notes The Net-Net SBC uses the transation timout value set in the **dns-server-attributes** configuration (part of the **dns-config**).

Path **media-manager-config** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > media-manager**.

Release First appearance: 5.0 / Most recent update: 7.1

Notes This is a single instance configuration element.

media-policy

The **media-policy** element sets the TOS/DiffServ values that define an individual type or class of service.

Syntax

```
media-policy <name | tos-settings | tos-values | select | no |
show | done | exit>
```

Parameters

name—Enter the name of this media policy.

tos-settings—Access the tos-settings subelement.

tos-values—Enter a list of TOS values for media types for this media policy providing a "policing" profile. This configuration parameter is entered in the format <media-type>:<tos-value> where

Values
- <media-type>—audio | video | h225 | h245 | sip
- <tos-value>—decimal or hexadecimal number that indicates the numerical value for the TOS required

Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <media-type>:<tos-value> [...]

Path

media-policy is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > media-policy**.

Release

First appearance: 5.0 / Most recent update: 7.1

Notes

This configuration element sets the Packet Marking for Media features and defines an individual type or class of service for the Net-Net SBC. Media policies can be chosen on a per-realm basis.
This is a multiple instance configuration element.

media-policy > tos-settings

The **tos-settings** configuration subelement bases media classification on type and subtype to create any media type combination allowed by IANA standards.

Syntax

```
tos-settings < media-type | media-sub-type | media-attributes |
tos-values | select | no | show | done | exit>
```

Parameters

media-type—Enter the type of media to use for this set of TOS settings.

Default None

Values Any IANA-defined media type, such as: audio, image, model

media-sub-type—Enter the media sub-type to use for the specified media type.

Default None

Values Any of the media sub-types IANA defines for the selected media type

media-attributes—Enter a list of one or more media attributes that will match in the SDP.

Default None

tos-value—Enter the TOS value to apply to matching traffic

Default None (must be a decimal or hexidecimal value)

Values Range from 0x00 to 0xFF

Path **tos-settings** is a subelement under the media-policy element. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > media-policy>tos-settings**.

Release First appearance: 7.1

RTC Status Supported

Notes This configuration element sets the Packet Marking for Media features and defines an individual type or class of service for the Net-Net SBC. Media policies can be chosen on a per-realm basis.
This is a multiple instance configuration element.

media-profile

The **media-profile** configuration element defines a set of media formats that the Net-Net SBC can recognize in SDP. SDP describes various media parameters that might be received, and the media description indicates the transport protocol and payload type.

Syntax

```
media-profile <name | subname | media-type | payload-type |
transport | req-bandwidth | frames-per-packet | parameters |
average-rate-limit | peak-rate-limit | max-burst-size | sdp-rate-
limit-headroom | sdp-bandwidth | select | no | show | done | exit>
```

Parameters

name—Enter the encoding name used in the SDP rtpmap attribute. This is a required field.

subname—Enter a description for the use of this subname. Subnames must be unique per name.

media-type—Select the type of media used in SDP m lines

Default audio

audio | video | application | data

payload-type—Select the format in SDP m lines. No payload type number is assigned for newer, dynamic codecs. For RTP/AVP media-profile elements, this field should only be configured when there is a standard payload type number that corresponds to the encoding name. Otherwise, this field should be left blank. This field is used by the system to determine the encoding type when the SDP included with a session identifies the standard payload type on the m line, but does not include an a-rtpmap entry.

transport—Select the type of transport protocol used in the SDP rtpmap attribute

Default RTP/AVP

Values UDP | RTP/AVP

req-bandwidth—Enter the total bandwidth in kilobits that the media requires

Default 0

Values Min: 1/ Max: 999999999

frames-per-packet—Enter the number of frames per RTP packet. A value of 0 means that this field is not being used.

Default 0

Values Min: 0 / Max: 256

parameters—Enter any additional information for codecs. This is an optional parameter.

average-rate-limit—Enter the maximum speed in bytes per second for a flow that this media profile applies to

Default 0

Values Min: 0 / Max: 125000000

peak-rate-limit—Enter the flowspec parameter r (bucket rate) / p (peak rate) value to insert into COPS message for RACF/PDP configuration

Values Min: 0 / Max: 125000000

max-burst-size—Enter the flowspec parameter b (bucket depth) / m (minimum policed unit) / M (maximum datagram size) value to insert into COPS message for RACF/PDP configuration

Values Min: 0 / Max: 125000000

sdp-rate-limit-headroom—Specify the percentage of headroom to be added while using the AS bandwidth parameter while calculating the `average-rate-limit` (rate limit for the RTP flow)

Default 0

Values Min: 0 / Max: 100

sdp-bandwidth—Enable or disable the use of the AS modifier in the SDP if the `req-bandwidth` and `sdp-rate-limit-headroom` parameters are not set to valid values in the corresponding media profile

Default disabled

Values enabled | disabled

Path

media-profile is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > media-profile**.

Release

First appearance: 5.0

Notes

This element supports new SDP formats when they are defined. This element is used to associate bandwidth requirements with SDP requirements from information passed during the establishment of sessions. The names established in the media-profile elements are used to populate the corresponding fields in other elements.
This is a multiple instance configuration element.

5 Configuration Elements N-Z

net-management-control

The **net-management-control** configuration element allows you to control multimedia traffic, specifically for static call gapping and 911 exception handling. These controls limit the volume or rate of traffic for a specific set of dialed numbers or dialed number prefixes.

Syntax

```
net-management-control <name | state | destination-identifier |
type | value | treatment | next-hop | realm-next-hop | protocol-
next-hop | status-code | cause-code | gap-rate-max-count | rph-
feature | rph-profile | rph-policy | gap-rate-window-size |
select | no | show | done | exit>
```

Parameters

name—Enter the name of this network management control rule

state—Enable or disable this network management control rule

Default enabled

Values enabled | disabled

destination-identifier—Enter the classification key. This parameter specifies information about the destination, which can be an IP address, an FQDN, and destination (called) number, or destination prefix. You can wildcard characters in the classification key using the carat symbol (^).

This parameter can accommodate a list of entries so that, if necessary, you can specify multiple classification keys. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<address>...]

type—Enter the control type you want to use

Values
- gap-rate
- gap-percent
- priority

value—Enter the control value of the network management control. This parameter applies only when you set the control type to either **gap-rate** or **gap-percent**.

Default 0

Values
- gap-rate: 0-2147483647
- gap-percentage: 0-100

treatment—Enter the treatment method you want to use or leave this parameter set to none.

Default none

Values reject | divert

next-hop—Enter the next hop for the Net-Net SBC to use when the treatment method is **divert**.

Values
- hostname (:port)
- IP address (:port)
- Name of a valid, configured session agent
- Name of a valid, configured session agent group. When you set this parameter to a session agent group, you must specify that it is a session agent group by prepending the name of the group with either **SAG:** or **sag:**. For example, the entry for a session agent group with **Group2** as its name would be **SAG:Group2** or **sag:Group2**.

realm-next-hop—Enter the realm identifier to designate the realm of the next hop when the treatment type is **divert**.

protocol-next-hop—Enter the signaling protocol for the next hop when the treatment type is **divert**.

status-code—Enter the SIP response code that you want the Net-Net SBC to use when the treatment method is **reject**

Default 503

Values Min: 1 / Max: 699

cause-code—Enter the Q.850 cause code that you want the Net-Net SBC to use when the treatment method is **reject**

Default 63

Values Min: 1 / Max: 2147483647

gap-rate-max-count—Enter the maximum token counter value for gapping rate

Default 0

Values Min: 0 / Max: 2147483647

rph-feature—Enable or disable the NSEP feature for this NMC rule.

Default disabled

Values enabled | disabled

rph-profile—Enter the name of the RPH profile that you want to apply for this NMC rule. This parameter is empty by default; if you do not set an RPH profile, none will be applied.

rph-policy—Enter the name of the RPH policy that you want to apply for this NMC rule. This parameter is empty by default; if you do not set an RPH policy, none will be applied.

gap-rate-window-size—Enter the window size in seconds for gapping rate calculation

Default 0

Values Min: 1 / Max: 2147483647

Path

net-management-control is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure-terminal > session-router > net-management-control**.

Release

First appearance: 5.1

network-interface

The **network-interface** element creates and configures a logical network interface.

Syntax

```
network-interface <name | description | sub-port-id | hostname |
ip-address | netmask | gateway | sec-gateway | gw-heartbeat | dns-
ip-primary | dns-ip-backup1 | dns-ip-backup2 | dns-domain | dns-
timeout | hip-ip-list | ftp | icmp | snmp | telnet | select | no |
show | done | exit>
```

Parameters

name—Enter the name of the physical interface with which this network-interface element is linked

description—Enter a description for this network interface. Surround the description by quotation marks if it contains any spaces between words.

sub-port-id—Enter the identification of a specific virtual interface in a physical interface (e.g., a VLAN tag). A value of 0 indicates that this element is not using a virtual interface. The sub-port-id field value is only required if the operation type is Media.

Default 0

Values Min: 0 / Max: 4096

hostname—Enter the hostname of this network interface. This is an optional entry that must follow FQDN Format or IP Address Format.

ip-address—Enter the IP address of this network interface. This is a required entry that must follow the IP Address Format.

netmask—Enter the netmask portion of the IP address for this network interface entered in IP address format. The network-interface element will not function properly unless this field value is valid.

gateway—Enter the gateway this network interface uses to forward packets. Entries in this field must follow the IP Address Format. No packets outside of the subnet are forwarded if this value is 0.0.0.0.

sec-gateway—Enter the secondary gateway address for the interface

gw-heartbeat—Access the gateway-heartbeat subelement

dns-ip-primary—Enter the IP address of the primary DNS to be used for this interface

dns-ip-backup1—Enter the IP address of the first backup DNS to be used for this interface

dns-ip-backup2—Enter the IP address of the second backup DNS to be used for this interface

dns-domain—Enter the default domain name used to populate incomplete hostnames that do not include a domain. Entries must follow the Name Format.

dns-timeout—Enter the maximum waiting time for a DNS response in seconds

Default 11

Values Min: 0 / Max: 65535

hip-ip-list—Enter the host in Path IP address of the Net-Net SBC, used to specify the IP address that the SD will use to respond to management requests for this interface

ftp—Enable or disable FTP on this interface

Default disabled

Values enabled | disabled

icmp—Enable or disable ICMP on this interface

Default disabled

Values enabled | disabled

snmp—Enable or disable SNMP on this interface

Default disabled

Values enabled | disabled

telnet—Enable or disable telnet on this interface

Default disabled

Values enabled | disabled

Path **network-interface** is an element under the system element. The full path from the topmost ACLI prompt is: **configure terminal > system > network-interface**.

Release First appearance: 5.0

Notes This is a multiple instance configuration subelement.

network-interface > gw-heartbeat

The **gw-heartbeat** subelement supports the front interface link failure detection and polling feature.

Syntax

```
gw-heartbeat <state | heartbeat | retry-count | retry-timeout |
health-score | select | no | show | done | exit>
```

Parameters

state—Enable or disable front interface link detection and polling functionality on the Net-Net SBC for this network-interface element

Default enabled

Values enabled | disabled

heartbeat—Enter the time interval in seconds between heartbeats for the front interface gateway

Default 0

Values Min: 0 / Max: 65535

retry-count—Enter the number of front interface gateway heartbeat retries before a gateway is considered unreachable

Default 0

Values Min: 0 / Max: 65535

retry-timeout—Enter the heartbeat retry timeout value in seconds

Default 1

Values Min: 0 / Max: 65535

health-score—Enter the amount to subtract from the health score if the front interface gateway heartbeat fails (i.e., expires). The health score will be decremented by the amount set in this field if the timeout value set in the gw-heartbeat: retry-timeout field is exceeded without the front interface gateway sending a response.

Default 0

Values Min: 0 / Max: 100

Path

gw-heartbeat is a subelement of the network-interface element. The full path from the topmost ACLI prompt is: **configure terminal > system > network-interface > gw-heartbeat**.

Release

First appearance: 5.0

Notes

The values configured in the fields of a gw-heartbeat subelement apply to the Net-Net SBC on a per-network-interface basis, and can override the values configured in the redundancy element's corresponding front interface link detection and polling fields.

This is a single instance configuration subelement.

network-parameters

The **network-parameters** element enables and configures the TCP keepalive feature used for keeping H.323 connections open.

Syntax

```
network-parameters <tcp-keepalive-count | tcp-keepinit-timer |
tcp-keepalive-idle-timer | tcp-keepalive-interval-timer | tcp-
keepalive-mode | options | select | no | show | done | exit>
```

tcp-keepalive-count—Enter the number of outstanding keepalives before the connection is torn down

Default 4

Values Min: 1 / Max: 999999

tcp-keepinit-timer—Enter the TCP connection timeout period if a TCP connection cannot be established.

Default 75

Values Min: 1 / Max: 999999

tcp-keepalive-idle-timer—Enter the idle time in seconds before triggering keepalive processing.

Default 400

Values Min: 30 / Max: 7200

tcp-keepalive-interval-timer—Enter the TCP retransmission time if a TCP connection probe has been idle for some amount of time

Default 75

Values Min: 15 / Max: 75

tcp-keepalive-mode—Enter the TCP keepalive mode

Default 0

Values
- 0—The sequence number is sent un-incremented
- 1—The sequence number is sent incremented
- 2—No packets are sent

options—Select optional features or parameters. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <options> [<option>...]

Path **network-parameters** is an element under the **system** path. The full path from the topmost ACLI prompt is: **configure terminal > system > network-parameters**.

Release First appearance: D6.0.1

ntp

The **ntp-sync** element sets the ntp-server IP address for correct and accurate time synchronization.

Syntax

```
ntp-sync <server | select | no | show | done | exit>
```

Parameters

server—Enter a list of IP addresses of the NTP server. Entries must follow the IP Address Format. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <address> [<address>...]

Path **ntp** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > ntp**.

Release First appearance: 5.0

Notes In order for any changes to the NTP synchronization functionality to take effect, a **save-config** must be performed followed by a system reboot.

password-policy

The **password-policy** configuration element allows you to configure the minimum acceptable length for a password.

Syntax

```
password-policy <min-secure-pwd-len | select | no | show | done | exit>
```

Parameters

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.

Default 8

Values Min: 8 / Max: 64

Path

password-policy is an element of the security path. The full path from the topmost ACLI prompt is: **configure-terminal > security > password-policy**.

Release

First appearance: 5.1

phy-interface

The **phy-interface** element is used to configure physical interfaces.

Syntax

```
phy-interface <name | operation-type | port | slot | admin-state | auto-negotiation | duplex-mode | speed | wancom-health-score | select | no | show | done | exit>
```

Parameters

name—Enter the name for this physical interface. Physical interfaces with an operation-type of Control or Maintenance must begin with "wancom." This is a required field. Entries in this field must follow the Name Format and must be unique.

operation-type—Select the type of physical interface connection

Values Media—NIU interfaces only. Port: 0-3 Slot: 0 or 1

port—Enter the physical port number on an interface of the phy-interface being configured

Default 0

Values Min: 0 / Max: 7

slot—Enter the physical slot number on the Net-Net SBC chassis

Default 0

Values Min: 0 / Max: 1

admin-state—Enable or disable the Net-Net SBC allowing incoming and outgoing traffic to be processed on this interface

Values enabled | disabled

auto-negotiation—Enable or disable auto negotiation on the interfaces taking place before either end begins sending packets over the Ethernet link. The value configured in this field does not change the Net-Net SBC status at runtime.

Values enabled | disabled

duplex-mode—Set whether the 10/100 Phy card interfaces located on the front panel of Net-Net SBC operate in full-duplex mode or half-duplex mode

Values full | half

speed—Set the speed in Mbps of the front-panel 10/100 Phy interfaces. This field is only used if the auto-negotiation field is set to disabled for 10/100 Phy cards.

Values 10 | 100 | 1000

wancom-health-score—Enter the amount to subtract from the Net-Net SBC's health score if a rear interface link goes down

Default 50

Values Min: 0 / Max: 100

Path **phy-interface** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > phy-interface**.

Release First appearance: 5.0

Notes Certain fields are visible based on the setting of the operation-type parameter. This is a multiple instance configuration subelement.

public-key

To generate an SSH key pair you must initially configure a public key record which serves as a container for the generated key pair.

Syntax `public-key <name | type | size | select | no | show | done | exit>`

Parameters

name—Enter the name of the public key

type—Select the type of key you want to create

Default rsa

Values rsa | dsa

size—Enter the size of the key you are creating

Default 1024

Values 512 | 1024 | 2048

Path **public-key** is an element under the **security** path. The full path from the topmost ACLI prompt is: **configure terminal > security > public-key**.

Release First appearance: D7.0

RTC Status Supported

q850-sip-map

The **q850-sip-map** configuration element is used to map q850 cause codes to SIP response codes.

Syntax

```
q850-sip-map <entries | select | no | show | done | exit>
```

entries—Enter the **entries** configuration subelement

Path

q850-sip-map is an element under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > q850-sip-map**.

Release

First appearance: D6.0.1

q850-sip-map>entries

The **entries** subelement is used to create the mapping of q850 cause to SIP reason code.

