Oracle® Communications Session Border Controller

ACLI Reference Guide

Release S-C6.2.0

Formerly Net-Net Session Director

October 2013

About this Guide

Overview

The *Net-Net 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.

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 4000 Session Director. Since the ACLI is one of the primary ways of configuring, monitoring, and maintaining your Net-Net 4000, 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.
- **Example**—Gives an example of how the command should be entered using one of the command's valid arguments.

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 that is required (e.g., <Tab>, <Ctrl-Alt-Delete>) from the text surrounding it.
[Keypress or Keypress Combination]	Square brackets distinguish a keypress or a keypress combination that is optional (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.

Style	Definition
`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.

Supported Platforms

Release Version S-C6.2.0 is supported on the Acme Packet 4500 and Acme Packet 3800 series platforms.

Related Documentation

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

Document Name	Document Description
Acme Packet 4500 System Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4500 system.
Acme Packet 3800 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3800 system.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration SBC.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about Net-Net SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the SBC’s accounting support, including details about RADIUS accounting.

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 (rev. 1.00)

Date	Revision Number	Description
December 18, 2009	Rev 1.0.1	• Changes the default value of the sip-manipulation>header-rules>element-rule type parameter
September 22, 2010	Rev 1.0.2	• Corrects description for: realm-config> add-additional-prefixes remove-additional-prefixes

Date	Revision Number	Description
March 19, 2012	Rev. 2.0	• Corrects typos • Corrects default values • Corrects value ranges • Corrects trunkgroup terminology: tgrp (and not trgp) • Updates descriptive text for QoS constraints • Removes references to bootflag 0x30008 • Updates descriptive text for show running-config • Revises definition for mm-in-system • Revises definition and corrects mode for delete realm-specifics • Revises definition for register-contact-host • Adds unique-sdp-id option and parameters: media-supervision-trap, and active-arp to media-manager-config • Corrects dnsalg-server-failover parameter name • Adds Note for customer-next-hop • Revises valid values and adds Note for application-protocol • Revises descriptive text for session-constraints • Removes all references to regenerate-config element • Removes [filename] from syntax for show support-info • Adds Note for local-routing-config • Adds permit-on-reject, disconnect-on-timeout, and gate-spec-mask parameter definitions for ext-policy-server • Revises definition of max-sustain-window • Adds Note for gateway parameter in host-route • Adds definition for reuse-connections parameter in session-agent • Corrects definition and values for next-hop parameter in net-management-control • Corrects definition for telnet-timeout parameter in system-config • Corrects descriptive text for codec-policy • Revises definition for cli-audit-trail in system-config • Adds Note regarding concurrent SSH and/or SFTP sessions in session-constraints • Corrects valid range for SSH password length • Adds Note regarding show prom-info: CAM is not supported • Revises definition for source-routing in system-config • Removes all references to packet-trace-config parameter and is replaced with capture-receiver parameter • Corrects password length and allowable characters for the secret command, which sets the user and superuser password • Corrects the default value and the minimum valid values for min-secure-pwd-len parameter for password-policy • Adds Note to realm-config: Only one network interface can be assigned to a single realm-config object

Date	Revision Number	Description
May 31, 2012	Rev. 2.10	• Adds three values to comparison-type: refer-case-sensitive, refer-case-insensitive, and boolean (sip-manipulation, header-rules) • Removes Note from Network-interface (no longer applicable with the introduction of SCTP Local Multi-Homing) • Revises the definition for ttr-no-response found in Configuration Elements N-Z, session-agent • Revises the definition for time-to-resume found in Configuration Elements N-Z, session-agent • Removes local-error from the valid list of choices for response-map-entries (under local-response-map > entries)
November 26, 2012	Rev. 2.20	• Removes deprecated set-front-interface command • Adds conditions under which arp-check command does not issue request • Corrects error in ping command related to applicable permission mode • Corrects default values for sip-int and SA redirect-action • Adds missing status parameter to show enum command • Adds missing status parameter to show registration command, which applies only to the Net-Net 3800 • Removes listing for non-existant ppi-to-pai parameter from sip-interface element • Corrects typo in force-report-trunk-info documentation • Adds refer-src-routing command • Removes deprecated packet-capture command • Adds missing output rows to show sipd and show enum commands • Specify 1023 as maximum number of characters in an ACLI command • Correctly state ntp-sync command as RTC supported • Added refer-src-routing as parameter to sip-config
Jan 31, 2013	Rev. 2.21	• Adds system-config > alarm-threshold configuration element
February 12, 2013	Rev. 2.22	• Chapter 5, for SIP Manipulation parameters, added information regarding the use of capital letters in header and element rule names.
March 22. 2013	Rev 2.30	• Specifies sip-nat parameter ext-address as non RTC • Specifies network-parameter SCTP parameters as non-RTC • Notes vsa-id-range entry specification caveat
August 14, 2013	Rev 2.31	• In Chapter 3, adds a note that the SBC no longer uses the “show backup-config” command.
August 22, 2013	Rev 2.32	• In Chapter 5, under “Session-Agent-Groups”, the “dest” parameter description was re-worded. It incorrectly stated that SAGs can be nested.

Contents

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.

Privilege Levels

There are two privilege levels in the ACLI, User and Superuser. Both are password-protected.

- User—At User level, you can access a limited set of Net-Net SBC monitoring capabilities. You can:
    - View configuration versions and a large amount if statistical data for the system's performance.
    - Handle certificate information for IPSec and TLS functions.
    - Test pattern rules, local policies, and session translations.
    - Display system alarms.
    - Set the system's watchdog timer.
    - Set the display dimensions for your terminal.

  You know you are in User mode when your system prompt ends in the angle bracket (>).
- Superuser—At Superuser level, you are allowed access to all system commands and configuration privileges. You can use all of the commands set out in this guide, and you can perform all configuration tasks.

  You know you are in Superuser mode when your system prompt ends in the pound sign (#).

Enabling Superuser Mode

To enable Superuser mode:

1. At the ACLI User prompt, type the enable command. You will be asked for your Superuser password.

   ```
   ACMEPACKET> enable
   Password:
   ```
2. Enter your password and press <Enter>.

```
Password: [Your password does not echo on the display.]
ACMEPACKET#
```

If your entry is incorrect, the system issues an error message and you can try again. You are allowed three failed attempts before the system issues an error message telling you that there are excess failures. If this occurs, you will be returned to User mode where you can start again.

System Access

You can access the ACLI using the different means described in this section.

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 unsecured 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.

ACLI Help and Display

The Net-Net 4000's ACLI offers several features that aid with navigation and allow you to customize the ACLI so that you can work more efficiently.

- Alphabetized help output—When you enter either a command followed by a question mark, the output is now sorted alphabetically and aligned in columns. The exception is the **exit** command, which always appears at the end of a column.
- Partial command entry help—When you enter a partial command followed by a question mark, the new Help output displays only commands that match the letter you type rather than the entire list.
- The **more** prompt—You can set a **more** option in the ACLI that controls whether or not you can use more with any of the following commands: **show**, **display**, **acl-show**, and **view-log-file**. Turning this option on gives you the ability to view output from the command one page at a time. By default, this option is enabled. Your setting is persistent across ACLI sessions.

  With the **more** feature enabled, the ACLI displays information one page at a time and does so universally across the ACLI. A line at the bottom of the screen prompts you for the action you want to take: view the displays's next line or next page, show the entire display at once, or quit the display. You cannot change setting persistently, and need to change them every time you log in.

- Configurable page size—The page size defaults to 24 X 80. You can change the terminal screen size by using the new **cli terminal height** and **cli terminal width** commands. The settings for terminal size are not preserved across ACLI sessions.

Exiting the ACLI

Typing `exit` at any ACLI prompt moves you to the next "higher" level in the ACLI. After exiting out of the User mode, you are logged 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.
	<UParrow>	Scrolls forward through former commands.
	<DOWNarrow>	Scrolls backward through former commands.
	<Tab>	Completes a partial 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 available commands or configurable elements/parameters .
Context-Sensitive Help	?	Provides context-sensitive help. It functions both for ACLI commands and configuration elements and is displayed in alphabetical order.

Category	Hotkey	Description
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.
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.

Command Abbreviation and Completion

This section describes how you can use abridged commands 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# gen
```

```
generate-certificate-request  generate-key
ACMEPACKET# generate-key
```

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(local-policy)# ?

from-address           from address list
to-address             to address list
source-realm           source realm list
activate-time          policy activation date & time
deactivate-time        policy deactivation date & time
state                  enable/disable local policy
policy-priority        priority for this local policy
policy-attributes      list of policy attributes
select                 select a local policy to edit
no                     delete selected local policy
show                   show selected local policy
done                   write local policy information
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. Within this one-line entry, you have access to context-sensitive help that tells you what values are valid for a given field and when you have completed an entry. When the `<ENTER> no further known parameters` line appears, the ACLI is informing you that there is no subsequent information to enter.

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 **show** command menu appears. Typing a **?** after a system command asks if the system requires further information to complete a specific command. The system responds with a list of available subcommands.

```
ACMEPACKET# show ?

about                credit information for acli
acl                  show host access table
algd                 ALG MGCP status
arp                  ARP table
buffers              show memory buffer statistics
clock                system clock
configuration        show current configuration
dns                  DNS information
enum                 ENUM information
ext-band-mgr         External Bandwidth Manager status
ext-clf-svr          External CLF Server status
features             currently enabled features
h248d                H248D status
h323d                H323D status
health               system health information
hosts                show host table
interfaces           show network interfaces
ip                   IP system information
logfile              Display a log file, 'enter' to display list
loglevel             loglevels of current processes
lrt                  LRT (local-routing) information
```

```
mbcd                        MBCD status
media                       show media interface information
memory                      memory statistics
mgcp                        ALG MGCP status
nat                         show NAT table
net-management-control       Network Management Controls Statistics
packet-trace                displays the current packet trace addresses
privilege                   show current privilege level
processes                   active process statistics
prom-info                   show prom information
radius                      radius accounting
redundancy                  redundancy status
registration                SIP Registration Cache status
route-stats                 show routing statistics
routes                      show routing table entries
running-config              current operating configuration
security                    security information
sessions                    Session Statistics
sipd                        SIPD status
snmp-community-table        show snmp community table
support-info                show all required support information
system-state                current system-state
temperature                 current SD temperature readings
trap-receiver               show snmp trap receivers
uptime                      system uptime
users                       currently logged in users
version                     system version information
virtual-interfaces          show virtual interfaces
voltage                     current SD voltages (SD-II only)
```

The system responds with a `no further known parameters` if there are no subcommands.

```
ACMEPACKET# show about ?

<ENTER!>  no further known parameters

ACMEPACKET# show about
```

Viewing Output With the More Prompt

When the output of a command is too large to fit your screen, the system displays the output in smaller sections. At the end of a section a message is displayed with your options:

- <Space>—Display the next section of output
- <q>—Quits and returns to the system prompt

- <c>—Displays the rest of the output in its entirety

```
ACMEPACKET# show ?

about                credit information for acli
acl                  show host access table
algd                 ALG MGCP status
arp                  ARP table
buffers              show memory buffer statistics
clock                system clock
configuration        show current configuration
dns                  DNS information
enum                 ENUM information
ext-band-mgr         External Bandwidth Manager status
ext-clf-svr          External CLF Server status
features             currently enabled features
h248d                H248D status
h323d                H323D status
health               system health information
hosts                show host table
interfaces           show network interfaces
ip                   IP system information
logfile              Display a log file, 'enter' to display list
loglevel             loglevels of current processes
('space' for next page; 'q' to quit; 'enter' for next line; 'c' to continue)
```

Disabling the More Prompt

If you don’t want the Net-Net SBC to display the More prompt, you can disable it using the `cli` command.

```
ACMEPACKET# cli more disabled
The ACLI 'more' option has been disabled
ACMEPACKET#
```

Configuring Using the ACLI

This section describes the two ACLI methods available for configuring the Net-Net SBC using line-by-line ACLI commands.

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
ACMEPACKET(trap-receiver)# done
```

Working with Configuration Elements

Configuring elements involves entering the ACLI path to the configuration element you want to configure, and then entering the parameter name followed by a space and proper data in accordance with the required format.

Creating

Creating elements involves using the ACLI path to enter configurations. Once you are in the element you want to configure, enter the appropriate information.

```
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

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

- The `done` command, which is entered within a configuration element.
- The hotkey <Ctrl-D>, which is entered within a configuration element. This 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 without saving your changes . This prompt only appears if you have changed old information and/or entered new information.

Using Show 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 line-by-line entry.

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

```
ACMEPACKET(media-profile)# show
media-profile
    name                      profile1
    media-type                audio
    payload-type
    transport                     rtp
    req-bandwidth                 100
    frames-per-packet             500
    parameters
    average-rate-limit            50
    peak-rate-limit               55
    max-burst-size                100
    sdp-rate-limit-headroom       10
    sdp-bandwidth                 disabled
```

Using Done 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

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 and press <Enter>. 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>: <Enter>
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                    lefty
      operation-type          Media
      port                    0
      slot                    0
      virtual-mac
      admin-state             enabled
      auto-negotiation         enabled
      duplex-mode             FULL
      speed                   100
```

6. Use the **done** command to save your updates.

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

Deleting

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 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>: <Enter>
   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>: <Enter>
   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. The following example shows how to view `media-profile` configuration summaries.

To view the settings for the media-profile element:

1. Enter the media-profile configuration element through the ACLI path.

   ```
   ACMEPACKET# co t
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)# media-profile
   ACMEPACKET(media-profile)#
   ```

2. From `media-profile`, use the `select` command. The **`<name>:`** prompt and a list of configured media-profile elements appear.

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

3. Select the configured media profile you want to view by entering the corresponding number and press the <Enter> key.

   ```
   selection: 1
   ```

4. Type **show** and press the <Enter> key.

```
    ACMEPACKET(media-profile)# show
media-profile
    name                        PCMU
    media-type                  audio
    payload-type
    transport                   rtp
    req-bandwidth               100
    frames-per-packet           500
    parameters
    average-rate-limit          50
    peak-rate-limit             55
    max-burst-size              100
    sdp-rate-limit-headroom     10
    sdp-bandwidth               disabled
```

Data Entry

To enter data using the ACLI, your entries must conform to required field formats. This section describes these formats, gives 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.

Note that, unless specified by the criteria of a specific field, the maximum number of characters that you can enter to a single ACLI command is 1023.

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.

Date and Time Format

The date and time format displays both the date and time and adheres to the yyyy-mm-dd hh:mm:ss.zzz or yyyy-mm-dd-hh:mm:ss.zzz where y=year, m=month, d=day, h=hours, m=minutes, s=seconds, and z=milliseconds.

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 cannot 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 can not 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 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.
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.

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
```

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.

Option Configuration

The options parameter shows up in many configuration elements. This parameter is used for configuring the Net-Net SBC to behave with either non-standard or customer-specific behavior.

Several options might be configured for a single configuration element. Every time you configure the option parameter, you overwrite the previously configured option list for the selected instance of the configuration element.

There is a shortcut to either add or delete a single option to the full option list. By typing a “+” to add or a “-” to subtract immediately before an option, you can edit the currently configured option list.

Append Example

With the `forceH245` option preconfigured, you can append a new option without deleting the previously configured option:

```
ACMEPACKET(h323)# options +noAliasInRCF
ACMEPACKET(h323)# show
h323-config
    state               enabled
    log-level           INFO
    response-tmo        4
    connect-tmo           32
    options               forceH245
                          noAliasInRCF
ACMEPACKET(h323)#
```

Delete Example

You can also delete a single existing option from the options list. Continuing from the previous example:

```
ACMEPACKET(h323)# options -forceH245
ACMEPACKET(h323)# show
h323-config
    state                 enabled
    log-level             INFO
    response-tmo          4
    connect-tmo           32
    options               noAliasInRCF
ACMEPACKET(h323)#
```

2 ACLI Commands A - M

acl-show

The **acl-show** command shows a list of denied ACL entries.

Syntax

```
acl-show
```

Mode

Superuser

Release

First appearance: 2.0

Notes

The **acl-show** command displays a list of the following denied ACL entries:

- Incoming port, slot, and VLAN tag
- Source IP, bit mask, port, and port mask
- Destination IP address and port
- Protocol
- ACL entry as static or dynamic
- ACL entry index

Example

```
ACMEPACKET# acl-show
```

acquire-config

The **acquire-config** command retrieves the configuration from one Net-Net SBC for configuration checkpointing an HA node.

Syntax

```
acquire-config <IPAddress>
```

Arguments

<IPAddress> Enter the IP address of Net-Net SBC to acquire configuration from

Mode

Superuser

Release

First appearance: 1.2.1 / Most recent update: 2.0

Notes

This command forces one Net-Net SBC in an HA node to learn the configuration from the other system. If configuration checkpointing is already running, the **acquire-config** command has no effect.

Only after the **acquire-config** command is executed and the Net-Net SBC is rebooted will process of acquiring the configuration be complete. In Net-Net SBC Software 2.0, only type `acquire-config <wancom0-IP address>.`

Example

```
ACMEPACKET# acquire-config 1.1.0.1
```

activate-config

The **activate-config** command activates the current configuration on the Net-Net SBC to make it the running configuration.

Syntax

```
activate-config
```

Mode Superuser

Release First appearance: 1.2.1

Notes Before executing this command, be aware of the real time configuration (RTC) consequences on the operation of the Net-Net SBC.

To use RTC, the **activate-config** command is executed to alert the Net-Net SBC that the current configuration has changed and that it needs reload configuration information.

Example

```
ACMEPACKET# activate-config
```

archives

The **archives** command is used for creating, moving, and manipulating archived log files. All archive files are created in .tar.gz format in SD Software versions 2.0 and above. All commands are executed from within the archives menu.

Log files contain a record of system events. Log files are stored in the `/code/logs` directory. The CFG archive type is no longer supported in C6.2.0. When an archive command is entered with the CFG type, the Net-Net SBC responds with an error message.

Path Type **archives** at the topmost prompt before executing any of the below commands to enter the archives shell.

Release First appearance: 1.1 / Most recent update: 2.0

archives > create

Syntax

```
create LOGS <logfile-name>
```

Arguments

<logfile-name>	Enter the name of archive file that contains all logs

To create an archive file of a log, type **create LOGS** and enter a logfile name. Archives are created in .tar.gz (tarred and gzipped) format.

Example

```
ACMEPACKET(archives)# create LOGS jun_30.gz
```

archives > delete

Syntax

```
delete LOGS <logfile-name>
```

Arguments

<filename>	Enter the filename of the log archive to delete

The **archives > delete** command deletes the specified archive file from the Net-Net SBC. You must append ".tar.gz" to the filename when using this command. Use the **archives > display** command to list the available log archives to delete.

Example

```
ACMEPACKET(archives)# delete LOGS july_16.gz
```

archives > display

Syntax

```
display LOGS
```

This command lists the log archives currently saved on the Net-Net SBC's file system.

Example

```
ACMEPACKET(archives)# display LOGS
```

archives > exit

Syntax

```
exit
```

Notes

This command exits from the archives session and returns you to the ACLI Superuser system prompt.

Example

```
ACMEPACKET(archives)# exit
```

archives > extract

This command is no longer supported in release C6.2.0.

archives > get

Syntax

```
get LOGS <archive-name> <remote-host> <user-name> <password>
```

Arguments

<remote-name>	Enter the full path and filename to retrieve
<host>	Enter the IP address of the remote host
<user-name>	Enter the user name on remote host
<password>	Enter the password on remote host

Notes

This command retrieves an archived log. If you do not include all the necessary arguments, the **get** command will prompt you for the arguments you omitted.

The **get** command writes the retrieved file to the /code/logs/<archive-name> path.

Example

```
ACMEPACKET(archives)# get LOGS may_31.gz
```

archives > rename

Syntax

```
rename LOGS <old-archive> <new-archive>
```

Arguments

<current_name>	Enter the old archive name
<new_name>	Enter the new archive name

Notes

Renames an archived log. You do not need to append ".tar.gz" to the filename when using this command.

Example

```
ACMEPACKET(archives)# rename LOGS june sept
```

archives > send

Syntax

```
send LOGS <archive-name> <host-ip-address> <username>
```

Arguments

<archive-name>	Enter the name of archive file to send
<host-ip-address>	Enter the IP address of FTP server
<username>	Enter the FTP username on server

Notes

This command sends an archived log file to a remote host using FTP. If you do not include all the necessary arguments, the **send** command will prompt you for the arguments you omitted.

Example

```
ACMEPACKET(archives)# send LOGS Oct_24.gz 1.0.100.7 user1
```

arp-add

The **arp-add** command manually adds ARP entries for media interfaces to the ARP table.

Syntax

```
arp-add <slot> <port> <vlan ID> <ip-address> <mac-address>
```

Arguments

<slot>	Select the media interface slot
Values	• 0—Left slot • 1—Right slot
<port>	Select the media interface port
Values	• 0—Leftmost port • 1—Second from left port • 2—Third from left port (not applicable for GigE cards) • Enter the 3—Rightmost port (not applicable for GigE cards)
<vlan ID>	VLAN identifier
<ip-address>	Enter the IP address
<mac-address>	Enter the MAC address in hexadecimal notation

Mode Superuser

Release First appearance: 1.0 / Most recent update: 1.2.1

Example

```
ACMEPACKET# arp-add 1 0 0 172.16.1.102 ab:cd:ef:01:23:14
```

arp-check

The **arp-check** command forces the SD to send an ARP request for the specified IP address. The command does not send an ARP request if the specified address is already in the ARP table or is in a different subnet.

Syntax

```
arp-check <slot> <port> <vlan-ID> <ip-address>
```

Arguments

<slot>	Select the media interface slot
Values	• 0—Left slot • 1—Right slot
<port>	Select the media interface port
Values	• 0—Leftmost port • 1—Second from left port • 2—Third from left port (not applicable for GigE cards) • 3—Rightmost port (not applicable for GigE cards)
<vlan ID>	Enter the VLAN identifier
<ip-address>	Enter the IP address

Mode Superuser

Release First appearance: 1.0 / Most recent update: 1.2.1

Example

```
ACMEPACKET# arp-check 0 0 0 11.21.0.10
```

arp-delete

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

Syntax

```
arp-delete <slot> <port> <vlan-ID> <ip-address>
```

Arguments

<slot>	Select the media interface slot
Values	• 0—Left slot • 1—Right slot
<port>	Select the media interface port
Values	• 0—Leftmost port • 1—Second from left port • 2—Third from left port (not applicable for GigE cards) • 3—Rightmost port (not applicable for GigE cards)
<vlan ID>	Enter the VLAN identifier
<ip-address>	Enter the IP address

Mode Superuser

Release First appearance: 1.0 / Most recent update: 1.2.1

Example

```
ACMEPACKET# arp-delete 1 0 1 12.11.0.100
```

backup-config

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

Syntax

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

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.

Mode Superuser

Release First appearance: 1.0 / Most recent update: 1.2.1

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

Example

```
ACMEPACKET# backup-config FEB_BACKUP.gz running
```

check-space-remaining

The **check-space-remaining** command displays the remaining amount of space in the boot directory, code (or flash memory), and ramdrv devices.

Syntax

```
check-space-remaining <device>
```

Argument	<device>	Select where to check the remaining space
	Values	• boot • code • ramdrv

Mode Superuser

Release First appearance: 1.1

Notes The output of this command is in bytes.

Example

```
ACMEPACKET# check-space-remaining boot
```

check-stack

The **check-stack** command outputs the system’s full stack to the ACLI.

Syntax

```
check-stack
```

Mode Superuser

Release First appearance: 1.1

Notes This command displays a summary of stack usage for a specified task, or for all tasks if no argument is entered. The command output includes:

- Name—task name
- Entry—entry id
- TID—task identification
- Size—total stack size
- CUR—current number of stack bytes used
- HIGH—maximum number of stack bytes used
- Margin—number of bytes never used at the top of the stack

Example

```
ACMEPACKET# check-stack
```

clear-alarm

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

Syntax

```
clear-alarm <alarm_id> <task_id>
```

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

<task_id> Enter the task ID of the task that sent the alarm

Release First appearance: 1.0

Notes For alarm identification and task codes for specific alarms, use the **display-alarms** command.

Example

```
ACMEPACKET# clear-alarm 65524 sip
```

clear-cache

The **clear-cache** command allows you to clear a specified cache entry on the Net-Net SBC.

clear-cache dns

Syntax

```
clear-cache dns <realm id | “all” > <cache entry key | “all”>
```

This command allows you to clear a specified DNS cache entry or all entries.

Arguments

<realm id | all> Specify the realm whose DNS cache you want to clear or enter `all` if you want to clear the cache of all realms

<cache entry key> Enter a specific cache entry key or enter `all` for all entries. A specified cache entry key should take one of the following forms.

–NAPTR entries—NAPTR:test.com

–SRV entries—SRV:_sip_udp.test.com

–A entries—A:test.com

Example

```
ACMEPACKET# clear-cache dns public A:test.com
```

clear-cache enum

This command allows you to clear a specified ENUM cache entry or all entries.

Syntax

```
clear-cache enum <EnumConfig Name | “all”> [cache entry key |
“all”]
```

Arguments

<EnumConfig Name> Enter the name of the specific EnumConfig for which you want to clear the cache

<cache entry key> Enter the cache key of the specific EnumConfig for which you want to clear the cache

<all> Enter **`all`** to clear all caches. In order for this command to work the DNS cache needs to be cleared.

Example

```
ACMEPACKET# clear-cache enum enum1
```

clear-cache registration

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

Syntax

```
clear-cache registration <sip | mgcp | h323> <type>
```

Arguments

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

–all

–by-ip <IPaddress>

–by-user <phone number>

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

–all

–by-endpoint <endpoint name>

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

–all

–by-alias <terminalAlias>

Example

```
ACMEPACKET# clear-cache registration sip all
```

clear-cache tls

This command allows you to clear the TLS cache.

Syntax

```
clear-cache tls
```

Example

```
ACMEPACKET# clear-cache tls
```

Mode Superuser

Release First appearance: 5.0

clear-deny

The **clear-deny** command deletes a denied ACL entry.

Syntax

```
clear-deny [<index> | “all”]
```

Arguments

<index> Enter the index number of the ACL entry to delete

<“all”> Delete all denied ACL entries

Mode Superuser

Release First appearance: 4.0

Notes Use the **acl-show** command to identify the index of a specific ACL entry. Use the **clear-deny all** command to delete all of the deny entries. This command replaces the **acl-delete** command from previous versions.

Example

```
ACMEPACKET# clear-deny all
```

clear-sess

The **clear-sess** command deletes SIP, H.323, and IWF sessions from the system.

Syntax

```
clear-sess <sipd | h323d> <“sessions”> <all | by-agent | by-
callid | by-ip | by-user>
```

Arguments

<all> Delete all sessions for the specified protocol

<by-agent> Delete sessions for a specified session agent

<by-callid> Delete sessions for a specified call identifier

<by-ip> Delete sessions for a specified endpoint IP address (entered in quotation marks)

<by-user> Delete sessions for a specified calling or called number

Mode Superuser

Release First appearance: 5.1

Notes Use the show <sipd | h323d> sessions with similar arguments to view information about sessions you might want to clear from the system.

Example

```
ACMEPACKET# clear-sess sipd sessions all
```

clear-trusted

The **clear-trusted** command deletes a trusted ACL entry.

Syntax

```
clear-trusted [<index> | “all”]
```

Arguments

<index>	Enter the index number of ACL entry to delete
<“all”>	Delete all trusted ACL entries

Mode Superuser

Release First appearance: 4.0

Notes Use the **acl-show** command to identify the index of a specific ACL entry. Use the **clear-trusted all** command to delete all of the trusted entries.

Example

```
ACMEPACKET# clear-trusted all
```

cli

The **cli** command allows you to modify ACLI session terminal settings and “more” options on your Net-Net SBC.

Syntax

```
cli <more> <terminal-height>
```

<more> Enable or disable the `more` prompt you see when the output on the screen is larger than the size of the screen.

Values	enabled | disabled

<terminal-height> Enter the number of rows in the terminal

Default	24
Values	Min: 0 / Max: 1000

Mode User

Release First appearance: 5.0

Example

```
ACMEPACKET# cli more disabled terminal-height 500
```

configure terminal

The **configure terminal** command enters you into the system level where you can configure all operating and system elements on your Net-Net SBC.

Syntax

```
configure terminal
```

Mode Superuser

Release First appearance: 1.0

Example

```
ACMEPACKET# configure terminal
```

delete realm-specifics

The **delete realm-specifics** command used with a realm identifier deletes the specified realm, and its configuration objects. This command should be used with the utmost care.

Syntax

```
delete realm-specifics <realm identifier>
```

Arguments `<realm identifier>`—Enter the identifier for the realm you want to delete

Mode Superuser (in addition, you need to be in configuration mode)

Release First appearance: S-C6.1.0

Notes This command should be used with the utmost care.

Example

```
ACMEPACKET# delete realm-specifics peer_1
```

delete-backup-config

The **delete-backup-config** command deletes a saved configuration file from the Net-Net SBC flash memory.

Syntax

```
delete-backup-config <backup-name>
```

Arguments <backup-name> Enter the name of the backup configuration you want to delete

Mode Superuser

Release First appearance: 1.2.1

Notes Use **display-backups** to list backup configurations to delete.

Example

```
ACMEPACKET# delete-backup-config JAN_BACKUP.gz
```

delete-config

The **delete-config** command deletes the current configuration located in the `/code/data` and `/code/config` directories from the system's flash memory.

Syntax

```
delete-config [cached]
```

Arguments [cached] Delete the cached config. This is an optional argument.

Mode Superuser

Release First appearance: 1.1 / Most recent update: 2.0

Example `ACMEPACKET# delete-config`

Notes When the **delete-config** command is entered, the system gives the warning asking if you really want to erase either the current config or the current cached config. Enter a `y` to complete the deletion.

delete-import

This command enables the user to delete imported SIP-manipulation rules as files from the /code/import directory.

Syntax

```
delete-import <file name>
```

Arguments <file name> Enter the name of the file to delete

Mode Superuser

Release First appearance: S-C6.2.0

Example

```
ACMEPACKET# delete-import 12012009.gz
```

Notes Include the complete file name in the argument, including `.gz`.

delete-status-file

The **delete-status-file** deletes the reboot status file.

Syntax

```
delete-status-file
```

Mode Superuser

Release First appearance: 1.1 / Most recent update: 1.3

Notes This command deletes the `/code/statsDump.dat` file which retains all system data if the Net-Net SBC has to reboot. This command also removes the contents of the `/code/taskCheckDump.dat` file which contains system failure information.

Example

```
ACMEPACKET# delete-status-file
```

display-alarms

The **display-alarms** command displays details about the specific alarms on the Net-Net SBC.

Syntax

```
display-alarms
```

Mode User

Release First appearance: 1.0

Notes This command shows the current alarms on the Net-Net SBC. Each alarm entry lists alarm ID, task ID, alarm severity code, number of occurrences, when the alarm first and last occurred, the number of times it has occurred, and a description of the alarm.

Example

```
ACMEPACKET# display-alarms
```

display-backups

The **display-backups** command displays the configuration backup files located in the /code/bkups directory.

Syntax

```
display-backups [sort-by-name]
```

Arguments <sort-by-name> Sort the output of the **display-backups** command output. This is an optional command.

Mode User

Release First appearance: 2.0

Example