Syntax

```
entries <q850-cause | sip-status | sip-reason | select | no | show
| done | exit>
```

q850-cause—Enter the q850 cause code to map to a SIP reason code

sip-status—Enter the SIP response code that maps to this p850 cause code

Values Min: 100 / Max: 870

sip-reason—Describe the mapped SIP response code

Path

entries is a subelement under the **q850-sip-map** element, under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > q850-sip-map > entries**.

Release

First appearance: D6.0.1

realm-config

The **realm-config** element is used to configure realms.

Syntax

```
realm-config <identifier | description | addr-prefix | network-
interfaces | additional-prefixes | mm-in-realm | mm-in-network |
mm-in-system | mm-same-ip | msm-release | symmetric-latching |
qos-enable | max-bandwidth | fallback-bandwidth | max-latency |
max-jitter | max-packet-loss | observ-window-size | parent-realm
| dns-realm | media-policy | class-profile | in-translationid |
out-translationid | average-rate-limit | access-control-trust-
level | invalid-signal-threshold | maximum-signal-threshold |
untrusted-signal-threshold | nat-trust-threshold | deny-period |
ext-policy-server | monthly-minutes | options | transcoding-
policy | transcode-in-realm | trunk-context | transcode-in-
network | in-manipulationid | out-manipulationid | restricted-
```

```
latching | restriction-mask | early-media-allow | accounting-
enable | user-cac-bandwidth | user-cac-sessions | user-cac-mode |
enforcement-profile | net-management-control | delay-media-update
| manipulation-string | icmp-detect-multiplier | icmp-
advertisement-interval | icmp-target-ip | session-constraints |
stun-enable | stun-server-ip | stun-server-port | stun-changed-ip
| stun-changed-port | sip-profile | sip-isup-profile |
manipulation-pattern | bw-cac-non-mm | select | no | show | done |
exit>
```

Parameters

identifier—Enter the name of the realm associated with this Net-Net SBC. This is a required field and the identifier field value must be unique.

description—Provide a brief description of this realm configuration. This is an optional argument.

addr-prefix—Enter the IP address prefix used to determine if an IP address is associated with the realm. This field is entered as an IP address and number of bits in the network portion of the address in standard slash notation. Not specifying the number of bits to use implies all 32 bits of the address are used to match.

Default 0.0.0.0

network-interfaces—Enter a list of network interfaces through which this realm can be reached. Entries in this parameter take the form: `<name>:<subport-id>`. Multiple entries are entered within parenthesis separated by spaces. Excluding keywords **`add`** and **`delete`** replaces the entire list.

Values [add | delete] <interface> [<interface>...]

additional-prefixes—Enter one or more additional address prefixes. Not specifying the number of bits to use implies all 32 bits of the address are used to match.

mm-in-realm—Enable or disable media steering through the Net-Net SBC when the communicating endpoints are located in the same realm

Default disabled

Values enabled | disabled

mm-in-network—Enable or disable media steering through the Net-Net SBC when the communicating endpoints are located in different realms within the same network (on the same network-interface). If this field is set to enabled, the Net-Net SBC will steer all media traveling between two endpoints located in different realms, but within the same network. If this field is set to disabled, then each endpoint will send its media directly to the other endpoint located in a different realm, but within the same network.

Default enabled

Values enabled | disabled

mm-in-system—Enable or disable media managing within the Net-Net SBC

Default enabled

Values enabled | disabled

mm-same-ip—Retain the default of `enabled` if you want media to go through this Net-Net SBC, if mm-in-realm is `enabled`. If set to `disabled`, the media will not go through the Net-Net SBC for endpoint that are behind the same IP.

Default enabled

Values enabled | disabled

msm-release—Enable or disable the inclusion of multi-system (multiple Net-Net SBCs) media release information in the SIP signaling request sent into the realm identified by this realm-config element. If this field is set to enabled, another Net-Net SBC is allowed to decode the encoded SIP signaling request message data sent from a SIP endpoint to another SIP endpoint in the same network to restore the original SDP and subsequently allow the media to flow directly between those two SIP endpoints in the same network serviced by multiple Net-Net SBCs. If this field is set to disabled, the media and signaling will pass through both SDs. If this field is set to enabled, the media is directed directly between the endpoints of a call.

Default disabled

Values enabled | disabled

symmetric-latching—Enable or disable symmetric latching between endpoints for RTP traffic

Default disabled

Values enabled | disabled

qos-enable—Enable or disable the use of QoS in this realm

Default disabled

Values enabled | disabled

max-bandwidth—Enter the total bandwidth budget in kilobits per second for all flows to/from the realm defined in this element. A max-bandwidth field value of 0 indicates unlimited bandwidth.

Default 0

Values Min: 0 / Max: 999999999

fallback-bandwidth—Enter the amount of bandwidth you want available once the Net-Net SBC has determined that the target is unreachable. If this value is less than the max-bandwidth value, the Net-Net SBC might start rejecting calls. It does so until enough calls are released to free adequate bandwidth to stay under the fallback limit and still accept calls.

Default 0

Values Min: 0 / Max: 999999999

max-latency—Enter the maximum latency in milliseconds allowed for flows within this realm. If this parameter is set to 0, then no alarm condition is set and no requests to/from the realm are rejected.

Default 0

Values Min: 0 / Max: 999999999

max-jitter—Enter the maximum jitter in milliseconds allowed for flows within this realm. If this field is set to 0, then no alarm condition is set and no requests to/from the realm are rejected.

Default 0

Values Min: 0 / Max: 999999999

max-packet-loss—Enter the maximum packet loss percentage in hundredths of a percent allowed for flows within this realm. If this parameter is set to 0, then no alarm condition is set and no requests to/from the realm are rejected.

Default 0

Values Min: 0 / Max: 999999999

observ-window-size—Enter the minimum time in milliseconds a threshold (latency, jitter, and packet loss) must be exceeded before triggering an alarm.

Default 0

Values Min: 0 / Max: 999999999

parent-realm—Enter the parent realm for this particular realm. This must reference an existing realm identifier.

dns-realm—Enter the realm whose network interface's DNS server should be used to resolve FQDNs for requests sent into the realm. If this field value is left empty, the Net-Net SBC will use the DNS of the realm's network interface.

media-policy—Select a media-policy on a per-realm basis (via an association between the name field value configured in this field). When the Net-Net SBC first sets up a SIP media session, it identifies the egress realm of each flow and then determines the media-policy element to apply to the flow. This parameter must correspond to a valid name entry in a media policy element.

class-profile—Enter the name of class-profile to use for this realm for ToS marking

in-translationid—Enter the identifier/name of a session-translation element. The Net-Net SBC applies this group of rules to the incoming addresses for this realm. There can be only one entry in this parameter.

out-translationid—Enter the identifier/name of a session-translation element. The Net-Net SBC applies this group of rules to the outgoing addresses for this realm. There can be only one entry in this parameter.

average-rate-limit—Enter the average data rate in bytes per second for host path traffic from a trusted source

Default 0 (disabled)

Values Min: 0 / Max: 999999999

access-control-trust-level—Select the trust level for the host within the realm

Default None

Values
- High—Hosts always remains trusted
- Medium—Hosts belonging to this realm can get promoted to trusted, but can only get demoted to untrusted. Hosts will never be put in black-list.
- Low—Hosts can be promoted to trusted list or can get demoted to untrusted list
- None—Hosts will always remain untrusted. Will never be promoted to trusted list or will never get demoted to the denied list

invalid-signal-threshold—Enter the acceptable invalid signaling message rate falling within a tolerance window

Default 0

Values Min: 0 / Max: 999999999

maximum-signal-threshold—Enter the maximum number of signaling messages allowed within the tolerance window

Default 0 (disabled)

Values Min: 0 / Max: 999999999

untrusted-signal-threshold—Enter the maximum number of untrusted signaling messages allowed within the tolerance window

Default 0

Values Min: 0 / Max: 999999999

nat-trust-threshold—Enter the number of individual devices behind the NAT that must be in the denied list before all the devices behind the NAT have their trust level set to denied. The default value of 0 means that the dynamic demotion feature is disabled.

Default 0

Min: 0 / Max: 65535

deny-period—Enter the length of time an entry is posted in the deny list

Default 30

Values Min: 0 / Max: 999999999

ext-policy-server—Enter the name of the external bandwidth manager configuration instance to be used for external CAC for this realm

monthly-minutes—Enter the monthly minutes allowed

Default 0

Values Min: 0 / Max: 71582788

options—Select optional features or parameters. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <options> [<option>...]

transcoding-policy—Enter the media transcoding policy

transcode-in-realm—Enable or disable transcoding within a single realm

Default disabled

Values enabled | disabled

trunk-context—Enter the default trunk context for this realm

transcode-in-network—Enable or disable transcoding within the same network

Default enabled

Values enabled | disabled

in-manipulationid—Enter the SIP manipulation rule name for received messages

out-manipulationid—Enter the SIP manipulation rule name for outgoing messages

restricted-latching—Enter the restricted latching mode

Default none

Values
- none—no latching used
- sdp—use the address provided in the SDP for latching
- peer-ip—use the layer 3 signaling address for latching

restriction-mask—Enter the number of address bits you want used for the source latched address. If set to 32 (the default), the complete IP address is matched. This field will be used only if the restricted-latching is used.

Default 32

Values Min: 0 / Max: 32

early-media-allow—Enter the early media suppression rule for the realm. If you leave this parameter blank, early media is allowed in either direction.

Values
- none—No early media is allowed in either direction
- both—Early media is allowed in both directions
- reverse—Early media received by the Net-Net SBC in the reverse direction is allowed

accounting-enable—Select whether you want accounting enabled within the realm

Default enabled

Values enabled | disabled

user-cac-bandwidth—Enter the maximum bandwidth per user for dynamic flows to and from the user. By leaving this parameter set to `0` (default), there is unlimited bandwidth and the per user CAC feature is disabled for constraint of bandwidth.

Default 0

Values Min: 0 / Max: 999999999

user-cac-sessions—Enter the maximum number of sessions per user for dynamic flows to and from the user. Leaving this parameter set to `0` (default), there is unlimited sessions and the CAC feature is disabled for constraint on sessions.

Default 0

Values Min: 0 / Max: 999999999

user-cac-mode—Set this parameter to the per user CAC mode that you want to use

Default none

Values
- none—No user CAC for users within this realm
- aor—User CAC per AOR
- ip—User CAC per IP

enforcement-profile—Enter the name of the enforcement profile (SIP allowed methods)

net-management-control—Enable or disable network management controls for this realm

Default disabled

Values enabled | disabled

delay-media-update—Enable or disable media update delay for this realm

Default disabled

Values enabled | disabled

manipulation-string—Enter a string that you want used in header manipulation rules for this realm

icmp-detect-multiplier—Enter the multiplier you want to use when determining how long to send ICMP pings before considering a target unreachable. This number is multiplied by the time you set for the **icmp-advertisement-interval** determines the length of time. For example, if you set this parameter to 10 and the advertisement interval to 20, the Net-Net SBC will send ICMP pings for 120 seconds before declaring the target unreachable.

Default 0

Values Min: 0 / Max: 999999999

icmp-advertisement-interval—Enter the time in seconds between ICMP pings the the Net-Net SBC sends to the target

Default 0

Values Min: 0 / Max: 999999999

icmp-target-ip—Enter the IP address to which the Net-Net SBC should send the ICMP pings so that it can detect when they fail and it needs to switch to the fallback bandwidth for the realm.

session-constraints—Enter the name of the session constraint you want to apply to this realm

stun-enable—Set this parameter to **enabled** to turn STUN server support for this realm on

Default disabled

Values enabled | disabled

stun-server-ip—Enter the IP address for the primary STUN server port

stun-server-port—Enter the port to use with the the **stun-server-ip** for primary STUN server port

Default 3478

Values Min: 1025 / Max: 65535

stun-changed-ip—Enter the IP address for the CHANGED-ADDRESS attribute in Binding Requests received on the primary STUN server port. This IP address must be different from than the one defined for the **stun-server-ip** parameter

stun-changed-port—Enter the port combination to define the CHANGED-ADDRESS attribute in Binding Requests received on the primary STUN server ports

Default 3479

Values Min: 1025 / Max: 65535

sip-profile—Enter the SIP profile to be used for this realm

manipulation-pattern—Enter the regular expression to be used in header manipulation rules

sip-isup-profile—Enter the name of the **sip-isup-profile** to apply to this realm.

match-media-profiles—Enter the media profiles you would like applied to this realm. These values correspond to the name and subname parameters in the media profile configuration. You can wildcard both portions (name and subname) of this

value. See the Net-Net 9000 ACLI Configuration Guide for information about wildcard values.This configuration parameter is entered in the format <name>::<subname> where

Values
- <name>
- <subname>

bw-cac-non-mm—Enable this parameter to turn on bandwidth CAC for media release.

Default disabled

Values enabled | disabled

max-priority-bandwidth—Enter the amount of bandwidth amount of bandwidth you want to want to use for priority (emergency) calls; the system first checks the max-bandwidth parameter, and allows the call if the value you set for priority calls is sufficient.

Default 0

Values Min: 0 / Max: Max: 2^{32}-1

Path **realm-config** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > realm-config.**

Release First appearance: 5.0 / Most recent update: 7.1

Notes This is a multiple instance configuration subelement.

realm-group

The **realm-group** configuration element allows you to configure realm groups. Realm groups are sets of source and destination realms that allow early media to flow in the direction you configure.

Syntax

```
realm-group <name | source-realm | destination-realm | early-
media-allow-direction | state | select | no | show | done | exit>
```

Parameters

name—Enter the name of the realm group

source-realm—Enter the list of one or more global/SIP realms that you want to designate as source realms for the purpose of blocking early media; this is the realm identifier value for the realms you want on the list. Values in this list refer to calling SDP realms. To enter more than one realm in the list, list all items separated by a command and enclose the entire entry in quotations.

destination-realm—Enter the list of one or more global/SIP realms that you want to designate as destination realms for the purpose of blocking early media; this is the realm identifier value for the realms you want on the list. Values in this list refer to called SDP realms. To enter more than one realm in the list, list all items separated by a comma and enclose the entire entry in quotation marks

early-media-allow-direction—Set the direction for which early media is allowed for this realm group

Default both

Values • none—Turns off the feature for this realm group by blocking early media
• reverse—Allows early media to flow from called to caller
• Allows early media to flow to/from called and caller

state—Enable or disable this realm group

Default disabled

Values enabled | disabled

Path **realm-group** is an element under the **media-manager** path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > realm-group**.

Release First appearance: D7.0

RTC Status Supported

rph-policy

The **rph-policy** configuration element allows you to configure an RPH policy to be applied to NMC rules.

Syntax

```
rph-policy <name | override-r-value | insert-r-value | select |
no | show | done | exit>
```

Parameters

name—Enter the name that uniquely identifies this RPH policy. This is the value you use to apply the policy in the NMC rules configuration.

override-r-value—Enter the value that the Net-Net SBC uses to override r-values in the original RPH. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<address>...]

insert-r-value—Enter the value that the Net-Net SBC inserts into the RPH. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<address>...]

Path

rph-policy is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure-terminal > session-router > rph-policy**.

Release

First appearance: 5.1

rph-profile

The **rph-profile** configuration element allows you to configure an RPH profile.

Syntax

```
rph-profile <name | r-values | media-policy | call-treatment |
select | no | show | done | exit>
```

Parameters

name—Enter the name that uniquely identifies this RPH profile. This is the value you use to apply the profile in the NMC rules configuration.

r-values—Enter one or more r-values that the Net-Net SBC is to recognize for matching purposes. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<address>...]

media-policy—Enter the name of a media policy configuration that you want applied for this RPH profile. The Net-Net SBC implements this media policy for the ETS call, and this media policy overrides any media policy set in the realm configuration.

call-treatment—Enter the call treatment method for a non-ETS call that contains RPH matching it to this profile.

Default accept

Values

- accept—The call proceeds as it normally would

• reject—The Net-Net SBC rejects the call with the `417 Unknown-Resource Priority` status code
• priority—The Net-Net SBC treats the call as a priority call

Path **rph-profile** is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure-terminal > session-router > rph-profile**.

Release First appearance: 5.1

session-agent

The **session-agent** element defines a signaling endpoint that can be configured to apply traffic shaping attributes and information regarding next hops or previous hops.