```
ACMEPACKET# display-backups
```

display-current-cfg-version

The **display-current-cfg-version** command displays the current configuration version.

Syntax

```
display-current-cfg-version
```

Mode User

Release First appearance: 1.2.1

Notes This command displays the saved version number of the current configuration. This integer value is incremented by one for each new configuration version.

Example

```
ACMEPACKET# display-current-cfg-version
```

display-logfiles

The **display-logfiles** command lists the current logfiles located in the logfile directory.

Syntax

```
display-logfiles
```

Mode User

Release First appearance: 1.0

Notes Logfiles are located in the `/code/logs` directory.

Example

```
ACMEPACKET# display-logfiles
```

display-running-cfg-version

The **display-running-cfg-version** command displays the current configuration version.

Syntax

```
display-running-cfg-version
```

Mode User

Release First appearance: 1.2.1

Notes This command displays the version number of the running configuration, and integer value that is incremented by one for each new configuration version.

Example

```
ACMEPACKET# display-running-cfg-version
```

enable

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

Syntax

```
enable
```

Mode User

Release First appearance: 1.0

Notes Observing the command prompt can tell you if the Net-Net SBC is in user or superuser mode. A ">" (close-angle-bracket) indicates User mode and a "#" (pound) sign indicates Superuser mode.

Example

```
ACMEPACKET# enable
```

exit

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

Syntax

```
exit
```

Mode User

Release First appearance: 1.0

Example

```
ACMEPACKET# exit
```

format

This command allows the user to partition the Storage Expansion Module into as many as 4 file directories.

Syntax

```
format <device>
```

Arguments <device> Enter the name of a device

Mode Superuser

Release First appearance: S-C6.2.0

Example

```
ACMEPACKET# format device1
```

generate-certificate-request

For TLS Support, the **generate-certificate-request** command allows you to generate a private key and a certificate request in the PKCS10 PEM format. The generated private key is stored in the certificate record configuration. If the certificate record is designed to hold a CA certificate, there is no need to generate a certificate request.

Syntax

```
generate-certificate-request <certificate-record-name>
```

Arguments <certificate-record-name> Enter the name of the certificate you want to view.

Mode Superuser

Release First appearance: 4.1

Example

```
ACMEPACKET# generate-certificate-request acmepacket
```

generate-key

The **generate-key** command allows you to generate a security key.

Syntax

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

Arguments <type> Select the type of key you want to generate. The following is a list of valid security keys.

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
- des— Generate a DES 64 bit, odd parity key
- hmac-md5—Generate an HMAC MD5 secret
- hmac-sha1—Generate an HMAC SHA1 secret

Mode User

Release First appearance: 5.0

Example

```
ACMEPACKET# generate-key aes-256
```

import-certificate

For TLS support, the **import-certificate** command allows you to import a certificate record.

Syntax

```
import-certificate <type>
```

Arguments <type> Enter the type of certificate you want to import. Each type of import certificate is described below:

Values

- pkcs7—Import using a password enhanced mail format
- x509—Import using a password enhanced mail format
- try-all—Try importing from both pkcs7 and x509

Mode User

Release First appearance: 4.1

Example

```
ACMEPACKET# import-certificate x509
```

ipv6

For IPv6 support, the **ipv6** command allows you to test ipv6 configurations.

Syntax

```
ipv6
```

Mode User

Release First appearance: S-C6.2.0

Example

```
ACMEPACKET# ipv6 <enter>
```

kill

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

Syntax

```
kill <id>
```

Arguments <id> Enter the id of the Telnet session you want to terminate

Mode Superuser

Release First appearance: 2.0

Notes You can use the **show users** command to view all active Telnet sessions and the index number associated with each session. You cannot use this command to terminate SSH or console sessions.

Example

```
ACMEPACKET# kill 11
```

load image

The **load image** command guides users through the upgrade process, thereby keeping errors to a minimum.

Syntax

```
load image <IP address> <filename> <username>
```

Arguments

<IP address>	Enter the IP address of the remote host
<filename>	Enter the remote filename with path
<username>	Enter the username for the remote host

Mode Superuser

Release First appearance: 5.1.1

Example

```
ACMEPACKET# load image 192.30.8.50 /image/nnC511p4.gz user
```

Notes You can either enter these arguments all in one line (with a <Space> between each), or you can press <Enter> after each entry to move to the next piece of information required to load the new information.

Once you have entered all of the required information, you will be prompted for the password for the remote host and the image loading process starts.

log-level

The **log-level** command sets the system wide log-level or the log-level for a specific task or process. In addition, you can set the log type for a specific log level on a per-task basis.

Syntax

```
log-level system <log-level>
log-level <task-name | “all”> <log-level>
```

Arguments

<log-level>	Select the log level either by name or by number
Values	• emergency (1) • critical (2) • major (3) • minor (4) • warning (5)

- notice (6)
- info (7)
- trace (8)
- debug (9)
- detail

<task-name>	Enter the task name for the log level being set
<all>	Change the log level for all Net-Net SBC tasks

Mode Superuser

Release First appearance: 1.0 / Most recent update: 1.1

Notes The log setting changes made by the log-level command are not persistent after a reboot. Upon reboot, you need to change the log settings in the system configuration in order for them to be persistent.

When entering multiple log types in the log-type-list argument, use a space for separation.

Example

```
ACMEPACKET# log-level system warning
```

management

The **management** command sets the starting state of Telnet and FTP services at boot time.

Syntax

```
management <state | show> <service>
```

Arguments

<state>	Select the operating state of service
Values	• enable—Enable the service set in the <service> argument from starting at boot time • disable—Disable the service set in the <service> argument from starting at boot time
<service>	Select the service that you are setting boot time status
Values	• ftp—Enter the FTP service • telnet—Enter the Telnet service

Mode Superuser

Release First appearance: 2.0

Example

```
ACMEPACKET# management enable ftp
```

monitor

The **monitor** command displays real-time media or signaling statistics.

Syntax

```
monitor <media | session>
```

Arguments

<media>	Enter the media you want to monitor
<session>	Enter the session you want to monitor

Mode User

Release First appearance: 1.0

Notes This command outputs real-time media and signaling statistics to the ACLI. Pressing a numerical digit (0-9) changes the refresh rate to that interval in seconds. By default, there is a 2 second refresh rate. Type "`q`" to exit the monitor display.

Note that **monitor session** will display the equivalent of **show sipd statistics**, and **monitor media** will display the equivalent of **show mbcd statistics**.

Example

```
ACMEPACKET# monitor media
```

3 ACLI Commands N - Z

notify

The **notify** command notifies a specific task or process of a condition that it should act.

Syntax

```
notify <all | <process-name>> trace <all|<socket-address><file-name>> [<out-udp-port>]

notify <all | <process-name>> notrace all|<socket-address>
```

Arguments

<process-name> Enter the name of the process you want to notify

<socket-address> Enter the IP address and the port on which the socket is connected

<file-name> Enter the name of the file you want to notify

<out-udp-port> Enter the IP address and port to which the log messages are sent; if the <out-udp-port> is not specified, logs are written to the <file-name>

Used for runtime protocol tracing for UDP/TCP sockets, this command provides for all protocol messages for ServiceSocket sockets to be written to a log file or sent out of the Net-Net SBC to a UDP port.

Example

```
ACMEPACKET# notify all trace all aug.gz
```

notify algd

Syntax

```
notify algd <log>
```

Arguments

<log> Each log argument is listed and described below.

Values
- nolog—Disable MBCD and MGCP message exchanges processed by the ALGD task
- log—Enable ALGD and MGCP messages in the alg.log

Example

```
ACMEPACKET# notify algd log
```

notify algd mgcp-endpoint

Syntax

```
notify algd mgcp-endpoint <endpoint>
```

Arguments

<endpoint> Delete session and corresponding gateway entries for a specified gateway. The value is the endpoint name from the Audit Name field of the RSIP. If a gateway has multiple endpoints, then the last endpoint that sent the RSIP should be used as the endpoint ID.

Example

```
ACMEPACKET# notify algd mgcp-endpoint 1.2.0.1
```

notify berpd force

Syntax

```
notify berpd force
```

Force a manual switchover between Net-Net SBCs in an HA node, regardless of the Net-Net SBC on which the command is executed.

Example

```
ACMEPACKET# notify berpd force
```

notify mbcd

Syntax

```
notify mbcd <arguments>
```

Arguments

<arguments> The following are arguments for this command:

Values

- nolog—Disable MBCD logging
- log—Enable MBCD logging
- debug—Set the log level for MBCD. Unless a specific log type is specified, this command will use its defaults: FLOW and Media
- nodebug—Disable setting the log level for MBCD

Example

```
ACMEPACKET# notify mbcd debug
```

notify radd reload

Syntax

```
notify radd reload
```

Changes the configurations for RADIUS dynamically by reloading the configuration data in the accounting configuration.

Example

```
ACMEPACKET# notify radd reload
```

notify sipd

Syntax

```
notify sipd <arguments>
```

Arguments

<arguments> The following are arguments for this command:

Values

- reload—Update configuration changes dynamically by reloading the configuration data that SIP functionality might need. This command cannot tear down any in-progress sessions, and it cannot tear down any listening sockets.
- nosiplog—Disable the logging of SIP messages, including SIP messages as seen from the perspective of the Net-Net SBC's SIP proxy
- siplog—Enable SIP logging messages in the `sipmsg.log`
- report—Write all SIP process statistics to the log file
- dump limit—Write CPU limit information to the log file
- debug—Set log level for SIP protocol for some SIP activity
- nodebug —Disable setting the log level for the SIP protocol for some SIP activity

Example

```
ACMEPACKET# notify sipd nosiplog
```

notify syslog

Syntax

```
notify syslog <arguments>
```

Arguments

<arguments> Arguments for this command

Values

- ip-address—Add a syslog server with the given IP address to the configured syslog servers. When this command is executed without any arguments, the Net-Net SBC is prompted to re-read the current configuration, replace any pre-existing configuration information for syslog, and begin sending syslog messages to any configured syslog servers.
- udplog
- noudplog
- trace
- notrace

Example

```
ACMEPACKET# notify syslog 100.1.0.20
```

notify * rotate-logs

Syntax

```
notify <task> rotate-logs
```

Arguments

<task> Enter the tasks' process and protocol trace logs to rotate

Values

- sipd
- sysmand
- berpd
- brokerd
- lemd
- mbcd
- h323d
- algd
- radd
- all

Notes This command only applies until a reboot occurs; it is not persistent after a reboot.

Example

```
ACMEPACKET# notify mbcd rotate-logs
```

notify nosyslog

Syntax

```
notify nosyslog <ipaddress>
```

Arguments <ipaddress> Enter the IP address of syslog server to disable the logging of syslog messages. The **notify nosyslog** command executed without an argument prompts the Net-Net SBC to disable the logging of syslog messages sent from the system to all syslog destinations.

Mode Superuser

Release First appearance: 1.0 / Most recent update: 1.1

Example

```
ACMEPACKET# notify nosyslog 100.1.20.30
```

packet-capture

The **packet-capture** command captures and views packets from a designated interface.

Syntax

```
packet-capture <state> <slot> <port>
```

Arguments

<state>	Select the state of packet capturing on the slot and port pair
Values	• enabled—Enable packet capturing • disabled—Disable packet capturing
<slot>	Select the media interface slot
Values	• 0—Left slot • 1—Right slot
<port>	Select the media interface port
Values	• 0—Leftmost port • 1—Second from left port • 2—Third from left port (not applicable for GigE cards) • 3—Rightmost port (not applicable for GigE cards)

Example

```
ACMEPACKET# packet-capture enabled 0 1
```

packet-capture clear

Syntax

```
packet-capture clear
```

Empty the packet buffer of captured packets

Example

```
ACMEPACKET# packet-capture clear
```

packet-capture modify

Syntax

```
packet-capture modify <integer> <y [es] | n [o]>
```

Arguments

<integer>	Enter the number of packets to show in the buffer
Default	100
Values	Min: 0 / Max: 1000
<y[es] | n[o]>	Signify whether the packet buffer wraps when full
Default	n

Values y[es] | n [o]

Example

```
ACMEPACKET# packet-capture modify 50 y
```

packet-capture show

Syntax

```
packet-capture show
```

Notes Displays a summary of the most recently captured packets on the screen

Example

```
ACMEPACKET# packet-capture show
```

packet-capture detail

Syntax

```
packet-capture detail <integer>
```

Arguments <integer> Identify the packet number to view

Mode Superuser

Release First appearance: 1.0 / Most recent update: 1.2.1

Example

```
ACMEPACKET# packet-capture detail 100
```

packet-trace

The **packet-trace-start** 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 are sent or received on the specified Net-Net SBC network interface.

Syntax

```
packet-trace <start> <stop>
```

Arguments <start> Start 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 are sent or received on the specified Net-Net SBC network interface.

- network-interface—The name of the network interface on the Net-Net SBC from which you want to trace packets; this value can be entered as either a name alone or as a name and subport identifier value (name:subportid)
- ip-address—IP address of the endpoint to and from which the Net-Net SBC will mirror calls

- local-port—Layer 4 port number on which the Net-Net SBC receives and from which it sends. This is an optional parameter; if no port is specified or if it is set to 0, then all ports will be traced.
- remote-port—Layer 4 port to which the Net-Net SBC sends and from which it receives. This is an optional parameter; if no port is specified or if it is set to 0, then all ports are traced.

<stop> Manually stop packet tracing on the Net-Net SBC. With this command you can either stop an individual packet trace or all packet traces that the Net-Net SBC is currently conducting.

- network-interface—The name of the network interface on the Net-Net SBC from which you want to stop packet tracing. This value can be entered either as a name alone or as a name and subport identifier value (name:subportid).
- ip-address—IP address of the endpoint to and from from which you want the Net-Net SBC to stop mirroring calls.
- local-port—Layer 4 port number on which to stop from receiving and sending. This is an optional parameter; if no port is specified or if it is set to 0, then all port tracing will be stopped.
- remote-port—Layer 4 port number on which to stop the Net-Net SBC from receiving and sending. This is an optional parameter; if no port is specified or if it is set to 0, then all port tracing will be stopped.

Mode Superuser

Release First appearance: 5.0

Example

```
ACMEPACKET# packet-trace start public:0 111.0.12.5
```

password-secure-mode

The **password-secure-mode** command allows you to enable and view the status of the password secure mode functionality on the Net-Net SBC.

Syntax

```
password-secure-mode <enable> <status>
```

Arguments

<enable> Enable the password secure mode on the Net-Net SBC

<status> Display the current status of the password secure mode functionality on the Net-Net SBC.

Mode Superuser

Release First appearance: 5.0

Example

```
ACMEPACKET# password-secure-mode enable
```

ping

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

Syntax

```
ping <ip-address> [vlan] [source-ip]
```

Arguments

<ip-address>	Enter the IP address of host to ping
<vlan>	Enter the network interface or vlan to use. This is an optional argument.
<source-ip>	Enter the source IP address to use. This is an optional argument.

Mode

Superuser

Release

First appearance: 1.0

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 default ping timeout is 64ms.

Example

```
ACMEPACKET# ping 100.20.11.30
```

prompt-enabled

The Net-Net SBC lets you know if a configuration has been changed and you’ve applied the `done` command, but have not saved and activated yet. When you issue the `done` command and return to Superuser mode, the ACLI prompt prefixes two asterisks (**). When you have saved, but not yet activated, the ACLI prompt prefixes one asterisk (*).

The **prompt-enabled** command allows you to decide whether or not you want the Net-Net SBC to give you this prompt. When this command is entered without an argument, the Net-Net SBC displays the current setting of the prompt.

Syntax

```
prompt-enabled <enabled | disabled>
```

<enabled>	Enable the `prompt-enabled` feature
<disabled>	Disable the `prompt-enabled` feature

Mode

Superuser

Release First appearance: 5.0

Example

```
ACMEPACKET# prompt-enabled disabled
```

realm-specifics

The **realm-specifics** command displays all configuration elements that have a specified realm ID configured.

Syntax

```
realm-specifics <realm-ID>
```

Arguments <realm-ID> Enter the name of realm

Mode User

Release First appearance: 2.0

Notes If a specified realm-ID appears as a configuration parameter in any configuration element, that full element is displayed on the screen. The **realm-specifics** command acts as a "grep" command for a realm name that appears in any configuration element.

Example

```
ACMEPACKET# realm-specifics test1
```

reboot

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

Syntax

```
reboot <arguments>
```

Arguments <arguments> The following are arguments for this command:

Values

- force—Reboot the Net-Net SBC system using the last running configuration. The confirmation prompt is bypassed when using this command.
- activate—Reboot the Net-Net SBC system using the last-saved configuration. You are presented with a confirmation prompt when using this command.
- no argument—Reboot the Net-Net SBC system using the last running configuration

Mode Superuser

Release First appearance: 1.0 / Most recent update: 1.2.1

Example

```
ACMEPACKET# reboot activate
```

request audit

The request audit command allows you to request the audit of a specified endpoint for SIP, H.323, or MGCP.

Syntax

```
request audit <registration>
```

<registration> Select SIP, H.323, or MGCP registration

Mode Superuser

Release First appearance: 5.0

Example

```
ACMEPACKET# request audit SIP
```

request collection

The **request collection** command allows you to start and stop data collection manually in one or all collection groups.

Syntax

```
request collection <start | stop | restart | > <collection object>
```

<start> Start data collection. If a collection object is not specified, collection is performed on all groups.

<stop> Stop data collection

<restart> Restart data collection in general or for the collection object specified

<purge> Delete all data files resident on the Net-Net SBC for collection function

<collection-object> Enter the collection groups you can configure to collect data information from. This is an optional argument and when no group is specified, the Net-Net SBC collects information from all groups. The following is a list of collection groups:

Values

- algd-ACL—Request collection on the ALGD ACL Operations group
- algd-state—Request collection on the ALGD State group
- fan—Request collection on the fan group
- h323-stats—Request collection on the H323 Statistics group
- interface—Request collection on the interface group
- mgcp-ACL—Request collection on ALGD MGCP ACL Status group
- mgcp-media-events—Request collection on the ALGD MGCP Media Events group
- mgcp-trans—Request collection on the ALGD MGCP transactions group
- session-agent—Request collection on the session agent group
- session-realm—Request collection on the session realm group
- sip-ACL-oper—Request collection on the SIP ACL Operations group

- sip-ACL-status—Request collection on the SIP ACL Status group
- sip-client—Request collection on the SIP Client Transaction group
- sip-errors—Request collection on the SIP Errors/Events group
- sip-policy—Request collection on the SIP Policy/Routing group
- sip-server—Request collection on the SIP Server Transaction group
- sip-sessions—Request collection on the SIP Session Status group
- sip-status—Request collection on the SIP Status group
- system—Request collection on the system group
- temperature—Request collection on the temperature group
- voltage—Request collection on the voltage group

Mode Superuser

Release First appearance: 5.0

Example

```
ACMEPACKET# request collection stop h323-stats
```

reset

The **reset** command resets statistic counters.

Syntax

```
reset <statistic>
```

Arguments

<statistic> The following is a list of specific statistics which you can tell the Net-Net SBC to reset:

Values

• algd—Reset algd-related statistics shown in the **show algd** command

• all—Reset the statistics shown in the following commands: **show sipd**, **show mbcd**, **show algd**, **show mbcd redundancy**, **show algd redundancy**, **show sipd redundancy**, **show redundancy mbcd**, **show redundancy algd**, **show redundancy**, **show memory**

• application—Reset the application statistics shown in the **show application** command

• ebmd—Reset EMBD statistics

• h323d—Reset the h323-related signaling statistics

• mbcd—Reset mbcd-related statistics shown in the **show mbcd** command (except statistics related to high availability)

• nsep-stats—Reset counters for NSEP-related statistics; to reset counters for a specific r-value, add the specific r-value to the end of the command

• redundancy—Reset the redundancy statistics shown in the **show mbcd redundancy**, **show algd redundancy**, **show sipd redundancy**, **show redundancy mbcd**, **show redundancy algd**, and **show redundancy sipd** commands

• security-associations—Reset Security Association statistics

• session-agent <hostname>—Reset statistics for a specified session agent

• sipd—Reset sipd statistics in the **show sipd** command

• snmp-community-table—Reset the counters on SNMP community table statistics

- trap-receiver—Reset the counters for trap receiver statistics
- net-management-control—Reset Network Management Control statistics
- lrt—Reset Local Routing statistics
- enum—Reset ENUM statistics
- dns—Reset DNS statistics

Mode Superuser

Release First appearance: 1.0.1 / Most recent update: 2.0.1

Notes This command is used to clear existing SIP, MBCD, ALGD, high availability, and application statistics and to reset the values for one or all of these statistics to zero. Executing the reset command sets the period and lifetime statistics totals to zero, but the active statistics counts are still retained.

Example

```
ACMEPACKET# reset h323d
```

restore-backup-config

The **restore-backup-config** command restores a named backup configuration.

Syntax

```
restore-backup-config <config-name> [saved | running]
```

Arguments

<config-name> Enter the name of backup configuration to restore

<saved> Restore the configuration to the last saved configuration. This is an optional argument.

<running> Restore the configuration to the last running configuration. This is an optional argument.

Mode Superuser

Release First appearance: 1.0

Notes Use the **display-backups** command to view the backups that are available to be restored.

Example

```
ACMEPACKET# restore-backup-config FEB_07.gz saved
```

save-config

The **save-config** command saves the current configuration to the Net-Net SBC's last-saved configuration, stored in flash memory.

Syntax

```
save-config
```

Mode Superuser

Release First appearance: 1.0 / Most recent update: 1.2.1

Notes

When this command is executed and resources are sufficient, the Net-Net SBC notifies you that the configuration has been saved successfully and the current configuration number will be incremented by one.

Example

```
ACMEPACKET# save-config
```

secret

The **secret** command sets the User and Superuser passwords.

Syntax

```
secret <user level>
```

Arguments

<user level> Each user level argument is listed and explained below.

Values

- login—Set the Net-Net SBC's user password
- enable—Set the Net-Net SBC's superuser password
- backup—Set the backup password
- config—Set the configuration password

Mode

Superuser

Release

First appearance: 1.0

Notes

For security reasons, the ACLI does not echo the password information you enter. You will be prompted to enter the new password twice for both commands. The passwords must be 6-9characters including one non-alpha character. No special characters are allowed, for example: #, %, &, *, etc. For security purposes, please use different passwords for the user and superuser accounts.

We recommend that you do not change the default User and Superuser passwords on Net-Net SBCs in your lab and testing facilities.

Example

```
ACMEPACKET# secret login
```

set-system-state

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

Syntax

```
set-system-state <state>
```

Arguments

<state> Select the system state

Values

- online—Enable online system state
- offline—Enable offline system state

Mode

Superuser

Release

First appearance: 2.0

Notes

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
```

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 about

Syntax

```
show about
```

This command displays credit information including version number for the Net-Net SBC.

Example

```
ACMEPACKET# show about
```

show accounting

This command displays a summary of statistics for all configured external accounting servers.

Syntax

```
show accounting <accounting-stats>
```

Arguments

Values

- ipport—Display the IP port accounting status
- all—Display the all accounting servers statistics

Mode Superuser

Release First appearance: S-C6.2.0

Notes Entering the **show accounting** command with no arguments returns the equivalent of the **show accounting all** command

Example

```
ACMEPACKET# show accounting ipport
```

show acl

Syntax

```
show acl <arguments>
```

Displays ACL information regarding either a specified entry or all entries.

Arguments

<arguments> The following are **show acl** arguments:

Values

- denied—Display denied ACL entries
- untrusted—Display untrusted ACL entries
- trusted—Display trusted ACL entries
- all—Display all ACL entries
- info—Display amount of space used in the CAM with regard to ACL entries. Number of entries, percent utilization, and

maximum entries are displayed for each ACL type. The following are the ACL types displayed:

–Denied

–Trusted

–Media

–Untrusted

- ip—Display the same output as show acl all, but takes an IP address as an argument to filter all ACL statistics for the given IP address
- reset—Reset the summary counts of all host ACL entries
- summary—Display a summary of all host ACL entries

Example

```
ACMEPACKET# show acl untrusted
```

show algd

Syntax

```
show algd <algd-stats>
```

Displays ALGD statistics for either a specified command or all command statistics.

Arguments

<algd-stats> The following is a list of algd stats:

Values

- statistics—Display MGCP statistics
- errors—Display MGCP error statistics
- acls—Display ACL statistics for MGCP
- rsip—Display RSIP command statistics
- rqnt—Display RQNT command statistics
- ntfy—Display NTFY command statistics
- crcx—Display CRCX command statistics
- mdcx—Display MDCX command statistics
- dlcx—Display DLCX command statistics
- auep—Display AUEP command statistics
- aucx—Display AUCX command statistics
- epcf—Display EPCF command statistics
- other—Display other MGCP command statistics
- redundancy—Display MGCP redundancy statistics
- all—Display all ALG statistics

Notes

Executing the **show algd** command with no arguments returns the equivalent of the **show algd statistics** command.

Example

```
ACMEPACKET# show algd rsip
```

show arp

Syntax

```
show arp
```

This command displays the current Internet-to-Ethernet address mappings in the ARP table.

The first section of the **show arp** command displays the following information about the wancom (rear) interface and media (front) interfaces:

- destination
- gateway
- flags
- reference count
- use
- interface

The second section of the **show arp** command displays contains the following information that refers only to media (front) interfaces:

- interface
- VLAN
- IP Address
- MAC address
- time stamp
- type

The third section of the show **arp command** shows reachability data for all configured IP gateways.

A section on ARP table information which contains CAM entry data is also included.

Example

```
ACMEPACKET# show arp
```

show backup-config

Note: The Net-Net SBC no longer uses this command.

Syntax

```
show backup-config <config-file>
```

Arguments

<config-file> Enter the name of the saved configuration file

The **show backup-config** command displays a specified configuration file saved on the Net-Net SBC's standard backup file directory.

Example

```
ACMEPACKET# show backup-config config1_25jun.gz
```

show buffers

Syntax

```
show buffers
```

This command shows memory buffer statistics divided into three sections.

- The first section displays the number of specific buffer types.
- The second section displays the total number of buffers and number of times the system failed, waited, or had to empty a protocol to find space.
- The third section displays the cluster pool table.

Example

```
ACMEPACKET# show buffers
```

show built-in-sip-manipulations

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

Syntax

```
show built-in-sip-manipulations
```

Mode Superuser

Release First appearance: S-C6.2.0

Example

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

show call-recording-server

Syntax

```
show call-recording-server [crs-id]
```

This command displays information regarding the IP call replication for call recording (IPRCR) feature configured on the Net-Net SBC. Entering this command without the optional IPRCR ID displays all IPRCR endpoints configured on the Net-Net SBC along with their state.

Arguments

[crs-id] You can specify a IPRCR whose information you want to view. When you specify an ID, the ACLI displays all session agents created for the IPRCR endpoint, it’s IP address, its state, and the last time a failover occurred.

Example

ACMEPACKET# show call-recording-server crs1

show clock

Syntax

```
show clock
```

This command displays the current date and time for your Net-Net SBC.

Example

```
ACMEPACKET# show clock
```

show configuration

Syntax

```
show configuration [to-file] [configuration-element]
```

This command entered without any arguments displays the current configuration. If you use any configuration element as an argument, this show command will display each instance of only the specified configuration element.

Arguments

<to-file> Send all output from the **show config** command to a specified file located on the local flash file system instead of to the ACLI. This is an optional argument.

<configuration-element>Specify the configuration element you want to view. This is an optional argument. If you do not specify a configuration element, the Net-Net SBC displays the entire configuration. The following is a list of valid configuration elements:

Values

- account-config—Show account-config configuration
- access-control—Show access-control configuration
- audit-logging—Show the audit logging configurations
- auth-params—Show the auth-params configurations
- authentication—Show the authentication configuration
- cert-status-profile—Show certificate status profile
- call-recording-server—Show call-recording-server configurations
- certificate-record—Show the certificate record configuration
- class policy—Show all ClassPolicy configuration
- data-flow—Show the data-flow configurations
- dns-config—Show all dns-config configurations
- dpd-params—Show the dpd-params configurations
- enum-config—Show the enum-config configuration
- ext-policy-server—Show the external-policy-server configuration
- h323-config—Show h323 configuration
- h323-stack—Show all h323-stack configurations
- ike-certificate-profile—Show the ike-certificate-profile configurations
- ike-config—Show the ike-config configuration
- ike-interface—Show the ike-interface configurations
- ike-sainfo—Show the ike-sainfo configurations
- ims-aka-profile—Show the ims-aka-profile configurations
- ipsec-global-config—Show the ipsec-global-config configurations
- iwf-stack—Show iwf-stack configuration
- host-route—Show all host-route configurations
- local-address-pool—Show the local-address-pool configurations
- local-policy—Show all local-policy configurations
- local-response-map—Show sip-local-map configuration
- login-config—Show the login configurations
- media-profile—Show all media-profile configurations
- media-manager—Show media-manager configuration

- media-policy—Show all MediaPolicy configurations
- mgcp-config—Show mgcp-config configurations
- network-interface—Show all network-interface configurations
- network-parameters—Show all network-parameters configurations
- ntp-config—Show ntp-config configuration
- capture-receiver—Show capture-receiver configurations
- phy-interface—Show all phys-interface configurations
- public-key—Show the public-key configurations
- realm-config—Show all realm configurations
- q850-sip-map—Show q850-sip-map configurations
- qos-constraints—Show the qos-constraints configurations
- redundancy-config—Show redundancy-config configuration
- sip-response-map—Show all response map configurations
- rph-profile—Show rph-profile configurations
- rph-policy—Show rph-policy configurations
- session-agent—Show all session-agent configurations
- session-group—Show all session-group configurations
- session-translation—Show all session-translation configurations
- session-router—Show session-router configuration
- sip-config—Show all sip-config configurations
- sip-feature—Show all sip-feature configurations
- sip-interface—Show all sip-interface configurations
- sip-manipulation—Show all of the sip-manipulation configurations
- sip-nat—Show all sip-nat configurations
- sip-profile—Show the sip-profile configurations
- sip-isup-profile—Show the sip-isup-profile configurations
- enforcement-profile—Show enforcement-profile configurations
- sip-q850-map—Show sip-q850-map configuration
- snmp-community—Show all snmp-community configurations
- ssh-config—Show the SSH configurations
- static-flow—Show all static-flow configurations
- steering-pool—Show all steering-pool configurations
- realm-group—Show realm-group configurations
- surrogate-agent—Show all of the surrogate-agent configurations
- system-config—Show system-config configuration
- tls-profile—Show TLS profile configurations
- translation-rules—Show all translation-rules configurations
- trap-receiver—Show all TrapReceiver configurations
- codec-policy—Show all codec-policy configurations
- local-routing-config—Show all local-routing configurations
- net-management-control—Show all net-management-control configurations
- security-association—Show all security-association configurations
- security-policy—Show all security-policy configurations
- password-policy—Show password-policy configuration

- session-constraints—Show all session-constraint configurations
- system-access-list—Show all system-access-list configurations
- tls-global—Show all tls-global configurations
- inventory—Display an inventory of all configured elements on the Net-Net SBC

Example

```
ACMEPACKET# show configuration snmp-community
```

show directory

This command displays a list of CDR file directories on the storage expansion module. Disk space on the Storage Expansion Module appears as a local volume on the Net-Net SBC.

Arguments

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

Mode Superuser

Release First appearance: S-C6.2.0

Example

```
ACMEPACKET# show directory /logs
```

show dns

Sytnax

```
show dns <arguments>
```

This command displays DNS statistics.

<arguments> Each valid dns argument is listed below:

Arguments

Values

- stats—Show the statistics for the dns configuration
- cache-entry—Look in the DNS cache for a specific entry

  Your entries must follow the formats below:

  –NAPTR records—NAPTR:abc.com

  –SRV records—SRV:_sip._tcp.abc.com

  –A records—A:abc.com

Example

```
ACMEPACKET# show dns stats
```

show enum

Sytnax

```
show enum <arguments>
```

Displays ENUM statistics for your Net-Net SBC.

<arguments> Each valid enum argument is listed below:

Arguments

Values

- stats—Show the statistics for the ENUM configuration
- cache-entry—Look in the ENUM cache for a specific entry
- lookup—Query an ENUM cache for a specific E.164 number
- status—Show the state of configured ENUM agents

–Enum Agent—Name of enum agents

–Queries Total—Number of enum queries

–Successful Total—Number of successful enum queries

–Not Found Total—Number of enum queries returning not found

–Timeout Total—Number of enum query timeouts

Example

```
ACMEPACKET# show enum lookup
```

show ext-band-mgr

Sytnax

```
show ext-band-mgr
```

This command shows the external bandwidth manager / PDP/RACF statistics for the active, period, and lifetime monitoring spans. COPS message counts are shown for Recent and lifetime monitoring spans.

Example

```
ACMEPACKET# show ext-band-mgr
```

show ext-clf-svr

Syntax

```
show ext-clf-svr
```

This command shows the CLF connection statistics for the active, period, and lifetime monitoring spans. CLF message counts are shown for Recent and lifetime monitoring spans.

Example

```
ACMEPACKET# show ext-clf-svr
```

show features

Syntax

```
show features
```

This command shows the currently enabled features based on added licenses.

Example

```
ACMEPACKET# show features
```

show h323d

Syntax

```
show h323d <h323d-statistics>
```

This command displays H.323 statistics for your Net-Net SBC.

Arguments

<h323d-stats> The following is a list of h323d statistics:

Values

- status—Display H.323 server status. The following statistics are displayed when this command is entered:

–Incoming Calls—Number of incoming H.323 calls; displayed for period, lifetime, and active counts

–Outgoing Calls—Number of outgoing H.323 calls; displayed for period, lifetime, and active counts

–Connected Calls—Number of currently connected H.323 calls; displayed for period, lifetime, and active counts

–Incoming Channels—Number of established incoming channels; displayed for period, lifetime, and active counts

–Outgoing Channels—Number of established outgoing channels; displayed for period, lifetime, and active counts

–Contexts—Number of established H.323 contexts; displayed for period, lifetime, and active counts

–Queued Messages—Number of messages queued; displayed for current and lifetime durations

–TPKT Channels—Number of TPKT channels open(ed); displayed for current and lifetime durations

–UDP Channels—Number of UDP channels open(ed); displayed for current and lifetime durations

- config—Display the H.323 configuration
- stacklist—Display the configured H.323 stacks
- stackconfig—Display detailed H.323 stack information. **show h323d stackconfig** <stack-name> shows detailed information about the stack-name you specify.
- agentlist—Display H323 session agents
- grouplist—Display H.323 session agent groups
- agentconfig—Display H.323 session agents configuration. **show h323d agentconfig** <hostname> shows detailed information about the session agent specified by its IP address in the <hostname> argument.
- groupconfig—Display H.323 session agent group configuration
- agentstats—Display H.323 session agent statistics. **show h323d agentstats** <agent> shows the activity for the H.323 session agent that you specify in the <agent> argument.
- groupstats—Display session information for session agent groups
- h323stats—Display H.323 stacks and statistics on the Net-Net SBC. The display identifies the H.323 stack by its name and then provides the data for each H.323 stack. **show h323d h323stats** <stack-name> displays detailed statistics for the

H.323 stack that you specify in the <stack name> argument. This information is displayed according to the following categories: H.225, H.245, and RAS.
• registrations—Display H.323 registration endpoints information
• sessions all—Display all H.323 sessions currently on the system
• sessions by-agent <agent name>—Display H.323 sessions for the session agent specified; adding **iwf** to the end of the command shows sessions for the IWF; adding **detail** to the end of the command expands the displayed information
• sessions by-callid <call ID>—Display H.323 sessions for the call ID specified; adding **iwf** to the end of the command shows sessions for the IWF; adding **detail** to the end of the command expands the displayed information
• sessions by-ip <endpoint IP address>—Display H.323 sessions for the specified IP address for an endpoint; adding **iw** to the end of the command shows sessions for the IWF; adding **detail** to the end of the command expands the displayed information
• sessions by-user <calling or called number.—Display H.323 sessions for the specified user; adding **iw** to the end of the command shows sessions for the IWF; adding **detail** to the end of the command expands the displayed information
• stack-alarms—Display a list of H.323 stacks that raised an alarm
• stackCallstats—Show a summary of H.323 call statistics for all stacks
• stackPvtstats—Show a summary of H.323 stack's internal data structures
• stackDisconnectInstats—Show a summary of H.323 pvt statistics for all stacks
• stackDisconnectOutstats— Show Summary of H.323 pvt statistics for all stacks

Executing the **show h323** command without any arguments will return the same output as using the status argument.

Example

```
ACMEPACKET# show h323d status
```

show health

Syntax

```
show health
```

In HA architectures, the show health command displays the following information:

- Health score
- Current Net-Net SBC HA state as active, standby, or out of service
- If media flow information is synchronized for all supported protocols: SIP, H.323, and MGCP (true/false). If media flow information is not available, `Media Synchronized disabled` will be displayed in the show health output.

- If SIP signaling information is synchronized (true/false). If SIP signaling is not available, `SIP Synchronized disabled` will be displayed in the show health output.
- If MGCP signaling information is synchronized (true/false). If MGCP signaling is not available, `MGCP Synchronized disabled` will be displayed in the show health output.
- If configuration information is synchronized (true/false). If configuration checkpointing is not available, `Config Synchronized disabled` will be displayed in the show health output.
- IP address of the current HA Net-Net SBC's active peer (no peer is denoted with an IP address of 0.0.0.0)
- Last message received from the HA Net-Net SBC peer
- A switchover log containing the last 20 switchover events

Example

```
ACMEPACKET# show health
```

show hosts

Syntax

```
show hosts
```

The **show hosts** command shows a list of remote hostnames, their IPv4 addresses, and aliases.

Examples

```
ACMEPACKET# show hosts
```

show imports

This command displays the list of sip-manipulation rules exported as files to the **/code/imports** directory.

Syntax

```
show imports
```

Mode Superuser

Release First appearance: S-C6.2.0

Example

```
ACMEPACKET# show imports
```

show interfaces

Syntax

```
show interfaces [brief]
```

The **show interfaces** command shows all information concerning the Net-Net SBC's rear interfaces:

- Flags (such as loopback, broadcast, promiscuous, ARP, running, and debug)
- Type
- Internet address

- VLAN ID (if applicable)
- Broadcast address (if applicable)
- Netmask
- Subnet mask (if applicable)
- Gateway (if applicable)
- Ethernet (MAC) address (if applicable)
- Route metric
- Maximum transfer unit size
- Number of octets sent and received on this interface (if applicable)
- Number of packets sent and received on this interface
- Number of non-unicast packets sent and received on this interface (if applicable)
- Number of unicast packets sent and received on this interface (if applicable)
- Number of multicast packets sent and received on this interface (if applicable)
- Number of input discards (if applicable)
- Number of input unknown protocols (if applicable)
- Number of input and output errors
- Number of collisions
- Number of drops

This command also displays information for loopback interfaces.

Arguments

<brief> Allows you to view key running statistics about the interfaces within a single screen. This is an optional argument.

Example

```
ACMEPACKET# show interfaces
```

show ip

Syntax

```
show ip <ip-stats>
```

Displays IP statistics for your Net-Net SBC.

Arguments

<ip-stats> The following is a list of valid ip-stats:

Values

- statistics—Display detailed IP statistics
- connections—Display all TCP and UDP connections
- sctp—Display all SCTP statistics
- TCP—Display all TCP statistics
- UDP—Display all UDP statistics

Executing the **show ip** command with no arguments returns the equivalent of the **show ip statistics** command.

Example

```
ACMEPACKET# show ip connections
```

show logfile

Syntax

```
show logfile [filename]
```

Display log files saved onto the Net-Net SBC. Entering this command without specifying a filename displays a complete list of log files.

Arguments

[filename] Specify the file whose logs you want to view. This is an optional argument.

Example

```
ACMEPACKET# show logfile
```

show loglevel

Syntax

```
show loglevel <task> [<type> | <verbose>] [filename]
```

This command displays loglevel statistics for your Net-Net SBC.

Arguments

<task> Enter the name of the Net-Net SBC task for which you are requesting information. By typing **all**, you are given an abbreviated display of all running processes.

<type> Select the log type whose level is to be displayed.

<verbose> Type **verbose** at the end of the **show loglevel** command to view a verbose display of either a specified task or all tasks. This is an optional argument.

[file-name] Enter the name of the specific logfile you want to view. This is an optional argument.

Example

```
ACMEPACKET# show loglevel sipd verbose
```

show lrt

Syntax

```
show lrt <route-entry | “stats”>
```

This command displays Local Routing Table (LRT) statistics on the Net-Net SBC.

Arguments

<route-entry> Display a specific entry in the LRT

<stats> Display all LRT statistics

Example

```
ACMEPACKET# show lrt stats
```

show mbcd

Syntax

```
show mbcd <mbcd-stats>
```

The **show mbcd** command displays MBCD statistics for your Net-Net SBC.

Arguments

<mbcd-stats> The following is a list of all mbcd-stats:

Values

- statistics—Display information related media flows established by the MBCD task. The following is a list of the MBCD statistics displayed when you enter this command:

–Client Sessions—Number of media sessions established by application clients of the MBCD task. Clients of MBCD include all signaling protocol tasks (SIP, MGCP, and H.323).

–Client Trans—Number of MBCD transactions in the application clients to create, modify and remove flows

–Contexts—Number of Contexts in the MBCD task. A Context represents the MBCD Server side of a media session. It contains all flows for the media session.

–Flows—Number of unidirectional flows established in MBCD. This includes both static flows defined by the signaling configuration, and dynamic flows for media sessions.

–Flow-Port—Number of "anchor" ports established by MBCD. MBCD maintains a mapping of the RTP steering port allocated for a flow so it can recognize flows that hairpin or spiral through the SD. This statistic reflects the number of entries in that table.

–Flow-NAT—Number of entries in the MBCD table that maps CAM entry indexes to flows. An entry is added to this table when a NAT entry is added to the CAM for a flow.

–Flow-RTCP—Number of special NAT table entries for RTCP. For Hosted NAT Traversal (HNT), the RTP and RTCP flows must be treated separately because the source port of the RTCP cannot be predicted.

–Flow-Hairpin—Number of hairpined/spiraled flows recognized by MBCD. This occurs when the signaling originates in an access realm, goes into a backbone realm, and then back into the same access realm, or another access realm on the same network interface.

–Flow-Released—Number of hairpined/spiraled flows released back into the original realm (when mm-in-realm or mm-in-network is disabled)

–MSM-Release—Number of flows that have been released as part of the SIP distributed (multi-system) release feature

–NAT Entries—Number of NAT table entries in the CAM established by MBCD for its flows. The NAT table can be viewed with the **show nat** commands.

–Free Ports—Number of ports available from configured steering pools

–Used Ports—Number of ports allocated to flows

–Port Sorts—Number of times the free ports list had to be sorted because consecutive ports (for RTP & RTCP) could not be found

–MBC Trans—Number of MBC transactions currently in progress

–MBC Ignored—Number of requests ignored because it is in standby mode in an HA configuration

–ARP Trans—Number of ARP Transactions. In some cases, MBCD must obtain the MAC address of the destination of a flow before an entry can be added to the NAT table. This statistic shows the number of outstanding ARP requests for MBCD flows.

- nat—Display statistics about MBCD's usage of the NAT Table and flow guard timer events. The following is a list of all MBCD NAT statistics:

–Adds—Number of times an entry was added to the NAT table

–Deletes—Number of times an entry was removed from the NAT table

–Updates—Number of times a NAT table entry was updated, including updates due to the "latching" event when the first packet for a flow is received

–Non-Starts—Number of initial flow guard timeouts (i.e. number of times a packet was never received for a NAT table entry)

–Stops—Number of subsequent flow guard timeouts (i.e. number of times that packets stopped for a NAT table entry)

–Timeouts—Number of total session limit timeouts (i.e. number of times the session limit for a flow was exceeded)

- acls—Display MBCD Access Control statistics, starting with a time stamp showing when the current period began. The following is a list of each entry count:

The following ACL statistics are shown for the Period and Lifetime monitoring spans:

–Static Trusted

–Static Blocked

–Dynamic Trusted

–Dynamic Blocked

The following ACL statistics are shown for the Lifetime monitoring span:

–Add Requests

–Added

–Removed

–Dropped

- errors—Display MBCD task error statistics, starting with a time stamp showing when the current period began; statistics for client and server are included. The following is a list of MBCD error statistics displayed when you enter this command:

Client statistics count errors and events encountered by applications that use the MBCD to set up and tear down media sessions:

–Client Errors—Number of errors in the client application related to MBC transactions that are otherwise uncategorized

–Client IPC Errors—Number of errors in the client application related to the Inter-Process Communication

–No Session (Open)—Number of MBC transactions creating or updating a media session that could not be sent to MBCD because the media session state information could not be located

–No Session (Drop)—Number of MBC transactions deleting a media session that could not be sent to MBCD because the media session state information could not be located

–Exp Flow Events—Number of flow timer expiration notifications received from the MBCD by all applications

–Exp Flow Not Found—Number of flow timer expiration notifications received from the MBCD by all applications for which no media session or flow information was present in the application

–Transaction Timeouts—Number of MBC transaction timeouts

Server statistics count errors and events encountered by MBCD:

–Server Errors—Number of uncategorized errors in the MBC server

–Server IPC Errors—Number of errors on the server related to the IPC

–Flow Add Failed—Number of errors encountered when attempting to add an entry to the NAT table

–Flow Delete Failed—Number of errors encountered when attempting to remove an entry from the NAT table

–Flow Update Failed—Number of errors encountered when attempting to update an entry in the NAT table upon receipt of the first packet for a media flow

–Flow Latch Failed—Number of errors when attempting to locate an entry in the NAT table upon receipt of the first packet for a media flow

–Pending Flow Expired—Number of flow timer expirations for pending flows that have not been added to the NAT table

–ARP Wait Errors—Number of errors and timeouts related to obtaining the Layer 2 addressing information necessary for sending media

–Exp CAM Not Found—Number that the NAT table entry for an expired flow could not find in the NAT table. This usually occurs due to a race condition between the removal of the NAT entry and the flow timer expiration notification being sent to MBCD.

–Drop Unknown Exp Flow—Number of flows deleted by the MBCD because of a negative response from the application to a flow timer expiration notification

–Unk Exp Flow Missing—Number of negative responses from the application to a flow timer expiration notification for which the designated flow could not be found in MBCD's tables

–Exp Notify Failed—Number of errors encountered when the MBCD attempted to send a flow timer expiration notification to the application

–Unacknowledged Notify—Number of flow expiration notification messages sent from MBCD to the application for which MBCD did not receive a response in a timely manner

–No Ports Available—Number of steering port allocation requests not be satisfied due to a lack of free steering ports in the realm

–Invalid Realm—Number of flow setup failures due to an unknown realm in the request from the application

–Insufficient Bandwidth—Number of flow setup failures due to insufficient bandwidth in the ingress or egress realm

–Open Streams Failed—Number of MBC transactions creating or updating a media session that could not be sent to the MBCD because the media session state information could not be located

–Drop Streams Failed—Number of MBC transactions deleting a media session that could not be sent to MBCD because the media session state information could not be located

–Drop/Exp Flow Missing—Number of negative responses from the application to a flow timer expiration notification for which the designated flow could not be found in MBCD’s tables

–Stale Ports Reclaimed—For an HA node, this is the number of ports that were reclaimed when the standby had a stale flow that the active system replaced; when the flow is replaced, the steering ports are also reallocated properly (i.e., according to the active system)

–Stale Flows Replaced—For an HA node, this is the number of times that the standby system had entries in its flow tables that did not match those on the active system; the active system replaced the standby’s stale flows with valid ones

–Pipe Alloc Errors—For communication between the Net-Net SBC’s tasks (sipd, h323d, and algd) and middlebox control protocol tasks, this is the number of times that buffer allocation failed

–Pipe Write Errors—For communication between the Net-Net SBC’s tasks (sipd, h323d, and algd) and middlebox control protocol tasks, this is the number of times that messages were not sent (possibly because of a pipe/buffer allocation error)

- add—List statistics of mbcd transactions that include an Add command. Statistics are given for Recent, Total, and PerMax periods. The following is a list of MBCD add statistics displayed when you enter this command:

Add incoming statistics when an add message is received by the Net-Net SBC:

–Incoming requests received—Number of mbcd add commands received

–Incoming replies sent—Number of responses sent in response to an mbcd add

–Incoming errors sent—Number of errors sent in response to an mbcd add

Add outgoing statistics when an mbcd add message is sent by the Net-Net SBC:

–Outgoing requests sent—Number of MBCD add commands sent from the Net-Net SBC

–Outgoing replies received—Number of responses received in response to a sent Add message

–Outgoing errors received—Number of errors received in response to a sent Add message

- modify—List statistics of mbcd transactions that include a modify command. The following is a list of MBCD modify statistics displayed when you enter this command:

Add incoming statistics when a modify message is received by the Net-Net SBC:

–Incoming requests received—Number of mbcd modify commands received

–Incoming replies sent—Number of responses sent in response to an mbcd modify

–Incoming errors sent—Number of errors sent in response to an mbcd modify

Add outgoing statistics when an mbcd modify message is sent by the Net-Net SBC.

–Outgoing requests sent—Number of MBCD modify commands sent from the Net-Net SBC

–Outgoing replies received—Number of responses received in response to a sent modify message

–Outgoing errors received—Number of errors received in response to a sent modify message

- subtract—List statistics of mbcd transactions that include a subtract command. The following is a list of MBCD subtract statistics that are displayed when you enter this command:

Add incoming statistics when a subtract message is received by the Net-Net SBC:

–Incoming requests received—Number of mbcd subtract commands received

–Incoming replies sent—Number of responses sent in response to an mbcd subtract

–Incoming errors sent—Number of errors sent in response to an mbcd subtract

Add outgoing statistics when an MBCD subtract message is sent by the Net-Net SBC:

–Outgoing requests sent—Number of MBCD subtract commands sent from the Net-Net SBC

–Outgoing replies received—Number of responses received in response to a sent subtract message

–Outgoing errors received—Number of errors received in response to a sent subtract message

- notify—List statistics of mbcd transactions that include a notify command. The following is a list of MBCD notify statistics that are displayed when you enter this command:

Add incoming statistics when a notify message is received by the Net-Net SBC:

–Incoming requests received—Number of mbcd notify commands received

–Incoming replies sent—Number of responses sent in response to an mbcd notify

–Incoming errors sent—Number of errors sent in response to an mbcd notify

Add outgoing statistics when an mbcd notify message is sent by the Net-Net SBC:

–Outgoing requests sent—Number of MBCD notify commands sent from the Net-Net SBC

–Outgoing replies received—Number of responses received in response to a sent notify message

–Outgoing errors received—Number of errors received in response to a sent notify message

- other—List statistics of mbcd transactions related to non-compliant protocols used by specific customers. The following is a list of statistics displayed when you enter this command:

Add incoming statistics when a customer-specific message is received by the Net-Net SBC:

–Incoming requests received—Number of customer-specific mbcd commands received

–Incoming replies sent—Number of responses sent in response to a customer-specific mbcd command

–Incoming errors sent—Number of errors sent in response to a customer-specific mbcd command

Add outgoing statistics when a customer-specific mbcd message is sent by the Net-Net SBC:

–Outgoing requests sent—Number of MBCD notify commands sent from the Net-Net SBC

–Outgoing replies received—Number of responses received in response to a customer-specific message

–Outgoing errors received—Number of errors received in response to a sent customer-specific message

- 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

- redundancy—Display the equivalent of the **show redundancy mbcd command**
- all—Display information related to many of the show mbcd subcommands. Only those MBC messages for which there are statistics are shown. Rather than entering the individual subcommands, all information is displayed for the following:

–MBC status

–NAT entries

–MBC errors

–MBC messages including: add, modify, subtract, notify, and other

- stun—Display STUN server statistics

–Servers—The number of STUN servers (the same as the number of realms configured with a STUN server).

–Server Ports—Number of ports per STUN server; there will be four ports per STUN server.

–Binding Requests—Number of STUN Binding Request messages received by all STUN servers.

–Binding Responses—Number of STUN Binding Response messages sent by all STUN servers.

–Binding Errors—Number of STUN Binding Error messages sent by all STUN servers.

–Messages Dropped—Number of messages dropped by all STUN servers.

Example

```
ACMEPACKET# show mbcd errors
```

show media

Syntax

```
show media <media-stats> <slot> <port> <vlan>
```

Arguments

<media-stats> The following is a list of admin state arguments:

Values

- classify—Display network processor statistics; requires slot and port arguments
- host-stats—Display statistics for the host processor including number of packets received at a specific port and types of packets received; requires slot and port arguments
- frame-stats—Display frame counts and drops along the host path; does not require port and slot specification
- network—Display network interface details; does not require port and slot specification
- physical—Display all phy-interface information; does not require port and slot specification
- phy-stats—Display data/packets received on the front interface (media) ports; shows the physical level of front interface statistics according to slot and port numbers and is displayed according to received data/packets and transmitted data/packets; requires slot and port arguments
- tm-stats—Show all of the traffic manager statistics and shows the results of the traffic policing due to NetSAFE configuration.
- utilization—Show physical level utilization

<slot> Select the media interface slot

Values 0 (left slot) | 1 (right slot)

<port>	Select the media interface port
Values	0 (leftmost) | 1 | 2 | 3 (rightmost)
<vlan>	Enter the VLAN ID if required

Example

```
ACMEPACKET# show media network 1 2 0
```

show memory

Syntax

```
show memory <memory-stats>
```

This command displays statistics related to the memory of your Net-Net SBC.

Arguments

<memory-stats> The following is a list of each memory statistic:

Values

- usage—Display system-wide memory usage statistics. If the show memory command is issued without any arguments, the equivalent of this argument is displayed.
- application—Display application memory usage statistics
- l2—Display layer 2 cache status
- l3—Display layer 3 cache status

Example

```
ACMEPACKET# show memory application
```

show mgcp

Syntax

```
show mgcp <type>
```

This command displays MGCP statistics on the Net-Net SBC.

<type> The type of MGCP statistics you want to view.

Values

- acls—Display MGCP ACL statistics
- all—Display all ALG statistics
- aucx—Display AUCX command statistics
- auep—Display AUEP command statistics
- crcx—Display CRCS command statistics
- dlcx—Display DLCX command statistics
- epcf—Display EPCF command statistics
- errors—Display MGCP error statistics
- mdcx—Display MDCX command statistics
- ntfy—Display NTFY command statistics
- other—Display Other MGCP command statistics
- redundancy—Display MGCP redundancy statistics
- rqnt—Display RQNT command statistics
- rsip—Display RSIP command statistics
- statistics—Display ALG MGCP statistics

Example

```
ACMEPACKET# show mgcp ntfy
```

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 nat

Syntax

```
show nat <display-type>
```

Displays NAT statistics for a specified NAT time on the Net-Net SBC.

Arguments

<display-type> The following is a list of each method to display the nat table:

Values

- by-index —Display a specified range of entries in the NAT table, with a maximum of 5024 entries. The syntax for using the show nat by-index command is:
  show nat by-index <*starting entry*> <*ending entry*>
  The default range is 1 through 200. The range corresponds to line numbers in the table, and not to the number of the entry itself.
- in-tabular —Display a specified range of entries in the NAT table display in table form, maximum of 5024 entries.
  The syntax is modeled on the show nat by-index command:
  show nat in-tabular <*starting entry*> <*ending entry*>
- by-addr—Display NAT table information matching source and destination addresses. You must specify source address (SA) and/or destination address (DA) values.
  If no addresses are entered, the Net-Net SBC shows all of the table entries. NAT entries can be matched according to SA or DA or both.
  show nat by-addr <*source IPv4 address*> <*destination IPv4 address*>
- info—Display general NAT table information. The output is used for quick viewing of a Net-Net SBC’s overall NAT functions, including the maximum number of NAT table entries, the number of used NAT table entries, the length of the NAT table search key, the first searchable NAT table entry address, the length of the data entry, the first data entry address, and whether or not aging and policing are enabled in the NAT table.
- flow-info—Display NAT table entry debug information. You must specify if you want to view NAT data for all entries or if you want to specify an address or a switch ID.

show nat flow-info *<all> <by-addr><by-switchid>*

Example

```
ACMEPACKET# show nat by-index
```

show net-management-control

Syntax

```
show net-management-control [string | all]
```

This command displays network management control statistics on the Net-Net SBC.

Arguments

<string> Enter a name for the **net-management-control** configuration whose statistics you want to view. This is an optional argument.

<all> Enter **all** to view statistics for all net-management-control entries. This is an optional argument.

Example

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

show nsep-stats

Syntax

```
show nsep-stats [all | rvalue]
```

The **show nsep-stats** command displays information about inbound sessions and r-values.

Arguments

<all> Display information about inbound sessions and r-values for the Net-Net SBC's NSEP support feature. This is an optional argument.

<rvalue> View statistics for a specific r-value. An r-value is a namespace and priority combination entered in the following format: `namespace.priority`. The display also shows the specified r-value for which it is displaying data. This is an optional argument.

Mode User, Superuser

Release First appearance: 5.1

show ntp

Syntax

```
show ntp <arguments>
```

The **show ntp** command displays information about NTP servers configured for use with the system

Arguments

<arguments> The following is a list of valid arguments:

Values

• servers—Display information about the quality of the time being used in terms of offset and delay measurement; maximum error bounds are also displayed
• status—Display information about configuration status, NTP daemon synchronization, NTP synchronizations in process, if NTP is down

Mode User, Superuser

Release First appearance: 5.1

Example

```
ACMEPACKET# show ntp servers
```

show packet-trace

Syntax

```
show packet-trace
```

The **show packet-trace** command allows you to check whether the Net-Net SBC’s tracing status is currently enabled or disabled.

Mode Superuser

Release First appearance: 5.0

Example

```
ACMEPACKET# show packet-trace
```

show power

The **show power** command allows you to view Net-Net SBC power supply information including the state of the power supply and the installation position.

Example

```
ACMEPACKET# show power
```

show privilege

Syntax

```
show privilege
```

Displays the current level of privilege on which the user is operating:

- Privilege level 0 refers to Level 0:User Mode
- Privilege level 1 refers to Level1: Superuser Mode

Example

```
ACMEPACKET# show privilege
```

show processes

Syntax

```
show processes <process>
```

The **show processes** command, executed without arguments, displays statistics for all active processes. The following task information is displayed: names of tasks, entries, task identification codes, task priorities, status, program counter, error numbers, and protector domain (PD) identification.

Arguments

<process> The following is a list of each process argument:

Values

- sysmand—Display sysmand process statistics related to the system's startup tasks
- acliSSH0— Show acliSSH0 process statistics
- acliSSH1—Show acliSSH1 process statistics
- acliSSH2—Show acliSSH2 process statistics
- acliSSH3— Show acliSSH3 process statistics
- acliSSH4— Show acliSSH4 process statistics
- acliTelnet0— Show acliTelnet0 process statistics
- acliTelnet1— Show acliTelnet1 process statistics
- acliTelnet2— Show acliTelnet2 process statistics
- acliTelnet3— Show acliTelnet3 process statistics
- acliTelnet4— Show acliTelnet4 process statistics
- ebmd— Show embd process statistics
- h323d— Show h323d process statistics
- lid— Show lid process statistics
- pusher— Show pusher process statistics
- snmpd— Show snmpd process statistics
- cliworker— Show CliWorker process statistics
- berpd—Display statistics for the border element redundancy protocol tasks; only accessible if your system is operating in an HA node
- lemd—Display lemd process statistics
- brokerd—Display brokerd process statistics
- mbcd—Display mbcd process statistics related to the middlebox control daemon
- radd—Display radd process statistics related to RADIUS; only accessible if your Net-Net SBC is using RADIUS
- algd—Display algd process statistics
- sipd—Display sipd process statistics
- acliConsole—Display acliConsole process statistics
- current—Show the date and time that the current monitoring period began and statistics for the current application process events. The following fields explain the output of the **show processes current** command:

–Svcs—Number of times the process performs actions for different services (e.g., sockets, timeout queues, etc.)

–TOQ—Number of active timers (in the Timed Objects) placed in the timeout queue

–Ops—Number of times the process was prompted (or polled) to perform an action

–Rcvd—Number of messages received by the process

–Sent—Number of messages sent by the process

–Events—Number of times a TOQ entry timed out

–Alrm—Number of alarms the process sent

–Slog—Number of times the process wrote to the system log

–Plog—Number of times the process wrote to the process log

–CPU—Average CPU usage over the last minute

–Now—CPU usage for the last second

- total—Display the total statistics for all of the application processes applicable to your Net-Net SBC. The following fields explain the output of the **show processes total** command:

–Svcs—Number of times the process performed actions for different services (e.g., sockets, timeout queues, etc.)

–Rcvd—Number of messages received by the process

–Sent—Number of messages sent by the process

–Events—Number of times a TOQ entry timed out

–Alarm—Number of alarms the process sent

–Slog—Number of times the process wrote to the system log

–Plog—Number of times the process wrote to the process log

–CPU—Average CPU usage since last reboot

–Max—Maximum percentage of CPU usage in a 60 second period

- CPU—Display information about the CPU usage for your Net-Net SBC, categorized on a per task/process basis. The following fields explain the output of the **show processes cpu** command:

–Task Name—Name of the Net-Net SBC task or process

–Task Id—Identification number for the task or process

–Pri—Priority for the CPU usage

–Status—Status of the CPU usage

–Total CPU—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—CPU usage in the last second

- collect—Show collector process statistics
- all—Display many of the show processes subcommands. You can see all of the information displayed for the processes including the following:

–sysmand

–tSnmpd

–berpd

–lemd

–brokerd

–mbcd

–radd

–tCliWorker

Only those processes for which there are statistics will be shown.

- memory—Show memory process statistics

Example

```
ACMEPACKET# show processes sysmand
```

show prom-info

Syntax

```
show prom-info <devices>
```

The **show prom-info** command displays hard-coded information about Net-Net SBC hardware.

Arguments

<devices> The following is a list of each prom-info argument:

Values

- mainboard—Display mainboard PROM information
- CPU—Display CPU PROM information
- PHY0—Display left physical interface card PROM information
- PHY1—Display right physical interface card PROM information
- CAM— Display CAM PROM information

Note: show prom-info CAM is not supported.

- all—Show all above PROM information

Example

```
ACMEPACKET# show prom-info mainboard
```

show qos

Syntax

```
show qos <history | usage>
```

The **show qos** command displays information about the Net-Net SBC's QoS FPGA.