Syntax

```
session-agent <hostname | ip-address | port | state | app-protocol
| app-type | transport-method | realm-id | description | carriers
| allow-next-hop-lp | constraints | max-sessions | max-inbound-
sessions | max-outbound-sessions | max-burst-rate | max-inbound-
burst-rate | max-outbound-burst-rate | max-sustain-rate | max-
inbound-sustain-rate | max-outbound-sustain-rate | max-register-
sustain-rate | min-seizures | min-asr | time-to-resume | ttr-no-
response | in-service-period | burst-rate-window | sustain-rate-
window | req-uri-carrier-mode | proxy-mode | redirect-action |
loose-routing | response-map | ping-method | ping-interval |
options | media-profiles | in-translationid | out-translationid |
trust-me | request-uri-headers | stop-recurse | local-response-map
| ping-to-user-part | ping-from-user-part | li-trust-me | in-
manipulationid | out-manipulationid | p-asserted-id | invalidate-
registrations | trunk-group | ping-in-service-response-codes |
out-service-response-codes | early-media-allow | rfc2833-mode |
rfc2833-payload | enforcement-profile | max-register-burst-rate |
register-burst-window | manipulation-string | tcp-keepalive |
rate-constraints | sip-profile | sip-isup-profile | manipulation-
pattern | select | no | show | done | exit>
```

Parameters

hostname—Enter the hostname of this session agent. This is a required entry that must follow the Hostname (or FQDN) Format or the IP Address Format. Hostname values must be unique.

ip-address—Enter the IP address of session agent if hostname value is an FQDN

port—Enter the port number for this session agent. If this value is set to 0, the Net-Net SBC will not initiate communication with this session-agent (although the Net-Net SBC will accept messages from this session-agent).

Default 5060

Values Min: 0 / Max: 65535

state—Enable or disable the session agent

Default enabled

Values enabled | disabled

app-protocol—Select the signaling protocol used to signal with the session agent

Values SIP | H.323 | NONE

app-type—Set the H.323 session agent type as a gateway or a gatekeeper. This field is mandatory if the app-protocol parameter is set to H.323. If the app-protocol parameter is set to SIP, then this field must be left blank.

Values H323-GW | H323-GK

transport-method—Select the IP protocol used for communicating with this session agent

Default UDP

Values
- UDP—UDP used as the transport method
- UDP+TCP—Initial transport method of UDP, followed by a subsequent transport method of TCP if and when a failure or timeout occurs in response to a UDP INVITE. If this transport method is selected, then INVITEs are always sent via UDP as long as a response is received.
- DynamicTCP—Dynamic TCP connections are the transport method for this session agent. A new connection must be established for each session originating from the session agent. This connection is torn down at the end of a session.
- StaticTCP— Static TCP connections are the transport method for this session agent. Once a connection is established, it will remain and not be torn down.

realm-id—Enter the realm for sessions coming from or going to this session agent. Entries in this field must follow the Name Format. This field must correspond to a valid identifier field entry in a realm-config.

description—Describe the session-agent element. Entries in this field must follow the Text Format.

carriers—Enter carrier names associated with this session agent. If this list is empty, any carrier is allowed. If it is not empty, only local policies that reference one or more of the carriers in this list will be applied to requests coming from this session agent. This list can contain as many entries within it as necessary. Entries in this field must follow the Carrier Format. Excluding keywords **`add`** and **`delete`** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

allow-next-hop-lp—Enable or disable the use of this session agent as the next hop in a local policy

Default enabled

Values enabled | disabled

constraints—Enable or disable the constraints established in this element in the fields that follow (maximum numbers of sessions allowed, maximum session rates, and timeout values) being applied to the sessions sent to the session agent

Default disabled

Values enabled | disabled

max-sessions—Enter the maximum number of sessions allowed by the session agent; 0 means there is no constraint

Default 0

Values Min: 0 / Max: 999999

max-inbound-sessions—Enter the maximum number of inbound sessions allowed from this session agent

Default 0

Values Min: 0 / Max: 999999999

max-outbound-sessions—Enter the maximum number of simultaneous outbound sessions that are allowed to the session agent; 0 means there is no constraint

Default 0

Values Min: 0 / Max: 999999

max-burst-rate—Enter the number of session invitations per second allowed to be sent to or received from the session agent. A session is rejected if the calculated per-second rate exceeds this value.

Default 0

Values Min: 0 / Max: 999999

max-inbound-burst-rate—Enter the maximum inbound burst rate in INVITEs per second from this session agent

Default 0

Values Min: 0 / Max: 999999999

max-outbound-burst-rate—Enter the maximum outbound burst rate in INVITEs per second

Default 0

Values Min: 0 / Max: 999999999

max-sustain-rate—Enter the maximum rate of session invitations per second allowed to or from the session agent within the current window. The period of time over which the rate is calculated is always between one and two window sizes. A session is rejected only if the calculated per-second rate exceeds the max-sustain-rate value. The value set for the max-sustain-rate field must be larger than the value set for the max-burst-rate field.

Default 0

Values Min: 0 / Max: 999999

max-inbound-sustain-rate—Enter the maximum inbound sustain rate in INVITEs per second

Default 0

Values Min: 0 / Max: 999999999

max-outbound-sustain-rate—Enter the maximum outbound sustain rate in INVITEs per second

Default 0

Values Min: 0 / Max: 999999999

max-register-sustain-rate—Specify the registrations per second for this session agent. The constraints parameter must be enabled for this parameter to function.

Default 0 (disabled)

Values Min: 0 / Max: 999999999

min-seizures—Enter the minimum number of seizures that, when exceeded, cause the session agent to be marked as having exceeded its constraints. Calls will not be routed to the session agent until the time-to-resume has elapsed.

Default 5

Values Min: 1 / Max: 999999999

min-asr— Enter the minimum percentage, that if the session agent's ASR for the current window falls below this percentage, the session agent is marked as having exceeded its constraints and calls will not be routed to it until the time-to-resume has elapsed

Default 0%

Values Min: 0% / Max: 100%

time-to-resume—Enter the number of seconds after which the SA (Session Agent) is put back in service (after the SA is taken out-of-service because it exceeded some constraint).

Default 0

Values Min: 0 / Max: 999999

ttr-no-response—Enter the time delay in seconds to wait before the SA (Session Agent) is put back in service (after the SA is taken out-of-service because it did not respond to the Net-Net SBC).

Default 0

Values Min: 0 / Max: 999999

in-service-period—Enter the time in seconds the session-agent must be operational (once communication is re-established) before the session agent is declared to be in-service. This value gives the session agent adequate time to initialize.

Default 0

Values Min: 0 / Max: 999999

burst-rate-window—Enter the burst window period in seconds used to measure the burst rate. The term "window" refers to the period of time over which the burst rate is computed.

Default 0

Values Min: 0 / Max: 999999

sustain-rate-window—Enter the sustained window period in seconds used to measure the sustained rate. The term "window" refers to the period of time over which the sustained rate is computed.

Default 0

Values Min: 0 / Max: 999999

The value you set here must be higher than or equal to the value you set for the burst rate window.

> ***Note:*** *If you are going to use this parameter, you must set it to a minimum value of 10.*

req-uri-carrier-mode—Select how a selected carrier, as determined by the local policy element, should be added to the outgoing message

Default None

Values
- None—Do not add carrier information to the outgoing message
- URI-param—Add a parameter to the Request-URI (e.g., cic-XXX)
- Prefix—Add the carrier code as a prefix to the telephone number in the Request-URI (in the same manner as is done in the PSTN)

proxy-mode—Select how SIP proxy forwards requests coming from the session agent. If this parameter is empty, its value is set to the value of the proxy-mode parameter in the sip-interface element by default. If the proxy-mode field in the sip-config element is also empty, the default is proxy.

Values
- proxy—If the Net-Net SBC is a Net-Net SR, the system will proxy the request coming from the session agent and maintain the session and dialog state. If the Net-Net SBC is an SD, the system will behave as a B2BUA when forwarding the request
- redirect—The system will send a SIP 3xx reDIRECT response with contacts (found in the local-policy) to the previous hop
- record-route—Forward requests with Record-Route (for stateless and transaction and operation modes only)

redirect-action—Select the action the SIP proxy takes when it receives a Redirect (3xx) response from the session agent. If the response comes from a session agent and this field is empty, the redirect action value will be recurse. If no session agent is found (i.e., if a message comes from an anonymous user agent), the redirect action value will be proxy. If the Redirect (3xx) response does not have any Contact header, the response will be sent back to the previous hop.

Values
- Proxy—SIP proxy passes the response back to the previous hop. The response will be sent based on the proxy-mode of the original request.
- Recurse—SIP proxy sends the original request to the list of contacts in the Contact header of the response, serially (in the order in which the contacts are listed in the response)

loose-routing—Enable or disable loose routing

Default enabled

Values enabled | disabled

response-map—Enter the name of the sip-response-map element set in the session router element to use for translating inbound final response values

ping-method—Enter the SIP message/method to use to "ping" a session agent

ping-interval—Select how often to ping a session agent in seconds

Default 0

Values Min: 0 / Max: 999999

options—Select optional features or parameters. Excluding keywords **`add`** and **`delete`** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

media-profiles—Enter a list of media profiles. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

in-translationid—Enter the identifier/name of the configured session translation to apply. The Net-Net SBC applies this group of rules to the incoming leg of the call for this session agent. There can be only one entry in this field.

out-translationid—Enter the identifier/name of the configured session translation to apply. The Net-Net SBC applies this group of rules to the outgoing leg of the call for this session agent. There can be only one entry in this field.

trust-me—Enable or disable the trust of this session agent, used for DoS/ACL support

Default disabled

Values enabled | disabled

request-uri-headers—Enter a list of embedded headers extracted from the Contact header that will be inserted in the re INVITE message. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

stop-recurse—Enter a list of returned response codes that this session agent will watch for in order to stop recursion on the target's or contact's messages

local-response-map—Enter the name of local response map to use for this session agent. This value should be the name of a sip-response-map configuration element.

ping-to-user-part—Set the user portion of the To: header in a session agent ping message

ping-from-user-part—Set the user portions of the Request-URI and the From: header in a session agent ping message

li-trust-me—Set this parameter to enabled to designate this session agent as trusted for P-DCS-LAES use

Default disabled

Values enabled | disabled

in-manipulationid—Enter the name of the SIP header manipulations configuration to apply to the traffic entering the Net-Net SBC via this session agent

out-manipulationid—Enter the name of the SIP header manipulations configuration to apply to the traffic exiting the Net-Net SBC via this session agent

p-asserted-id—Set the configurable P-Asserted-Identity header for this session agent. This value should be a valid SIP URI.

invalidate-registrations—Enable or disable the invalidation of all registrations going to this session agent

Default disabled

Values enabled | disabled

trunk-group—Enter the trunk group names and trunk group contexts to match in either IPTEL or custom format. If left blank, the Net-Net SBC uses the trunk group in the realm for this session agent. Multiple entries are surrounded in parentheses

and separated from each other with spaces. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

Entries for this list must one of the following formats: `trgp:context` or `trgp.context`.

ping-in-service-response-codes—Enter the response codes that keep a session agent in service when they appear in its response to the Net-Net SBC's ping request.

Default None

Values SIP Response codes

out-service-response-codes—Enter the response codes that take a session agent out of service when they appear in its response to the Net-Net SBC's ping request.

Default None

Values SIP Response codes

early-media-allow—Enter the early media suppression rule for the session agent. If you leave this parameter blank, early media is allowed in either direction.

Values
- none—No early media is allowed in either direction
- both—Early media is allowed in both directions
- reverse—Early media received by the Net-Net SBC in the reverse direction is allowed

rfc2833-mode—Select whether 2833/UII negotiation will be transparent to the Net-Net SBC , or use 2833 for DTMF

Default none

Values
- transparent—The session-agent will behave exactly the same way as before and the 2833 or UII negotiation will be transparent to the Net-Net SBC. This overrides any configuration in the H323-stack even if the stack is configured for "preferred" mode.
- preferred—The session-agent prefers to use 2833 for DTMF transfer and would signal that in its TCS. However, the final decision depends on the remote H323EP.
- dual—The Net-Net SBC behaves the same as it does when set to preferred mode and it forwards both the original DTMF mechanism and the translated one to the remote endpoint
- none—The 2833-UII interworking will be decided based on the h323-stack configuration.

rfc2833-payload—Enter the payload type used by the SA in" preferred" `rfc2833-mode`

Default 101

Values Min: 96 / Max: 127

enforcement-profile—Enter the enforcement policy set of allowed SIP methods you want to use for this session agent

max-register-burst-rate—Enter the maximum number of new registrations you want this session agent to accept within the registration burst rate window.

Default 0

Values Min: 0 / Max: 999999999

register-burst-window—Define the window size in seconds for the maximum number of allowable SIP registrations.

Default 0

Values Min: 0 / Max: 999999999

manipulation-string—Enter a string you want used in the header manipulation rules for this session-agent

tcp-keepalive—Enable or disable standard keepalive probes to determine whether or not connectivity with a remote peer is lost

Default none

Values none | enabled | disabled

rate-constraints—Accesses the **rate-constraints** subelement

sip-profile—Enter the name of the **sip-profile** you want to add to the **session-agent**

manipulation-pattern—Enter the regular expression to be used in header manipulation rules

ping-all-addresses—Enable pinging each IP address dynamically resolved via DNS. If **disabled** (default), the Net-Net SBC only pings the first available resolved IP address.

Default disabled

Values enabled | disabled

sip-isup-profile—Enter the name of the **sip-isup-profile** you want to add to the **session-agent.**

Path **session-agent** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-agent.**

Release First appearance: 5.0 / Most recent update: 7.1

Notes This is a multiple instance configuration element.

session-agent>rate-constraints

The **rate-constraints** subelement for the session-agent configuration element allows you to configure rate constraints for individual session agents, which can then be applied to the SIP interface where you want them used.

Syntax

```
rate-constraints <method | max-inbound-burst-rate | max-outbound-
burst-rate | max-inbound-sustain-rate | max-outbound-sustain-rate
| select | no | show | done | exit>
```

Parameters

method—Enter the SIP method name for the method you want to throttle

Values
- NOTIFY
- OPTIONS
- MESSAGE

- PUBLISH
- REGISTER

max-inbound-burst-rate—For the SIP method you set in the methods parameter, enter the number to restrict the inbound burst rate on the SIP interface where you apply these constraints

Default 0

Values Min: 0 / Max: 999999999

max-outbound-burst-rate—For the SIP method you set in the methods parameter, enter the number to restrict the outbound burst rate on the SIP interface where you apply these constraints

Default 0

Values Min: 0 / Max: 999999999

max-inbound-sustain-rate—For the SIP method you set in the methods parameter, enter the number to restrict the inbound sustain rate on the SIP interface where you apply these constraints

Default 0

Values Min: 0 / Max: 999999999

max-outbound-sustain-rate—For the SIP method you set in the methods parameter, enter the number to restrict the outbound sustain rate on the SIP interface where you apply these constraints

Default 0

Values Min: 0 / Max: 999999999

Path **rate-constraints** is a subelement under the **session-agent** element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-agent > rate-constraints**.

Release First appearance: D7.0

RTC Status Supported

session-constraints

The **session-constraints** configuration element allows you to create session layer constraints in order to manage and police session-related traffic including maximum concurrent sessions, maximum outbound concurrent sessions, maximum session burst rate, and maximum session sustained rate.

The SIP interface configuration's constraint-name parameter invokes the session constraint configuration you want to apply. Using the constraints you have set up, the Net-Net SBC checks and limits traffic according to those settings for the SIP interface. Of course, if you do not set up the session constraints or you do not apply them in the SIP interface, then that SIP interface will be unconstrained. If you apply a single session-constraint element to multiple SIP interfaces, each SIP interface will maintain its own copy of the session-constraint.

Note: The Net-Net SBC supports five concurrent SSH and/or SFTP sessions.

Syntax

```
session-constraints <name | state | max-sessions | max-inbound-
sessions | max-outbound-sessions | max-burst-rate | max-inbound-
burst-rate | max-outbound-burst-rate | max-sustain-rate | max-
inbound-sustain-rate | max-outbound-sustain-rate | min-seizures |
min-asr | time-to-resume | burst-rate-window | sustain-rate-
window | rate-constraints | select | no | show | done | exit>
```

name—Enter the name for this session constraints configuration; this is a unique identifier that you will use in the SIP interface when you want the session constraints applied there.

state—Enable or disable these session constraints

Default enabled

Values enabled | disabled

max-sessions—Enter the maximum sessions allowed for this constraint.

Default 0

Values Min: 0 / Max: 999999999

max-inbound-sessions—Enter the maximum inbound sessions allowed for this constraint.

Default 0

Values Min: 0 / Max: 999999999

max-outbound-sessions—Enter the maximum outbound sessions allowed for this constraint.

Default 0

Values Min: 0 / Max: 999999999

max-burst-rate—Enter the maximum burst rate (invites per second) allowed for this constraint. This value should be the sum of the **max-inbound-burst-rate** and the **max-outbound-burst-rate**.

Default 0

Values Min: 0 / Max: 999999999

max-inbound-burst-rate—Enter the maximum inbound burst rate (number of session invitations per second) for this constraint.

Default 0

Values Min: 0 / Max: 999999999

max-outbound-burst-rate—Enter the maximum outbound burst rate (number of session invitations per second) for this constraint.

Default 0

Values Min: 0 / Max: 999999999

max-sustain-rate—Enter the maximum rate of session invitations per second allowed within the current window for this constraint.

Default 0

Values Min: 0 / Max: 999999999

max-inbound-sustain-rate—Enter the maximum inbound sustain rate (of session invitations allowed within the current window) for this constraint.

Default 0

Values Min: 0 / Max: 999999999

max-outbound-sustain-rate—Enter the maximum outbound sustain rate (of session invitations allowed within the current window) for this constraint.