<history>	Display the QoS history for an FPGA entry
<revision>	Display the QoS FPGA hardware revision
<usage>	Display the current QoS FPGA usage

Example

```
ACMEPACKET# show qos usage
```

show radius

Syntax

```
show radius <radius-stats>
```

This command displays radius statistics.

Arguments

<radius-stats> The following is a list of each radius argument:

Values

- accounting—Display the status of established RADIUS accounting connections. A successful RADIUS connection is displayed as READY, and an unsuccessful connection is displayed as DISABLED.

  The command's output is divided into three sections:

  Client Display—Display general accounting setup (as established in the accountconfig element); includes the following information:

–state of the RADIUS client

–accounting strategy

–IP address and port on which the Net-Net SBC's server is listening

–maximum message delay in seconds

–number of configured accounting servers

Waiting Queue—Display the number of accounting (RADIUS) messages waiting to be sent that are queued on the client side

<IP Address:Port>—IP Address and port headings indicated will be per the referenced RADIUS server active on the IP Address and port shown; also includes information about the accounting server's state

- authentication—Show the authentication statistics
- all—Show both accounting and authentication statistics
- cdr—Display all CDR statistics

Example

```
ACMEPACKET# show radius authentication
```

show ramdrv

Displays RAMdrive usage, including the log cleaner threshold values and the size of the most recently saved configuration.

Example

```
ACMEPACKET# show ramdrv
```

show realm

Syntax

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

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

<realm-id> Specify the realm-id whose realm-specific data you want to view; includes QoS routing data for internal and external transactions

Example

ACMEPACKET# show realm realm1

show redundancy

Syntax

```
show redundancy <redundancy-stats>
```

Display HA statistics for a redundant Net-Net SBC.

Arguments

<redundancy-stats> The following is a list of all redundancy arguments:

Values

- mbcd—Display the synchronization of media flows for the members of an HA Net-Net SBC pair
- algd—Display the synchronization of MGCP signaling for the members of an HA Net-Net SBC pair
- sipd—Display the synchronization of SIP signaling for the members of an HA Net-Net SBC pair
- config—Display the synchronization of configuration information for the members of an HA Net-Net SBC pair
- collect—Display the Collect redundancy statistics
- link—Display the Link redundancy statistics
- radius-cdr—Display the number of CDRs that have been synchronized from active to standby when the local CDR storage is enabled
- iked—Display IKE redundancy statistics
- manuald—Display manual redundancy statistics
- rotated-cdr—Display statistics for rotated CDRs on the Net-Net SBC

The following HA statistics are shown for the Period and Lifetime monitoring spans.

–Queued entries—Number of transactions not yet sent to standby Net-Net SBC peer

–Red Records—Total number of HA transactions created

–Records Dropped—Number of HA transaction records lost because the standby Net-Net SBC fell behind in synchronization

–Server Trans—Number of HA transactions in which the Net-Net SBC acted was the server

–Client Trans—Number of HA transactions where the Net-Net SBC was the client

The following HA transaction statistics are shown for the Lifetime monitoring span.

–Requests received—Number of HA requests received by the Net-Net SBC, acting as server

–Duplicate requests—Number of situations in which an HA request was received by the Net-Net SBC, and (acting as the server side in the client-server relationship) the Net-Net SBC responded to it, but the client system did not receive the response in time and retransmitted its original request

–Success responses—Number of HA requests that were received followed by a successful response to the client

–Error responses—Number of HA requests that were received followed by a error response to the client

–Request sent—Number of HA requests that were sent by the standby Net-Net SBC

–Retransmission sent—Number of times an HA request was retransmitted after no response

–Success received—Number of HA requests receiving a reply from the other SD in an HA pair

–Errors received—Number of errors received in response to HA requests

–Transaction timeouts—Number of HA transactions that timed out

The numerical identifier for the last redundant transaction processed is also displayed in the **show redundancy** output.

Example

```
ACMEPACKET# show redundancy sipd
```

show registration

Syntax

```
show registration <protocol> <by-ip | by-user> <ip-address | by-
endpoint> | <statistics>
```

To expand the capabilities of the **show registration** command, enter either **by-user** or **by-ip** after the protocol argument. The “statistics” argument applies only to the Net-Net 3800.

Arguments

<protocol> Select the protocol whose registration you want to view

Values
- sipd
- mgcp
- h323

<by-user> Show registration information for a specific IP address

Values
- IP address—IP address of an endpoint, or a wildcarded IP address value with an asterisk (*) at the end.

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

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

<by-registrar> 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> 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-endpoint> Show registration information for a specific phone number or username

Values • IP address—IP address of an endpoint, or a wildcarded IP address value with an asterisk (*) at the end. This command is only available if you configure the reg-via-key parameter in the SIP interface configuration prior to endpoint registration. The reg-via-key parameter keys all registered endpoints by IP address and username.
• Phone number or username—Full phone number or username, or a wildcarded number/username with an asterisk (*)

The display shows statistics for the Period and Lifetime monitoring spans.

–user Entries—The number of unique SIP Addresses of Record in the cache

–Local Contacts—The number of contact entries in the cache

–Free Map Ports—The number of ports available in the free signaling port pool

–Used Map Ports—The number of signaling ports allocated for registration cache entries

–Forwards—Number of registration requests forwarded to the real registrar

–Refreshes—Number of registrations the Net-Net SBC answered without having to forward registrations to the real registrar

–Rejects—Number of unsuccessful registrations sent to real registrar

–Timeouts—Number of times a refresh from the HNT endpoint was not received before the timeout

–Fwd Postponed—The number of times sipd responded out of the cache instead of forwarding to the registrar due to the max-register-forward threshold

–Fwd Rejected—The number of REGISTER 503s done after checking for a cached entry

–Refr Extension—The number of times the max-register-refresh threshold was exceeded. The "Active" and "High" show the number of seconds added to the expiration

–Refresh Extended—The number of times the expire time in a REGISTER response was extended due to the max-register-refresh threshold

–Surrogate Regs— The total number of surrogate registers

–Surrogate Sent— The total number of surrogate registers sent

–Surrogate Reject—The total number of surrogate register rejects

–Surrogate Timeout— The total number of surrogate register timeouts

<statistics> Display a table of counters showing the total and periodic number of registrations, by protocol. This argument applies to the Net-Net 3800 only.

Example

```
ACMEPACKET# show registration sipd by user*
```

show route-stats

Syntax

```
show route-stats
```

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

Example

```
ACMEPACKET# show route-stats
```

show routes

Syntax

```
show routes
```

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

- destination
- netmask
- TOS
- gateway
- flags
- reference count
- use
- interface
- protocol information

Example

```
ACMEPACKET# show routes
```

show running-config

Syntax

```
show running-config <to-file> | <configuration-element>  <element
key field>
```

The **show running-config** entered without any arguments displays the running configuration information in use on the Net-Net SBC. If you use any configuration element key field as an argument, this show command will display only that specified configuration element.

Arguments

<to-file> Send all output from the **show config** command to a specified file located on the local flash file system instead of to the ACLI. This is an optional argument.

<configuration-element> Specify the configuration element you want to view. This is an optional argument. If you do not specify a configuration element, the Net-Net SBC displays the entire configuration. The following is a list of valid configuration elements:

Values

- access-control—Show access-control configuration
- account-config—Show account-config configuration
- audit-logging—Show the audit logging configurations
- auth-params—Show the auth-params configurations
- authentication—Show authentication configuration
- call-recording-server—Show call-recording-server configurations
- certificate-record—Show certificate records configuration
- cert-status-profile—Show certificate status profile
- ext-policy-server—Show external-policy-server configuration
- h323-config—Show h323-config configuration
- h323-stack—Show all h323-stack configurations
- data-flow—Show the data-flow configurations
- dpd-params—Show the dpd-params configurations
- enum-config—Shows enum-config configuration
- ike-certificate-profile—Show the ike-certificate-profile configurations
- ike-config—Show the ike-config configuration
- ike-interface—Show the ike-interface configurations
- ike-sainfo—Show the ike-sainfo configurations
- ims-aka-profile—Show the ims-aka-profile configurations
- ipsec-global-config—Show the ipsec-global-config configurations
- iwf-stack—Show iwf-stack configuration
- host-route—Show all host-route configurations
- local-address-pool—Show the local-address-pool configurations
- local-policy—Show all local-policy configurations
- media-profile—Show all media-profile configurations

- media-manager—Show media-manager configuration
- mgcp-config—Show mgcp-config configuration
- dns-config—Show all dns-config configurations
- network-interface—Show all network-interface configurations
- network-parameters—Show all network parameters
- ntp-config—Show ntp-config configuration
- capture-receiver—Show capture-receiver configurations
- phys-interface—Show all phys-interface configurations
- public-key—Show the public-key configurations
- qos-constraints—Show the qos-constraints configurations
- realm—Show all realm configurations
- MediaPolicy—Show all MediaPolicy configurations
- ClassPolicy—Show all ClassPolicy configurations
- redundancy-config—Show redundancy-config configuration
- ResponseMap—Show all ResponseMap configurations
- rph-profile—Show rph-profile configurations
- rph-policy—Show rph-policy configurations
- session-agent—Show all session-agent configurations
- session-group—Show all session-group configurations
- session-translation—Show all session-translation configurations
- translation-rules—Show all translation-rules configurations
- session-router—Show session-router configuration
- sip-config—Show all sip-config configurations
- sip-feature—Show all sip-feature configurations
- sip-interface—Show all sip-interface configurations
- sip-manipulation—Show all sip-manipulation configurations
- sip-nat—Show all sip-nat configurations
- sip-profile—Show the sip-profile configurations
- sip-isup-profile—Show the sip-isup-profile configurations
- sip-response-map—Show all SIP response map objects
- enforcement-profile—Show enforcement-profile configurations
- snmp-community—Show all snmp-community configurations
- static-flow—Show all static-flow configurations
- steering-pool—Show all steering-pool configurations
- realm-group—Show realm-group configurations
- ssh-config—Show the SSH configurations
- surrogate-agent—Show all surrogate-agent configurations
- system-config—Show system-config configuration
- tls-profile—Show tls configurations
- TrapReceiver—Show all TrapReceiver configurations
- local-response-map—Show sip-local-map configuration
- sip-q850-map—Show sip-q850-map configuration
- q850-sip-map—Show q850-sip-map configuration
- codec-policy—Show all codec-policy configurations
- local-routing-config—Show all local-routing configurations
- net-management-control—Show all net-management-control configurations

- security-association—Show all security-association configurations
- security-policy—Show all security-policy configurations
- password-policy—Show password-policy configuration
- session-constraints—Show all session-constraint configurations
- system-access-list—Show all system-access-list configurations
- tls-global—Show all tls-global configurations
- tunnel-orig-params—Show tunnel origination parameters
- inventory—Display an inventory of all configured elements on the Net-Net SBC

Example

```
ACMEPACKET# show running-config host-route
```

show sa

Syntax

`show sa` or `show sa stats`

This command displays the security associations information for IMS-AKA.

Example

```
ACMEPACKET# show sa stats
```

show security

Syntax

```
show security <argument>
```

This command displays configured security information on the Net-Net SBC.

Arguments

<certificates> Show certificate information on the Net-Net SBC.

Values

- brief—Display a brief certificate description
- detail—Display a detailed certificate description
- pem—Display certificate information in Privacy Enhanced Mail (PEM) form

<ipsec> Show IPSEC related information on the Net-Net SBC. You can specify the name of the network interface whose IPSEC information you want to view.

Values

- sad—Display IPSEC SAD information
- spd—Display IPSEC SDP information
- statistics—Display IPSEC statistics
- status—Display the interface IPSEC status

<ssm-accelerator> Display the SSM status on the Net-Net SBC

<tls> Display TLS related information

Values

- session-cache—Display TLS session cache information

<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

<ike> Displays statistics for IKE transactions

Values
- data-flow—Display data-flow information for IKE2
- local-address-pool<pool ID | brief>—Display local address pool information for IKE2

-pool ID—Display a specific local address pool in detail
-brief—Display all local address pools briefly

Example

```
ACMEPACKET# show security ipsec spd m10
```

show sessions

Syntax

```
show sessions
```

Displays session capacity for license and session use.

–Capacity—The total call capacity based on license

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/MGCP connection) 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

–MGCP Connections—The total current active MGCP connections

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 Session 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.

Example

```
ACMEPACKET# show sessions
```

show sipd

Syntax

```
show sipd <sipd-stats>
```

The **show sipd** command displays SIP statistics on your Net-Net SBC.

Arguments

<sipd-stats> The following is a list of all **show sipd** arguments:

Values

- status—Display information about SIP transactions. These statistics are given for the Period and Lifetime monitoring spans. This display also provides statistics related to SIP media events. The following statistics are displayed when using the **show sipd status** command.

–Dialogs—Number of end-to-end SIP signaling connections

–CallID Map—Total number of successful session header Call ID mappings

–Sessions—Number of sessions established by an INVITE

–Subscriptions—Number of sessions established by SUBSCRIPTION

–Rejections—Number of rejected INVITEs

–ReINVITEs—Number of ReINVITEs

–Media Sessions—Number of successful media sessions

–Media Pending—Number of media sessions waiting to be established

–Client Trans—Number of client transactions

–Server Trans—Number of server transactions that have taken place on the Net-Net SBC

–Resp Contexts—Number of current response contexts

–Saved Contexts—Total number of saved contexts

–Sockets—Number of active SIP sockets

–Req Dropped—Number of requests dropped

–DNS Trans—Number of DNS transactions

–DNS Sockets—Number of DNS Sockets

–DNS Results—Number of dns results

–Session Rate—The rate, per second, of SIP invites allowed to or from the Net-Net SD during the sliding window period. The rate is computed every 10 seconds

–Load Rate—Average Central Processing Unit (CPU) utilization of the Net-Net SD during the current window. The average is computed every 10 seconds unless the load-limit is configured in the SIPConfig record, in which case it is 5 seconds

- errors—Display statistics for SIP media event errors. These statistics are errors encountered by the SIP application in processing SIP media sessions, dialogs, and session descriptions (SDP). Errors are only displayed for the lifetime monitoring span.

–SDP Offer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Offer in the Offer/Answer model (RFC 3264)

–SDP Answer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Answer in the Offer/Answer model (RFC 3264)

–Drop Media Errors—Number of errors encountered in tearing down the media for a dialog or session that is being terminated due to: a) non-successful response to an INVITE transaction; or b) a BYE transaction received from one of the participants in a dialog/session; or c) a BYE initiated by the Net-Net SBC due to a timeout notification from MBCD

–Transaction Errors—Number of errors in continuing the processing of the SIP client transaction associated with setting up or tearing down of the media session

–Missing Dialog—Number of requests received by the SIP application for which a matching dialog count not be found

–Application Errors—Number of miscellaneous errors in the SIP application that are otherwise uncategorized

–Media Exp Events—Flow timer expiration notifications received from MBCD

–Early Media Exps—Flow timer expiration notifications received for media sessions that have not been completely set up due to an incomplete or pending INVITE transaction

–Exp Media Drops—Number of flow timer expiration notifications from the MBCD that resulted in the termination of the dialog/session by the SIP application

–Multiple OK Drops—Number of dialogs terminated upon reception of a 200 OK response from multiple UASs for a given INVITE transaction that was forked by a downstream proxy

–Multiple OK Terms—Number of dialogs terminated upon reception of a 200 OK response that conflicts with an existing established dialog on the Net-Net SBC

–Media Failure Drops—Number of dialogs terminated due to a failure in establishing the media session

–Non-ACK 2xx Drops— Number of sessions terminated because an ACK was not received for a 2xx response

–Invalid Requests— Number of invalid requests; an unsupported header for example

–Invalid Responses—Number of invalid responses; no Via header for example

–Invalid Messages—Number of messages dropped due to parse failure

–CAC Session Drop—Number of call admission control session setup failures due to user session count exceeded

–Expired Sessions—Number of sessions terminated due to the session timer expiring

–CAC BW Drop—Number of call admission control session setup failures due to insufficient bandwidth

Lifetime displays show information for recent, total, and period maximum error statistics:

–Recent—Number of errors occurring in the number of seconds listed after the time stamp

–Total—Number of errors occurring since last reboot

–PerMax—Identifies the highest individual Period Total over the lifetime of the monitoring

- policy—Display SIP local policy / routing statistics for lifetime duration

–Local Policy Lookups— Number of Local policy lookups

–Local Policy Hits— Number of successful local policy lookups

–Local Policy Misses— Number of local policy lookup failures

–Local Policy Drops— Number of local policy lookups where the next hop session agent group is H323

–Agent Group Hits— Number of successful local policy lookups for session agent groups

–Agent Group Misses— Number of successful local policy lookups where no session agent was available for session agent group

–No Routes Found— Number of successful local policy lookups but temporarily unable to route; session agent out of service for instance

–Missing Dialog— Number of local policy lookups where the dialog not found, for a request addressed to the SBC with a To tag or for a NOTIFY-SUBSCRIBE sip request

–Inb SA Constraints— Number of successful local policy lookups where inbound session agent exceeded constraints

–Outb SA Constraints— Number of successful outbound local policy lookups where session agent exceeded constraints

–Inb Reg SA Constraints— Number of successful inbound local policy lookups where registrar exceeded constraints

–Out Reg SA Constraints— Number of successful outbound local policy lookups where registrar exceeded constraints

–Requests Challenged— Number of requests challenged

–Challenge Found— Number of challenges found

–Challenge Not Found— Number of challenges not found

–Challenge Dropped— Number of challenges dropped

- 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.

–All States—Number of all server transactions

–Initial—Number of times the “initial” state was entered after a request was received

–Queued—Number of times the “queued” state is entered because resources are temporarily unavailable

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

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

–Cancelled—Number of INVITE transactions that received a CANCEL

–Established—Number of times the server sent a 2xx response to an INVITE

–Completed—Number of times the server received a 300 to 699 status code and entered the “completed” state

–Confirmed—Number of times that an ACK was received while the server was in “completed” state and transitioned to “confirmed” state

–Terminated—Number of times that the server received a 2xx response or never received an ACK in the “completed” state, and transitioned to the “terminated” state

- 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.

–All States—Number of all client transactions

–Initial—State when initial server transaction is created before a request is sent

–Trying—Number of times the “trying” state was entered due to the sending 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

–Early Media—Number of times that the “proceeding” state was entered due to the receipt of a provisional response that contained SDP while in the “calling” state

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

–SetMedia—Number of transactions in which the Net-Net SBC is setting up NAT and steering ports

–Established—Number of situations when client receives a 2xx response to an INVITE, but cannot forward it because it NAT and steering port information is missing

–Terminated—Number of times the “terminated” state was entered after a 2xx message

- acls—Display ACL information

Period and Lifetime monitoring spans are displayed for SIP ACL status.

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

–Trusted—Number of trusted ACL entries

–Blocked—Number of blocked ACL entries

Lifetime monitoring span is displayed for SIP ACL Operations.

–ACL Requests—Number of ACL requests

–Bad Messages —Number of bad messages

–Promotions—Number of ACL entry promotions

–Demotions—Number of ACL entry demotions

–Trust->Untrust—Number of ACL entries demoted from trusted to untrusted

–Untrust->Deny—Number of acl entries demoted from untrusted to deny

- sessions—Display the number of sessions and dialogs in various states

The following session statistics are shown for the Period and Lifetime monitoring spans, in addition to the current Active count:

–Sessions—Identical to the identically named statistic on the `show sipd status` command

–Initial—Displays sessions for which an INVITE of SUBSCRIBE is being forwarded

–Early—Displays sessions for which the first provisional response (1xx other than 100) is received

–Established—Displays sessions for which a success (2xx) response is received

–Terminated—Displays sessions for which the session is ended by receiving or sending a BYE for an “Established" session or forwarding an error response for an "Initial" or "Early" session. The session will remain in the "Terminated" state until all the resources for the session are freed.

–Dialogs—Identical to the identically named statistic on the `show sipd status` command

–Early—Displays dialogs that were created by a provisional response

–Confirmed—Displays dialogs that were created by a success response. An "Early" dialog will transition to "Confirmed" when a success response is received

–Terminated—Displays dialogs that were ended by receiving/sending a BYE for an Established" session or receiving/sending error response "Early" dialog. The dialog will remain in the "Terminated" state until all the resources for the session are freed.

- sessions all—Display all SIP sessions currently on the system

- sessions by-agent <agent name>—Display SIP sessions for the session agent specified; adding **iwf** to the end of the command shows sessions for the IWF; adding **detail** to the end of the command expands the displayed information
- sessions by-ip <endpoint IP address>—Display SIP sessions for the specified IP address for an endpoint; adding **iwf** to the end of the command shows sessions for the IWF; adding **detail** to the end of the command expands the displayed information
- sessions by-user <calling or called number>—Display SIP sessions for the specified user; adding **iwf** to the end of the command shows sessions for the IWF; adding **detail** to the end of the command expands the displayed information
- sessions by-callid <call ID>—Display SIP sessions for the specified call ID; adding **iwf** to the end of the command shows sessions for the IWF; adding **detail** to the end of the command expands the displayed information
- redundancy—Display sipd redundancy statistics. Executing the **show sipd redundancy** command is the equivalent to the **show redundancy sipd** command
- agents [hostname][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. For a specific session agent, identified by IP address, the **show sipd agents** command lists:

–session agent state

- I—in-service
- O—out-of-service
- S—transitioning from out-of-service to in-service
- D—disabled

–inbound and outbound statistics

–average and maximum latency for each session agent

–maximum burst rate for each session agent as total number of session invitations sent to or received from the session agent within the amount of time configured in the burst-rate-window field

Inbound Statistics:

–Active—Number of active sessions sent to each session agent listed

–Rate—Average rate of session invitations (per second) sent to each session agent listed

–ConEx—Number of times the constraints have been exceeded

Outbound Statistics:

–Active—Number of active sessions sent from each session agent

–Rate—Average rate of session invitations (per second) sent from each session agent listed

–ConEx—Number of times the constraints have been exceeded

Latency:

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

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

- 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.
- ip-cac <IP address>—Display CAC parameters for an IP address
- publish—Display statistics related to incoming SIP PUBLISH messages
- agent <agent>—Display activity for the session agent that you specify

Inbound Sessions:

–Rate Exceeded—Number of times session or burst rate was exceeded for inbound sessions

–Num Exceeded—Number of times time constraints were exceeded for inbound sessions

Outbound Sessions:

–Rate Exceeded—Number of times session or burst rate was exceeded for outbound sessions

–Num Exceeded—Number of times time constraints were exceeded for inbound sessions

–Burst—Number of times burst rate was exceeded for this session agent

–Out of Service—Number of times this session agent went out of service

–Trans Timeout—Number of transactions timed out for this session agent

–Requests Sent—Number of requests sent via this session agent

–Requests Complete—Number of requests that have been completed for this session agent

–Messages Received—Number of messages received by this session agent

- realm—Display realm statistics related to SIP processing
- routers—Display status of Net-Net SBC connections for session router functionality
- directors—Display the status of Net-Net SBC connections for session director functionality

- <message>—Add one of the below arguments to the end of a **show sipd** command to display information about that type of SIP message:

–INVITE—Display the number of SIP transactions including an INVITE method

–REGISTER—Display the number of SIP transactions including a REGISTER method

–OPTIONS—Display the number of SIP transactions including an OPTIONS method

–CANCEL—Display the number of SIP transactions including a CANCEL method

–BYE—Display the number of SIP transactions including a BYE method

–ACK—Display the number of SIP transactions including an ACK method

–INFO—Display the number of SIP transactions including an INFO method

–PRACK—Display the number of SIP transactions including a PRACK method

–SUBSCRIBE—Display the number of SIP transactions including a SUBSCRIBE method

–NOTIFY—Display the number of SIP transactions including a NOTIFY method

–REFER—Display the number of SIP transactions including a REFER method

–UPDATE—Display the number of SIP transactions including an UPDATE method

–other—Display the number of SIP transactions including non-compliant methods and protocols used by specific customers

The following lists information displayed for each individual SIP message statistic. Some or all of the following messages/events may appear in the output from a ***show sipd*** *command.*

–INVITE Requests—Number of times method has been received or sent

–Retransmissions—Information regarding sipd message command requests received by the Net-Net SBC

–100 Trying—Number of times some unspecified action is being taken on behalf of a call (e.g., a database is being consulted), but user has not been located

–180 Ringing—Number of times called UA identified a location where user has registered recently and is trying to alert the user

–200 OK—Number of times request has succeeded

–408 Request Timeout—Number of times server could not produce a response before timeout

–481 Does Not Exist—Number of times UAS received a request not matching existing dialog or transaction

–486 Busy Here—Number of times callee's end system was contacted successfully but callee not willing to take additional calls

–487 Terminated—Number of times request was cancelled by a BYE or CANCEL request

–4xx Client Error—Number of times the 4xx class of status code appeared for cases where the client seems to have erred

–503 Service Unavail—Number of times server was unable to handle the request due to a temporary overloading or maintenance of the server

–5xx Server Error—Number of times the 5xx class of status code appeared

–Response Retrsns—Number of response retransmissions sent and received

–Transaction Timeouts— Number of times a transaction timed out. The timer related to this transaction is Timer B, as defined in RFC 3261

–Locally Throttled—Number of locally throttled invites. Does not apply to a server.

show sipd <message> output is divided in two sections: Server and Client, with information for recent, total, and period maximum time frames. This command also displays information about the average and maximum latency. For each type of SIP message, only those transactions for which there are statistics are shown. If there is no data available for a certain SIP message, the system displays the fact that there is none and specifies the message about which you inquired.

- groups—Display cumulative information for all session agent groups on the Net-Net SBC. This information is compiled by totaling the session agent statistics for all of the session agents that make up a particular session agent group. While the **show sipd groups** command accesses the subcommands that are described in this section, the main **show sipd groups** command (when executed with no arguments) displays a list of all session agent groups.
- groups -v—Display statistics for the session agents that make up the session agent groups that are being reported. The -v (meaning “verbose”) executed with this command must be included to provide verbose detail.
- groups <specific group name>—Display statistics for the specified session agent group
- endpoint-ip <phone number>—Displays registration information for a designation endpoint entered in the <phone number> argument; also show IMS-AKA data
- all—Display all the **show sipd** statistics listed above
- sip-endpoint-ip—See **show sipd endpoint-ip**
- sa-nsep-burst—Display NSEP burst rate for all SIP session agents
- subscriptions-by-user—Display data for SIP per user subscribe dialog limit

Example

```
ACMEPACKET# show sipd errors
```

show snmp-community-table

Syntax

```
show snmp-community-table
```

The **show snmp-community-table** command displays all information for configured SNMP communities including request and responses for each community.

Example

```
ACMEPACKET# show snmp-community-table
```

show support-info

Syntax

```
show support-info [custom | standard]
```

This command allows you to gather 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.

Example

```
ACMEPACKET show support-info
```

show system-state

Syntax

```
show system-state
```

Displays the system state based on the latest setting of the **set-system-state** command.

Example

```
ACMEPACKET# show system-state
```

show temperature

Syntax

```
show temperature
```

Displays the temperature in Celsius for all given components with temperature sensors.

Example

```
ACMEPACKET# show temperature
```

show timezone

Syntax

```
show timezone
```

Displays the information set with the **timezone-zet** command including the name of the timezone, its minutes from UTC, and the start and stop date and hours for daylight saving time.

Example

```
ACMEPACKET# show timezone
```

show trap-receiver

Syntax

```
show trap-receiver
```

The show trap-receiver command displays trap receiver information for each configured SNMP community.

Example

```
ACMEPACKET# show trap-receiver
```

show uptime

Syntax

```
show uptime
```

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

Example

```
ACMEPACKET# show uptime
```

show users

Syntax

```
show users
```

The **show users** command displays all users currently logged into the Net-Net SBC by index number. Other display information includes:

- Task-ID
- remote IP address—Only displayed for telnet or SSH connections
- IdNumber
- Duration of connection
- Connection Type
- State—* Denotes the current connection

Example

```
ACMEPACKET# show users
```

show version

Syntax

```
show version
```

The **show version** command shows the OS version information including: the OS version number, the date that the current copy of the OS was made, and other information.

Example

```
ACMEPACKET# show version
```

show virtual-interfaces

Syntax

```
show virtual-interface
```

The **show virtual-interface** command shows the virtual interfaces for Net-Net SBC signaling services; for example, SIP-NAT external address, H.323 interface (stack) IP interface, and MGCP IP interface.

Example

```
ACMEPACKET# show virtual-interfaces
```

show voltage

Syntax

```
show voltage
```

Displays current operating voltages for components in the Net-Net SBC.

Mode User and Superuser

Release First appearance: 1.0 / Most recent update: 4.1

Example

```
ACMEPACKET# show voltage
```

show wancom

Syntax

```
show wancom
```

Displays negotiated duplex mode and speed for all Net-Net system control interfaces.

Mode User and Superuser

Release First appearance: S-C6.1.0

Example

```
ACMEPACKET# show wancom
```

ssh-password

The **ssh-password** command creates SSH login accounts and passwords for secure access into a Net-Net SBC.

Syntax

```
ssh-password <username> <password>
```

Arguments

<username> Enter the username of the new account or the username of the existing SSH account

<password> Enter a password for the new account or a new password for the existing account

Mode

Superuser

Release

First appearance: 2.0

Notes

Passwords must be 6-9 characters with at least one non-alphabetical character. To execute this command, you must type **ssh-password** and press <enter>. You will be prompted for the user name to create and the password for the account. You can change the password of a previously existing account by entering the existing username when prompted. You will be prompted a second time to re-enter the password for confirmation.

Example

```
ACMEPACKET# ssh-password user1 acme
```

ssh-pub-key

The **ssh-pub-key** command allows you to import and delete public key records on the Net-Net SBC.

Syntax

```
ssh-pub-key <import | delete> <login name>
```

Arguments

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

Mode Superuser

Release First appearance: 5.1.1

Example

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

stack

The **stack** command shows the function call stack trace for a specified stack.

Syntax

```
stack <task>
```

Arguments <task> Enter a task name or task ID

Mode Superuser

Release First appearance: 1.0

Notes This command displays a list of nested routine calls for the specified stack. Each routine call and its parameters are shown.

Example

```
ACMEPACKET# stack sipd
```

stop-task

The **stop-task** command shuts down a specified task.

Syntax

```
stop-task <task>
```

Arguments <task> Enter a task name or task ID

Mode Superuser

Release First appearance: 1.0

Notes Use this command with caution as there is no direct way to restart a task without rebooting the Net-Net SBC.

Example

```
ACMEPACKET# stop-task sipd
```

switchover-redundancy-link

The **switchover-redundancy-link** command allows you to switchover the physical interface to standby in a redundant link configuration.

arguments <slot> Select the slot number to switchover the link from active to standby.

Values 1 | 2

Mode Superuser

Release First appearance: 5.0

Example `ACMEPACKET# switchover-redundancy-link 2`

systime-set

The **systime-set** command sets the system clock.

Syntax `systime-set`

Mode Superuser

Release First appearance: 1.0 / Most recent update: 1.2.1

Notes The **systime-set** command prompts the user for the date and time and updates the system clock. The command will not set the system time if an invalid year, month, or day is entered. Attempting to change the date and time on the Net-Net SBC displays a warning message as use of this command could be service affecting.

Example `ACMEPACKET# systime-set`

tail-logfile-close

The **tail-logfile-close** command ends the echoing of a process's logfile to the screen as initiated by the **tail-logfile-open** command.

Syntax `tail-logfile-close <process> [<logfile>]`

Arguments <process> Enter the name of the process that is writing to the specified logfile.

<logfile> Enter the logfile's name that you want to stop being echoed to the screen. This argument is optional.

Mode Superuser

Release First appearance: 4.0

Notes Must be a valid logfile that is currently being written to.

Example `ACMEPACKET# tail-logfile-close sipd`

tail-logfile-open

The **tail-logfile-open** command displays all messages on the console that are normally written to a specified logfile. As a message is written to the logfile, it is also displayed on the screen. The specified logfile will continue to be updated on the Net-Net SBC's filesystem.

Syntax

```
tail-logfile-open <process> [<logfile>]
```

Arguments

<process> Enter the name of the process that is writing to the specified logfile

<logfile> Enter an alternate logfile's name for which you want new entries echoed to the console screen. Not entering the logfile argument forces the default log for the named process to be displayed on the screen. This argument is optional.

Mode Superuser

Release First appearance: 4.0

Notes Must be a valid logfile that is currently being written to. The level of detail displayed on the screen is related to the loglevel of the process.

Example

```
ACMEPACKET# tail-logfile-open sipd
```

tcb

The **tcb** command displays task control block (TCB) information for a particular task.

Syntax

```
tcb <task>
```

Arguments <task> Enter a task name or task ID

Mode Superuser

Release First appearance: 1.1

Notes This command returns a pointer to the TCB for a specified task. Although all task state information is contained in the TCB, you must not modify it directly. This command is used only for debugging purposes.

Example

```
ACMEPACKET# tcb sipd
```

test-audit-log

The test-audit-log command allows the user to test audit log functionality.

Arguments <log-msg> Enter the audit log string to be written into the audit file

Syntax

```
test-audit-log <log-msg>
```

Mode Superuser

Release First appearance: S-C6.2.0

Example

```
ACMEPACKET# test-audit-log log1
```

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

Release First appearance: 5.0

Example

```
ACMEPACKET# test-pattern-rule expression ‘.*;tgid=(.+).*’
```

Notes This command exists both as a command and as a configuration element.

test-policy

The **test-policy** command is used to test routes configured for the address translation feature. This command is also found in the session-router path. Details on its use are found in the Configuration Elements N-Z chapter.

Syntax

```
test-policy <argument>
```

Arguments

<argument> The following are **test-policy** arguments:

Values

- carriers—Enter names of permitted carriers set in the carriers fields set in configured local-policy elements. This field is formatted as a list of comma-separated text strings enclosed in quotation marks.
- from-address—Enter the “from” address of the local policy to look up/test. From addresses should be entered as SIP-URLs in the form of `sip:19785551212@netnetsystems.com`.
- media-profiles—List media profiles
- show—Show the next hop and the associated carrier information for all routes matching the “from” and “to” addresses entered
- source-realm—Enter the name set in the source-realm field of a configured local policy. Entering an “*” in this field matches for any source realm. Leaving the field empty indicates that only the “global” realm will be tested.

- time-of-day—Decide whether to use the time of day value set in the start-time and end-time fields set in configured local-policy elements

–enabled | disabled

- to-address—Enter the “to” address of the local policy to look up/test. To addresses should be entered as SIP-URLs in the form of `sip:19785551212@netnetsystems.com`.
- exit—End the test

Mode User

Release First appearance: 1.0

Notes This command exists both as a command and as a configuration element.

Example

```
ACMEPACKET# test-policy time-of-day enabled
```

test-translation

The **test-translation** command is used to test translation rules configured for the address translation feature. This command is also found in the session-router path. Details on its use are found in the Configuration Elements N-Z chapter.

Syntax

```
test-translation <argument>
```

Arguments

<argument> The following is a list of **test-translation** arguments:

Values

- called-address—Enter the address on which the called rules are be applied. This entry is required.
- calling-address—Enter the address on which the calling rules will be applied. This entry is required.
- show—Show results of translation
- translation-id—Enter translation rules to test
- exit—Exit the test translation

Mode User

Release First appearance: 1.3

Example

```
ACMEPACKET# test-translation show
```

timezone-set

The **timezone-set** command sets the time zone and daylight savings time on the Net-Net SBC.

Syntax

```
timezone-set
```

Mode Superuser

Release First appearance: 1.0.

Notes The **timezone-set** command prompts the user for time zone, UTC offset, and daylight saving time information. If daylight savings time for your time zone changes start and stop dates yearly, this command must be set yearly.

Example

```
ACMEPACKET# timezone-set
```

verify-config

The **verify-config** command verifies the Net-Net SBC's current configuration.

Syntax

```
verify-config
```

The **verify-config** command checks the consistency of configuration elements that make up the current configuration and should be carried out prior to activating a configuration on the Net-Net SBC.

Mode Superuser

Release First appearance: 1.3; Most recent update: S-C6.1.0

The **verify-config** command, entered either directly or via the **save-config** command, checks for address duplication for a given network-interface within a configuration. Addresses are checked for duplication based on the following criteria:

- Every address entered is checked against the Primary and Secondary Utility addresses
- All UDP, TCP, and TFTP addresses are checked against other UDP, TCP, and TFTP addresses respectively within the same port range

Notes For detailed information, refer to the *Net-Net 4000 ACLI Maintenance and Troubleshooting Guide*.

Example

```
ACMEPACKET# verify-config
```

watchdog

The **watchdog** command sets or queries the state of the watchdog timer. If the system becomes unstable causing the watchdog timer to not reset, the system reboots.

Syntax

```
watchdog <arguments>
```

Arguments

<arguments>	The following is a list of valid arguments:
Values	• enable—Enable the watchdog timer • disable—Disable the watchdog timer • fetch—Display the watchdog timer configuration

Mode User

Release First appearance: 2.0.1

Notes

The **fetch** argument can be accessed from user mode.

Example

```
ACMEPACKET# watchdog enable
```

4 Configuration Elements A-M

access-control

The **access-control** configuration element is used to manually create ACLs for the host path in the Net-Net SBC.

Syntax

```
access-control <realm-id | description | source-address |
destination-address | application-protocol | transport-protocol |
access | average-rate-limit | trust-level | minimum-reserved-
bandwidth | invalid-signal-threshold | maximum-signal-threshold |
untrusted-signal-threshold | deny-period | nat-trust-threshold |
cac-failure-threshold | untrust-cac-failure | 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 the **access-control** configuration element

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. This parameter is entered in the following format:

```
<ip-address>[/<num-bits>][:<port>][/<port-bits>]
```

Default	0.0.0.0

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

application-protocol—Select the application-layer protocol configured for this ACL entry

Values
- SIP
- H.323
- MGCP
- 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
- ALL
- TCP
- UDP

access—Select the access control type for this entry

Default permit

Values
- permit—Puts 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—Puts this entry in the deny list.

average-rate-limit—Enter the allowed 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—Hosts will always remain untrusted. Will never be promoted to trusted list or will never get demoted to deny list.
- low—Hosts can be promoted to trusted-list or can get demoted to deny-list
- medium—Hosts can get promoted to trusted, but can only get demoted to untrusted. Hosts will never be put in deny-list.
- high—Hosts always remain trusted

minimum-reserved-bandwidth—Enter the minimum reserved bandwidth in bytes per second that you want for the session agent, which will trigger the creation of a separate pipe for it. This parameter is only valid when the **trust-level** parameter is set to **high**. Only a non-zero value will allow the feature to work properly.

Default 0

Values Min: 0 / Max: 4294967295

invalid-signal-threshold—Enter the rate of 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 means no threshold.

Default 0

Values Min: 0 / Max: 999999999

maximum-signal-threshold—Enter the maximum number of signaling messages per second that one 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 means no 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 deny-listed or deny 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 maximum number of untrusted endpoints allowed before an entire NAT device is demoted to untrusted. 0 means dynamic demotion of NAT devices is disabled.

Default	0
Values	Min: 0 / Max: 999999999

cac-failure-threshold—Enter the number of CAC failures for any single endpoint that will demote it from the trusted queue to the untrusted queue.

Default	0
Values	Min: 0 / Max: 2^{32} -1

untrust-cac-failure-threshold—Enter the number of CAC failures for any single endpoint that will demote it from the untrusted queue to the denied queue.

Default	0
Values	Min: 0 / Max: 2^{32} -1

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: 2.0 / Most recent update: S-C6.2.0

RTC Status Supported

Notes This is a multiple instance configuration element.

account-config

The **account-config** configuration element allows you to set the location where accounting messages are sent.

Syntax

```
account-config <hostname | port | strategy | protocol | 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-compression | file-
delete-alarm | 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 | select | no | show | done |
exit>
```

Parameters

hostname—Enter the hostname of this Net-Net SBC; must be set to "localhost" or the accounting configuration will not work properly. Entries are in FQDN format.

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—Selects accounting servers in the order in which they are listed • failover—Uses first and subsequent servers in accounting server list until a failure is received from that server • roundrobin—Selects accounting server in order, distributing the selection of each accounting server evenly over time • fastestrtt—Selects accounting server with the fastest RTT observed during transactions with the servers • fewestpending—Selects accounting server with the fewest number of unacknowledged accounting messages

protocol—Set the type of message protocol type for accounting CDRs.

Default	radius
Values	radius | diameter

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: 2^{32}-1

max-wait-failover—Enter the number of accounting messages held in message waiting queue before a failover situation status is enacted

Default	100
Values	Min: 1/ Max: 4096

trans-at-close—Enable the Net-Net SBC to transmit accounting message information at the close of a session only. Setting this parameter to disabled tells 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—SBC to transmit a RADIUS Interim message

Default	reinvite-response
Values	• ok—RADIUS Start message is generated when an OK message is received in response to an INVITE • reinvite—RADIUS Interim message is generated when a SIP session reINVITE message is received • reinvite-response—RADIUS Interim message is generated when a SIP session reINVITE is received and the system responds to it • reinvite-cancel—RADIUS Interim message is generated when a SIP session reINVITE is received, and the Reinvite is cancelled before the Net-Net SBC responds to it • unsuccessful-attempt—RADIUS Interim message is generated when a session set-up attempt from a preference-ordered list of next-hop destinations is unsuccessful. This can happen when a local policy lookup, LRT lookup, ENUM query response, or SIP redirect returns a preference-ordered list of next-hop destinations. The interim message contains: the destination IP address, the disconnect reason, a timestamp for the failure, and the number that was called

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: 100000000

max-files—Set the maximum number of files to store on the Net-Net SBC

Default	5
Values	Min: 1 / Max: 10

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-delete-alarm—Enable or disable the raising of an alarm when CDR files are deleted due to lack of space.

Default	disabled
Values	enabled | disabled

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	60
Values	Min: 2 / Max: 2147483647

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: 1 / 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 for 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

intermediate-period—Set the time interval used to generate periodic interim records during a session

Default	0
Values	Min: 0 / Max: 999999999

account-servers—Access the account-server subelement

cdr-output-redundancy—Enable or disable the redundant storage of comma-delimited CDR files

Default	enabled
Values	enabled | disabled

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.

Limit this list to accounting VSAs. For example, VSA 254 is an authentication VSA, so it should not be included in the range. The system generates validateconfig errors if your range includes VSAs that are not accounting VSAs.

cdr-output-inclusive—Enable or disable the guarantees placement of attributes in CSV files used for local CDR storage and FTP push.

Default	disabled
Values	enabled | disabled

push-receiver—Access the **push-receiver** subelement.

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: 1.0 / Most recent update: S-C6.2.0

RTC Status Unsupported

Notes This is a single instance configuration element.

account-config > account-servers

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 is configured here

Default	1813
Values	Min: 1025 / Max: 65535

state—Enable or disable this account-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	250
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 bundling of the VSAs within RADIUS accounting on the account-server

Default	enabled
Values	enabled | disabled

secret—Enter the secret passed from the account-server to the client server; entries in this field must follow the Text Format

NAS-ID—Enter the value the account-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. The default is 0, meaning there is no set priority.

Default	0
Values	Min: 0

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-servers**.

Release

First appearance: 1.0

RTC Status

Unsupported

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 multiple CDR push receivers for use with the FTP push feature.

Syntax

```
push-receiver <server | port | admin-state | remote-path |
filename-prefix | priority | protocol | username | password |
public-key | select | no | show | done | exit>
```

Parameters

server—Send 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 serverto which the Net-Net SBC will send CDR files.

Default	21
Values	Min: 1 / Max: 65535

admin-state—Set the state of an FTP/SFTP push receiver to enabled for the Net-Net SBC to send CDR files to it

Default	enabled
Values	enabled | disabled

remote-path—Enter the pathname on which the CDR files are sent to the push receiver. CDR files are placed in this location on the FTP/SFTP server.

Default	none
Values	<string> remote pathname

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.

Default	none

Values	<string> prefix for filenames

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 uses first—is 0. The lowest priority—and the push receiver the system uses last—is 4.

Default	4
Values	Min: 0 (highest) / Max: 4 (lowest)

protocol—Select the transport protocol to be used for this push receiver. If this is an STFTP push receiver, 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 uses to connect to 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 the server is defined for SFTP push receiver. If you define this as an SFTP push receiver but do not set a public-key value, the Net-Net SBC will use password authentication.

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: S-C6.2.0

RTC Status

Supported

auth-params

The auth-params element provides a list of RADIUS servers used for authentication, along with protocol and operation details that define RADIUS access.

Syntax

```
auth-params <name | protocol | strategy | servers | select | no |
show | done | exit>
```

Parameters

name—Enter the name of this instance of the auth-params configuration element.

protocol—Enter the protocol to use for obtaining authentication data from a RADIUS server.

Default	eap
Values	eap

Notes

The current software version only supports EAP.

strategy—Enter the management strategy used to distribute authentication requests. This parameter is only relevant if multiple RADIUS servers have been identified by the **servers** parameter.

Default	hunt

Values	round-robin | hunt

server—Enter a RADIUS server by IP address.

Path **auth-params** is an element under the **security** path. The full path from the topmost ACLI prompt is: **configure terminal > security > auth-params**.

Release First appearance: S-C6.2.0

RTC Status Supported

Notes This is a multiple instance configuration element.

authentication

The **authentication** configuration element is used for configuring an authentication profile.

Syntax

```
authentication <source-port | type | protocol | allow-local-
authorization | login-as-admin | management-servers | ike-raidus-
params-name | management-servers | radius-servers | select | no |
show | done | exit>
```

Parameters

source-port—Enter the port number on the Net-Net SBC to send messages to the RADIUS server

Default	1812
Values	1645 | 1812

type—Enter the type of user authentication

Default	local
Values	local | radius

protocol—Select the protocol type to use with your RADIUS server(s)

Default	pap
Values	pap | chap | mschapv2

allow-local-authorization—Enable this parameter if you want the Net-Net SBC to authorize users to enter Super (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

management-strategy—Enter the management strategy used to distribute authentication requests.

Default	hunt
Values	round-robin | hunt

ike-radius-params-name—Enter the auth-params instance to be assigned to this element.

Default	None
Values	Name of an existing auth-params configuration element

management-servers—Enter a list of servers used for management requests

radius-servers—Enter the radius-servers subelement

Path

authentication is an element under the security path. The full path from the topmost prompt is: **configure terminal > security > authentication.**

Release

First appearance: 4.0

RTC Status

Supported

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 | realm-
id | retry-limit | retry-time | maximum-sessions | class | dead-
time | authentication-methods | select | no | show | done | exit>
```

Parameters

address—Enter the IP address for the RADIUS server

port—Enter the port number on the remote IP address for the RADIUS server

Default	1812
Values	1645 | 1812

state—Enable or disable this configured RADIUS server

Default	enabled
Values	enabled | disabled

secret—Enter the password the RADIUS server and the Net-Net SBC share. This password is not transmitted between the two when the request for authentication is initiated.

nas-id—Enter the NAS ID for the RADIUS server

realm-id—Enter the RADIUS server realm ID.

retry-limit—Set the number of times the Net-Net SBC retries to authenticate with this RADIUS server

Default	3

Values	Min: 1 / Max: 5

retry-time—Enter the time in seconds the Net-Net SBC waits before retrying to authenticate with this RADIUS server

Default	5
Values	Min: 5 / Max: 10

maximum-sessions—Enter the maximum number of sessions to maintain with this RADIUS server

Default	255
Values	Min: 1 / Max: 255

class—Select the class of this RADIUS server as either primary or secondary. A connection to the primary server is tried before a connection to the secondary server is tried.

Default	primary
Values	primary | secondary

dead-time—Set the time in seconds before the Net-Net SBC retries a RADIUS server that it has designated as dead

Default	10
Values	Min: 10 / Max: 10000

authentication-methods—Select the authentication method the Net-Net SBC uses when communicating with the RADIUS server

Default	pap
Values	all | pap | chap | mschapv2

Path

radius-servers is a subelement under the **authentication** configuration element under the security path. The full path from the topmost prompt is: **configure terminal > security > authentication > radius-servers.**

Release

First appearance: 4.0 / Most recent update: S-C6.2.0

RTC Status

Supported

bootparam

The **bootparam** command establishes the parameters that a Net-Net SBC uses when it boots.

Syntax

```
bootparam <boot device | processor number | hostname | file name |
inet on ethernet | inet on backplane | host inet | gateway inet |
user | ftp password | flags | target name | startup script |
other>
```

Notes

In the physical interface and the network interface configuration elements, you can set values that may override the values set within the boot configuration parameters. If you are configuring these elements and enter information that matches information in the boot configuration parameters, the system will warn you that your actions may change the boot configuration parameters.

The **bootparam** command presents you with the parameters to enter on a line-by-line basis. You can press <Enter> to accept a given default parameter and move to the next parameter.

boot device—Enter the name and port number of the device from which an image is downloaded (e.g., wancom0). This parameter is only required if you are booting from an external device; if you are doing so, the name must be wancom followed by the port number.

processor number—Enter the processor number on the backplane

host name—Enter the name of the boot host used when booting from an external device

file name—Enter the name of the file containing the image to be booted. If you are booting off the system flash memory, this filename must always match the filename that you designate when you FTP the image from the source to the Net-Net SBC. When booting off the system flash memory, this filename must always start with: /tffs0/.

Values	• tffs0=/boot • tffs1=/code

inet on ethernet—Enter the internet address of the Net-Net SBC's Ethernet interface. An optional subnet mask in the form inet_adrs:subnet_mask is available. If DHCP is used to obtain the configuration parameters, lease timing information may also be included. This information takes the form of lease_duration:lease_origin and is appended to the end of the field. The subnet mask for this parameter is given in hex.

inet on backplane—Not used

host inet—Enter the internet address of the boot host, used when booting from an external device

gateway inet—Enter the IP gateway for the management interface's subnet

user—Enter the FTP username on the boot host

ftp password—Enter the FTP password for the FTP user on the boot host

flags—Set the Net-Net SBC to know from where to boot. Also sets how to use the files in the booting process.

Values	• 0x08—Quickboot. The system bypasses the 7 second countdown prior to booting. • 0x10008—This flag does the same as 0x08. In addition, it connects to usr/acme on the boot host defined in the boot parameters. Connecting externally to usr/acme is useful for copying data off the Net-Net SBC to the external host over NFS.

- 0x70008—This flag does all of the above. In addition, it stores the configuration in usr/acme on the boot host defined in the boot parameters rather than in /code in the system flash memory file system.
- 0x80008—Source based routing.

target name—Enter the name of this Net-Net SBC. This field also sets the name of the Net-Net SBC as it appears in the system prompt (e.g., ACMEPACKET> or ACMEPACKET#).

startup script—Internal use only

other—Internal use only

Path

bootparam is in the configuration path. The full path from the topmost prompt is: **configure terminal > bootparam**.

Release

First appearance: 1.0

RTC Status

Unsupported

call-recording-server

The **call-recording-server** configuration element allows you to forward both signaling and media packets to and from a realm to a specified destination.

Syntax

```
call-recording-server <name | primary-network | primary-
signaling-addr | primary-media-addr | secondary-network |
secondary-signaling-addr | secondary-media-addr | ping-method |
ping-interval | select | no | show | done | exit>
```

Parameters

name—Enter the name of the IPRCR you are configuring

primary-realm—Enter the primary realm to which you want this IPRCR to be associated. This must be an existing realm or the IPRCR will be considered invalid and this server will be ignored.

primary-signaling-addr—Enter the primary address you want to use as a destination for forwarding signaling packets

primary-media-addr—Enter the primary address you want to use as a destination for forwarding media packets. If both the signaling and media primary addresses are the same, this parameter can be left blank

secondary-realm—Enter the secondary realm you want this IPRCR to be associated with if the primary-network becomes unreachable. This must be an existing realm or the IPRCR will be considered invalid and this server will be ignored.

secondary-signaling-addr—Enter the address you want to use as a destination for forwarding signaling packets if the address you entered in the **primary-signaling-addr** parameter becomes unreachable.

secondary-media-addr—Enter the address you want to use as a destination for forwarding media packets if the address you entered in the **primary-media-addr** parameter becomes unreachable

ping-method—Enter the SIP method you want to be used for ping messages send to the IPRCR

ping-interval—Enter the time in seconds to allow between the transmission of ping requests in an HA configuration. A value of 0 means this parameter is disabled.

Default	0
Values	Min: 0; 2 / Max: 9999999

Path **call-recording-server** is an element under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > call-recording-server**.

Release First appearance: 6.0

RTC Status Supported

Notes This is a multiple instance element.

capture-receiver

The **capture-receiver** configuration element allows you to configure packet tracing functionality on your Net-Net SBC.

Syntax

```
capture-receiver <state | address | network-interface | select |
no | show | done | exit>
```

state—Enable or disable the Net-Net SBC's TRACE capability

Default	disabled
Values	enabled | disabled

address—Enter the TRACE server IP address

network-interface—Enter the TRACE server outbound interface

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: 5.0

RTC Status Supported

certificate-record

This configuration element configures certificate records for TLS support.

Syntax

```
certificate-record <name | country | state | locality |
organization | unit | common-name | key-size | alternate-name |
trusted | key-usage-list | extended-key-usage-list | options |
select | no | show | done | exit>
```

name—Enter the name of the certificate record

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 for holding the certificate within the organization

common-name—Enter the common name for the certificate record

key-size—Set the size of the key for the certificate

Default 1024

Values 512 | 1024 | 2048

alternate-name—Enter the alternate name of the certificate holder

trusted—Enable or disable trust of this certificate

Default enabled

Values enabled | disabled

key-usage-list—Enter the usage extensions to use with this certificate record; can be configured with multiple values

Default **digitalSignature** and **keyEncipherment**

extended-key-usage-list—Enter the extended key usage extensions you want to use with this certificate record

Default serverAuth

Path **certificate-record** is an element under the security path. The full path from the topmost prompt is: **configure terminal > security > certificate-record**.

Release First appearance: 4.1.

RTC Status Supported

cert-status-profile

The **cert-status-profile** configuration element identifies an OCSP responder, the transport protocol used to access the responder, and the certificates used to sign the OCSP request and to validate the OCSP response.

Syntax

```
cert-status-profile <name | ip-address | port | type |
trans-proto | requester-cert | responder-cert | realm-id |
retry-count | dead-time | batch | select | done | no | show |
done | exit>
```

Parameters

name—Enter the name of this cert-status-profile instance, thus allowing the configuration of multiple configuration elements of this type. This parameter is required.

Default	None
Values	Any valid object name — the name must be unique within the cert-status-profile namespace

ip-address—Enter the IPv4 address of the destination OCSP responder. This parameter is required.

Default	None
Values	Any valid IPv4 address

port—Enter the destination port number. This parameter is optional.

Default	80
Values	Any valid port number

type—Enter the protocol type used for certificate checking. This parameter is optional.

Default	ocsp
Values	ocsp

Notes

The current software version only supports ocsp.

trans-protocol—Enter the protocol used to transmit the OSCP request; the single currently supported value is *http*. This parameter is optional.

Default	http
Values	http

requester-cert—Enter the name of the certificate configuration element used to sign the outgoing OCSP request; this parameter is required only if the OCSP responder mandates a signed request.

Default	None
Values	An existing certificate configuration element name

responder-cert—Enter the name of the certificate configuration element used to validate the incoming OCSP response.

Default	None
Values	An existing certificate configuration element name

realm-id—Enter the name of the realm used for transmitting OCSP requests. This parameter is optional.

Default	wancom
Values	Any valid realm name

retry-count—Enter the maximum number of times to retry an OCSP responder in the event of connection failure.

Default	1
Values	Min: 0/Max: 10

dead-time—Enter the interval (in seconds) between the trigger of the retry-count(er) and the next attempt to access the unavailable OCSP responder. This parameter is optional.

Default	0 (seconds)
Values	Min: 0/Max: 3600

Path **cert-status-profile** is a subelement under the security configuration element. The full path from the topmost ACLI prompt is: **configure-terminal>security>cert-status-profile**.

Release First appearance: S-C6.2.0

RTC Status Supported

Notes This is a multiple instance configuration.

class-profile

The **class-profile** configuration element lets you access the **class-policy** configuration element for creating classification policies for ToS marking for SIP or H.323.

Syntax

```
class-profile <policy | exit>
```

Parameters **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: 1.3 / Most recent update: 2.0

RTC Status Supported

class-profile > policy

The **class-policy** configuration subelement lets you create classification policies that are used to create a ToS marking on incoming traffic based upon a matching **media-policy** and destination address.

Syntax

```
policy <profile-name | to-address | media-policy | select | no |
show | done | exit>
```

Parameters **profile-name**—Enter the classification profile name

to-address—Enter a list of addresses to match for when determining when to apply this class-policy. Addresses can take the forms:

- `+<number>`—E164 address
- `<number>`—Default address type

- `[<host>].domain`—Host and/or domain 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 > policy.**

Release

First appearance: 1.3 / Most recent update: 2.0

RTC Status

Unavailable

codec-policy

The **codec-policy** configuration element allows you to configure codec policies, sets of rules that specify the manipulations to be performed on SDP offers.

Syntax

```
codec-policy <name | allow-codecs | order-codecs | select | no |
show | done | exit>
```

Parameters

name—Enter the unique name for the codec policy. This is the value you will use to refer to this codec policy when you apply it to realms or session agents. This is a required parameter.

allow-codecs—Enter the list of media format types (codecs) to allow for this codec policy. In your entries, you can use the asterisk (*) as a wildcard, the force attribute, or the no attribute so that the allow list you enter directly reflect your configuration needs. The codecs that you enter here must have corresponding media profile configurations.

order-codecs—Enter the order in which you want codecs to appear in the outgoing SDP offer. You can use the asterisk (*) as a wildcard in different positions of the order to directly reflect your configuration needs. The codecs that you enter here must have corresponding media profile configurations.

Path

codec-policy is an element of the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > codec-policy**.

Release

First appearance: 4.1.1

RTC Status

Supported

data-flow

The **data-flow** configuration element specifies pass-through data-traffic processing when using IKE.

Syntax

```
data-flow < name | realm-id | group-size | downstream-rate |
upstream-rate | batch | select | no | show | done | exit >
```

Parameters

name—Specify the name of this instance of the **data-flow** configuration element.

Default	None

Values	A valid configuration element name, unique within the **data-flow** namespace

realm-id—Specify the realm that supports the upstream (core side) data-flow.

Default	None
Values	The name of an existing **realm** configuration element

group-size—Specify the maximum number of user elements grouped together by this **data-flow** instance.

Notes

The optional **group-size** parameter specifies the divisor used by this data-flow instance to segment the total address pool into smaller, individually-policed segments.

For maximum efficiency, this value should be set to a power of 2.

Default	128
Values	2 | 4 | 8 | 16 | 32 | 64 | 128 | 256

upstream-rate — Specify the allocated upstream bandwidth.

Default	0 (allocates all available bandwidth)
Values	Min: 0 / Max: 2^{32} -1

downstream-rate—Specify the allocated downstream (access side) bandwidth.

Default	0 (unlimited, no bandwidth restrictions)
Values	Min: 0 / Max: 2^{32} -1

Path

data-flow is a subelement under the **ike** element. The full path from the topmost ACLI prompt is : **configure terminal > security > ike > data-flow**.

Release

First appearance: S-C6.2.0

RTC Status

Supported

Notes

This is a multiple instance configuration element.

Configures a data-flow configuration element name flow1.

The required **realm-id** parameter identifies the realm (carrier-7) providing access to the network core.

Default values are used for **downstream-rate** and **upstream-rate**, indicating that all available bandwidth is allocated for the **data-flow** instance.

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>
```

Parameters

client-realm—Enter the realm from which DNS queries are received. This value is the name of a configured realm.

description—Describe 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 field is required.

server-dns-attributes—Enter the server-dns-attributes subelement

Path

dns-config is a subelement under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > dns-config.**

Release

First appearance: 1.3

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>
```

Parameters

server-realm—Enter the realm from which DNS responses are sent. This value must be the name of a configured realm. This value is required.

domain-suffix—Enter the domain suffixes 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 field is required.

source-port—Enter the UDP port number from which the ALG sense queries to the DNS server (i.e., layer 3/layer 4 source address). This value is required.

Default	53
Values	Valid Range: 1025-65535

transaction-timeout—Enter the number of seconds that the ALG maintains information to map a DNS server response to the appropriate client request. This value is required.

Default	10 seconds
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: 1.3

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>
```

Parameters **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 media-manager element. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > dns-config > server-dns-attributes > address-translation**.

Release First appearance: 1.3

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.

dpd-params

The **dpd-params** configuration element enables creation of one or more sets of DPD Protocol parameters.

Syntax

```
dpd-params < name | max-loop | max-endpoints | max-cpu-limit |
load-max-loop | load-max-endpoints | batch | select | no | show |
done | exit >
```

Parameters **name**—Enter a unique identifier for this instance of the **dpd-params** configuration element.

Default None

Values Valid configuration element name that is unique within the **dpd-params** namespace

max-loop—Set the maximum number of endpoints examined every **dpd-time-interval**.

Default 100

Values

Notes If CPU workload surpasses the threshold set by **max-cpu-limit**, the **max-loop** value is over-ridden by **load-max-loop**.

max-endpoints—Set the maximum number of simultaneous DPD Protocol negotiations supported when the CPU is not under load (as specified by the **max-cpu-limit** property).

Default 25

Values an integer value, should be greater than **load-max-endpoints**

Notes If CPU workload surpasses the threshold set by **max-cpu-limit**, the **max-endpoints** value is over-ridden by **load-max-endpoints**.

max-cpu-limit—Set a threshold value (expressed as a percentage of CPU capacity) at which DPD protocol operations are minimized to conserve CPU resources.

Default 60 (percent)

Values an integer value, 0 (effectively disabling DPD) through 100

load-max-loop—Set the maximum number of endpoints examined every **dpd-time-interval** when the CPU is under load, as specified by the **max-cpu-limit** parameter.

Default 40

Values an integer value, should be less than **max-loop**

load-max-endpoints—Set the maximum number of simultaneous DPD Protocol negotiations supported when the CPU is under load, as specified by the **max-cpu-limit** property.

Default 5

Values an integer value, should be less than **max-endpoints**

Path **dpd-params** is a subelement under the ike element. The full-path from the topmost ACLI prompt is: **configure-terminal>security>ike>dpd-params**.

Release First appearance: S-C6.2.0

RTC Status Supported

Notes This is a multiple instance configuration element.

enforcement-profile

The **enforcement-profile** 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 |
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.

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

Path

enforcement-profile is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > enforcement-profile**.

Release

First appearance: 5.1; Last updated: S-C6.1.0

RTC Status

Supported

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

name—Enter a name for this enforcement profile

event-type—Enter the SIP subscription event type for which to set up limits. You can 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

Default 0

Values Min: 0 / Max: 65535

Path

subscribe-event is a subelement under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > enforcement-profile>subscribe-event**.

Release

First appearance: S-C6.1.0

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 |
query-method | timeout | cache-inactivity-timer | lookup-length |
max-response-size | service-type | health-query-number | health-
query-interval | failover-to | cache-addl-records | include-
source-info | select | no | show | done | exit>
```

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.

query-method—Enter the ENUM query distribution strategy

Default	hunt
Values	hunt | round-robin

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

Values Min: 0 / Max: 255

max-response-size—Set the maximum size in bytes for UDP datagram responses

service-type—Enter the ENUM service types you want supported in this ENUM configuration. Possible entries are E2U+sip and sip+E2U (the default), and the types outlines in RFCs 2916 and 3721. If you add to the pre-existing E2U+sip and sip+E2U list and want those values to remain, you must enter them with your new values.