Default 0

Values Min: 0 / Max: 999999999

min-seizures—Enter the minimum number of seizures for a no-answer scenario

Default 5

Values Min: 0 / Max: 999999

min-asr—Enter the minimum ASR in percentage

Default 0

Values Min: 0 / Max: 999999

time-to-resume—Enter the number of seconds that is used to place an element (like a session agent) in the standby state when it has been take out of service because of excessive transaction timeouts.

Default 0

Values Min: 0 / Max: 999999999

burst-rate-window—Enter the time in seconds that you want to use to measure the burst rate; the "window" is the time over which the burst rate is calculated, and is used for the over all burst rate as well as the inbound and outbound burst rates.

Default 0

Values Min: 0 / Max: 999999999

sustain-rate-window—Enter the time in seconds used to measure the sustained rate; the "window" is the time over which the sustained rate is calculated, and is used for the over all sustained rate as well as the inbound and outbound sustained rates.

Default 0

Values Min: 0 / Max: 999999999

rate-constraints—Access the **rate-constraints** subelement

Path **session-constraints** is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure-terminal > session-router > session-constraints**.

Release First appearance: 5.1

session-constraints>rate-constraints

The **rate-constraints** subelement for the **session-constraints** configuration element allows you to configure rate constraints for individual session constraints, which can then be applied to the SIP interface where you want them used.

Syntax

```
rate-constraints <method | max-inbound-burst-rate | max-outbound-
burst-rate | max-inbound-sustain-rate | max-outbound-sustain-rate
| select | no | show | done | exit>
```

Parameters

method—Enter the SIP method name for the method you want to throttle

Values
- NOTIFY
- OPTIONS
- MESSAGE
- PUBLISH
- REGISTER

max-inbound-burst-rate—For the SIP method you set in the methods parameter, enter the number to restrict the inbound burst rate on the SIP interface where you apply these constraints

Default 0

Values Min: 0 / Max: 999999999

max-outbound-burst-rate—For the SIP method you set in the methods parameter, enter the number to restrict the outbound burst rate on the SIP interface where you apply these constraints

Default 0

Values Min: 0 / Max: 999999999

max-inbound-sustain-rate—For the SIP method you set in the methods parameter, enter the number to restrict the inbound sustain rate on the SIP interface where you apply these constraints

Default 0

Values Min: 0 / Max: 999999999

max-outbound-sustain-rate—For the SIP method you set in the methods parameter, enter the number to restrict the outbound sustain rate on the SIP interface where you apply these constraints

Default 0

Values Min: 0 / Max: 999999999

Path

rate-constraints is a subelement under the **session-constraints** element. the full path from the topmost ACLI prompt is: **configure terminal > session-router > session-constraints > rate-constraints**.

Release

First appearance: D7.0

RTC Status

Supported

session-group

The **session-agent-group** element creates a group of Session Agents and/or groups of other SAGs. The creation of a SAG indicates that its members are logically equivalent and can be used interchangeably. This allows for the creation of constructs like hunt groups for application servers or gateways.

Syntax

```
session-group <group-name | description | strategy | app-protocol
| state | dest | trunk-group | stop-sag-recursion | sag-recursion
| select | no | show | done | exit>
```

Parameters

group-name—Enter the name of the session-agent-group element. This required entry must follow the Name Format, and must be unique.

description—Describe the session agent group element. This is an optional parameter.

strategy—Select the session agent allocation options for the session-agent-group. Strategies determine how session agents will be chosen by this session-agent-group element.

Default Hunt

Values
- Hunt—Select session agents in the order in which they are listed
- RoundRobin—Select each session agent in the order in which they are listed in the dest list, selecting each agent in turn, one per session. After all session agents have been used, the first session agent is used again and the cycle continues.
- LeastBusy—Select the session agent that has the fewest number of sessions relative to the max-outbound-sessions constraint or the max-sessions constraint (i.e., lowest percent busy) of the session-agent element
- PropDist—Based on programmed, constrained session limits, the Proportional Distribution strategy proportionally distributes the traffic among all of the available session-agent elements
- LowSusRate—Routes to the session agent with the lowest sustained rate of session initiations/invitations

app-protocol—Select the application protocol

Values SIP | H.323 | NONE

state—Enable or disable the session-agent-group element

Default enabled

Values enabled | disabled

dest—Enter the destinations (i.e., next hops) available for use by this session agent group. If this list is configured, it can contain as many destinations as necessary. A dest list value must correspond to a valid group name in another session agent group or to a valid hostname. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

trunk-group—Enter the trunk group names and trunk group contexts to match in either IPTEL or custom format. If left blank, the Net-Net SBC uses the trunk group in the realm for this session agent group. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

Entries for this list must follow one of the following formats: `trgp:context` or `trgp.context`.

stop-sag-recurse—Enter the list of SIP response codes that terminate recursion within the SAG. On encountering the specified response code(s), the Net-Net SBC returns a final response to the UAC. You can enter the response codes as a comma-separated list or as response code ranges.

Default 401, 407

sag-recursion—Enable or disable SIP SAG recursion for this SAG.

Default disabled

Values enabled | disabled

Path

session-agent-group is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-group.**

Release

First appearance: 5.0

Notes

This is a multiple instance configuration element.

session-router-config

The **session-router-config** element allows you to configure session alerts on the Net-Net SBC.

Syntax

```
session-router-config <short-call-duration | short-call-threshold
| short-call-window | force-report-trunk-info | match-lp-source-
parent-realms | nested-realm-stats | reject-message-threshold |
reject-message-window | additional-lp-lookups | max-routes-per-
lookup | total-lp-routes | select | no | show | done | exit>
```

short-session-duration—Enter the maximum call duration for a call to be considered a short call

Default 0

Values Min: 0 / Max: 999999999

short-session-threshold—Enter the minimum number of short duration calls within a window that triggers the trap

Default 0

Values Min: 0 / Max: 999999999

short-session-window—Enter the number of seconds for the short call count window

Default 10

Values Min: 1 / Max: 999999999

force-report-trunk-info—Enable or disable forcible reporting of trunk information

Default disabled

Values enabled | disabled

match-lp-source-parent-realms—Enable or disable the Net-Net SBC to perform local policy realm matching based on the parent realm (so that there are local policy entries for parent and child realms)

Default disabled

Values enabled | disabled

nested-realm-stats—Enable or disable using session constraints for nested realms across the entire system

Default disabled

Values enabled | disabled

reject-message-threshold—Enter the minimum number of message rejections allowed in the reject-message-window time on the Net-Net SBC (when using the SIP manipulation action reject) before generating an SNMP trap

Default 0 (no trap is sent)

Values Min: 0 / Max: 999999999

reject-message-window—Enter the time in seconds that defines the window for maximum message rejections allowed before generating an SNMPS trap

Default 0 (no trap is sent)

Values Min: 0 / Max: 999999999

additional-lp-lookups—Enter the number of additional local policy per message lookups.

Default 0 (disables multistaged local policy lookup)

Values Min: 0 / Max: 5

max-routes-per-lookup—Enter the maximum number of routes per local policy lookup.

Default 0 (no limit on the number of returned routes)

Values Min: 0 / Max: 2^{32}-1

total-lp-routes—Enter the total number of routes for all local policy lookups per message request.

Default 0 (no limit on the number of returned routes)

Values Min: 0 / Max: 2^{32}-1

Path **session-router** is an element under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-router-config**.

Release First appearance: 6.0 / Most recent update: 7.1

RTC Status Supported

session-translation

The **session-translation** element defines how translation rules are applied to incoming and outgoing numbers. Multiple translation rules can be referenced and applied; this configuration element group rules together and allows them to be referenced by a single identifier.

Syntax

```
session-translation <id | rules-calling | rules-called | select |
no | show | done | exit>
```

Parameters

id—Enter the identifier or name for this set of session translation rules. This parameter is required.

rules-calling—Enter the rule(s) defined in the translation rules element applied to the calling number. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

rules-called—Enter the rule(s) defined in the translation rules element applied to the called number. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

Path **session-translation** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-translation.**

Release

First appearance: 5.0

Notes

The Net-Net SBC applies the translation rules established in this field cumulatively, in the order in which they are entered. If this field is configured with a value of "rule1 rule2 rule3", rule1 will be applied to the original number first, rule2 second, and rule3 last.
This is a multiple instance configuration element.

sip-config

The **sip-config** element is used to define the parameters for this protocol specific to the Net-Net SBC communicating with SIP.

Syntax

```
sip-config <state | operation-mode | dialog-transparency | home-
realm-id | egress-realm-id | nat-mode | registrar-domain |
registrar-host | registrar-port | register-service-route | init-
timer | max-timer | trans-expire | invite-expire | inactive-
dynamic-conn | userinfo-mode | sip-message-len | add-reason-
header | response-map | local-response-map | enforcement-profile
| extra-method-stats | network-mode | rph-feature | nsep-user-
sessions-rate | nsep-sa-sessions-rate | acct-stop-on-challenge |
enum-sag-match | options | registration-cache-limit | register-
use-to-for-lp | pass-gruu-contact | select | no | show | done |
exit>
```

Parameters

state—Enable or disable the SIP operations

Default enabled

Values enabled | disabled

operation-mode—Select the SIP operation mode

Default Dialog

Values
- Disabled—SIP operation disabled
- Stateless—Stateless proxy forwarding. SIP requests are forwarded based on the Request-URI and local policy. No transaction, session or dialog state is maintained. No media state is maintained, and session descriptions in the SIP messages are not modified.
- Transaction - Transaction stateful proxy mode. SIP requests are forwarded based on the Request-URI and local policy. The Net-Net SBC maintains transaction state in accordance with RFC 3261. No session or dialog state is maintained. No media state is maintained, and session descriptions in the SIP messages are not modified.
- Session - Session stateful proxy mode. SIP requests are forwarded based on the Request-URI and local policy. The Net-Net SBC maintains transaction state in accordance with RFC 3261. The SD also maintains session state information. A Record-Route header is inserted in requests so that the Net-Net SBC will remain in the path. No media state is maintained, and session descriptions in the SIP messages are not modified.
- Dialog - Dialog stateful B2BUA mode. The Net-Net SBC maintains full transaction, session, and dialog state. If media management is enabled, full media state is also maintained and the Net-Net SBC modifies session descriptions in SIP messages to cause the media to flow through the Net-Net SBC.

dialog-transparency—Enable or disable the SIP dialog transparency service for use with Net-Net SBC PAC and non-PAC configurations to prevent the Net-Net SBC from generating a unique Call-ID and modifying dialog tags

Default enabled

Values enabled | disabled

home-realm-id—Enter the identifier of the home realm. This is the network to which the Net-Net SBC's SIP proxy (B2BUA) is logically connected. If configured, this field must correspond to a valid identifier field entry in a realm-config.

egress-realm-id—Default egress realm identifier

nat-mode—Select the home realm NAT mode. This is used to indicate whether the home realm is "public" or "private" address space for application of the SIP-NAT function.

Default Done

Values
- None—No SIP-NAT is necessary
- Private—Indicate that the home realm is private address space, and all other external realms are public address space. Addresses in the home realm will be encoded in SIP URIs sent into the external realm. The addresses are decoded when the URIs enter the home realm.
- Public—Indicate that the home realm is public address space. Addresses from external realms are encoded in SIP URIs as they enter the home realm. Addresses are decoded as they enter the external realm that the address originated in.

registrar-domain—Enter the domain name for identifying which requests for which Hosted NAT Traversal (HNT) or registration caching applies. The right-most portion of the "host" part of the Request-URI is matched against this value. An asterisk "*" is used to indicate any domain.

registrar-host—Enter the hostname or IP address of the SIP registrar for the HNT and registration caching function. An asterisk "*" is used when there are multiple SIP registrars and normal routing using the Request-URI or local policy is to be applied.

registrar-port—Enter the port number of the SIP registrar server

Default 0

Values Min: 0 / Max: 65535

register-service-route—Select the service-route usage for REGISTER requests

Default always

Values
- never
- always
- removal
- session
- session+removal

init-timer—Enter the initial timeout value in milliseconds for a response to an INVITE request, and it applies to any SIP request in UDP. In RFC 3261, this value is also referred to as TIMER_T1.

Default 500

Values Min: 1 / Max: 999999999

max-timer—Enter the maximum retransmission timeout in milliseconds for SIP. In RFC 3261, this value is also referred to as TIMER_T2.

Default 4000

Values Min: 1 / Max: 999999999

trans-expire—Enter the TTL1 in seconds for SIP transactions. This timer is equivalent to TIMER_B in RFC 3261, and the same value is used for TIMER_D, TIMER_F, TIMER_H, and TIMER_J as set out in the same RFC.

Default 32

Values Min: 1/ Max: 999999999

invite-expire—Enter the TTL in seconds for a SIP client transaction after receiving a provisional response. This timer is equivalent to TIMER_C in RFC 3261.

Default 180

Values Min: 1/ Max: 999999999

inactive-dynamic-conn—Enter the time limit in seconds for inactive dynamic connections

Default 32

Values Min: 1 / Max: 999999999

userinfo-mode—Select the contact userinfo mode

Default none

Values

- none—There is no special treatment. Cookies generated by the SIP-NAT function are included in the userinfo sent by the Net-Net SBC.
- contact—Retain the userinfo from the received Contact header. No cookies are added for the SIP-NAT or registration caching function
- from—The userinfo from the From or To header is used in Contact URIs sent by the Net-Net SBC. No cookies are added for the SIP-NAT or registration caching function. The To header is used for Contacts in REGISTER requests and for all responses. The From is used for Contacts in requests other than REGISTER.
- reg-hnt—For HNT endpoints, an HNT cookie is appended to the userinfo to make the user unique in the egress realm. The HNT cookie appears after any cookies added by the SIP-NAT function.
- reg-contact—Retain the userinfo from the received Contact header with registration caching (regular and HNT), a cookie is added to make the user unique in the egress realm. Cookies from the SIP-NAT function are not included in the userinfo.
- reg-from—The userinfo from the From or To header is used. With registration caching (regular and HNT), a cookie is added to make the user unique in the egress realm. Cookies from the SIP-NAT function are not included in the userinfo.

sip-message-len—Set the size constraint in bytes on a SIP message

Default 4096

Values Min: 0 / Max: 65535

add-reason-header—Add a reason header

Default disabled

Values enabled | disabled

response-map—Enter the name of the default response map

local-response-map—Enter the name of the default local response map

enforcement-profile—Enter the name of the enforcement profile (SIP allowed methods)

extra-method-stats—Enable or disable the expanded SIP Method tracking feature

Default disabled

Values enabled | disabled

network-model—Select the network model for transport balancing

Values
- access
- peering
- shared

rph-feature—Enable or disable the NSEP feature for the global SIP configuration.

Default disabled

Values enabled | disabled

nsep-user-sessions-rate—Enter the maximum INVITEs per second to admit for ETS calls on a per-user basis. A value of 0 disables CAC for ETS calls.

Default 0

Values Min: 0 / Max: 999999999

options—Select optional features or parameters. Excluding keywords **`add`** and **`delete`** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

acct-stop-on-challenge—Enable or disable the Net-Net SBC accounting sending a "stop" message when a challenge response is received during session teardown. If this is disabled, the accounting "stop" message is delayed.

Default enabled

Values enabled | disabled

enum-sag-match—Set this parameter to `enabled` so the Net-Net SBC will match session agent group (SAG) names with the hostname portion in the naming authority pointer (NAPTR) from an ENUM query or LRT next-hop entry.

Default disabled

Values enabled | disabled

registration-cache-limit—Set the maximum number of SIP registrations that you want to keep in the registration cache. Leaving this parameter blanks means there is no limit on the registration cache and, therefore, the feature is disabled.

Default 0

Values Min: 0 / Max: 999999999

register-use-to-for-lp—Set this parameter to enabled if you want the Net-Net SBC to use, for routing purposes, an ENUM query to return the SIP URI of the Registrar for a SIP REGISTER message

Default disabled

Values enabled | disabled

pass-gruu-contact—Enable or disable the **sip-config** to to parse for `gr` URI parameter in the contact header in non-registered endpoints' messages

proxy-sub-events—Enter the event package types (or refer header contents) that the Net-Net SBC should proxy in transaction mode only. Use the add and delete subcommands to add or delete one of multiply configured events types.

enum-agent-match—Set this parameter to enabled for the Net-Net SBC to mimic Net-Net 3000 and 4000 series behavior with respect to local policy routing with ENUM-provided session agent routes.

nsep-sa-sessions-rate—Enter maximum acceptable number of SIP INVITES (NSEP sessions) per second to allow for SIP session agents. This parameter defaults to 0, meaning there is no limit.

Default 0

Values Min: 0 / Max: 2^{32} - 1

sag-lookup-on-redirect—Enable SAG-based maddr resolution.

Default disabled

Values enabled | disabled

Path **sip-config** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-config.**

Release First appearance: 5.0 / Most recent update: 7.1

Notes This is a single instance configuration element.

sip-feature

The **sip-feature** element defines how the Net-Net SBC's B2BUA should treat specific option tags in SIP headers.

Syntax

```
sip-feature <name | realm | support-mode-inbound | require-mode-
inbound | proxy-require-mode-inbound | support-mode-outbound |
require-mode-outbound | proxy-require-mode-outbound | select | no
| show | done | exit>
```

Parameters

name—Enter the option tag name that will appear in the Require, Supported, or Proxy-Require headers of SIP messages

realm—Enter the realm with which the feature is associated; to make the feature global, leave this parameter blank

support-mode-inbound—Select the treatment of the feature (option tag) in a Supported header for an inbound packet

Default Pass

Values
- Pass—B2BUA should include the tag in the corresponding outgoing message
- Strip—Tag should be excluded in the outgoing message. Use strip mode to not use the extension.

require-mode-inbound—Select the treatment of the feature (option tag) in a Require header for an inbound packet

Default Reject

Values
- Pass—B2BUA should include the tag in the corresponding outgoing message
- Reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.

proxy-require-mode-inbound—Select the treatment of the feature (option tag) in a Proxy-Require header for an inbound packet

Default Pass

Values
- Pass—B2BUA should include the tag in the corresponding outgoing message
- Reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.

support-mode-outbound—Select the treatment of the feature (option tag) in a Supported header for an outbound packet

Default Pass

Values
- Pass—B2BUA should include the tag in the corresponding outgoing message
- Strip—Tag should be excluded in the outgoing message

require-mode-outbound—Select the treatment of the feature (option tag) in a Require header for an outbound packet

Default Reject

Values
- Pass—B2BUA should include the tag in the corresponding outgoing message
- Reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.

proxy-require-mode-outbound—Select the treatment of the feature (option tag) in a Proxy-Require header for an outbound packet

Default Pass

Values
- Pass—B2BUA should include the tag in the corresponding outgoing message
- Reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.

Path

sip-feature is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-feature.**

Release

First appearance: 5.0

Notes

If an option tag is encountered that is not configured as a SIP feature, the default treatments described in each of the field descriptions (name, support-mode, require-mode, and proxy-require-mode) included in this section will apply. Therefore, a sip-feature element only needs to be configured when non-default treatment is required.
This is a multiple instance element.

sip-interface

The **sip-interface** element allows you to configure SIP interfaces on the Net-Net SBC.

Syntax

```
sip-interface <state | realm-id | description | sip-ports |
carriers | proxy-mode | redirect-action | network-type | contact-
mode | nat-traversal | nat-interval | tcp-nat-interval |
registration-caching | registration-interval | min-reg-expire |
route-to-registrar | secured-network | options | trust-mode |
stop-recurse | in-manipulationid | out-manipulationid | sip-ims-
feature | ppi-to-pai | charging-vector-mode | charging-function-
address-mode | ccf-address | ecf-address | operator-identifier |
network-identifier | implicit-service-route | anonymous-priority
| max-incoming-conns | per-scr-ip-max-incoming-conns | inactive-
conn-timeout | untrusted-conn-timeout| port-map-start | port-map-
end | term-tgrp-mode | response-map | local-response-map |
enforcement-profile | route-unauthorized-calls | trans-expire |
invite-expire | max-redirect-contacts | session-constraints |
rfc2833-mode | rfc2833-payload | manipulation-string | tcp-
keepalive | add-sdp-invite | add-sdp-profiles | sip-profile |
sip-isup-profile | manipulation-pattern | reg-cache-route | sip-
dynamic-hnt | max-nat-interval | nat-int-increment | nat-test-
increment | select | no | show | done | exit>
```

Parameters

state—Enable or disable the SIP interface

Default enabled

Values enabled | disabled

realm-id—Enter the name of the realm to which the SIP interface applies

description—Provide a brief description for this **sip-interface** configuration. This is an optional parameter.

sip-ports—Access the sip-ports subelement

carriers—Enter a list of carriers related to the sip-config. Entries in this field must follow the Carrier Format. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

proxy-mode—Set the default SIP request proxy mode

Values
- Proxy—Forward all SIP requests to other session agents
- Redirect—Send a SIP 3xx redirect response with contacts (found in the local policy) to the previous hop
- Record-route—Forward requests with Record-Route (for stateless and transaction and operation modes only)

redirect-action—Set handling of Redirect (3xx) response messages from a session agent

Values
- Proxy—Send the response back to the previous hop
- Recurse—Recurse on the contacts in the response

network-type—Select the network type for transport balancing

Values
- access
- core
- any

contact-mode—Select the contact header routing mode

Default None

Values
- None
- Maddr
- Strict-route
- Loose-route

nat-traversal—Select the type of HNT functionality for SIP

Default None

Values
- None—Disable NAT Traversal
- Always—Perform HNT when SIP-Via and transport addresses do not match
- Rport—Perform HNT when Via rport parameter is present and SIP-Via and transport addresses do not match

nat-interval—Enter the expiration time in seconds for the Net-Net SBC's cached registration entry for an endpoint doing HNT

Default 30

Values Min: 0 / Max: 99999

tcp-nat-interval—Enter the TCP NAT traversal registration interval in seconds

Default 90

Values Min: 0 / Max: 99999

registration-caching—Enable or disable the registration cache used for all UAs rather than those behind NATs

Default disabled

Values enabled | disabled

registration-interval—Enter the expiration time in seconds for the Net-Net SBC's cached registration entry for an endpoint (non-HNT)

Default 3600

Values Min: 0 / Max: 999999

min-reg-expire—Enter the minimum registration expiration time in seconds for HNT registration caching

Default 300

Values Min: 0 / Max: 999999

route-to-registrar—Enable or disable the forwarding of a request by the SD addressed to the registrar to the SIP registrar as opposed to sending the request to the registered contact in the registration cache

Default disabled

Values enabled | disabled

secured-network—Enable or disable sending messages on unsecured transport

Default disabled

Values enabled | disabled

options—Select optional features or parameters. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

trust-mode—Select the trust mode for this SIP interface

Default All

Values
- All—Trust all previous and next hops except untrusted session agents
- Agents-only—Trust only trusted session agents
- Realm-prefix—Trust only trusted session agents or address matching realm prefix
- Registered—Trust only trusted session agents or registered endpoints
- None—Trust nothing

stop-recurse—Enter a list of returned response codes that this SIP interface will watch for in order to stop recursion on the target's or contact's messages. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

in-manipulationid—Enter the name of the SIP header manipulations configuration to apply to the traffic entering the Net-Net SBC via this SIP interface

out-manipulationid—Enable or disable the name of the SIP header manipulations configuration being applied to the traffic exiting the Net-Net SBC via this SIP interface

sip-ims-feature—Enable or disable IMS functionality on this SIP interface

Default disabled

Values enabled | disabled

ppi-to-pai—Select the preferred/asserted identity conversion mode

Values
- None—No action is taken and there is no conversion
- Trusted—The trust-level of the ingress phone is checked. If it is not trusted, the PPI headers in the message will be deleted. If it is trusted, the PPI will be converted to PAI.
- Always—The PPI is always converted to PAI
- Remove—The PPI headers are always removed

charging-vector-mode—Set the state of P-Charging-Vector header handling

Default Pass

Values
- Pass—Pass the P-Charging-Vector header received in an incoming SIP message untouched as the message is forwarded out of the Net-Net SBC
- Delete—Delete the P-Charging-Vector header received in an incoming SIP message before it is forwarded out of the Net-Net SBC
- Insert—Insert the P-Charging-Vector header in an incoming SIP message that does not contain the P-Charging-Vector header. If the incoming message contains the P-Charging-

Vector header, the Net-Net SBC will overwrite the P-Charging-Vector header with its values.
• Delete-and-Respond—Delete and charge header received, but save out-of-dialog values to insert in future in-dialog messages.
• None—The Net-Net SBC will not look for P-Charging-Vector headers in non-IMS environments

charging-function-address-mode—Set the state of P-Charging-Function-Address header handling

Default Pass

Values
• Pass—Pass the P-Charging-Function-Address header received in an incoming SIP message untouched as the message is forwarded out of the Net-Net SBC
• Delete—Delete the P-Charging-Function-Address header received in an incoming SIP message before it is forwarded out of the Net-Net SBC
• Insert—Insert the P-Charging-Function-Address header in an incoming SIP message that does not contain the P-Charging-Function-Address header. If the incoming message contains the P-Charging-Function-Address header, the Net-Net SBC will prepend its configured values to the header.
• Insert-Reg-Cache—Remove any existing charging headers and insert previously saved value (including registration cache).
• Delete-and-Respond—Delete and charge header received, but save out-of-dialog values to insert in future in-dialog messages.
• None—The Net-Net SBC will not look for P-Charging-Vector headers in non-IMS environments

ccf-address—Set the CCF address value that will be inserted into the P-Charging-Function-Address header

ecf-address—Set the ECF address value that will be inserted into the P-Charging-Function-Address header

operator-identifier—Set the operator identifier value to be inserted into a P-Charging-Vector header. The direction of the call determines whether this value is inserted into the orig-ioi or the term-ioi parameter in the P-Charging-Vector header. This string value MUST begin with an alpha character.

network-id—Set the value that will be inserted into the P-Visited-Network-ID header

implicit-service-route—Enable or disable implicit Service-Route to Registrar/proxy

Default disabled

Values enabled | disabled

anonymous-priority—Enter the priority level for unknown endpoints\

Default none

Values
• none
• normal
• non-urgent

- urgent
- emergency

max-incoming-conns—Enter the maximum number of simultaneous TCP/TLS connections for this SIP interface.

Default 0 (disabled)

Values Min: 0 / Max: 40000

per-scr-ip-max-incoming-conns—Enter the maximum number of TCP/TLS connections allowed from an endpoint. This parameter is applied only when the `realm-config access-control-trust-level` parameter is set to low or medium.

Default 0 (disabled)

Values Min: 0 / Max: 40000

inactive-conn-timeout—Enter the timeout, measured in seconds, for idle TCP/TLS connections

Default 0 (disabled)

Values Min: 0 / Max: 999999999

untrusted-conn-timeout—Enter the time, in seconds, that you want the Net-Net SBC to keep TCP and TLS connections open for untrusted endpoints.

Default 0

Values Min: 0 / Max: 99999

port-map-start—Set the starting port for the range of SIP ports available for SIP port mapping. A value of 0 disables SIP port mapping.

Default 0

Values Min: 0 / Max: 65535

port-map-end—Set the ending port for the range of SIP ports available for SIP port mapping. A value of 0 disables SIP port mapping. This value must be larger than the port-map-start parameter's value.

Default 0

Values Min: 0 / Max: 65535

term-tgrp-mode—Select the routing mode for terminating trunk group URIs

Default None

Values
- None—Disable routing based on trunk groups
- Iptel—Use trunk group URI routing based on the IPTEL formats
- Egress-uri—Use trunk group URI routing based on the egress URI format

response-map—Enter the name of the response map being applied to this interface

local-response-map—Enter the name of the local response map being applied to this interface

enforcement-profile—Enter the name of the enforcement profile (SIP allowed methods)

route-unauthorized-calls—Enter the name of the SA or SAG to which you want to route unauthorized calls

trans-expire—Enter the TTL in seconds for SIP transactions. This timer controls the following timers specified in RFC 3261:

- Timer B—SIP INVITE transaction timeout
- Timer F—non-INVITE transaction timeout
- Timer H—Wait time for ACK receipt
- Timer TEE—Used to transmit final responses before receiving an ACK

If you set this parameter to 0, then the Net-Net SBC uses the timer value from the global SIP configuration.

Default 0

Values Min: 0 / Max: 999999999

invite-expire—Enter the TTL in seconds for a SIP client/server transaction after receiving a provisional response. You set this timer for the client and the sever by configuring it on the SIP interface corresponding to the core or access side. If you set this parameter to 0, then the Net-Net SBC uses the timer value from the global SIP configuration.

Default 0

Values Min: 0 / Max: 999999999

max-redirect-contacts—Enter the maximum number of contacts or routes for the Net-Net SBC to attempt in when it receives a SIP Redirect (3xx Response). When this number is exceeded, the Net-Net SBC sends a "408 Exhausted Redirects" error to the endpoint. If you leave this parameter set to `0` (default), then the Net-Net SBC will exercise no restrictions on the number of contacts or routes.

Default 0

Values Min: 0 / Max: 10

session-constraints—Enter the name of the session constraints configuration that you want to apply to this SIP interface.

rfc2833-mode—Choose whether the SIP interface will be have exactly the same way as before and the 2833 or UII negotiation will be transparent to the Net-Net SBC, transparent, or whether the sip-interface prefers to use 2833 for DTMF transfer and would signal that in its SDP, preferred. However, the final decision depends on the remote endpoint.

Default transparent

Values
- transparent—The SIP interface behaves exactly the same way as before and the 2833 or UII negotiation is transparent to the Net-Net SBC. This overrides any configuration in the H323-stack even if the stack is configured for "preferred" mode.
- preferred—The SIP interface prefers to use 2833 for DTMF transfer and signals that in its TCS. However, the final decision depends on the remote H323EP
- dual—The Net-Net SBC behaves the same as it does when set to preferred mode and it forwards both the original DTMF mechanism and the translated one to the remote endpoint

rfc2833-payload—Enter the payload type used by the SIP interface in "preferred" `rfc2833-mode`

Default 101

Values Min: 96 / Max: 127

manipulation-string—Enter a string you want to use for header manipulation rules for this sip-interface

tcp-keepalive—Enable or disable standard keepalive probes to determine whether or not connectivity with a remote peer is lost

Default none

Values none | enabled | disabled

add-sdp-invite—Select if you want to enable or disable SDP insertion for INVITEs and ReINVITEs

Values
- disabled—This feature is disabled
- invite—Enable SDP insertion for INVITEs
- reinvite—Enable SDP insertion for ReINVITEs
- both—Enable SDP insertion for both INVITEs and ReINVITEs.

add-sdp-profiles—Enter a list of one or more media profile configurations you want to use when the Net-Net SC inserts SDP into incoming INVITEs that have no SDP. The media profile contains media information the Net-Net SBC inserts in outgoing INVITE.

sip-profile—Enter the SIP profile to apply to this interface.

manipulation-pattern—Enter the regular expression to be used in header manipulation rules.

reg-cache-route—Enable this parameter in order to perform registration cache lookups on top-route

Default disabled

Values enabled | disabled

add-sdp-invite—Select if you want to enable or disable SDP insertion for INVITEs and ReINVITEs

Values
- disabled—This feature is disabled
- invite—Enable SDP insertion for INVITEs
- reinvite—Enable SDP insertion for ReINVITEs
- both—Enable SDP insertion for INVITEs and ReINVITEs

options—Select optional features or parameters. Excluding keywords **`add`** and **`delete`** when a list is already configured replaces the entire list.

[add | delete] <name> [<name>...]

sip-isup-profile—Enter the name of the **sip-isup-profile** to apply to this interface.

sip-dynamic-hnt—Enable this parameter if you want to use adaptive HNT.

Default disabled

Values enabled | disabled

max-nat-interval—Set the amount of time in seconds that testing should not exceed. The Net-Net SBC will keep the expires interval at this value.

Default 3600

Values Min: 0 / Max: 2^{32}-1

nat-int-increment—Set the amount of time in seconds to use as the increment in value in the SIP expires header.

Default 10

Values Min: 0 / Max: 2^{32}-1

nat-test-increment—Set the amount of time in seconds that will be added to the test timer.

Default 30

Values Min: 0 / Max: 2^{32}-1

Path **sip-interface** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-interface.**

Release First appearance: 5.0 / Most recent update: 7.1

Notes This is a multiple instance configuration element.

sip-interface > sip-ports

The **sip-ports** subelement indicates the ports on which the SIP proxy or B2BUA will listen for connections.

Syntax

```
sip-ports <address | port | transport-protocol | allow-anonymous
| tls-profile | select | no | show | done | exit>
```

Parameters

address—Enter the IP address of the host associated with the sip-port entry. This field must match the ip-address field value configured for the home realm network-interface element.

port—Enter the port number for this sip-port

Default 5060

Values Min: 0 / Max: 65535

transport-protocol—Select the transport protocol associated for this sip-port

Default UDP

Values
- TCP
- UDP
- TLS

allow-anonymous—Select the type of anonymous connection from session agents allowed

Default All

Values
- All—Allow all anonymous connections
- Agents-only—Only requests from session agents allowed

• Realm-prefix—Session agents and address matching realm prefix
• Registered—Session agents and registered endpoints (REGISTER allowed from any endpoint)
• Register-prefix—All connects from SAs that match agents-only, realm-prefix, and registered agents

tls-profile—Enter the name of the TLS profile you want applied. This is the same value you enter for the `name` parameter in the `tls-profile` configuration element. This profile is only applied when the `transport-protocol` parameter value is set to TLS.

Path

sip-ports is a subelement under the sip-config element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-interface > sip-ports.**

Release

First appearance: 5.0

Notes

There must be at least one sip-port entry configured within the sip-config and there can be as many entries as necessary for the sip-port. This is a multiple instance configuration element.

sip-isup-profile

Syntax

```
sip-isup-profile <name | mode | isup-version | convert-isup-format
| select | no | show | done | exit>
```

The **sip-isup-profile** element allows you to set up SIP ISUP format interworking. You can apply a configured SIP ISUP profile to a realm, session agent or SIP interface.

name—Enter a unique identifier for this SIP ISUP profile. This name is used when you apply the profile to realms, session agents, and SIP interfaces.

isup-version—Specify the ISUP version to which you want to convert.