Default E2U+sip and sip+E2U

Values Min: 0 / Max: 999999999

Default 512

Values Min: 512 / Max: 65535

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

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.

include-source-info—Set this parameter to enabled to send source URI information to the ENUM server with any ENUM queries.

Path

enum-config is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > enum-config**.

Release

First appearance: 2.1.1/ Most recent update: S-C6.2.0

RTC Status

Supported

ext-policy-server

The **ext-policy-server** is used for configuring PDP/RACF or CLF functionality on the Net-Net SBC.

Syntax

```
ext-policy-server <name | state | operation-type | protocol |
address | port | realm | num-connections | reserve-incomplete |
permit-conn-down | permit-on-reject | disconnect-on-timeout |
product-name | application-mode | application-id | framed-ip-
addr-encoding | dest-realm-format | ingress-realm-location |
domain-name-suffix | gate-spec-mask | allow-srv-proxy | watchdog-
ka-timer | options | select | no | show | done | exit>
```

Parameters

name—Enter the name of this external policy server configuration

state—Enable or disable the operational state of this external policy server configuration

Default	enabled
Values	enabled | disabled

operation-type—Select the function this external policy server performs

Default	disabled
Values	• disabled • admission-control—Net-Net SBC acts as a PEP in a PDP/RACF deployment • bandwidth-mgmt—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 • C-SOAP—Not used • DIAMETER—Connects the Net-Net SBC to the policy-server

address—Enter the IP address of external policy server

port—Enter the port on the external policy server to connect to for COPS messages. The standard port for COPS is 3288.

Default	80
Values	Valid Range: 0-65535

realm—Enter the realm where the external policy server exists

num-connections—Enter the number of TCP connections to external policy server

Default	1
Values	Min: 0 / Max: 65535

reserve-incomplete—Enable or disable admission requests being made before all of the details of the call are known

Default	enabled
Values	• Enabled—Supports the usual behavior when the AAR is sent upon SDP offer as well as SDP answer. This mode ensures backwards compatibility with releases prior to Release S-C6.1.0. • Orig-realm-only—Allows calls originating from a realm with a policy server associated with it to send the AAR upon

SDP offer; calls terminating at a realm with a policy server associated with it send the AAR post SDP exchange.

- Disabled—Allows no bandwidth reservation for incomplete flows.

permit-conn-down—Enable or disable the Net-Net SBC's ability to permit calls if there is no connection to the external policy server

Default	disabled
Values	enabled | disabled

permit-on-reject—Change this parameter to **enabled** if you want the Net-Net SBC to forward 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	enabled
Values	enabled | disabled

product-name—Enter the vendor product name

application-mode—Select the mode in which the policy server interface is operating

Default	none
Values	Rq | Rx | Gq | e2 | pktmm3

application-id—Enter the application mode of this interface

Default	0
Values	Min: 0 / Max: 999999999

framed-ip-addr-encoding—Set the format of the Frame-IP-Address (AVP 8) value in Diameter messages.

Default	octet-string
Values	octet-string (i.e., 0xC0A80A01) | ascii-string (i.e., 192.168.10.1)

dest-realm-format—Set the format for the Destination-Realm AVP.

Default	user_with_realm
Values	user_with_realm | user_only | realm_only

ingress-realm-location—Set this parameter to configure the child realm or its parent for the Address-Realm in the Globally-Unique-Address AVL in DIAMETER UDR messages that the Net-Net SBC sends to the policy server.

Default	realm-in

Values	• realm-in—This setting means that the Net-Net SBC will use the same realm on which the REGISTRATION request arrived • sip-interface—This setting means that the Net-Net SBC will use the realm associated with the SIP interface on which the REGISTRATION request arrived

domain-name-suffix—Sets the suffix for Origin-Realm and Origin-Host AVPs that have a payload string constructed as a domain name. If your entry does not include the dot, the system prepends 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-srv-proxy—Enable this parameter if you want to include the proxy bit in the header. The presense 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

allow-srv-proxy—Enable this parameter if you want to the proxy bit in the header

Default	enabled
Values	enabled | disabled

watchdog-ka-timer—Enter the number of seconds to define the interval for watchdog/keep-alive messages; this is the time in which the Net-Net SBC must receive a COPS-KA message from the policy server to ensure collection is still valid.

Default	0
Values	Min: 0 / Max: 999999999

options—Enter any customer-specific features and/or parameters for this external policy server. This parameter is optional.

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: 4.0

RTC Status

Supported

h323

The **h323** configuration element is the top level of the H.323 configuration, and it contains h323 parameters that apply globally.

Syntax

```
h323 <state | log-level | response-tmo | connect-tmo | options |
h323-stacks | rfc2833-payload | alternate-routing | codec-
fallback | enum-sag-match | 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 functionality. This parameter overrides the process-log level field value set in the system-config element only for H.323 functionality. If the state parameter in this element is set to disabled, this parameter still overrides the process-log-level field from the system-config element for H.323.

Default INFO

Values EMERGENCY | CRITICAL | MAJOR | MINOR | WARNING | NOTICE | INFO | TRACE | DEBUG

response-tmo—Set the number of seconds Net-Net SBC waits between sending a SETUP message and receiving no response before the call is torn down

Default 4

Values Min: 0 / Max: 999999999

connect-tmo—Set the number of seconds Net-Net SBC waits between sending out 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

options—Enter customer-specific features and/or parameters that affect H.323 behavior globally. This parameter sets a comma-separated list of “feature=value” or “feature” parameters.

h323-stacks—Enter the h323-stacks subelement

rfc2833-payload—Enter the payload type used by the H.323 stack in preferred rfc2833-mode

Default 101

Values Valid Range: 96-127

alternate-routing— Choose between pre-4.1 or 4.1 behavior:

- Pre-4.0 behavior—Alternate routing is disabled, and the Net-Net SBC sends a release complete message back to the caller, `proxy`
- 4.1 behavior—The Net-Net SBC performs alternate routing, `recur`

Default	proxy
Values	proxy | recur

codec-fallback—Enable or disable slow start to fast start codec negotiation

Default	disabled
Values	enabled | disabled

enum-sag-match—Enable or disable matching against the hostnames in ENUM/LRT lookup responses and session agent groups

Default	disabled
Values	enabled | disabled

Path

h323 is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > h323**.

Release

First appearance: 1.2.1 / Most recent update: 4.1

RTC Status

Supported

Notes

Unlike other single-instance configuration elements, the h323 element does not have to be selected before it can be viewed. The options field does not appear in the output for the show command within the h323 element or for running-config subcommand unless it contains configured values.
This is a single instance configuration element.

h323 > h323-stacks

The **h323-stack** subelement supports the SFIWF, FSIWF, H.323<—>SIP traffic, and general H.323 functionality.

Syntax

```
h323-stacks <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 | q931-port | alternate-transport |
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 | rfc2833-mode
| alarm-threshold | select | no | show | done | exit>
```

Parameters

name—Enter the name of H.323 stack. This value is required and must be unique. The value you enter in this parameter for your H.323 interface (stack) configuration cannot start with a number; it must start with a letter. The Net-Net SBC considers names that start with numbers to be invalid.

description—Provide a brief description of the **h323-config** configuration element

state—Enable or disable this h323-stack

Default	enabled
Values	enabled | disabled

Notes This parameter is not RTC supported.

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

Notes This parameter is not RTC supported.

realm-id—Enter the realm served by this H.323 stack. This value must be a valid identifier for a realm configuration.

Notes This parameter is not RTC supported

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 a local-policy element). If you wish to use static stack selection, 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.

Notes This parameter is not RTC supported.

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

Notes This command is not RTC supported

max-calls—Enter the maximum number of calls allowed for the network associated with this H.323 stack

Default 200

Values Min: 0 / Max: 2^{32}-1

Notes This command is not RTC supported.

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: 2^{32}-1

Notes This command is not RTC supported.

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: 2^{32}-1

Notes This command is not RTC supported.

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 (e.g., h323-ID=acme01). This field is only applicable when the isgateway field is set to enabled.

Values

- h323-ID
- e164
- url
- email
- ipAddress

Notes This command is not RTC supported.

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: 0, Max: 65535

Notes This command is not RTC supported.

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

Notes This parameter is not RTC supported.

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. 224.0.1.41:1718 is the well known value used to discover the Gatekeeper.

Default 0.0.0.0:0

Notes This parameter is not RTC supported.

gatekeeper—Enter the IP address and RAS port of the Gatekeeper. In order to clear this field, you must enter an empty string.

Default 0.0.0.0:0

Notes This parameter is not RTC supported.

gk-identifier—Enter the gatekeeper identifier with which the H.323 stack registers

Values 1 to 128 characters

Notes This parameter is not RTC supported.

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: 65535

Notes This parameter is not RTC supported.

alternate-transport—Enter the alternate transport addresses and ports (i.e., the Annex E address(es) and port(s)). If this field is left empty, the H.323 stack will not listen for incoming Annex E requests.

Notes This parameter is not RTC supported.

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: 65535

Notes This parameter is not RTC supported.

h245-tunneling—Enable or disable H.245 tunneling supported by this H.323 stack

Default disabled

Values enabled | disabled

Notes This parameter is not RTC supported.

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 set up 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-slow 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

Values	e164 | url | h323-ID | ipAddress
Notes	This parameter is not RTC supported.

process-registration—Enable or disable registration request processing for this H.323 stack . Net-Net SBC will process any RRQs that arrive on this H.323 stack if enabled. Net-Net SBC will not acknowledge any requests and drop all RRQ 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—allow all anonymous connections • agents-only—only requests from session agents allowed • realm-prefix—session agents and address matching realm prefix

options—Enter customer-specific features and/or parameters on a per-stack basis. This parameter sets a comma-separated list of “feature=value” or “feature” parameters. This options field affects H.323 behavior for this particular h323 stack whereas the options field in the main h323 element affects H.323 behavior globally.

Notes	This command is not RTC supported.

proxy-mode—Select the proxy functionality for signaling only operation

Values	H225 | H245
Notes	This command is not RTC supported.

h245-stage—Select the H.245 stage at which the Net-Net SBC allows either of the following:

- Transfer of the H.245 address to 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 Q.931 port range used for Q.931 call signalling

Default	0
Values	0 | 1024 | 2048 | 4096 | 8192 | 16384 | 32768

q931-number-ports—Set the number of ports in Q.931 port range used for the H.323 registration proxy feature

Default	0
Values	0 | 1024 | 2048 | 4096 | 8192 | 16384 | 32768

dynamic-start-port—Set the starting port number for Q.931 port range used for the H.323 registration proxy feature

Default	0
Values	0 | 1024 | 2048 | 4096 | 8192 | 16384 | 32768

dynamic-number-ports—Enter the number of ports in port range used for dynamic TCP connections the H.323 registration proxy feature

Default	0
Values	0 | 1024 | 2048 | 4096 | 8192 | 16384 | 32768

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.

Notes This parameter is not RTC supported.

tcp-keepalive—Enable or disable TCP keepalive processing on call-signaling port

Default	disabled
Values	enabled | disabled

rfc2833-mode—Select whether 2833/UII negotiation will be transparent to the Net-Net SBC (pre-4.1 behavior), or use 2833 for DTMF and signal it in its TCS

Default	transparent
Values	transparent | preferred

alarm-threshold—Access the **alarm-threshold** subelement.

Path

h323-stacks is a subelement under the h323 element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > h323 > h323-stacks**.

Release

First appearance: 1.2 / Most recent update: S-C6.2.0

RTC Status

Supported

Notes

This is a multiple instance configuration subelement.

h323>h323-stacks>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>
```

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 under the h323-stacks subelement. The full path from the topmost ACLI prompt is: **configure terminal > session-router > h323 > h323-stacks>alarm-threshold**.

Release

First appearance: S-C6.2.0

RTC Status

Supported

host-route

The **host-route** configuration element establishes routing exceptions on the Net-Net SBC for management traffic.

Syntax

```
host-route <dest-network | netmask | gateway | description |
select | no | show | done | exit>
```

Parameters

dest-network—Enter the IP address of the destination network for this host route. No two host-route elements can have the same dest-network field value.

netmask—Enter the destination network subnet mask. The network-interface element will not function properly unless this field value is valid.

gateway—Enter the gateway used to leave the local network. The gateway field identifies the next hop to use when forwarding a packet out of the originator's LAN.

> ***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

Path

host-route is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > host-route**.

Release

First appearance: 1.0.1

RTC Status

Supported

Notes

This is a multiple instance configuration element.

ike-certificate-profile

The **ike-certificate-profile** subelement references a public certificate that authenticates a specific IKEv2 identity, as well as one of more CA certificates used to validate a certificate offered by a remote peer.

Syntax

```
ike-certificate-profile < identity | end-entity-certificate |
trusted-ca-certificates | verify-depth | batch | select | no |
show | done | exit >
```

Parameters

identity—Enter the local IKEv2 entity that using the authentication and validation credentials provided by this **ike-certificate-profile** instance.

Default	None
Values	An IP address or fully-qualified domain name (FQDN) that uniquely identifies the user of resources provided by this **ike-certificate-profile** instance

end-entity-certificate—Enter the unique name of a **certificate-record** configuration element referencing the identification credential (specifically, an X509.v3 certificate) offered by a local IKEv2 entity in support of its asserted identity.

Default	None
Values	Name of an existing **certificate-record** configuration element

trusted-ca-certificates—Enter the unique names of one or more **certificate-record** configuration elements referencing Certification Authority (CA) certificates used to authenticate a remote IKEv2 peer.

Default	None
Values	A comma separated list of existing CA **certificate-record** configuration elements

verify-depth—Enter the maximum number of chained certificates that will be processed while authenticating the IKEv2 peer.

Default	10
Values	Min: 1 | Max: 10

Path **ike-certificate-profile** is a subelement under the **ike** element. The full path from the topmost ACLI prompt is: **configure-terminal>security>ike>ike-certificate-profile**.

Release First appearance: S-C6.2.0

RTC Status Supported

Notes This is a multiple instance configuration element.

ike-config

The **ike-config** subelement defines a single, global Internet Key Exchange (IKE) configuration object.

Syntax

```
ike <state | ike-version | log-level | udp-port | negotiation-
timeout | event-timeout | phase1-mode | phase1-dh-mode | ike-v2-
ike-life-secs | ike-v2-ipsec-life-secs | phase1-life-seconds |
phase1-life-secs-max | phase2-life-seconds | phase2-life-secs-max
| phase2-exchange-mode | shared-password | options | eap-protocol
| address-assignment | eap-bypass-identity | red-port | red-max-
trans | red-sync-start-time | red-sync-comp-time | dpd-time-
interval | overload-threshold | overload-interval | overload-
action | overload-critical-threshold | overload-critical-interval
| sd-authentication-method | certificate_profile_id | select | no
| show | done | exit>
```

Parameters

state—Enter the state (enabled or disabled) of the **ike-config** configuration element.

Default	enabled
Values	disabled | disabled

ike-version—Enter an integer value that specifies IKE version.

Select 1 for IKEV1 protocol implementation.

Select 2 for IKEV2 protocol implementation.

Default	2
Values	1 | 2

log-level—Enter the IKE log level; events of this level and other events deemed more critical are written to the system log.

Events are listed below in descending order of criticality.

Default	info

Values	emergency | critical | major | minor | warning | notice | info | trace | debug | detail

udp-port—Enter the UDP port used for IKEv1 protocol traffic.

Default	500
Values	Min: 1025 / Max: 65535

negotiation-timeout—Enter the maximum interval between Diffie-Hellman message exchanges.

Default	15 (seconds)
Values	Min: 1 / Max: 2^{32} - 1 (seconds)

Notes In the event of timer expiration, the IKE initiator must restart the Diffie-Hellman exchange.

event-timeout—Enter the maximum time allowed for the duration of an IKEv1 event, defined as the successful establishment of an IKE or IPsec Security Association (SA).

Default	60 (seconds)
Values	Min: 1 / Max: 2^{32} - 1 (seconds)

Notes In the event of timer expiration, the IKE initiator must restart the Phase 1 (IKE SA) or Phase 2 (IPsec SA) process.

phase1-mode—Enter the IKE phase 1 exchange mode: aggressive or main.

Default	main
Values	• aggressive—is less verbose (requiring only three messages), but less secure in providing no identity protection, and less flexible in IKE SA negotiation • main—is more verbose, but provides greater security in that it does not reveal the identity of the IKE peers. Main mode requires six messages (3 requests and corresponding responses) to (1) negotiate the IKE SA, (2) perform a Diffie-Hellman exchange of cryptographic material, and (3) authenticate the remote peer

phase1-dh-mode—Enter the Diffie-Hellman group used during IKE phase 1 negotiation.

Default	first-supported
Values	• dh-group1— as initiator, propose Diffie-Hellman group 1 (768-bit primes, less secure • dh-group2—as initiator, propose Diffie-Hellman group 2 (1024-bit primes, more secure) • first-supported— as responder, use the first supported Diffie-Hellman group proposed by initiator

Notes Diffie-Hellman groups determine the lengths of the prime numbers exchanged during the symmetric key generation process.

v2-ike-life-secs—Enter the default IKEv2 SA lifetime in seconds.

Default	86400 (24 hours)

Values Min: 1 / Max: 2^{32} - 1 (seconds)

Notes This global default can be over-ridden at the IKEv2 interface level.

v2-ipsec-life-secs—Enter the default IPsec SA lifetime in seconds.

Default 28800 (8 hours)

Values Min: 1 / Max: 2^{32} - 1 (seconds)

Notes This global default can be over-ridden at the IKEv2 interface level.

phase1-life-seconds—Set the time (in seconds) proposed for IKE SA expiration during IKE Phase 1 negotiations.

Default 3600 (1 hour)

Values Min: 1 / Max: 2^{32} - 1 (seconds)

Notes Relevant only when the Net-Net SBC is acting in the IKE initiator role.

phase1-life-seconds-max—Set the maximum time (in seconds) accepted for IKE SA expiration during IKE Phase 1 negotiations.

Default 86400 (24 hours)

Values Min: 1 / Max: 2^{32} - 1 (seconds)

Notes Relevant only when the Net-Net SBC is acting in the IKE responder role.

phase2-life-seconds—relevant only when the Net-Net SBC is acting in the IKE initiator role, contains the time proposed (in seconds) for IPsec SA expiration during IKE Phase 2 negotiations.

Default 28800 (8 hours)

Values Min: 1 / Max: 2^{32} - 1 (seconds)

Notes During IKE Phase 2, the IKE initiator and responder establish the IPsec SA.

phase2-life-seconds-max—Set the maximum time (in seconds) accepted for IPsec SA expiration during IKE Phase 2 negotiations.

Default 86400 (24 hours)

Values Min: 1 / Max: 2^{32} - 1 (seconds)

Notes Relevant only when the Net-Net SBC is acting in the IKE responder role.

phase2-exchange-mode—Enter the Diffie-Hellman group used during IKE Phase 2 negotiation.

Default phase1-group

Values

- dh-group1— use Diffie-Hellman group 1 (768-bit primes, less secure)
- dh-group2—use Diffie-Hellman group 2 (1024-bit primes, more secure)
- no-forward-secrecy— use the same key as used during Phase 1 negotiation
- phase1-group— use the same Diffie-Hellman group as used during Phase 1 negotiation

Notes During IKE Phase 2, the IKE initiator and responder establish the IPsec SA.

Diffie-Hellman groups determine the lengths of the prime numbers exchanged during the symmetric key generation process.

shared-password—Enter the default PSK used during IKE SA authentication.

This global default can be over-ridden at the IKE interface level.

Default	None
Values	A string of ACSII-printable characters no longer than 255 characters (not displayed by the ACLI)

eap-protocol—Enter the EAP protocol used with IKEv2.

Default	eap-radius-passthru
Values	eap-radius-passthru

Notes The current software performs EAP operations by a designated RADIUS server or server group; retain the default value.

addr-assignment—Set the method used to assign addresses in response to an IKEv2 Configuration Payload request.

Default	local
Values	• local— use local address pool • radius-only— obtain local address from RADIUS server • radius-local— try RADIUS server first, then local address pool

Notes This parameter specifies the source of the returned IP address, and can be over-ridden at the IKE interface level.

eap-bypass-identity—Contains a value specifying whether or not to bypass the EAP (Extensible Authentication Protocol) identity phase.

EAP, defined in RFC 3748, provides an authentication framework widely used in wireless networks.

An Identity exchange is optional within the EAP protocol exchange. Therefore, it is possible to omit the Identity exchange entirely, or to use a method-specific identity exchange once a protected channel has been established.

Default	disabled (requires an identity exchange)
Values	disabled | enabled

red-port—Enter the port number monitored for IKEv2 synchronization messages; used in high-availability environments.

The default value (0) effectively disables redundant high-availability configurations. Select a port value other than 0 (for example, 1995) to enable high-availability operations.

Default	0
Values	Min: 1024 / Max: 65535

red-max-trans—For HA nodes, set the maximum number of retained IKEv2 synchronization message.

Default	10000 (messages)
Values	Min: 1 / Max: 2^{32} - 1 (messages)

red-sync-start-time—For HA nodes, set the timer value for transitioning from standby to active role — the amount of time (in milliseconds) that a standby device waits for a heartbeat signal from the active device before transitioning to the active role.

Default	5000 (milliseconds)
Values	Min: 1 / Max: 2^{32} - 1 (milliseconds)

red-sync-comp-time—For HA nodes, set the interval between synchronization attempts after the completion of an IKEv2 redundancy check.

Default	1000 (milliseconds)
Values	Min: 1 / Max: 2^{32} - 1 (milliseconds)

dpd-time-interval—Set the maximum period of inactivity (in seconds) before the Dead Peer Detection (DPD) protocol is initiated on a specific endpoint.

The default value, *0*, disables the DPD protocol; setting this parameter to a non-zero value globally enables the protocol and sets the inactivity timer.

Default	0 (DPD disabled)
Values	Min: 1 / Max: 2^{32} - 1 (seconds)

overload-threshold—Set the percentage of CPU usage that triggers an overload state.

Default	100 (disabling overload processing)
Values	An integer from 1 to 100, and less than the value of **overload-critical-threshold**

overload-interval—Set the interval (in seconds) between CPU load measurements while in the overload state.

Default	1
Values	Min: 0 / Max: 60

overload-action—Select the action to take when the Net-Net SBC (as a Net-Net SG) CPU enters an overload state. The overload state is reached when CPU usage exceeds the percentage threshold specified by the **overload-threshold** parameter.

Default	none
Values	• drop-new-connection—use to implement call rejection • none—use to retain default behavior (no action)

overload-critical-threshold—Set the percentage of CPU usage that triggers a critical overload state. This value must be greater than the value of **overload-threshold.**

Default	100 (disabling overload processing)

Values Min: 0 / Max: 100

overload-critical-interval—Set the interval (in seconds) between CPU load measurements while in the critical overload state.

Default 1

Values Min: 0 / Max: 60

sd-authentication-method—Select the method used to authenticate the IKEv2 SA. Two authentication methods are supported.

This global default can be over-ridden at the IKEv2 interface level.

Default shared-password

Values
- certificate—uses an X.509 certificate to digitally sign a block of data
- shared-password—uses a PSK that is used to calculate a hash over a block of data

certificate-profile-id—When **sd-authentication-method** is **certificate**, identifies the default **ike-certificate-profile** configuration element that contains identification and validation credentials required for certificate-based IKEv2 authentication.

This parameter can be over-ridden at the IKEv2 interface level.

Default None

Values Name of an existing **ike-certificate-profile** configuration element

Path **ike-config** is a subelement under the ike element. The full path from the topmost ACLI prompt is: **configure-terminal>security>ike>ike-config.**

Release First appearance: S-C6.2.0

RTC Status Supported

Notes This is a single instance configuration element.

ike-interface

The **ike-interface** configuration element enables creation of multiple IKE-enabled interfaces.

Syntax

```
ike-interface < address | realm-id | ike-mode | dpd-params-name |
shared-password | batch | select | no | show | done >
```

address—Enter the IPv4 address of a specified IKEv1 interface.

Default None

Values Any valid IPv4 address

realm-id—Enter the name of the realm that contains the IP address assigned to this IKEv1 interface.

Default None

Values Name of an existing **realm** configuration element

ike-mode—Select the IKE operational mode.

Default responder

Values initiator | responder

local-address-pool —Select a list local address pool from a list of configured **local-address-pools**.

dpd-params-name—Enter the specific set of DPD operational parameters assigned to this IKEv1 interface (relevant only if the Dead Peer Detection (DPD) Protocol is enabled).

Default None

Values Name of an existing **dpd-params** configuration element

v2-ike-life-secs—Enter the default IKEv2 SA lifetime in seconds.

Default 86400 (24 hours)

Values Min: 1 / Max: 2^{32} - 1 (seconds)

Notes This global default can be over-ridden at the IKEv2 interface level.

v2-ipsec-life-secs—Enter the default IPsec SA lifetime in seconds.

Default 28800 (8 hours)

Values Min: 1 / Max: 2^{32} - 1 (seconds)

Notes This global default can be over-ridden at the IKEv2 interface level

shared-password—Enter the interface-specific PSK used during IKE SA authentication.

This IKEv1-interface-specific value over-rides the global default value set at the IKE configuration level.

Default none

Values a string of ACSII printable characters no longer than 255 characters (not displayed by the ACLI)

eap-protocol—Enter the EAP protocol used with IKEv2.

Default eap-radius-passthru

Values eap-radius-passthru

Notes The current software performs EAP operations by a designated RADIUS server or server group; retain the default value.

addr-method—

Values

- radius-only—Use the radius server for the local address
- radius-local—Use the radius server first and then try the local address pool
- local—Use the local address pool to assign the local address

sd-authentication-method—Enter the allowed Net-Net SBC authentication methods

Default none

Values
- none—Use the authentication method defined in ike-config for this interface
- shared-password—Endpoints authenticate the Net-Net SBC using a shared password
- certificate—Endpoints authenticate the Net-Net SBC using a certificate

certificate-profile-id-list—Select an IKE certificate profile from a list of configured **ike-certificate-profiles**.

Path **ike-interface** is a subelement under the **ike** element. The full path from the topmost ACLI prompt is: **configure terminal>security>ike>ike-interface.**

Release First appearance: S-C6.2.0

RTC Status Supported

Notes This is a multiple instance configuration element.

ike-sainfo

The ike-sainfo configuration element enables negotiation and establishment of IPsec tunnels.

Syntax

```
ike-sainfo <name | security-protocol | auth-algo | encryption-
algo | ipsec-mode | tunnel-local-addr | tunnel-remote-addr |
select | no | show | done | exit>
```

Parameters

name—Enter the unique name of this instance of the **ike-sainfo** configuration element.

Default None

Values A valid configuration element name, that is unique within the **ike-sainfo** namespace

security-protocol—Enter the IPsec security (authentication and encryption) protocols supported by this SA.

Default ah

Values
- ah—RFC 4302 authentication services
- esp—RFC 4303 encryption services
- esp-auth—RFC 4303 encryption and authentication services
- esp-null—RFC 4303 encapsulation, lacks encryption — not for production environments

auth-algo — Set the authentication algorithms supported by this SA.

Default any

Values
- any—Choose any
- md5—Message Digest algorithm 5

- sha1—Secure Hash Algorithm

encryption-algo — Set the encryption algorithms allowed by this SA.

Default	any
Values	• any—Choose any • des—Data Encryption Standard • 3des—Tripes DES • aes—Advanced Encryption Standard • null—NULL encryption

ipsec-mode — Select the IPSec operational mode.

Transport mode provides a secure end-to-end connection between two IP hosts. Tunnel mode provides VPN service where entire IP packets are encapsulated within an outer IP envelope and delivered from source (an IP host) to destination (generally a secure gateway) across an untrusted internet.

Default	transport
Values	transport | tunnel

tunnel-local-addr—Enter the IP address of the local IP interface that terminates the IPsec tunnel (relevant only if the **ipsec-mode** is tunnel, and otherwise is ignored).

Default	None
Values	Any valid local IP address

tunnel-remote-addr—Enter the IP address of the remote peer or host (relevant only if the **ipsec-mode** is **tunnel**, and is otherwise ignored).

Default	* (matches all IP addresses)
Values	Any valid IP address

Path **ike-sainfo** is a subelement under the **ike** element. The full path from the topmost ACLI prompt is : **configure terminal > security > ike > ike-sainfo**.

Release First appearance: S-C6.2.0

RTC Status Supported

Notes This is a multiple instance configuration element.

Configures an **ike-sainfo** instance named *star*.

Default values for **auth-algo** (any) and **encryption-algo** (any) provide support for MD5 and SHA1 authentication and AES/3DES encryption. The default value for **tunnel-remote-address** (*) matches all IPv4 addresses.

Non-default values specify IPsec tunnel mode running ESP, and identify the local tunnel endpoint.

ims-aka-profile

The **ims-aka-profile** configuration element establishes supports IP Media Subsystem-Authentication and Key Agreement, defined in 3GPPr7 (specifications in TS 33.203 and call flows in TS 24.228).

Syntax

```
ims-aka-profile <name | protected-server-port | protected-client-
port | encr-alg-list | auth-alg-list | select | no | show | done |
exit>
```

Parameters

name—Enter the name for this IMS-AKA profile

protected-server-port—Enter the port number on which the Net-Net SBC receives protected messages; 0 disables the function

Default	0
Values	Min: 1025 / Max: 65535

protected-client-port—Enter the port number on which the Net-Net SBC sends out protected messages

Default	0
Values	Min: 1025 / Max: 65535

encr-alg-list—Enter the list of encryption algorithms

Default	aes-cbc | des-ede3-cbc | null

auth-alg-list—Enter the list of authentication algorithms

Default	hmac-sha-1-96

Path

ims-aka-profile is an element under the security path. The full path from the topmost ACLI prompt is: **configure terminal > security > ims-aka-profile**.

Release

First appearance: S-C6.1.0

RTC Status

Supported

Notes

This is a multiple instance configuration element.