Default ansi-2000

Values ansi-2000 | itu-99 | gr-317 | etsi-356

convert-isup-format—Enable or disable this parameter to perform SIP ISUP format version interworking. If this feature is set to **disabled**, the feature is turned off.

Default disabled

Values enabled | disabled

Path

sip-isup-profile is an element under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-isup-profile**.

Release

First appearance: D7.1.0

RTC Status

Supported

Notes

This is a multiple instance configuration element.

sip-manipulation

The **sip-manipulation** feature lets the Net-Net SBC add, modify, and delete SIP headers and SIP header elements.

Syntax

```
sip-manipulation <name | description | header-rules | mime-isup-rules | mime-rules | select | no | show | done | exit>
```

Parameters

name—Enter the name of this list of header rules

description—Enter a description of the sip manipulation rule

header-rules—Access the header rules subelement

mime-isup-rules—Access the mime-isup-rules-rules subelement.

mime-rules—Access the mime-rules subelement.

Path

sip-manipulation is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation.**

Release

First appearance: 5.0

RTC Status

Supported

sip-manipulation > header-rules

The **header-rules** subelement is used to define one action to perform on a given SIP header.

Syntax

```
header-rules <name | header-name | action | match-value | msg-
type | comparison-type | new-value | methods | element-rules |
select | no | show | done | exit>
```

Parameters

name—Enter the name of the header to which this rule applies. This name must match an actual header name.

header-name—Enter the header name for which rule needs to be applied

action—Enter the action you want applied to the header specified in the name parameter

Default None

Values
- Add—Add a new header, if that header does not already exist
- Delete—Delete the header, if it exists
- Manipulate—Manipulate this header according to the element rules configured
- None—Take no action

match-value—Enter the exact value to be matched. The action you specifiy is only performed if the header value matches.

msg-type—Enter the type of message to which this header rule is applied

Default Any

Values
- Any—Both Requests and Reply messages
- Request—Request messages only
- Reply— Reply messages only
- out-of-dialog—Enable diaog-matching header manipulation

comparison-type—Select the type of comparison to be used for the match value

Values
- case-sensitive
- case-insensitive
- pattern-rule
- refer-case-sensitive
- refer-case-insensitive
- boolean

new-value—Enter the new value to be used in add or manipulate actions

methods—Enter a list of SIP methods that this header rule applies to. An empty value applies this header rule to all SIP method messages. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

element-rules—Access the element rules sub-subelement

Path **header-rules** is a subelement under the **sip-manipulation** configuration element, under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > header-rules.**

Release Most recent update: 7.1

RTC Status Supported

sip-manipulation > header-rules > element-rules

The **element-rules** subelement is used to define a list of actions to perform on a given SIP header.

Syntax

```
element-rules <name | parameter-name | type | action | match-val-
type | comparison-type | match-value | new-value | select | no |
show | done | exit>
```

name—Enter the name of the element to which this rule applies. The name parameter does not apply for the following element types: header-value, uri-user, uri-host, uri-port, uri-header. You still need to enter a dummy value here for tracking purposes.

parameter-name—Enter the element parameter name for which rule needs to be applied

type—Select the type of element on which to perform the action

Values
- Header-value—Full value of the header
- Header-param—Parameter portion of the header
- URI-user—User portion of the SIP URI
- URI-host—Host portion of the SIP URI
- URI-port—Port number portion of the SIP URI
- URI-param—Parameter included in the SIP URI
- URI-header—Header included in a request constructed from the URI
- URI-user-param—User parameter of the SIP URI
- Teluri-param—Parameter included in the tel: URI

action—Select the action to take to the element specified in the name parameter, if there is a match value

Default None

Values
- None—No action taken
- Add—Add a new element, if it does not already exist
- Replace—Replace the elements
- Delete-element—Delete the specified element, if it exists
- Delete-header—Delete the specified header, if it exists

match-val-type—Select the type of value that needs to be matched for the action to be performed

Default ANY

Values
- IP—IP address value
- FQDN—FQDN value
- ANY—Both IP or FQDN values

comparison-type—Select the type of comparison to be used for the match value

Values

- case-sensitive
- case-insensitive
- pattern-rule
- refer-case-sensitive
- refer-case-insensitive
- boolean

match-value—Enter the value to match against the element value for a manipulation action to be performed

new-value—Enter the explicit value for a new element or replacement value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

•Use double quotes around string values.

•Pre-defined parameters always start with a $. Valid pre-defined parameters are:

Parameter	Description
$ORIGINAL	Original value of the element is used.
$LOCAL_IP	Local IP address is used when you receive an inbound address.
$REMOTE_IP	Remote IP address is used.
$REMOTE_VIA_HOST	Remote VIA host part is used.
$TRUNK_GROUP	Trunk group is used.
$TRUNK_GROUP_CONTEXT	Trunk group context is used.

•Operators are:

Operator	Description
+	Append the value to the end. For example: “acme”+”packet” generates “acmepacket”
+^	Prepends the value. For example: “acme”+^”packet” generates “packetacme”
-	Subtract at the end. For example: “112311”-”11” generates “1123”
-^	Subtract at the beginning. For example: “112311”-^”11” generates “2311”

Path

element-rules is a sub-subelement under the **header-rules** subelement under the **sip-manipulation** configuration element, under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > header-rules > element-rules.**

Release

First appearance: 5.0

sip-manipulation>mime-isup-rules

The **mime-isup-rules** configuration allows you to perform HMR operations on SIP ISUP binary bodies.

Syntax

```
sip-mime-isup-rules <name | content-type | isup-spec | isup-msg-
types | action | match-value | comparison-type | msg-type |
methods | new-value | mime-headers | isup-param-rules | select |
no | show | done | exit>
```

Parameters

name—Enter a unique identifier for this MIME ISUP rule.

content-type—Enter the content type for this MIME rule. This value refers to the specific body part in the SIP message body that is to be manipulated.

isup-spec—Enter the ISUP encoding specification for the ISUP body; this specifies how the Net-Net SBC is to parse the binary body.

Default ansi-2000

Values ansi-2000 | itu-t926

isup-msg-types—Enter the specific ISUP message types (such as IAM and ACM). that the Net-Net SBC uses with the msg-type parameter (which identifies the SIP message) in the matching process. The values of this parameter are a list of numbers rather than enumerated values because of the large number of ISUP message types. There is no default for this parameter.

Values Min: 0 / Max: 255

action—Select the type of action you want to be performed.

Default none

Values add | delete | manipulate | store | sip-manip | find-replace-all | none

match-value—Enter the value to match against the body part in the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

comparison-type—Select a method to determine how the body part of the SIP message is compared. This choice dictates how the Net-Net SBC processes the match rules against the SIP header.

Default case-sensitive

Values case-sensitive | case-insensitive | refer-case-sensitive | refer-case-insensitive | boolean

msg-type—Enter the SIP message type on which you want the MIME rules to be performed.

Default any

Values any | request | reply

methods—Enter the list of SIP methods to which the MIME rules apply, such as INVITE, ACK, or CANCEL. There is no default for this parameter.

new-value—When the **action** parameter is set to **add** or to **manipulate**, enter the new value that you want to substitute.

mime-header-rules—Access the **mime-headers** subelement.

isup-param-rules—Access the **isup-param-rules** subelement.

Path

sip-mime-isup-rules is a subelement under the **sip-manipulation** element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-isup-rules**.

Release

First appearance: D7.1.0

RTC Status

Supported

Notes

This is a multiple instance configuration element.

sip-manipulation>mime-isup-rules>isup-param-rules

The **isup-parameter-rules** element is used to create, manipulate, and store different parameters in the body of an ISUP message.

Syntax

```
sip-isup-param-rules <name | type | format | action | comparison-
type | match-value | new-value | select | no | show | done | exit>
```

Parameters

name—Enter a unique identifier for this ISUP parameter rule. This parameter is required and has no default.

type—Using ISUP parameter mapping, enter the ISUP parameters on which you want to perform manipulation. This parameter takes values between 0 and 255, and you must know the correct ISUP mapping value for your entry. The Net-Net SBC calculates the offset and location of this parameter in the body. Note that the value returned from the body does not identify the type or length, only the parameter value. For example, a parameter-type value of 4 acts on the Called Party Number parameter value.

Default 0

Values Min: 0 / Max: 255

format—Enter the method for the Net-Net SBC to convert a specific parameter to a string representation of that value.

Default hex-ascii

Values number-param | hex-ascii | binary-ascii | ascii-string | bcd

action—Choose the type of action you want to be performed.

comparison-type—Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Net-Net SBC processes the match rules against the SIP header.

Default case-sensitive

Values case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

match-value—Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

new-value—When the action parameter is set to **add** or to **manipulate**, enter the new value that you want to substitute.

Path

isup-param-rules is a subelement under the **sip-manipulation>mime-isup-rules** element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-isup-rules > isup-param-rules**.

Release

First appearance: D7.1.0

RTC Status

Supported

Notes

This is a multiple instance configuration element.

sip-manipulation>mime-isup-rules>mime-header-rules

The **mime-header-rules** subelement of **mime-isup-rules** allows you to configure a SIP header manipulation to add an ISUP body to a SIP message.

Syntax

```
sip-mime-header-rules <name | mime-header-name | action |
comparison-type | match-value | new-value | select | no | show |
done | exit>
```

Parameters

name—Enter a unique identifier for this MIME header rule.

mime-header-name—Enter the value used for comparison with the specific header in the body part of the SIP message. There is no default for this parameter.

action—Choose the type of action you want to be performed.

Default none

Values add | replace | store | sip-manip | find-replace-all | none

comparison-type—Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Net-Net SBC processes the match rules against the SIP header.

Default case-sensitive

Values case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

match-value—Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

new-value—When the **action** parameter is set to **add** or to **manipulate**, enter the new value that you want to substitute.

Path

mime-headers is a subelement under the **sip-manipulation>mime-isup-rules** element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-isup-rules > mime-headers**.

Release

First appearance: D7.1.0

RTC Status

Supported

Notes This is a multiple instance configuration element.

sip-manipulation>mime-rules

Syntax

```
mime-rules <name | content-type | action | match-value |
comparison-type | msg-type | methods | new-value | mime-header-
rules | select | no | show | done | exit>
```

The **mime-rules** configuration element allows you to set parameters in the MIME rules that the Net-Net SBC uses to match against specific SIP methods and message types.

Parameters

name—Enter a unique identifier for this MIME rule.

content-type—Enter the content type for this MIME rule. This value refers to the specific body part in the SIP message body that is to be manipulated.

action—Choose the type of action you want to be performed.

Default none

Values add | delete | manipulate | store | sip-manip | find-replace-all | none

match-value—Enter the value to match against the body part in the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

comparison-type—Select a method to determine how the body part of the SIP message is compared. This choice dictates how the Net-Net SBC processes the match rules against the SIP header.

Default case-sensitive

Values case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

msg-type—Enter the SIP message type on which you want the MIME rules to be performed.

Default any

Values any | request | reply

methods—Enter the list of SIP methods to which the MIME rules apply. There is no default for this parameter.

new-value—When the action parameter is set to **add** or to **manipulate**, enter the new value that you want to substitute.

mime-header-rules—Access the mime-header-rules subelement.

format—Specify the encode/decode format of the body.

Default none

Values ascii-string | hex-ascii | binary-ascii

Path **mime-rules** is a subelement under the **sip-manipulation** element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-rules**.

Release First appearance: D7.1.0

RTC Status Supported

Notes This is a multiple instance configuration element.

sip-manipulation>mime-rules>mime-header-rules

Syntax

```
sip-mime-header-rules <name | mime-header | action | comparison-
type | match-value | new-value | select | no | show | done | exit>
```

The **mime-header-rules** configuration allows you to configure MIME headers, which operate on the specific headers in the match body part of the SIP message.

Parameters

name—Enter a name for this MIME header rule. This parameter is required and has no default.

mime-header—Enter the value to be used for comparison with the specific header in the body part of the SIP message. There is no default for this parameter.

action—Choose the type of action you want to be performed.

Default none

Values add | delete | manipulate | store | sip-manip | find-replace-all | none

comparison-type—Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Net-Net SBC processes the match rules against the SIP header.

Default case-sensitive

Values case-sensitive | case-insensitive | refer-case-sensitive | refer-case-insensitive | pattern-rule | boolean

match-value—Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

new-value—When the action parameter is set to **add** or to **manipulate**, enter the new value that you want to substitute.

Path **mime-headers** is a subelement under the **sip-manipulation>mime-rules** element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-rules>mime-headers**.

Release First appearance: D7.1.0

RTC Status Supported

Notes This is a multiple instance configuration element.

sip-nat

The **sip-nat** element is used for configuring SIP-NAT across realms.

Syntax

```
sip-nat <realm-id | domain-suffix | ext-proxy-address | ext-
proxy-port | ext-address | home-address | home-proxy-address |
home-proxy-port | route-home-proxy | address-prefix | tunnel-
redirect | use-url-parameter | parameter-name | user-nat-tag |
host-nat-tag | headers | select | no | show | done | exit>
```

Parameters

realm-id—Enter the name of the external realm. This required realm-id must be unique.

domain-suffix—Enter the domain name suffix of the external realm. This suffix is appended to encoded hostnames that the SIP-NAT function creates. This is a required field.

ext-proxy-address—Enter the IP address of the SIP element (a SIP proxy) in the external network. This is a required field. Entries in this field must follow the IP Address Format.

ext-proxy-port—Enter the port number of the SIP element (a SIP proxy) in the external network

Default 5060

Values Min: 0 / Max: 65535

ext-address—Enter the IP address on the media interface in the external realm. This required entry must follow the IP address format.

home-address—Enter the IP address on the media interface in the home realm. The value entered in this field must be different from the value configured as the IP address of the home realm network-interface element. This required entry must follow the IP address format.

home-proxy-address—Enter the IP address for the home proxy (from the perspective of the external realm). An empty home-proxy-address field value signifies that there is no home proxy, and the external address will translate to the address of the Net-Net SBC's SIP proxy. Entries in this field must follow the IP Address Format. This is an optional parameter.

home-proxy-port—Enter the home realm proxy port number. This is an optional parameter.

Default 0

Values Min: 0 / Max: 65535

route-home-proxy—Enable or disable the routing of requests from a given SIP-NAT to the home proxy

Default disabled

Values enabled | disabled | forced

address-prefix—Enter the address prefix subject to SIP-NAT encoding. This field is used to override the address prefix from the realm config for the purpose of SIP-NAT encoding.

<ipv4[/num-bits]>

Default *

Values
- <IP address>:[/num-bits]
- *—Indicates that the addr-prefix in the realm-config is to be used
- 0.0.0.0—Indicates that addresses NOT matching the address prefix of the home realm should be encoded

tunnel-redirect—Enable or disable the NAT functionality on certain headers in a 3xx Response message received when sent to the initiator of the SIP INVITE message

Default disabled

Values enabled | disabled

use-url-parameter—Set how SIP headers use the URL parameter (parameter-name) for encoded addresses that the SIP-NAT function creates. A value of none indicates that Net-Net SBC functionality remains unchanged and results in the existing behavior of the Net-Net SBC. From-to and phone are used for billing issues related to extracting digits from the encoded portion of SIP messages along with the parameter-name field.

Default None

Values
- None
- From-to
- Phone
- All

parameter-name—Enter the URL parameter name used when constructing messages. This field is used in SIP-NAT encoding addresses that have a use-url-parameter field value of either from-to or all. This field can hold any value, but it should not be a recognized name that another proxy might use.

user-nat-tag—Enter the username prefix used for SIP URLs

Default -acme-

host-nat-tag—Enter the hostname prefix used for SIP URLs

Default ACME-

headers—Enter the SIP headers to be affected by the Net-Net SBC's SIP-NAT function. The URIs in these headers will be translated and encrypted, and encryption will occur according to the rules of this SIP-NAT element. Entries in this field must follow this format: <header-name>=<tag>. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

The following lists valid SIP headers and their abbreviations:

- Via—v
- Call-ID—i
- Contact—m
- Record-Route—no abbreviation
- Route—no abbreviation
- From—f

- To—t
- Reply-To—no abbreviation
- Replaces—no abbreviation
- Refer-To—r

The default behavior receives normal SIP-NAT treatment. SIP-NAT header tags for SIP IP address replacement are listed below:

–fqdn-ip-tgt—Replaces the FQDN with the target address

–fqdn-ip-ext—Replaces the FQDN with the SIP-NAT external address

–ip-ip-tgt—Replaces FROM header with target IP address

–ip-ip-ext—Replaces FROM header with SIP-NAT external address

Path

sip-nat is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-nat.**

Release

First appearance: 5.0

Notes

This is a multiple instance configuration element.

sip-profile

The **sip-profile** configuration element allows you to configure SIP profiles on the Net-Net SBC.