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 | ipsec-global-
config | exit>
```

Parameters

security-policy—Enter the security-policy configuration element.

security-association—Enter the security-association configuration element.

ipsec-global-config—Access the **ipsec-global-config** 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: 5.0

RTC Status

Supported

ipsec>ipsec-global-config

The **ipsec-global-config** subelement allows you to configure establish the parameters governing system-wide IPSec functions and behavior, including IPSec redundancy.

Syntax

```
ipsec-global-config <red-ipsec-port | red-max-trans | red-sync-
start-time | red-sync-comp-time | options | select | no | show |
done | exit>
```

Parameters

red-ipsec-port—Enter the port on which the Net-Net SBC should listen for redundancy IPSec synchronization messages

Default	1994
Values	Min: 1025 / Max: 65535

red-max-trans—Enter the maximum number of redundancy transactions to retain on the active

Default	10000
Values	Min: 0 / Max: 999999999

red-sync-start-time—Enter the time in milliseconds before the system starts to send redundancy synchronization requests

Default	5000

Min: 0 / Max: 999999999

red-sync-comp-time—Enter the time in milliseconds to define the timeout for subsequent synchronization requests once redundancy synchronization has completed

Default	1000

Min: 0 / Max: 999999999

options—Enter the appropriate option name for the behavior you want to configure

Path

security-association is a subelement of the ipsec path. The full path from the topmost ACLI prompt is: **configure terminal > security> ipsec>security-association.**

Release

First appearance: S-C6.1.0

RTC Status

Notes

This is a single instance configuration element.

ipsec>security-association

The **security-association** subelement allows you to configure a security association (SA), the set of rules that define the association between two endpoints or entities that create the secured communication.

Syntax

```
security-association <manual | exit>
```

Parameters

manual—Enter the `manual` subelement where you can manually configure a security association

Path

security-association is a subelement of the ipsec path. The full path from the topmost ACLI prompt is: **configure terminal > security> ipsec>security-association.**

Release

First appearance: 5.0

RTC Status

Supported

ipsec>security-association>manual

The **manual** subelement is where you manually configure a security association on the Net-Net SBC.

Syntax

```
manual <name | spi | network-interface | local-ip-addr | remote-
ip-addr | local-port | remote-port | trans-protocol | ipsec-
protocol | direction | ipsec-mode | auth-algo | encr-algo | auth-
key | encr-key | aes-ctr-nounce | tunnel-mode | select | no | show
| done>
```

name—Enter the name for this security policy

spi—Set 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 local IP address to match for traffic selectors for this SA

remote-ip-addr—Enter the remote IP address to match for traffic selectors for this SA

local-port—Enter the local port to match for traffic selectors for this SA

Default	0
Values	Min: 0 (disabled) / Max: 65535

remote-port—Enter the remote port to match for traffic selectors for this SA

Default	0
Values	Min: 0 (disabled) / Max: 65535

trans-protocol—Select the transport protocol to match for traffic selectors for this SA

Default	ALL
Values	• UDP • TCP • ALL • ICMP

ipsec-protocol—Select the IPsec protocol used for this SA

Default	esp
Values	esp | ah

direction—Set the direction of traffic this security association can apply to

Default	both
Values	in | out | both

ipsec-mode—Select the IPsec mode of this SA

Default	transport
Values	tunnel | transport

auth-algo—Select 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 nounce. This only applies if `aes-128-ctr` or `aes-256-ctr` are chosen as your encryption algorithm.

Default	0

tunnel-mode—Enter the `tunnel-mode` subelement

Path

security-association is a subelement under the ipsec element. The full path from the topmost ACLI prompt is: **configure-terminal > security > ipsec > security-association**.

Release

First appearance: 5.0

RTC Status Supported

ipsec>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 of this tunnel mode profile

remote-ip-addr—Enter the remote IP address of this tunnel mode profile

Path **tunnel-mode** is a subelement under the ipsec>security-association element. The full path from the topmost ACLI prompt is: **configure-terminal > security > ipsec > security-association>tunnel-mode**.

Release First appearance: 5.0

RTC Status Supported

ipsec>security-policy

This configuration element defines multiple policy instances with each policy defining match criteria and an operational action performed on matching traffic flows.

Syntax

```
security-policy < name | network-interface | priority |
local-ip-addr-match | remote-ip-addr-match | local-port-match |
remote-port-match | trans-protocol-match | direction |
local-ip-mask | remote-ip-mask | action |
outbound-sa-fine-grained-mask | ike-sainfo-name |
select | no | show | done | exit >
```

Parameters

name—Enter a unique identifier for this **security-policy** instance.

Default	None
Values	A valid configuration element name that is unique within the **security-policy** namespace

network-interface—Enter the unique name of the network-interface supported by this **security-policy** instance.

Identify the network interface by providing the interface name and VLAN ID separated by a colon; for example *access:10*.

Default	None
Values	Name and VLAN ID of an existing **network-interface** configuration element

priority—Set the priority of this **security-policy** instance, where 0 is the highest priority.

Default	0
Values	Min: 0 / Max: 126

local-ip-addr-match—Enter an IPv4 address; in conjunction with **local-ip-mask** and **local-port-match,** this parameter specifies address-based matching criteria for inbound traffic.

Notes

Specifically, **local-ip-addr-match** works with **local-ip-mask** to define a range of inbound IP addresses subject to this **security-policy** instance. Using default values for both properties, the **security-policy** instance matches all IPv4 addresses.

Default	0.0.0.0
Values	A valid IPv4 address; the special address value, 0.0.0.0, matches all IPv4 addresses

remote-ip-addr-match—Enter an IPv4 address; in conjunction with **remote-ip-mask** and **remote-port-match** specifies address-based matching criteria for outbound traffic.

Notes

Specifically, **remote-ip-addr-match** works with **remote-ip-mask** to define a range of outbound IP addresses subject to this **security-policy** instance. Using default values for both properties, the **security-policy** instance matches all IPv4 addresses.

Default	0.0.0.0
Values	A valid IPv4 address; the special address value, 0.0.0.0, matches all IPv4 addresses

local-port-match—Enter a port number, or the special value 0; in conjunction with **local-ip-addr-match** and **local-ip-mask**, this parameter specifies address-based matching criteria for inbound traffic.

The default value disables port-based matching, meaning port numbers are ignored in the default state.

Default	0 (disables port-based matching)
Values	Min: 0 / Max: 65535

remote-port-match—Enter a port number, or the special value 0; in conjunction with **remote-ip-addr-match** and **remote-ip-mask**, this parameter specifies address-based matching criteria for outbound traffic.

The default value disables port-based matching, meaning port numbers are ignored in the default state.

Default	0 (disables port-based matching)
Values	Min: 0 / Max: 65535

trans-protocol-match—Select a specified protocol or the special value *all* that specifies transport-protocol-based matching criteria for inbound and outbound traffic

The default value (all) matches all supported transport layer protocols.

Default	all
Values	all | ICMP | SCTP | TCP | UDP

direction—Select an indicator of the directionality of this **security-policy** instance.

Default	both
Values	• both—the policy applies to all traffic • in—the policy applies only to inbound traffic • out—the policy applies only to outbound traffic

local-ip-mask—Enter an IPv4 address; in conjunction with **local-ip-addr-match** and **local-port-match**, this parameter specifies address-based matching criteria for inbound traffic.

Specifically, **local-ip-addr-match** works with **local-ip-mask** to define a range of inbound IP addresses subject to this **security-policy** instance. Using default values for both properties, the **security-policy** instance matches all IPv4 addresses.

Default	255.255.255.255
Values	A dotted decimal IP address mask

remote-ip-mask—Enter an IPv4 address; in conjunction with **remote-ip-addr-match** and **remote-port-match**, this parameter specifies address-based matching criteria for outbound traffic.

Specifically, **remote-ip-addr-match** works with **remote-ip-mask** to define a range of outbound IP addresses subject to this **security-policy** instance. Using default values for both properties, the **security-policy** instance matches all IPv4 addresses.

Default	255.255.255.255
Values	A valid IPv4 address mask

action—Select the process of trafficking that conforms to the match criteria specified by this **security-policy** instance.

Default	ipsec
Values	• allow—forwards matching traffic but performs no security processing • discard—discards matching traffic • ipsec—processes matching traffic per configured IPsec properties

outbound-sa-fine-grained-mask—not used for IKE operations.

ike-sainfo-name—Enter the name of the **ike-sainfo** configuration element assigned to this **security-policy** instance.

Default	None
Values	A valid configuration element name that is unique within the **ike-sainfo** namespace

Notes

The **ike-sainfo** configuration element identifies the algorithms and protocols available for the establishment if IPsec Security Associations (SA).

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 | trans-protocol-mask | vlan-
mask | ip-protocol-mask | trans-protocol-mask | valid | select |
no | show | done | exit>
```

Parameters

local-ip-mask—Enter the local IP address mask

Default	255.255.255.255

remote-ip-mask—Enter the remote IP address mask

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

trans-protocol-mask—Enter the transport protocol mask for this security policy

Default	0
Values	Min: 0 / Max: 255

vlan-mask—Enter the VLAN ID mask

Default	0x000
Values	0x000 (disabled)-0xFFF

Path

outbound-sa-fine-grained-mask is a subelement under the `ipsec>security-policy` element. The full path from the topmost ACLI prompt is: **configure-terminal > security > ipsec > security-policy** > **outbound-sa-fine-grained-mask**.

Release

First appearance: 5.0

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 | media-profiles | logging | add-reason-hdr |
select | no | show | done | exit>
```

Parameters

state—Enable or disable the Net-Net SBC's IWF

Default	disabled
Values	enabled | disabled

media-profiles—Set the default media SDP profiles that Net-Net SBC uses for Slow Start IWF calls. This field does not have a relationship with the media-profiles field found in the h323-stack subelement, as the values configured there affect calls that take place entirely in H.323. This list must be populated with the SDP codec names.

Values

- PCMU
- PCMA
- G722
- G723
- G726-32
- G728
- G729
- H261
- H263

logging—Enable or disable IWF-related SIP messages logging

Default	disabled
Values	enabled | disabled

add-reason-hdr—Enable or disable adding the Reason header to IWF calls

Default	disabled
Values	enabled | disabled

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: 1.2.1

RTC Status

Supported

Notes

This is a single instance configuration element.

license

The **license** configuration element is used for configuring Acme Packet licenses.

Syntax

```
license <add | no | show | exit>
```

Parameters

add—Add a license by entering a key obtained from Acme Packet

no—Delete licenses by feature. You are prompted to choose a license for deletion based on license features.

Path

licenses is an element under the system-config path. The full path from the topmost ACLI prompt is: **configure terminal > system > license**.

Release

First appearance: 2.0

RTC Status Supported

local-address-pool

The **local-address-pool** configuration element enables creation of local address pools, which can be used to provide a local (internal) address in response to remote requests for IP addresses.

Syntax

```
local-address-pool <name | address-range | dns-realm-id | data-
flow | batch | select | no | show | done | exit>
```

Parameters

name—Enter a unique identifier for this **local-address-pool** instance.

Default None

Values A valid configuration element name that is unique within the **local-address-pool** namespace

address-range—Access the **address-range** subelement.

dns-realm-id—Enter a DNS realm that supports this **local-address-pool** instance.

Default None

Values Name of an existing **dns-realm** configuration element

data-flow-list—Enter a **data-flow** configuration element assigned to this **local-address-pool** instance. This parameter specifies bandwidth available to the pool of addresses specified by this **local-address-pool** instance.

Default None

Values Name of an existing **data-flow** configuration element

Path **local-address-pool** is a subelement under the **ike** element. The full path from the topmost ACLI prompt is: **configure terminal > security > ike > local-address-pool**.

Release First appearance: S-C6.2.0

RTC Status Supported

Notes This is a multiple instance configuration element.

local-address-pool>address-range

The **address-range** configuration element specifies a single range of contiguous IPv4 addresses that are available to fulfill remote requests for a local address.

Syntax

```
address-range < network-address | subnet-mask | batch | select |
no | show | done | exit >
```

Parameters

network-address —In conjunction with **subnet-mask**, this parameter defines a range of IPv4 addresses available for dynamic assignment.

Default	None
Values	A valid IPv4 network address

subnet-mask —In conjunction with **network-address**, this parameter defines a range of IPv4 addresses available for dynamic assignment.

Default	None
Values	A valid IPv4 subnet mask

Path

local-address-pool>address-range is a subelement under the ike element. The full path from the topmost ACLI prompt: **configure-terminal>security>ike>local-address-pool>address-range**.

Release

First appearance: S-C6.2.0

RTC Status

Supported

Notes

This is a multiple instance configuration.

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 |
description | activate-time | deactivate-time | state | policy-
priority | policy-attributes | select | no | show | done | exit>
```

Parameters

from-address—Enter the source IP address, POTS number, E.164 number, or hostname for the local-policy element. At least one address must be set within this list, but it can include as many addresses as necessary. This parameter may be wildcarded, or entered with a DS: prefix (dialed string).

to-address—Enter the destination IP address, POTS number, E.164 number, or hostname for the local-policy element. At least one address must be set within this list, but it can include as many addresses as necessary. This parameter may be wildcarded.

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.

Default	*

description—Provide a brief description of the **local-policy** configuration element

activate-time—Set 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—Set 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 policy priority parameter for this local policy. It is used to facilitate emergency sessions from unregistered endpoints. This value is compared against a policy priority parameter in a SIP interface configuration element.

Default	none
Values	none | normal | non-urgent | urgent | emergency

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: 1.0 / Most recent update: 1.2.1

RTC Status Supported

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

```
policy-attributes <next-hop | realm | action | carrier | start-
time | end-time | days-of-week | cost | state | app-protocol |
media-profiles | terminate-recursion | methods | lookup | next-
key | eloc-str-lkup | eloc-str-match | select | no | show | done |
exit>
```

Parameters **next-hop**—Enter the next signaling host IP address, SAG, hostname, or ENUM config; ENUM is also an accepted value. 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 this parameter to redirect if you want to send a redirect next-hop message back to the calling party with the information in the Contact. The calling party then needs to send an INVITE using that information.

Default none

Values
- none—No specific action requested
- replace-uri—To replace the Request-URI with the next hop
- redirect—To send a redirect response with this next hop as contact

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—Set the time of day these policy attributes considered for preference determination

Default 0000

Values Min: 0000 / Max: 2400

end-time—Set 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 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 (H.323<—>SIP or SIP<—>H.323) if the signaling type does not match the value configured in the app-protocol field.

Values	H323 | SIP

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.

terminate-recursion—Terminate route recursion with this next hop

Default	disabled
Values	enabled | disabled

methods—Enter the SIP methods you want to use for matching 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.

Values	$TO | $FROM | $PAI

eloc-str-lkup—Set this parameter to **enabled** for the Net-Net SBC to parse the emergency location string, as received in a CLF Line Identifyier AVP, for emergency LRT lookup.

Default	enabled
Values	enabled | disabled

eloc-str-match—Set this parameter to the attribute name found in the **location-string** whose value will be used as a lookup key in the LRT named in the next-hop parameter.

Values	<string> string used as key for emergency LRT lookup

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: 1.0 / Most recent update: S-C6.1.0

RTC Status

Supported

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-response-map

The **local-response-map** configuration element is used for RFC3326 support.

Syntax

```
local-response-map <entries | delete | edit | select | no | show |
done | exit>
```

Arguments

entries—Enter the entries configuration subelement

delete—Remove the specified response map entry type

Values

- invalid-message—response map for invalid message
- cpu-overload—response map for CPU overload
- media-released—response map for media released condition
- media-not-allocated—response map for media not allocated

edit—Select a pre-configured RFC 3326 response map to edit

Path **local-response-map** is an element under the session router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > local-response-map**.

Release First appearance: 4.0

RTC Status Supported

local-response-map > entries

The **entries** subelement is used to add a local response map entry for RFC3326 support.

Syntax

```
entries <sip-status | q850-cause | sip-reason | q850-reason |
method | register-response-expires | select | no | show | done |
exit>
```

Parameters

sip-status—Enter the SIP response code to use for this error

Values Min: 100 / Max: 699

q850-cause—Enter the Q.850 cause code

sip-reason—Enter the SIP response code description

q850-reason—Enter the Q850 cause code description

method—Enter the name of the locally generated SIP failure response message you want to map to a 200 OK. When this parameter is left blank, the SIP registration response mapping feature is turned off.

register-response-expires—Enter the time, in seconds, you want to use for the expires time when mapping the SIP method you identified in the **method** parameter.

Values Min: 0 / Max: 999999999

Path **local-response-map-entries** is an subelement under the local-response-map configuration element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > local-response-map > local-response-map-entries**.

Release First appearance: 4.0

RTC Status Supported

local-routing-config

The **local-routing-config** element allows you to configure local route tables, giving the Net-Net SBC the ability to determine nest hops and map E.164 to SIP URIs locally, providing extensive flexibility for routing.

> *Note: Entering XML comments on the same line as LRT XML data is not currently supported.*

Syntax

```
local-routing-config <name | filename | prefix-length | select |
no | show | done | exit>
```

Parameters **name**—Enter a unique identifier for the local route table. This is the name you use to refer to this local route table when you configure policy attributes. This is a required parameter.

filename—Enter the name for the file from which the database corresponding to this local route table is created. You should use the `.gz` format, and the file should be placed in the `/code/lrt/` directory. This is a required parameter.

prefix-length—Enter the number of significant digits/bits to be used for lookup and cache storage

Default 0

Values Min: 0 / Max: 999999999

Path **local-routing-config** is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > local-routing-config**.

Release First appearance: 4.1.1

RTC Status Supported

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 | algd-log-level | mbcd-log-level | red-flow-port | red-
mgcp-port | red-max-trans | red-sync-start-time | red-sync-comp-
time | media-policing | max-signaling-bandwidth | app-signaling-
bandwidth | min-media-allocation | min-trusted-allocation | deny-
allocation | max-untrusted-signaling | min-untrusted-signaling |
tolerance-window | trap-on-demote-to-deny | syslog-on-demote-to-
deny | rtcp-rate-limit | anonymous-sdp | arp-message-bandwidth |
fragment-msg-bandwidth | rfc2833-timestamp | default-2833-duration
| rfc2833-end-pkts-only-for-non-sig | translate-non-rfc2833-event
| media-supervision-traps | active-arp | dnsalg-server-failover |
select | no | show | done | exit>
```

Parameters

state—Enable or disable 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 first packet of a flow arrives. If first packet does not arrive within this time limit, 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: 2 / Max: 5

hnt-rtcp—Enable or disable 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

algd-log-level—Select the log level for the MGCP process

Default	notice
Values	• emergency • critical • major • minor • warning • notice • info • trace • debug • detail

mbcd-log-level—Select the log level for the MBCD process

Default	notice
Values	• notice • emergency

- critical
- major
- minor
- warning
- notice
- info
- trace
- debug
- detail

red-flow-port—Enter the number of the port for checkpointing media flows associated with the HA interface. Setting the red-flow-port value to 0 disables media flow HA.

Default	1985
Values	Min: 1025 / Max: 65535

Notes This parameter is not RTC supported.

red-mgcp-port—Enter the number of the port for checkpointing MGCP signaling associated with the HA interface. Setting the red-mgcp-port value to 0 disables MGCP HA.

Default	1986
Values	Min: 1025 / Max: 65535

Notes This parameter is not RTC supported.

red-max-trans—Set the size of media flow and MGCP signaling transaction lists (i.e., Number of media flow or MGCP signaling transactions to store in memory at a time)

Default	10000
Values	Min: 0 / Max: 999999999

Notes This parameter is not RTC supported.

red-sync-start-time—Enter the time in milliseconds before this HA Net-Net SBC should start media flow or MGCP signaling state checkpointing. This timer begins immediately upon entering the Active state. After the timer expires, the HA Net-Net SBC checks to see if it is still active. If this Net-Net SBC is no longer active and becomes standby, it needs to checkpoint with its HA Net-Net SBC peer, now the active Net-Net SBC peer.

Default	5000
Values	Min: 0 / Max: 999999999

Notes This parameter is not RTC supported.

red-sync-comp-time—Enter the time in milliseconds that this standby Net-Net SBC waits before checkpointing again with the active Net-Net SBC to obtain the latest media flow and/or MGCP signaling transaction information once the initial checkpointing process is complete

Default	1000
Values	Min: 0 / Max: 999999999

Notes This parameter is not RTC supported.

media-policing—Enable or disable the media policing feature

Default	enabled
Values	enabled | disabled

max-signaling-bandwidth—Enter the maximum signaling bandwidth allowed to the host-path in bytes per second

Default	1000000
Values	Min: 71000 / Max: 10000000

app-signaling-bandwidth—Select the percentage of the untrusted bandwidth reserved for specific application messages. Currently the only supported application message is RSIP for MGCP and NCS.

Default	0
Values	Min: 1 / Max: 100

min-media-allocation—Enter the minimum number of entries devoted specifically to media flows

Default	32000
Values	Min: 0 / Max: 62988 for 64K Cam; 251952 for 256K Cam

min-trusted-allocation—Enter the minimum number of entries devoted specifically to trusted flows

Default	1000
Values	Min: 0 / Max: 62988 for 64K Cam; 120000 for 256K Cam

deny-allocation—Enter the number of entries devoted specifically to denied entries

Default	1000
Values	Min: 0 / Max: 62988 for 64K Cam; 251952 for 256K Cam

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

trap-on-demote-to-deny—Enable or disable the Net-Net SBC to send a trap in the event of an endpoint demotion.

Default	disabled
Values	enabled | disabled

syslog-on-demote-to-deny—Enable or disable the Net-Net SBC to send a message to the syslog in the event of an endpoint demotion.

Default	disabled
Values	enabled | disabled

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 username and session name fields anonymous in SDP

Default	disabled
Values	enabled | disabled

arp-msg-bandwidth—Enter the maximum bandwidth that can be used by an ARP message

Default	32000
Values	Min: 2000 / Max: 200000

fragment-msg-bandwidth—Enter the maximum bandwidth that can be used by IP fragment messages

Default	0
Values	Min: 0 (fragment packets are treated as untrusted bandwidth); 2000 / 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.

Default	100
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

media-supervision-traps—The Net-Net SBC will send the following trap when the media supervision timer has expired:

```
apSysMgmtMediaSupervisionTimerExpTrap NOTIFICATION-TYPE
OBJECTS { apSysMgmtCallId }
STATUS current
```

Default	disabled
Values	enabled | disabled

active-arp—When enabled, this option causes all ARP entries to get refreshed every 20 minutes.

> *Note: As a security measure, in order to mitigate the effect of the ARP table reaching its capacity, configuring active-arp is advised.*

Default	disabled
Values	enabled | disabled

dnsalg-server-failover—Enable or disable allowing 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; uses the transaction timeout value set in the **dns-server-attributes** configuration (part of the **dns-config**).

Default	disabled
Values	enabled | disabled

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: 1.0 / Most recent update: 5.1

RTC Status

state, latching, flow-time-limit, initial-guard-timer, and subsq-guard-timer are supported. The remaining parameters are not supported.

Notes

This is a single instance configuration element.

Option

unique-sdp-id—Enables or disables codec negotiation by updating the SDP session ID and version number. When enabled, the Net-Net SBC will hash the session ID and IP address of the incoming SDP with the current date/time of the Net-Net SBC in order to generate a unique session ID.

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 | select | no | show | done |
exit>
```

Parameters

name—Name of this media policy

tos-settings—Enter into the tos-values subelement

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: 1.2.1

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-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-attribute—Enter a list of one or more media attributes that will match in the SDP

Default	None

tos-values—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: 1.2.1

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

Syntax

```
media-profile <name | 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 | police-rate | subname | select | no |
show | done | exit>
```

Parameters

name—Enter the encoding name used in the SDP rtpmap attribute. This is a required field. No two media-profile elements can have the same name field value.

media-type—Select the type of media used in SDP m lines

Values

- audio
- video
- application
- data
- image
- text

payload-type—Enter 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: 0 / Max: 2^{32}-1

frames-per-packet—Enter the number of frames per RTP packet. This field is used to specify a media profile to facilitate Slow Start translations to Fast Start. 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

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

Default	0
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

Default	0
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

police-rate—Enter the rate at which the Net-Net SBC polices media for external bandwidth

Default	0
Values	Min: 0 / Max: 999999999

subname—Enter a subname to create multiple media profiles with the same codec name; using a bandwidth value is convenient. For example, you might set a subname of 64k for a **media-profile** with a **name** value of **PCMU**.

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: 1.0 / Most recent update: 4.0

RTC Status Supported

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.

mgcp-config

The **mgcp-config** element provides ALG functionality for MGCP messages between media gateways and media gateway controllers.

Syntax

```
mgcp-config <private-realm | private-address | private-port |
public-realm | public-ca-host | public-ca-address | public-ca-
port | public-gw-host | public-gw-address | public-gw-port |
second-public-gw-port | alg-port | mode | divisor | unit-prefix |
audit-interval | nat-traversal | dns-authentication | dns-
translation | ca-redundancy | ca-ping-method | ca-ping-interval |
rsip-failures | ca-failover-ip-addresses | options | port-map-
start | port-map-end | select | no | show | done | exit>
```

Parameters

private-realm—Enter the private realm (location of the media gateways). This is a required field. This private-realm field value must correspond to a valid identifier field entry in a realm-config.

private-address—Enter the IP address on the media interface in the private realm that the media gateways use as their call agent or softswitch IP address. This is a required field.

private-port—Enter the port of IP address on the media interface in the private realm that call agent or softswitch use

Default	2727
Values	Min: 1025 / Max: 65535

public-realm—Enter the public realm of the call agent or softswitch. This is a required field. This public-realm field value corresponds to a valid identifier field entry in a realm-config that has already been configured.

public-ca-host—Enter the hostname for the public CA

public-ca-address—Enter the public IP address of call agent or softswitch. This is a required field. Entries in this field must follow the IP Address format.

public-ca-port—Enter the public UDP Port of call agent or softswitch

Default	2727
Values	Min: 1025 / Max: 65535

public-gw-host—Enter the FQDN to use in the endpoint MGCP messages on the public side of the Net-Net SBC. If this field is left empty, the host part of the endpoint name will be the public gateway IP address (i.e., the public-gw-address field value).

public-gw-address—Enter the IP address on the media interface in the public realm. This field value is the media gateway address that the Net-Net SBC uses to communicate with the call agent or softswitch. This is a required parameter. If this parameter is entered with a subnet mask in slash notation, 1:1 gateway mapping is enabled.

Default	0.0.0.0

public-gw-port—Enter the port on media interface in the public realm. This field value is the media gateway port that the Net-Net SBC uses to communicate with the call agent or softswitch.

Default	2427
Values	Min: 1025 / Max; 65535

second-public-gw-port—Enter the second UDP port on public-gw-address where Net-Net SBC receives packets from the call agent or softswitch. Net-Net SBC can receive messages from the call agent or softswitch on either the public-gw-port or the second-public-gw-port.

Default	0
Values	Min: 1025 / Max: 65535

alg-port—Enter the port used to send a packet from the network processor to the host processor. Each mgcp-config must have a unique ALG port so the ALG function can distinguish which mgcp-config element applies to packets sent up from the network processor.

Default	2427
Values	Min: 1025 /Max; 65535

mode—Set the MGCP-NAT mode. This field defines how endpoint names are translated as MGCP flows traverse the Net-Net SBC. This is a required field.

Default	LineUnit
Values	• Host—A “unit” term is added to endpoint name on public side to uniquely identify the gateway/host on the private side. The left-most part of the private FQDN is used as the unit term (or unit name). • LinePrefix—Divisor field value is used to compute a number to insert into the localname part of the endpoint name. The number to be inserted is the IP address modulo the divisor. This mode inserts this number before the channel number. Example: aaln/1 becomes aaln/1231. The IP address part is replaced by the public-gw-address. • LineUnit—Divisor field value is used to compute a number to insert into localname part of endpoint name. The number inserted is the IP address modulo the divisor. This mode adds the unit-number term defined in the conventions section of

ftp://ftp.rfc-editor.org/in-notes/rfc3435.txt (e.g., aaln/2 becomes aaln/123/2). The IP address part is replaced by the public-gw-address (also defined in this element).
- FQDN—Dots are removed from the host portion of the private endpoint. Example: the address aaln/2@abc.xyz.com on the private (i.e., gateway) side would become aaln/abcxyzcom/2@sd.com on the public (i.e., call agent) side.
- FQDN2—Dots are retained in the host portion of the private endpoint. Example: the address aaln/2@abc.xyz.com on the private (i.e., gateway) side would become aaln/abc.xyz.com/2@sd.com on the public (i.e., call agent) side.
- OnlyHost—Endpoint name is not translated.
- None—Endpoint name is not translated.

divisor—Enter the unit for computing name of an endpoint. This field is used to determine the number for the LinePrefix or LineUnit. The remainder of the private IP address divided by this number becomes the prefix/unit number. If FQDNs are used for network addressing, the divisor field is not used.

Default	256
Values	256 | 65535 | 16777216 | 4294967296

unit-prefix—Enter the prefix for the unit term of the endpoint name. For modes that add a unit term to the user part of the endpoint name, this field value is placed in front of the unit number or name when creating a public endpoint name.

audit-interval—Enter the number of seconds between AUEP commands that the Net-Net SBC sends to the endpoint (gateway/IAD). No AUEPs are sent by default.

Default	0
Values	Min: 0 / Max: 999999999

nat-traversal—Enable or disable whether or not MGCP ALG assumes that all (gateway) endpoints are behind a NAT

Default	disabled
Values	enabled | disabled

dns-authentication—Enable or disable MGCP DNS authentication functionality on the Net-Net SBC

Default	disabled
Values	enabled | disabled

dns-translation—Enter the translation rule to use, i.e., what characters in the address will be added, replaced, or deleted. If you enable the MGCP DNS authentication feature, then this field is required. The value of this field must be a configured session translation.

ca-redundancy—Enable or disable the call agent redundancy feature

Default	disabled
Values	enabled | disabled

ca-ping-method—Enter the ping method used for call agent redundancy. This parameter is the prototype of a ping method sent to a call agent to determine its state.

ca-ping-interval—Enter the amount of time in seconds between pings sent to the call agent to check for health

Default	0
Values	Min: 0 / Max: 999999999

rsip-failures—Enter the range of 5xx return codes that trigger MGCP endpoint removal or that will fail to create an MGCP session. To empty the default, enter a <Space> enclosed in quotation marks.

Default	500-509,511-519,522-599
Values	5xx return codes per RFC 3435

ca-failover-ip-addresses—Enter the IP addresses for call agent redundancy support. You must enter the list of IP addresses enclosed in parentheses and separate each IP address with a <Space>. You can enter one or more entries.

options—Enter the MGCP options. Used to place 911 calls for MGCP by use of the Via parameter. This parameter is set by entering `#options x-via= <endpoint | both>` in the ACLI

Values	• endpoint—Endpoint is either a router or a phone • both—There are two addresses, the phone number of the endpoint and the IP address of the Net-Net SBC

Also used to communicate with send-only devices by typing **`#options drain-sendonly`**

port-map-start—Enter the port number marking the beginning of the range of ports you want to use for MGCP port mapping.

Default	0 (disabled)
Values	Min: 0; 1025/ Max: 65535

port-map-end—Enter the port number marking the end of the range of ports you want to use for MGCP port mapping. When MGCP port mapping is enabled, this value must be greater than the **port-map-start** value.

Default	0 (disabled)
Values	Min: 0; 1025 / Max: 65535

Path **mgcp-config** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > mgcp-config**.