Syntax

```
sip-profile <name | ingress-conditional-cac-admit | egress-
conditional-cac-admit | forked-cac-bw | redirection | select | no
| show | done | exit>
```

Parameters

name—Enter the name of this sip-profile. You will need this SIP profile's **name** when you want to apply this profile to a realm, SIP interface, or SIP session agent

ingress-conditional-cac-admit—Set this parameter to enabled if you want to use conditional bandwidth CAC for media release on the ingress side of a call. Set this parameter to inherit if you want the value inherited from the realm-config, sip-interface, or sip-interface

Values enabled | disabled | inherit

Default inherit

egress-conditional-cac-admit—Set this parameter to enabled if you want to use conditional bandwidth CAC for media release on the egress side of a call

Values enabled | disabled | inherit

Default inherit

forked-cac-bw—Select the way you want the CAC bandwidth to be configured between the forked sessions

Values • per-session—The CAC bandwidth is configured per forked session

• shared—The CAC bandwidth is shared across the forked sessions
• inherit—Inherit value from realm-config or sip-interface

Default inherit

redirection— Choose the redirection mode you want to use: **none** (default), **isup**, or **redirection**. The **inherit** value is reserved for future use.

Default none

Values none | isup | redirection

Notes When you set this parameter to **isup**, you should configure along with it a SIP ISUP profile; this will avoid any possible incompatibility when support for this feature expands (as expected).

Path **sip-profile** is an element of the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-profile**.

Release First appearance: D7.0

RTC Status Supported

sip-q850-map

The **sip-q850-map** configuration element is used to map SIP response codes to q850 cause codes.

Syntax

```
sip-q850-map <entries | select | no | show | done | exit>
```

entries—Enter the **entries** configuration subelement

Path **sip-q850-map** is an element under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > q850-sip-map**.

Release First appearance: D6.0.1

sip-q850-map>entries

The **entries** subelement is used to create the mapping of SIP response codes to q850 cause codes.

Syntax

```
entries <q850-cause | sip-status | q850-reason | select | no |
show | done | exit>
```

q850-cause—Enter the q850 cause code to map to a SIP reason code

sip-status—Enter the SIP response code that maps to this q850 cause code

Values Min: 100 / Max: 870

q850-reason—Enter a description to accompany the mapped SIP response code

Path

entries is a subelement of the **sip-q850-map** element, under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > q850-sip-map > entries.**

Release

First appearance: D6.0.1

sip-response-map

The **sip-response-map** element establishes SIP response maps associated with the upstream session agent.

Syntax

```
sip-response-map <name | entries | edit | select | no | show |
done | exit>
```

Parameters

name—Enter the name of the SIP response map

entries—Access the entries subelement

Path

sip-response-map is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-response-map.**

Release

First appearance: 5.0

Notes

This is a multiple instance configuration element.

sip-response-map > entries

The **entries** subelement establishes the status code(s) for both received and transmitted messages and the reason phrase(s) of a SIP response map.

Syntax

```
entries <recv-code | xmit-code | rhdr-protocol | rhdr-cause |
rhdr-text | reason | method | register-response-expires | select
| no | show | done | exit>
```

Parameters

recv-code—Enter the original SIP response code received

Values Min: 1 / Max: 699

xmit-code—Enter the setting of translated SIP response code transmitted

Values Min: 1 / Max: 699

reason—Enter the setting of translated response comment or reason phrase to send denoted by an entry in quotation marks

method—Enter the SIP method name you want to use for this SIP response map entry

register-response-expires—Enter the time you want to use for the expires time when mapping the SIP method you identified in the method parameter. By default, the expires time is the Retry-After time (if there is one in the response) of the expires value in the Register request (if there is no Retry-After expires time). Any value you configure in this parameter (when not using the defaults) should never exceed the Register request's expire time.

Values Min: 0 / Max: 999999

rhdr-protocol—Enter the reason header protocol type

rhdr-cause—Enter the reason header cause value

Values Min: 0 / Max: 999999

rhdr-text—Enter the value to appear in the 'reason text' field of the Reason Header in the SIP response

Path **entries** is a subelement of the sip-response-map element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-response-map > entries**.

Release First appearance: 5.0

Notes This is a multiple instance configuration element.

snmp-community

The **snmp-community** element defines the NMSs from which the Net-Net SBC will accept SNMP requests.

Syntax

```
snmp-community <community-name | access-mode | ip-addresses |
select | no | show | done | exit>
```

Parameters

community-name—Enter the name of the SNMP community to which an NMS and the SD belong. This required entry must follow the Name Format. The community-name field values must be unique.

access-mode—Select the access level for each snmp-community element

Values • READ-ONLY—Allow GET requests

ip-addresses—Enter the IP address(es) for SNMP communities for authentication purposes. Entries must follow the IP Address Format. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <address> [<address>...]

Path **snmp-community** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > snmp-community.**

Release First appearance: 5.0

Notes This is a multiple instance configuration element.

soap-config

The **soap-config** element allows you to configure SOAP settings on the Net-Net SBC.

Syntax

```
soap-config <http-enabled | idle-time | select | no | show | done
| exit>
```

Parameters

http-enabled—Enable or disable the Soap Server over HTTP

Default disabled

Values enabled | disabled

idle-time—Enter the length of time a connection will stay up if inactive, measured in minutes

Default 10

Values Min: 0 / Max: 43200

Path **soap-config** is an element under the system path. The full path from the topmost prompt is: **configure terminal > system > soap-config**.

Release First appearance: 5.1

static-flow

The **static-flow** element sets preconfigured flows that allow a specific class of traffic to pass through the Net-Net SBC unrestricted.

Syntax

```
static-flow <in-realm-id | description | in-source | in-
destination | out-realm-id | out-source | out-destination |
protocol | alg-type | start-port | end-port | flow-time-limit |
initial-guard-timer | subsq-guard-timer | average-rate-limit |
select | no | show | done | exit>
```

Parameters

in-realm-id—Enter the ingress realm or interface source of packets to match for static flow translation. This in-realm-id field value must correspond to a valid identifier field entry in a realm-config. This is a required field. Entries in this field must follow the Name Format.

description—Provide a brief description of this static-flow configuration. This is an optional parameter.

in-source—Enter the incoming source IP address and port of packets to match for static flow translation. An IP address of 0.0.0.0 matches any source address. Port 0 matches packets received on any port. The port value has no impact on system operation if either ICMP or ALL is the selected protocol. The in-source parameter takes the format:

```
in-source <ip-address>[:<port>]
```

Default 0.0.0.0

in-destination—Enter the incoming destination IP address and port of packets to match for static-flow translation. An IP address of 0.0.0.0 matches any source address. Port 0 matches packets received on any port. The port value has no impact on system operation if either ICMP or ALL is the selected protocol. The in-destination parameter takes the format:

```
in-destination <ip-address>[:<port>]
```

Default 0.0.0.0

out-realm-id—Enter the ingress realm or interface source of packets to match for static flow translation. This out-realm-id field value must be a valid identifier for a configured realm. This required entry must follow the Name Format.

out-source—Enter the outgoing source IP address and port of packets to translate to for static flow translation. IP address of 0.0.0.0 translates to any source address. Port 0 translates to packets sent on any port. The port value has no impact on system

operation if either ICMP or ALL is the selected protocol. The out-source parameter takes the format:

```
out-source <ip-address>[:<port>]
```

Default 0.0.0.0

out-destination—Enter the outgoing destination IP address and port of packets to translate to for static-flow translation. An IP address of 0.0.0.0 matches any source address. Port 0 translates to packets sent on any port. The port value has no impact on system operation if either ICMP or ALL is the selected protocol. The out-destination parameter takes the format:

```
out-destination <ip-address>[:<port>]
```

Default 0.0.0.0

protocol—Select the protocol for this static-flow. The protocol selected must match the protocol in the IP header. The protocol remains the same for the inbound and outbound sides of the packet flow.

Default UDP

Values
- UDP—UDP used for this static-flow element
- TCP—TCP used for this static-flow element
- ICMP—ICMP used for this static-flow element
- ALL—Static-flow element can accept flows via any of the available protocols

alg-type—Select the type of NAT ALG to use

Values
- NAPT—Configure as NAPT ALG
- TFTP—Configure as TFTP ALG

start-port—Enter the internal starting ALG ephemeral port

Default 0

Values Min: 0 / Max: 65535

end-port—Enter the internal ending ALG ephemeral port

Default 0

Values Min: 0 / Max: 65535

flow-time-limit—Enter the time limit, in seconds, for ALG flows

Default 0

Values Min: 0 / Max: 999999999

initial-guard-timer—Enter the initial guard timer, in seconds, for ALG flows

Default 60

Values Min: 0 / Max: 999999999

subsq-guard-timer—Enter the subsequent guard timer, in seconds for ALG flows

Default 60

Values Min: 0 / Max: 999999999

average-rate-limit—Enter the maximum speed in bytes per second for this static flow

Default 0

Default Min: 0 / Max: 999999999

Path **static-flow** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > static-flow.**

Release First appearance: 5.0

Notes This is a multiple instance configuration element.

steering-pool

The **steering-pool** element defines sets of ports that are used for steering media flows through the Net-Net SBC. The Net-Net SBC can provide packet steering in order to ensure a determined level of quality or routing path.

Syntax

```
steering-pool <ip-address | start-port | end-port | realm-id |
network-interface | select | no | show | done | exit>
```

Parameters

ip-address—Enter the target IP address of the steering pool. This required entry must follow the IP Address Format. The combination of entries in the ip-address, start-port, and realm-id fields must be unique. No two steering-pool elements can have the same entries in the ip-address, start-port, and realm-id fields.

start-port—Enter the port number that begins the range of ports available to this steering pool element. This is a required entry. The steering pool will not function properly unless this entry is a valid port.

Default 0

Values Min: 1 / Max: 65535

end-port—Enter the port number that ends the range of ports available to this steering-pool element. This is a required field. The steering-pool element will not function properly unless this field is a valid port value.

Default 0

Values Min: 1 / Max: 65535

realm-id—Enter the steering-pool element's realm identifier used to restrict this steering pool to only the flows that originate from this realm. This required entry must be a valid identifier of a realm.

network-interface—Enter the name of network interface that this steering pool directs its media toward. A valid value for this parameter must match a configured name parameter in the network-interface configuration element. This is an optional parameter.

Path **steering-pool** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > steering-pool.**

Release First appearance: 5.0

Notes This is a multiple instance configuration element.

surrogate-agent

The **surrogate-agent** configuration element allows you to configure surrogate registration on the Net-Net SBC.

Syntax

```
surrogate-agent <register-host | register-user | description |
realm-id | state | customer-host | customer-next-hop | register-
contact-host | register-contact-user | password | register-
expires | replace-contact | options | route-to-registrar | aor-
count | auth-user | max-register-attempts | register-retry-time |
count-start | select | no | show | done | exit>
```

Parameters

register-host—Enter the registrar's hostname to be used in the Request-URI of the REGISTER request. This name is also used as the host portion of the AoR To and From headers.

register-user—Enter the user portion of the AoR.

description—Enter a description of this surrogate agent. This is an optional parameter.

realm-id—Enter the name of realm where the surrogate agent resides (where the IP-PBX proxy resides).

state—Enable or disable the use of the surrogate agent by the application.

Default enabled

Values enabled | disabled

customer-host—Enter the domain or IP address of the IP-PBX, which is used to determine whether it is different than the one used by the registrar. This is an optional parameter.

customer-next-hop—Enter the next hop to this surrogate agent.

> *Note: Even though the customer-next-hop field allows specification of a SAG or FQDN, the functionality will only support these values if they resolve to a single IP address. Multiple IP addresses, via SAG, NAPTR, SRV, or DNS record lookup, are not allowed.*

register-contact-host—Enter the hostname to be used in the Contact-URI sent in the REGISTER request. This should always point to the Net-Net SBC. If specifying a IP address, use the egress interface's address. If there is a SIP NAT on the registrar's side, use the home address in the SIP NAT.

register-contact-user—Enter the user part of the Contact-URI that the Net-Net SBC generates.

password—If you are configuring the auth-user parameter, enter the password used in case the registrar sends the 401 or 407 response to the REGISTER request.

register-expires—Enter the expires in seconds to be used in the REGISTER requests.

Default 600,000 (1 week)

Values Min: 0 / Max: 999999999

replace-contact—Specify whether the Net-Net SBC needs to replace the Contact in the requests coming from the surrogate agent. If this is enabled, Contact will be replaced with the Contact-URI the Net-Net SBC sent in the REGISTER request.

Default disabled

Values enabled | disabled

options—Select optional features or parameters. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <options> [<option>...]

route-to-registrar—Indicates whether requests coming from the surrogate agent should be routed to the registrar if they are not explicitly addressed to the Net-Net SBC.

Default enabled

Values enabled | disabled

aor-count—Enter the number of registrations to do on behalf of this IP-PBX. If you enter a value greater then 1 (default), the Net-Net SBC increments the register-user and the register-contact-user values by that number. For example, if this count is 3 and register-user is john then users for three different register messages will be john, john1, john2. It does the same for the register-contact-user values.

Default 1

Values Min: 0 / Max: 999999999

auth-user—Enter the authentication user name you want to use for the surrogate agent. This name is used when the Net-Net SBC receives a 401or 407 response to the REGISTER request and has to send the REGISTER request again with the Authorization or Proxy-Authorization header. The name you enter here is used in the Digest username parameter. If you do not enter a name, the Net-Net SBC uses the value of the register-user parameter.

max-register-attempts—Enter the total number of times to attempt a successful registration. A value of 0 indicates there is no limit.

Default 3

Values Min: 0 / Max: 10

register-retry-time—Enter the number of seconds to wait after a failed registration before you reattempt.

Default 300

Values Min: 30 / Max: 3600

count-start—Enter the starting value for numbering when performing multiple registrations

Default 1

Values Min: 0 / Max: 999999999

Path

surrogate-agent is an element under the session-router path. The full path from the topmost prompt is: **configure terminal > session-router > surrogate-agent.**

Release

First appearance: 5.1

system-access-list

The **system-access-list** configuration element allows you to configure system access control of the management interface on the Net-Net SBC. Once configured, any access from hosts that are not part of the system access IP address or subnet are denied. When this element is not configured, any host can access management ports.

Syntax

```
system-access-list <source-address | netmask | description |
select | no | show | done | exit>
```

Parameters

source-address—Enter the IP address representing the source network for which you want to allow traffic over the management interface

netmask—Enter the netmask portion of the source network for the traffic you want to allow. The netmask is in dotted decimal notation.

description—Provide a brief description of this system-access-list configuration. This is an optional parameter.

Path

system-access-list is an element under the **system** path. The full path from the topmost ACLI prompt is: **configure terminal > system > system-access-list**.

Release

First appearance: 6.0

RTC Status

Supported

system-config

The **system-config** element establishes general system information and settings.

Syntax

```
system-config <description | location | mib-system-contact | mib-
system-name | mib-system-location | snmp-enabled | enable-snmp-
auth-traps | enable-snmp-syslog-notify | enable-snmp-monitor-
traps | enable-env-monitor-traps | snmp-syslog-his-table-length |
snmp-syslog-level | system-log-level | process-log-level |
process-log-mode | process-log-ip-address | process-log-port |
syslog-servers | log-compression | task-logging | telnet-timeout
| console-timeout | restart | exceptions | tcu-double-active |
failover | miu0-monitor-ip-address | miu1-monitor-ip-address |
xcode-path-monitor | testman | source-routing | dump-logs-on-
failure | alarm-threshold | call-tracing | call-trace-mode |
debug-timeout | cli-audit-trail | trap-event-lifetime | select |
no | show | done | exit>
```

Parameters

description—Describe the Net-Net SBC briefly. Entries must follow the Text Format.

location—Enter the physical location of the Net-Net SBC used for informational purposes. Entries must follow the Text Format.

mib-system-contact—Enter the contact information for this Net-Net SBC for SNMP purposes. This field value is the value reported for MIB-II when an SNMP GET is issued by the NMS. Entries must follow the Text Format.

mib-system-name—Enter the identification of the Net-Net SBC for SNMP purposes. By convention, this is the node's FQDN. If this field remains empty, the Net-Net SBC name that appears in SNMP communications will be the target name configured in the boot parameters and nothing else.

mib-system-location—Enter the physical location of the Net-Net SBC for SNMP purposes. This parameter has no direct relation to the location field identified above. Entries must follow the Text Format.

snmp-enabled—Enable or disable SNMP on the system. If SNMP is enabled, then the system will initiate the SNMP agent. If SNMP is disabled, then the SNMP agent will not be initiated, and the trap-receiver and snmp-community elements will not be functional.

Default enabled

Values enabled | disabled

enable-snmp-auth-traps—Enable or disable SNMP authentication traps

Default disabled

Values enabled | disabled

enable-snmp-syslog-notify—Enable or disable the sending of syslog notifications to an NMS via SNMP; determines whether SNMP traps are sent when a Net-Net SBC generates a syslog message

Default disabled

Values enabled | disabled

enable-snmp-monitor-traps—Enable or disable the sending of traps out in ap-smgmt.mib trap. (See 400-0010-00, MIB Reference Guide for more information)

Default disabled

Values enabled | disabled

enable-env-monitor-traps—Enable or disable the sending of the environmental monitoring MIB from the Net-Net SBC. This trap will be sent any time there is a change in state in fan speed, temperature, voltage (SD 2 only), power supply (SD 1 for rev 1.32 or higher, SD 2 w/QoS for rev 1.32 or higher, SD II no QoS for rev 1.3 or higher), phy-card insertion, or I^2C bus status. If this parameter is set to enabled, fan speed, temperature, and power supply notifications are not sent out in other traps.

Default disabled

Values enabled | disabled

snmp-syslog-his-table-length—Enter the maximum entries that the SNMP Syslog message table contains. The system will delete the oldest table entry and add the newest entry in the vacated space when the table reaches maximum capacity.

Default 1

Min: 1 / Max: 500

snmp-syslog-level—Set the log severity levels that send syslog notifications to an NMS via SNMP if enable-snmp-syslog-notify is set to enabled

If the severity of the log being written is of equal or greater severity than the snmp-syslog-level value, the log will be written to the SNMP syslog history table.

If the severity of the log being written is of equal or greater severity than the snmp-syslog-level field value and if enabled-snmp-syslog-notify field is set to enabled, the system will send the syslog message to an NMS via SNMP.

If the severity of the log being written is of lesser severity than the snmp-syslog-level value, then the log will not be written to the SNMP syslog history table and it will be disregarded.

Default Warning

Values
- Zero
- Emergency
- Critical
- Major
- Minor
- Warning
- Notice
- Info
- Trace
- Debug

system-log-level—Set the system-wide log severity levels written to the system log

Default Warning

Values Zero | Emergency | Critical | Major | Minor | Warning | Notice | Info | Trace | Debug

process-log-level—Set the default log level that tasks running on the Net-Net SBC start

Default Notice

Values Zero | Emergency | Critical | Major | Minor | Warning | Notice | Info | Trace | Debug

process-log-mode—Set the default starting log mode for all tasks

Default local

Values local | remote | both

process-log-ip-address—Enter the IP address of server where process log files are stored. Entries must follow the IP Address Format. The default value of 0.0.0.0 causes log messages to be written to the local log file.

Default 0.0.0.0

process-log-port—Enter the port number associated with server IP address where process log files are stored. The default value of 0 writes log messages to the local log file.

Default 0

Values Min: 1025 / Max: 65535, & 0

syslog-servers—Enter a list of syslog servers. Excluding keywords **`add`** and **`delete`** when a list is already configured replaces the entire list.

Values [add|delete] <ip-addr>[:<port>[:<facility>]] [...]

log-compression—Enable or disable the compression of your archived log files

Default enabled

Values enabled | disabled

task-logging—Access the task-logging subelement

telnet-timeout—Enter the telnet session inactivity timeout

Default 0

Values Min: 0 / Max: 86400

console-timeout—Enter the console session inactivity timeout

Default 0

Values Min: 0 / Max: 86400

restart—Enable or disable the rebooting of cards if a task failure is detected on the Net-Net SBC. This is for debugging purposes only.

Default enabled

Values enabled | disabled

exceptions—Enable or disable a list of tasks to ignore if they fail. This is for debugging purposes only.

Values enabled | disabled

tcu-double-active—Enable or disable the lock in the TCU HA for 2+1 operation

Default disabled

Values enabled | disabled

failover—Enable or disable automatic switchover on card failure on the Net-Net SBC

Default enabled

Values enabled | disabled

miu0-monitor-ip-address—Enter the remote IPV4 address used to verify MIU0 link health

Default 0.0.0.0

miu1-monitor-ip-address—Enter the remote IPV4 address used to verify MIU1 link health

Default 0.0.0.0

xcode-path-monitor—Enable or disable the health monitor of xcode path

Default enabled

Values enabled | disabled

testman—Enable or disable the unit test suite. This command is for debugging purposes only.

Default disabled

Values enabled | disabled

source-routing—Enable or disable the routing of outgoing HIP packets to the interface associated with the source IP address

Default disabled

Values enabled | disabled

Default

dump-logs-on-failure—Enable or disable the panic log feature on the Net-Net SBC

Default disabled

Values enabled | disabled

alarm-threshold—Select the remote ACP control for user-configurable alarmthresholds

Values
- type—CPU, memory, session
- severity—Minor, major, critical

call-tracing—Enable or disable call tracing on the Net-Net SBC

Default disabled

Values enabled | disabled

call-trace-mode—Set the call trace log mode that you want to use

Default local

Values
- 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

debug-timeout—Enter the debug timeout, in seconds.

Default 0 (disabled)

Values Min: 0 / Max: 65535

trap-event-lifetime—Set this parameter to the number of days you want to keep trap event information. Leaving this parameter set to 0 (default) turns alarm synchronization off.

Default 0

Values Min: 0 / Max: 7

cli-audit-trail—Set this parameter to enabled for the CLI audit trail feature to run.

Default enabled

Values disabled | enabled

Path

system-config is an element under the system system path. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config.**

Release

First appearance: 5.0 / Most recent update: 7.1

Notes

This is a single instance configuration element.

system-config>alarm-threshold

The **alarm-threshold** configuration subelement allows you to manually configure some alarm thresholds, overriding the default health degradations. The configurable alarms are CPU usage, memory usage, and licensed session capacity.

Syntax

```
alarm-threshold <type | severity | value | select | no | show |
done | exit>
```

type—Enter the type of threshold you wish to configure

Default cpu

Values
- cpu
- memory
- sessions

severity—Enter the severity level you will configure a custom health deduction for.

Default minor

Values
- minor
- major
- critical

value—Enter the percent of resource (type) in use that triggers the configured alarm (severity).

Default 0

Values Min: 0 / Max: 100

Path **alarm-threshold** is a subelement under the system>system-config path. The full path from the topmost prompt is: **configure terminal > system > system-config > alarm-threshold.**

Release First appearance: 5.1

system-config>task-logging

The **task-logging** subelement allows you to configure task logging on the Net-Net SBC.

Syntax

```
task-logging <task-name | level | mode | log-address | facility-
logging | internal-trace | select | no | show | done | exit>
```

Parameters

task-name—Enter the name of the task you are logging

level—Select the log level of the task

Values Zero | Emergency | Critical | Major | Minor | Warning | Notice | Info | Trace | Debug

mode—Select the task logging mode

Values local | remote | both

log-address—Enter the remote log server address and port

facility-logging—Access the facility-logging subelement

internal-trace—Enable the Net-Net SBC to generate a protocol trace for this task

Default disabled

Values enabled | disabled

Path **task-logging** is a subelement under the system-config element. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > task-logging.**

Release First appearance: 5.0

system-config>task-logging>facility-logging

The **facility-logging** subelement allows you to configure facility logging on the Net-Net SBC.

Syntax

```
facility-logging <facility | level | mode | log-address | select |
no | show | done | exit>
```

Parameters

facility—Enter the log type

level—Enter the logging level

mode—Select the logging mode

Values local | remote | both

log-address—Enter the remote log server address and port

Path **facility-logging** is a subelement under the system-config>task-logging element. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > task-logging>facility-logging.**

Release First appearance: 5.0

timezone

The **timezone** configuration element sets the time zone and daylight savings time on the Net-Net SBC.

Syntax

```
timezone <name | minutes-from-utc | dst-start-month | dst-start-
day | dst-start-hour | dst-end-month | dst-end-day | dst-end-hour
| select | no | show | done exit>
```

Parameters

name—Enter the name of the timezone

Values 1-10 characters

minutes-from-utc—Enter the number of minutes from UTC

Default 0

Values -720 - 720

dst-start-month—Enter the month that DST starts

Default 0

Values 1-12

dst-start-day—Enter the day of the month that DST starts

Default 0

Values 1-31

dst-start-hour—Enter the hour of the day that DST starts

Default 0

Values 0-24

dst-end-month—Enter the month that DST starts

Default 0

Values 1-12

dst-end-day—Enter the day of the month that DST starts

Default 0

Values 1-31

dst-end-hour—Enter the hour of the day that DST starts

Default 0

Values 0-24

Path **timezone** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > timezone**.

Release First appearance: 5.0.

tls-config

The **tls-config** configuration element allows you to configure global TLS parameters.

Syntax

```
tls-global <session-caching | session-cache-timeout | select | no
| show | done | exit>
```

Parameters

session-caching—Enable or disable the Net-Net SBC's session caching capability

Default disabled

Values enabled | disabled

session-cache-timeout—Enter the session cache timeout, in hours

Default 12

Values Min: 0 / Max: 24

Path **tls-config** is an element of the **security** path. The full path from the topmost ACLI prompt is: **configure terminal > security > tls-config**.

Release First appearance: 6.0

RTC Status Supported

tls-profile

The **tls-profile** configuration element holds the information required to run SIP over TLS.

Syntax

```
tls-profile <name | end-entity-certificate | trusted-ca-
certificates | cipher-list | verify-depth | mutual-authenticate |
select | no | show | done | exit>
```

Parameters

name—Enter the name of the TLS profile. This is a required parameter.

end-entity-certificate—Enter the name of the entity certification record

trusted-ca-certificates—Enter the names of the trusted CA certificate records

cipher-list—Enter a list of ciphers you want to support

Default all

verify-depth—Specify the maximum depth of the certificate chain that will be required

Default 5

mutual-authenticate—Enable or disable mutual authentication of the client by the Net-Net SBC

Default disabled

Values enabled | disabled

Path **tls-profile** is an element of the **security** path. The full path from the topmost ACLI prompt is: **configure terminal > security > tls-profile**.

Release First appearance: 6.0

RTC Status Supported

transcoding-policy

The **transcoding-policy** configuration element allows you to configure transcoding policies on the Net-Net SBC.

Syntax

```
transcoding-policy <name | allow-codecs | add-codecs-on-egress |
order-codecs | force-ptime | packetization-time | dtmf-in-audio |
select | no | show | done | exit>
```

Parameters

name—Enter the name by which this policy is referenced

allow-codecs—Enter the codecs accepted by this policy. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <name> [<name>...]

add-codecs-on-egress—Enter the codecs to be appended to an offer. Excluding keywords **add** and **delete** when a list is already configured replaces the entire list.

Values [add | delete] <enum> [<enum>...]

Only codecs that can be transcoded may be specified. The following is a valid list:

- PCMU
- PCMA
- G729
- G729A
- iLBC
- telephone-event
- T.38
- G711FB
- G726
- G723
- G728
- GSM
- 0F0FB

order-codecs—Specify the ordering of codecs. Excluding keywords **add** and **delete** replaces the entire list.

Values [add | delete] <name> [<name>...]

force-ptime—Enable or disable a forced ptime being used

Default disabled

Default enabled | disabled

packetization-time—Enter a preferred ptime when the **force-ptime** parameter is enabled

Default 20

Values Min: 5 / Max: 240

dtmf-in-audio—Select how the Net-Net SBC should support the conversion of signaling messages or RFC 2833 to DTMF Audio tones in the realm where this transcoding policy is active

Values
- disabled—Does not support DTMF audio tones as transcoded in this realm
- preferred—Supports DTMF audio tones as transcoded in this realm
- dual—Supports both transcoded DTMF audio tones and signaling-based DTMF indications if possible

Path

transcoding-policy is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > transcoding-policy.**

Release

First appearance: 5.0.

translation-rules

The **translation-rules** element creates unique sets of translation rules to apply to calling and called party numbers. The fields within this element specify the type of translation to be performed, the addition for deletion to be made, and where in the address that change should be made.

Syntax

```
translation-rules <id | description | type | add-string | add-
index | delete-string | delete-index | select | no | show | done |
exit>
```

Parameters

id—Enter the identifier or name for this translation rule. This field is required.

description—Enter optional descriptive text

type—Select the address translation type to be performed

Default None

Values
- Add—Add a character or string of characters to the address
- Delete—Delete a character or string of characters from the address
- Replace—Replace a character or string of characters within the address
- None—Set the translation rule to disabled

add-string—String to be added during address translation to the original address. The value in this field should always be a real value; i.e., this field should not be populated with at-signs (@) or dollar-signs ($).

When the type is set to `replace`, this field is used in conjunction with the delete-string value. The value specified in the delete-string field is deleted and the value specified in the add-string field is inserted. If no value is specified in the delete-string field and the type field is set to replace, then nothing will be inserted into the address.

Default blank string

add-index—Enter the location in the original address where the string specified in the add-string value is inserted. This value is the character position starting at 0 to insert the add-string value.

When a dollar-sign ($) is used for the add-index, it appends the add-string to the end of the number. This is represented by "999999999" when a show is performed.

Default 0

Values Min: 0 / Max: 999

delete-string—Enter the string to be deleted from the original address during address translation. Unspecified characters are denoted by the at-sign symbol (@).

When the type is set to `replace`, this value is used in conjunction with the add-string value. The value specified in the delete-string field is deleted and the value specified in the add-string field is inserted. If no value is specified in the delete-string parameter and the type field is set to replace, then nothing will be inserted into the address.

Default blank string

delete-index—Enter the location in the address to delete the string specified in the delete-string field. The value of this field is the character position starting at 0 to insert the add-string value. This is not used when only deleting a given string.

Default 0

Values Min: 0 / Max: 999

Path **translation-rules** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > translation-rules.**

Release First appearance: 5.0

Notes You can delete unspecified characters from an original address by using the at-sign (@).
This is a multiple instance configuration element.

trap-receiver

The **trap-receiver** element defines the NMSs to which the Net-Net SBC sends SNMP traps for event reporting.

Syntax

```
trap-receiver <ip-address | filter-level | community-name |
select | no | show | done | exit>
```

Parameters **ip-address**—Enter the IP address and port for an NMS. If no port value is specified, the Net-Net SBC uses a default port of 162. This required field must follow the IP Address format.

Default 0.0.0.0:0

filter-level—Unused

community-name—Enter the name of the community to which a particular NMS belongs. This required entry must follow the Name Format.

Path **trap-receiver** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > trap-receiver.**

Release First appearance: 5.0

Notes This is a multiple instance configuration element.

6 ACLI Command Summary

ACLI Commands

Command	Mode	Notes
activate	Superuser	
add	Superuser	
save backup	Superuser	
check	Superuser	
clear	Superuser	multi-parameter
configure	Superuser	
connect	User	
debug	Superuser	
delete	Superuser	multi-parameter
dump	Superuser	
enable	User	
exit	User	
kill	User	
mirror	Superuser	
nodebug	Superuser	
ping	User	
power	Superuser	
reboot	Superuser	
reset	Superuser	multi-parameter
restore	Superuser	
save	Superuser	
security	Superuser	multi-parameter
set	Superuser	multi-parameter
show	User	multi-parameter
start	Superuser	multi-parameter
stop	Superuser	

Command	Mode	Notes
switchover	Superuser	
tail	User	
test pattern-rule	Superuser	
test sip-manipulation	Superuser	multi-parameter
upgrade	Superuser	multi-parameter
verify-config	Superuser	

Multi-parameter ACLI Commands

Some commands are multi-parameter commands. This means that the command's functionality is dependent on the first argument you pass to it. The following table lists the multi-parameter commands along with their arguments:

Table 1:

Command	Parameter
clear	acl
	alarm
	dns
	enum
	log
	lrt
	registration
	sessions
delete	arp
	backup
	collection
	config
	dumps
	image
reset	arp
	card
	collection
	dns
	enum
	gateway

Table 1:

Command	Parameter
	h323
	hip
	log
	lrt
	mbcd
	media
	nat
	net-management-control
	qos
	session-agent
	sip
security	certificate
	generate-key
	tls
set	alarm
	cfgchange-prompt
	ftp
	log
	mbcd limit
	nat limit
	password
	sip
	telnet
	terminal
	bootparams
	autoreset
	autofailover
	system state
	xcode-path-monitor
show	acl
	alarm
	amp
	arp

Table 1:

Command	Parameter
	auditlog
	backups
	bootparams
	built-in-manipulations
	cfgchange-prompt
	clock
	collection
	config
	cpu
	directory
	dns
	dumps
	enum
	features
	ftp
	h323
	health
	hip
	i2c
	images
	interfaces
	ip
	log
	lrt
	manifest
	mbcd
	media
	monthly-minutes
	msfe
	nat
	net-management-control
	npu
	ntp

Table 1:

Command	Parameter
	packet-trace
	policy-server
	qos
	radius
	rdp
	realm-specifics
	redundancy
	registration
	routes
	route-stats
	running config
	security
	sessions
	sfe
	sip
	snmp
	snr
	space
	ssh
	status
	system-state
	support-info
	switch
	system
	task
	tcu
	telnet
	terminal
	uptime
	users
	version
	virtual-interface
	xclient

Table 1:

Command	Parameter
	xserv
start	collection
	packet-trace
stop	collection
	packet-trace
test sip-manipulation	debugging
	direction
	display-sip-message
	execute
	load-sip-message
	local-ip
	manipulation-pattern
	manipulation-string
	refresh-manipulations
	remote-ip
	reset
	show
	sip-manipulation
	tgrp-context
upgrade	cancel
	resume
	status
	type

7 ACLI Configuration Element Tree