Release First appearance: 1.0 / Most recent update: 4.1

RTC Status Supported

Notes The combination of entries in the private-realm field and the private-address field must be unique. No two mgcp-config elements can have the same entries in the private-realm field and the private-address entries.
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 | type | value | treatment |
next-hop | realm-next-hop | protocol-next-hop | status-code |
cause-code | gap-rate-max-count | gap-rate-window-size |
destination-identifier | add-destination-identifier | remove-
destination-identifier | rph-feature | rph-profile | rph-policy |
select | no | show | done>
```

Parameters

name—Enter the name of this network management control rule

state—Select the state of this network management control rule

Default	enabled
Values	enabled | disabled

type—Enter the control type that you want to use

Values	GAP-RATE | GAP-PERCENT | PRIORITY

value—Enter the control value of the net 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`

Values	REJECT | DIVERT

next-hop—Enter the next hop for the Net-Net SBC to use when the treatment method is `DIVERT`. This value should contain one of the following:

- hostname(:port) or IPv4 address or IPv6 address of a configured session agent
- IPv4 address (:port) or IPv6 address (:port) of a specific endpoint

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-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: 999999999

gap-rate-max-count—Enter the maximum token counter value for gapping rate

Default	0
Values	Min: 0 / Max: 999999999

gap-rate-window-size—Enter the window size (in seconds) for gapping rate calculation

Default	0
Values	Min: 0 / Max: 999999999

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.

add-destination-identifier—Add a destination identifier

remove-destination-identifier—Remove a destination identifier

rph-feature—Set the state of NSEP support for this NMC rule

Default	disabled
Values	enabled | disabled

rph-profile—Enter the name of the RPH profile to apply to this NMC rule

Default	None
Values	Name of an rph-profile

rph-policy—Enter the name of the RPH policy to apply to this NMC rule

Default	None
Values	Name of an rph-policy

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: 4.1.1

RTC Status

Supported

network-interface

The **network-interface** element creates and configures a logical network interface.

Syntax

```
network-interface <name | sub-port-id | description | hostname |
ip-address | pri-utility-addr | sec-utility-addr | netmask |
gateway | sec-gateway | gw-heartbeat | dns-ip-primary | dns-ip-
backup1 | dns-ip-backup2 | dns-domain | dns-timeout | add-hip-ip
| remove-hip-ip | add-ftp-ip | remove-ftp-ip | add-icmp-ip |
remove-icmp-ip | add-snmp-ip | remove-snmp-ip | add-telnet-ip |
remove-telnet-ip | add-ssh-ip | remove-ssh-ip | select | no | show
| done | exit>
```

Parameters

name—Enter the name of the physical interface with which this network-interface element is linked. Network-interface elements that correspond to phy-interface elements with an operation type of Control or Maintenance must start with “wancom.”

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: 4095

description—Enter a brief description of this network interface

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.

pri-utility-addr—Enter the utility IP address for the primary HA peer in an HA architecture

sec-utility-addr—Enter the utility IP address for the secondary Net-Net SBC peer in an HA architecture

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 are forwarded if this value is 0.0.0.0.

sec-gateway—Enter the gateway to use on the secondary Net-Net SBC in an HA pair. Entries in this field must follow the IP address format.

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—Set 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 total time in seconds you want to elapse before a query (and its retransmissions) sent to a DNS server timeout

Default	11
Values	Min: 1/ Max: 999999999

add-hip-ip—Enter a list of IP addresses allowed to access signaling and maintenance protocol stacks via this front interface using the HIP feature

remove-hip-ip—Remove an IP address added using the add-hip-ip parameter

add-ftp-ip—Enter a list of IP addresses from which FTP traffic can be received and acted upon by a front media interface

remove-ftp-ip—Remove an IP address added using the add-ftp-ip parameter

add-icmp-ip—Enter a list of IP addresses from which ICMP traffic can be received and acted upon by a front media interface

remove-icmp-ip—Remove an IP address added using the add-icmp-ip parameter

add-snmp-ip—Enter a list of IP addresses from which SNMP traffic can be received and acted upon by a front media interface

remove-snmp-ip—Remove an IP address added using the add-snmp-ip parameter

add-telnet-ip—Enter a list of IP addresses from which telnet traffic can be received and acted upon by a front media interface

remove-telnet-ip—Remove an IP address added using the add-telnet-ip field

add-ssh-ip—Enter a list of IP addresses from which SSH traffic can be received and acted upon by a front media interface.

Default	None
Values	A valid IPv4 network address

Notes The gateway address of this interface must be the default gateway address

remove-ssh-ip—Remove an IP address added using the **add-ssh-ip** parameter.

Default	None
Values	A valid IPv4 network address

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: 1.0 / Most recent update: 4.1.

RTC Status Supported

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: 1 / 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: 1.2.1

RTC Status

Supported

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-keepalive-timer |
tcp-keepalive-mode | tcp-keepinit-timer | tcp-keepalive-interval-
timer | sctp-send-mode | options | show | done | exit>
```

Parameters

tcp-keepalive-count—Enter the number of outstanding keepalives before connection is torn down

Default	8
Values	Min: 0 / Max: $2^{32-}1$

tcp-keepalive-idle-timer—Enter the idle time in seconds before triggering keepalive processing. If you have upgraded the release you are running and a value outside of the acceptable range was configured in an earlier release, the default value is used and a log message is generated.

Default	7200
Values	Min: 30 / Max: 7200

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

tcp-keepinit-timer—Enter the TCP connection timeout period if a TCP connection cannot be established. If you have upgraded the release you are running and a value outside of the acceptable range was configured in an earlier release, the default value is used and a log message is generated.

Default	75
Values	0-999999999

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

sctp-send-mode—Leave this parameter set to its default (unordered) so data delivery can occur without regard to stream sequence numbering. If data delivery must follow stream sequence number, change this parameter to **ordered**.

Default	unordered
Values	ordered | unordered

options—Enter any optional features or parameters

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: 2.0; Last updated: S-C6.1.0

RTC Status Supported with exceptions. SCTP parameter changes require reboot.

Notes This is a single instance configuration subelement.

ntp-sync

The **ntp-sync** element sets the ntp server IP address for correct and accurate time synchronization.

Syntax

```
ntp-sync <add-server | del-server | select | no | show | done |
exit>
```

Parameters **add-server**—Add IP address of NTP server; entries must follow the IP Address Format

del-server—Remove a previously entered NTP server. Entries must follow the IP Address Format.

Path **ntp-sync** is a top-level element. The full path from the topmost ACLI prompt is: **configure terminal > ntp-sync**.

Release First appearance: 1.0 / Most recent update: 1.1

RTC Status Supported

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.

qos-constraints

The **qos-constraints** configuration element allows you to enable QoS based routing, which uses the R-Factor on a per-realm basis to cut back on the traffic allowed by a specific realm. Net-Net SBC QoS reporting is a measurement tool that collects statistics on Voice over IP (VoIP) call flows for SIP and H.323. To provide information, the Net-Net SBC writes additional parameters to the Remote Authentication Dial-in User Service (RADIUS) call record and Historical Data Recording (HDR) records.

Syntax

```
qos-constraints <name | state | major-factor | critical-factor |
call-load-reduction | select | no | show | done | exit>
```

Parameters

name—Enter the name of a QoS constraints configuration

state—Enable or disable a set of QoS constraints

Default	enabled
Values	enabled | disabled

major-factor—Enter a numeric value set the threshold that determines when the Net-Net SBC applies the call reduction rate; must be less than the **critical-rfactor**

Default	0
Values	Min: 0 / Max: 9321

critical-rfactor—Enter a numeric value to set the threshold that determines when the Net-Net SBC rejects all inbound calls for the realm, and rejects outbound calls when there is no alternate route

Default	0
Values	Min: 0 / Max: 9321

call-load-reduction—Enter the percentage by which the Net-Net SBC will reduce calls to the realm if the **major-rfactor** is exceeded; a value of 0 means the call load will not be reduced

Default	0
Values	Min: 0 / Max: 100

Path

qos-constraints is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router> qos-constraints**.

Release

First appearance: S-C6.1.0

RTC Status

Supported

password-policy

The **password-policy** element configures password rules for password secure mode.

Syntax

```
password-policy <min-secure-pwd-len | select | no | show | done |
exit>
```

Parameters

min-secure-pwd-len—Enter the minimum password length to use when system is in secure password mode. The maximum allowable length for any password is 64 characters.

Default	9
Values	9-64

Path

password-policy is an element under the security path. The full path from the topmost ACLI prompt is: **configure terminal> security> password-policy**.

Release

First appearance: 5.1

RTC Status

Supported

Notes

The password using this minimum length value must contain three out of four of these requirements: upper case letters, lower case letters, numbers, punctuation marks. No special characters are allowed, for example: #, &, @, *, etc.

> ***Note: The password must be 6-9 characters with at least one non-alphanumeric character.***

phy-interface

The **phy-interface** element is used to configure physical interfaces.

Syntax

```
phy-interface <name | operation-type | port | slot | virtual-mac |
admin-state | auto-negotiation | duplex-mode | speed | wancom-
health-score | overload-protection | network-alarm-threshold |
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. Name values for the phy-interface must be unique.

operation-type—Select the type of physical interface connection

Default	Control
Values	• Media—Front-panel interfaces only. Port: 0-3 Slot: 0 or 1 • Control—Rear-panel interfaces only. Port 0, 1, or 2 Slot: 0 • Maintenance—Rear-panel interfaces only. Port 0, 1, or 2 Slot: 0

port—Select the physical port number on an interface of the phy-interface being configured

Default	0
Values	• 0-2 for rear-panel interfaces

• 0-1 for two possible GigE ports on front of Net-Net SBC chassis
• 0-3 for four possible FastE ports on front of Net-Net SBC chassis

slot—Select the physical slot number on the Net-Net SBC chassis

Default 0

Values • 0 is the motherboard (rear-panel interface) if the name begins with "wancom"
• 0 is the left Phy media slot on front of Net-Net SBC chassis
• 1 is the right Phy media slot on front of Net-Net SBC chassis

virtual-mac—Enter the MAC address identifying a front-panel interface when the Net-Net SBC is in the Active state. This field value should be generated from the unused MAC addresses assigned to a Net-Net SBC. The virtual-mac field is only applicable for front interfaces.

admin-state—Enable or disable the Net-Net SBC to allow incoming and outgoing traffic to be processed using the front physical interface cards

Default enabled

Values enabled | disabled

auto-negotiation—Enable or disable auto negotiation on front Phy card interfaces taking place before either end begins sending packets over the Ethernet link. The auto-negotiation field is only applicable for front interfaces. The value configured in this field does not change the Net-Net SBC status at runtime.

Default enabled

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

Default full

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

Default 100

Values 10 | 100

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

network-alarm-threshold—Access the **network-alarm-threshold** subelement.

overload-protection—Enable this parameter to turn graceful call control on. Disable (default) if you do not want to use this feature.

Default disabled

Values enabled | disabled

Notes This parameter is not RTC supported

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: 1.0 / Most recent update: S-C6.2.0

RTC Status Supported

Notes Certain fields are visible based on the setting of the operation-type parameter. This is a multiple instance configuration subelement.

phy-interface>network-alarm-threshold

The network-alarm-threshold subelement enables the Net-Net SBC to monitor network utilization of its media interfaces and send alarms when configured thresholds are exceeded.

Syntax

```
network-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 threshold percentage of network utilization that triggers an SNMP trap and alarm for each **severity** value.

Default 0

Values Min: 0 | Max: 100

Path **network-alarm-threshold** is a subelement under the **system** path. The full path from the topmost ACLI prompt is: **configure terminal > system > phy-interface**.

Release First appearance: S-C6.2.0

RTC Status Supported

public-key

The **public-key** configuration element is used to generate an SSH public key to authenticate SSH sessions.

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: S-C6.2.0

RTC Status Supported

Notes This is a multiple instance configuration element.

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 | delete | edit | select | no | show | done
| exit>
```

Parameters **entries**—Enter the entries configuration subelement

delete—Delete a q850 to SIP mapping. Enter the q850 code.

edit—Edit a response map by number

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: 4.0

RTC Status Supported

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>
```

Parameters **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: 699

sip-reason—Describe the mapped SIP response code

Path

entries is a subelement under the **q850-sip-map** configuration element, which is located 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: 4.0

RTC Status

Supported

realm-config

The **realm-config** element is used to configure realms.

Syntax

```
realm-config <identifier | description | addr-prefix | network-
interfaces | mm-in-realm | mm-in-network | msm-release | qos-
enable | max-bandwidth | ext-policy-svr | max-latency | max-
jitter | max-packet-loss | observ-window-size | parent-realm |
dns-realm | media-policy | class-profile | in-translationid |
out-translationid | in-manipulationid | out-manipulationid |
early-media-allow | additional-prefixes | add-additional-prefixes
| remove-additional-prefixes | accounting-enable | mm-same-ip |
mm-in-system | untrusted-signal-threshold | restricted-latching |
restriction-mask | average-rate-limit | access-control-trust-
level | invalid-signal-threshold | maximum-signal-threshold |
deny-period | cac-failure-threshold | untrust-cac-failure-
threshold | symmetric-latching | pai-strip | trunk-context | bw-
cac-non-mm | user-cac-mode | user-cac-bandwidth | user-cac-
sessions | monthly-minutes | net-management-control | delay-
media-update | refer-call-transfer | dyn-refer-term | codec-
policy | codec-manip-in-realm | generate-udp-checksum |
enforcement-profile | options | constraint-name | manipulation-
string | manipulation-pattern | stun-enable | stun-server-ip |
stun-server-port | stun-changed-ip | stun-changed-port | call-
recording-server-id | icmp-detect-multiplier | icmp-
advertisement-interval | icmp-target-ip | fallback-bandwidth |
max-priority-bandwidth | nat-trust-treshold | sip-profile | sip-
isup-profile | match-media-profiles | qos-constraints | select |
no | show | done | exit>
```

Parameters

identifier—Enter the name of the realm associated with this Net-Net SBC. This is a required field. The identifier field value must be unique.

description—Provide a brief description of the **realm-config** configuration element

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.

Default 0.0.0.0

network-interface—Enter the network interface through which this realm can be reached. Entries in this parameter take the form: `<network-interface-ID>:<subport>`.

Note: Only one network interface can be assigned to a single realm-config object.

mm-in-realm—Enable or disable media being steered 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 being steered 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

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 Net-Net SBCs. If this field is set to enabled, the media is directed directly between the endpoints of a call.

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: 2^{32}-1

ext-policy-svr—Enter the name of the external policy server configuration used for this realm

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. Reserved for future use.

Default	0

Values	Min: 0 / Max: 2^{32}-1

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. Reserved for future use.

Default	0
Values	Min: 0 / Max: 2^{32}-1

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. Reserved for future use.

Default	0
Values	Min: 0 / Max: 2^{32}-1

observ-window-size—Enter the minimum time in milliseconds a threshold (latency, jitter, and packet loss) must be exceeded before triggering an alarm. Reserved for future use.

Default	0
Values	Min: 0 / Max: 2^{32}-1

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 or H.323 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.

in-manipulationid—Enter the inbound SIP manipulation rule name

out-manipulationid—Enter the outbound SIP manipulation rule name

early-media-allow—Select the early media suppression for the realm

Values
- none: No early media is allowed in either direction
- both: Early media is allowed in both directions
- reverse: Early media received by Net-Net SBC in the reverse direction is allowed

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.

add-additional-prefixes—Add 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.

remove-additional-prefixes—Remove 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.

accounting-enable—Select whether you want accounting enabled within the realm

Default enabled

Values enabled | disabled

mm-same-ip—Enable the media to go through this Net-Net SBC if the mm-in-realm . When not enabled, the media will not go through the Net-Net SBC for endpoints that are behind the same IP.

Default enabled

Values enabled | disabled

mm-in-system—Set this parameter to enabled to manage/latch/steer media in the Net-Net SBC. Set this parameter to disabled to release media in the Net-Net SBC.

> *Note: Setting this parameter to disabled will cause the Net-Net SBC to NOT steer media through the system (no media flowing through this Net-Net SBC).*

Default enabled

Values enabled | disabled

untrusted-signal-threshold—Enter the allowed maximum signaling messages within a tolerance window

Default 0

Values Min: 0 / Max: 4294967295

restricted-latching—Set the restricted latching mode

Default None

Values
- none: No restricted latching
- sdp: Use the IP address specified in the SDP for latching purpose
- peer-ip: Use the peer-ip (Layer 3 address) for the latching purpose

restriction-mask—Set the restricted latching mask value

Default	32
Values	Min: 1 / Max: 32

average-rate-limit—Enter the average data rate in bits per second for host path traffic from a trusted source

Default	0 (disabled)
Values	Min: 0 / Max: 4294967295

access-control-trust-level—Select a 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 untrusted list

invalid-signal-threshold—Enter the acceptable invalid signaling message rate falling within a tolerance window

Default	0
Values	Min: 0 / Max: 4294967295

maximum-signal-threshold—Enter the maximum number of signaling messages allowed within the tolerance window

Default	0 (disabled)
Values	Min: 0 / Max: 4294967295

pai-strip—Enable or disable P-Asserted-Identity headers being stripped from SIP messages as they exit the Net-Net SBC. The PAI header stripping function is dependent on this parameter and the trust-me parameter.

Default	disabled
Values	enabled | disabled

deny-period—Enter the length of time an entry is posted in the deny list

Default	30
Values	Min: 0 / Max: 4294967295

cac-failure-threshold—Enter the number of CAC failures for any single endpoint that will demote it from the trusted queue to the untrusted queue for this realm.

Default	0
Values	Min: 0 / Max: 2^{32} -1

untrust-cac-failure-threshold—Enter the number of CAC failures for any single endpoint that will demote it from the untrusted queue to the denied queue for this realm.

Default	0

Min: 0 / Max: 2^{32} -1**symmetric-latching—**Enable or disable symmetric latching between endpoints for RTP traffic

Default	disabled
Values	enabled | disabled

trunk-context—Enter the default trunk context for this realm

bw-cac-non-mm—Set this parameter to `enabled` to turn on bandwidth CAC for media release

Default	disabled
Values	enabled | disabled

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 in this realm • AOR—User CAC per AOR • IP—User CAC per IP

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

monthly-minutes—Enter the monthly minutes allowed

Default	0
Values	Min: 0 / Max: 71582788

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

Default	disabled
Values	enabled | disabled

refer-call-transfer—Enable or disable the refer call transfer feature for this realm

Default	disabled
Values	enabled | disabled

dyn-refer-term—Enable or disable the Net-Net SBC to terminate a SIP REFER and issue a new INVITE. If the **dyn-refer-term** value is **disabled** (the default), proxy the REFER to the next hop to complete REFER processing. If the **dyn-refer-term** value is **enabled**, terminate the REFER and issue an new INVITE to the referred party to complete REFER processing.

Default	disabled
Values	enabled | disabled

codec-policy—Select the codec policy you want to use for this realm

codec-manip-in-realm—Enable or disable codec policy in this realm

Default	disabled
Values	enabled | disabled

generate-udp-checksum—Enable or disable the realm to generate a UDP checksum for RTP/RTCP packets.

Default	disabled
Values	enabled | disabled

enforcement-profile—Enter the name of the enforcement profile (SIP allowed methods).

options—Enter any optional features or parameters

constraint-name—Enter the name of the constraint you want to use for this realm

manipulation-pattern—Enter the regular expression to be used in header manipulation rules for this realm.

manipulation-string—Enter a string to be used in header manipulation rules for this realm.

call-recording-server-id—Enter the name of the call recording server associated with this realm

icmp-detect-multiplier—Enter the multiplier to use when determining how long to send ICMP pings before considering a target unreachable. This number multiplied by the time set for the **icmp-advertisement-interval** determines the length of time

Default	0
Values	Min: 0

icmp-advertisement-interval—Enter the time in seconds between ICMP pings the Net-Net SBC sends to the target.

Default	0
Values	Min: 0

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.

Default	(empty)

fallback-bandwidth—Enter the amount of bandwidth available once the Net-Net SBC has determined that the target (of ICMP pings) is unreachable.

Default	0
Values	Min: 0

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: 999999999

nat-trust-threshold—Enter maximum number of untrusted endpoints allowed before an entire NAT device is demoted to untrusted. 0 means dynamic demotion of NAT devices is disabled.

Default	0
Values	Min: 0 / Max: 999999999

sip-profile—Enter the name of the **sip-profile** to apply to this realm.

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 in the form <name>::<subname>. See the *Net-Net 4000 ACLI Configuration Guide* for information about wildcard values.

qos-constraints—Enter the name value from the QoS constraints configuration you want to apply to this realm

stun-enable—Enable or disable the STUN server support for this realm

Default	disabled
Values	enabled | disabled

stun-server-ip—Enter the IP address for the primary STUN server port

Default	0.0.0.0

stun-server-port—Enter the port to use with 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; must be different from than the one defined for the **stun-server-ip**

Default	0.0.0.0

stun-changed-port—Enter the port combination to define the CHANGED-ADDRESS attribute in Binding Requests received on the primary STUN server port

Default	3479
Values	Min. 1025/Max. 65535

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: 1.0 / Most recent update: S-C6.1.0

RTC Status Supported

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>
```

name—Enter the name of this 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. To enter more than one realm in this list, list all items separated by a comma and enclose the entire entry in quotation marks.

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. 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 • both—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 of the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > realm-group**.

Release First appearance: 4.1.4

RTC Status Supported

redundancy

The **redundancy** element establishes HA parameters for a Net-Net SBC that participates in an HA architecture.

Syntax

```
redundancy <state | log-level | health-threshold | emergency-
threshold | port | advertisement-time | percent-drift | initial-
time | becoming-standby-time | becoming-active-time | cfg-port |
cfg-max-trans | cfg-sync-start-time | cfg-sync-comp-time |
gateway-heartbeat-interval | gateway-heartbeat-retry | gateway-
heartbeat-timeout | gateway-heartbeat-health | media-if-
peercheck-time | peers | select | no | show | done | exit>
```

Parameters

state—Enable or disable HA for the Net-Net SBC

Default	enabled
Values	enabled | disabled

Notes

This parameter is not RTC supported.

log-level—Select the starting log level for the HA process. This value supersedes the value configured in the process-log-level field in the system-config element for the HA process.

Default	info
Values	• emergency • critical • major • minor • warning • notice • info • trace • debug • detail

health-threshold—Enter the health score at which standby Net-Net SBC switches over to the Active state and takes control of all system functionality as the active Net-Net SBC

Default	75
Values	Min: 1 / Max: 100

emergency-threshold—Enter the low health score value that triggers the initializing standby Net-Net SBC to become the active Net-Net SBC immediately. In addition, the active but unhealthy Net-Net SBC, regardless of its health, will not relinquish its Active state if the HA Net-Net SBC peer poised to become active upon switchover also has a health score below this emergency-threshold value.

Default	50
Values	Min: 1 / Max: 100

port—Enter the port number on which the border element redundancy protocol is listening

Default	9090
Values	Min: 1025 / Max: 65535

Notes

This parameter is not RTC supported.

advertisement-time—Enter the time in milliseconds the Net-Net SBC continually sends its health score to its HA Net-Net SBC peer(s)

Default	500
Values	Min: 50 / Max: 999999999

percent-drift—Set the percentage of an HA Net-Net SBC peer's advertisement time for this HA Net-Net SBC to wait before considering its peer to be out of service

Default	210
Values	Min: 100 Max: 65535

initial-time—Enter the number of milliseconds to set the longest amount of time the Net-Net SBC will wait at boot time to change its state from initial to either becoming active or becoming standby. This field is independent of the advertisement-time and percent-drift parameters; it is a timer used to decide the state transition.

Default	1250
Values	Min: 5 / Max: 999999999

becoming-standby-time—Enter the time in milliseconds to wait before transitioning to the Standby state. This field allows the HA Net-Net SBC enough time to synchronize with its HA Net-Net SBC peer. If the HA Net-Net SBC has not become fully synchronized within the time frame established in this field, it will be declared out of service. We recommend setting this parameter to no less than 180000 if configuration checkpointing is used.

Default	45000
Values	Min: 5 / Max: 999999999

becoming-active-time—Enter the time in milliseconds a previously standby Net-Net SBC takes to become active. This field applies to the following scenarios:

- When the health of an active Net-Net SBC has failed
- When the standby Net-Net SBC is healthier than the active Net-Net SBC

This is a transitional state.

Default	100
Values	Min: 5 / Max: 999999999

cfg-port—Enter the port number from which HA checkpoint messages are sent and received. This field supports Configuration Checkpointing. Setting the cfg-port field value to 0 disables configuration checkpointing.

Default	1987

Values Min: 1025 / Max: 65535; 0

Notes This parameter is not RTC supported.

cfg-max-trans—Enter the size of the HA checkpoint transaction list to store in memory at a time

Default 10000

Values Min: 0 / Max: 2^{32}-1

Notes This parameter is not RTC supported.

cfg-sync-start-time—Enter the time in milliseconds before HA Net-Net SBC begins sending HA configuration checkpointing requests. This timer begins immediately upon entering the Active state. As long as the active peer is healthy and active, it remains in a constant cycle of (re)setting this parameter's timer and checking to see if it has become standby.

Default 5000

Values Min: 0 / Max: 2^{32}-1

Notes This parameter is not RTC supported.

cfg-sync-comp-time—Enter the time in milliseconds the standby Net-Net SBC waits before checkpointing with the active Net-Net SBC to obtain the latest configuration transaction information once the initial checkpointing process is complete.

Default 1000

Values Min: 0 / Max: 2^{32}-1

Notes This parameter is not RTC supported.

gateway-heartbeat-interval—Enter the time in seconds between heartbeats on the front interface gateway. This parameter is applicable until a front interface gateway failure occurs. This parameter applies globally to Net-Net SBCs operating in an HA node, but can be overridden on a network interface-by-network interface basis by the value configured in the gw-heartbeat: heartbeat field of the gw-heartbeat subelement in the network-interface element.

Default 0

Values Min: 0 / Max: 65535

Notes This parameter is not RTC supported.

gateway-heartbeat-retry—Enter the number of front interface gateway heartbeat retries after a front interface gateway failure occurs. The value configured in this field applies globally to Net-Net SBCs operating in HA pair architectures, but can be overridden on a per network interface basis by the value configured in the gw-heartbeat: retry-count field.

Default 0

Values Min: 0 / Max: 65535

Notes This parameter is not RTC supported.

gateway-heartbeat-timeout—Enter the heartbeat retry timeout value in seconds between subsequent ARP requests to establish front interface gateway communication after a front interface gateway failure occurs. The value configured in this field applies globally to Net-Net SBCs operating in HA pair architectures, but can be overridden on a network interface basis by the value configured in the gw-heartbeat: retry-timeout field.

Default 1

Values Min: 0 / Max: 65535

Notes This parameter is not RTC supported.

gateway-heartbeat-health—Enter the health score amount to subtract if the timeout value set in the gateway-heartbeat-timeout field has been exceeded without receiving a response from the front interface gateway. The value configured in this field applies globally to Net-Net SBCs operating in HA nodes, but can be overridden on a network interface basis by the value configured in the gw-heartbeat > health-score field of the gw-heartbeat. A field value of 0 means that the health score is not affected.

Default 0

Values Min: 0 / Max: 100

Notes This parameter is not RTC supported.

media-if-peercheck-time—Enter the amount of time in milliseconds for the standby system in an HA node to receive responses to its ARP requests via the front interface before it takes over the active role from its counterpart. A value of 0 turns the HA front interface keepalive off.

Default 0

Values Min: 0 / Max: 500

peers—Access the **peers** subelement

Path **redundancy** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > redundancy.**

Release First appearance: 1.1 / Most recent update: 1.2.1

RTC Status This element has both supported and unsupported parameters. Unsupported parameters are marked with a note.

Notes This is a single instance configuration element.

redundancy > peers

The **peers** subelement establishes the name and state of an HA node.

Syntax

```
peers <name | state | type | destinations | select | no | show |
done | exit>
```

Parameters **name**—Enter the hostname of the HA Net-Net SBC peer. The name configured in this field identifies each Net-Net SBC in an HA node uniquely.

state—Enable or disable HA

Default enabled

Values enabled | disabled

type—Select the HA peer type and which utility address to use

Default unknown

Values

- primary—HA peer set as the primary Net-Net SBC. It is associated with the utility address configured in the pri-utility-addr field of each network-interface element.
- secondary—HA peer set as the secondary Net-Net SBC. It is associated with the utility address configured in the sec-utility-addr field of each network-interface element.
- unknown—Not assigned HA peer type with associated utility address unknown. This type field option is not valid for configuration checkpointing. Although unknown is the default value, Primary or Secondary field option must be set in order for configuration checkpointing to function properly.

destinations—Access the destinations subelement

Path **peers** is a subelement under the redundancy element. The full path from the topmost ACLI prompt is: **configure terminal > system > redundancy > peers.**

Release First appearance: 1.0.1 / Most recent update: 1.2.1

RTC Status Unsupported

Notes This is a multiple instance configuration subelement.

redundancy > peers > destinations

The **destinations** subelement establishes locations where health and state information is sent and received.

Syntax

```
destinations <address | network-interface | select | no | show |
done | exit>
```

Parameters

address—Enter the IP address and port on the interface of the HA Net-Net SBC peer where this HA Net-Net SBC peer sends HA messages. The parameter format is an IP address and port combination (IP address:port). This IP address must match the interface identified in its HA Net-Net SBC peer's corresponding rdncy-peer-dest > network-interface field. The port portion of this parameter must match the port identified in its HA Net-Net SBC peer's corresponding port field.

network-interface—Enter the name and subport ID of the interface where the HA Net-Net SBC receives HA messages (e.g., wancom1:0). Valid interface names are wancom1 and wancom2 only.

Path **destinations** is a subelement under the peers subelement. The full path from the topmost ACLI prompt is: **configure terminal > system > redundancy > peers > destinations.**

Release First appearance: 1.0.1

RTC Status Unsupported

Notes The **destinations** prompt is displayed as: rdncy-peer-dest.
This is a multiple instance configuration element.

rph-policy

The **rph-policy** element defines an override resource value and an insert resource value for ETS/WPS namespaces. These are applied to NMC rules.

Syntax

```
rph-policy <name | override-r-value | insert-r-value | select |
no | show | done | exit>
```

Parameters

name—Enter the name of this RPH policy; this is the value used when applying this RPH policy to an NMC rule.

Default None

override-r-value—Set the value the Net-Net SBC uses to override the r-values in the original RPH.

Default None

insert-r-value—Set the value the Net-Net SBC inserts into the RPH.

Path **rph-policy** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router> rph-policy**.

Release First appearance: 5.1

RTC Status Supported

rph-profile

The **rph-profile** contains information about how the Net-Net SBC should act on the namespace(s) present in Resource-Priority headers.

Syntax

```
rph-profile <name | r-values | media-policy | call-treatment |
select | no | show | done | exit>
```

Parameters

name—Enter the name of this RPH profile; this is the value used when applying this RPH profile to an NMC rule.

Default None

r-value—Enter a list of one or more r-values used for matching; WPS values must be entered before ETS values.

Default None

media-policy—Enter the name of the media-policy to apply; overrides media policies set for realms when there is an ETS call.

Default None

call-treatment—Select the call treatment method for a non-ETS call that contains RPH matching this profile.

Default	accept
Values	accept | reject | priority

Path

rph-profile is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router> rph-profile**.

Release

First appearance: 5.1

RTC Status

Supported

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 | 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.

Default	5060
Values	Min: 0; 1025 / 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

Default	SIP
Values	H323 | SIP

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 H323. 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.
- SCTP—SCTP is used as the transport method.

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.

egress-realm-id—Enter the name of the realm you want defined as the default egress realm used for ping messages. The Net-Net SBC will also use this realm when it cannot determine the egress realm for normal routing.

description—Describe the session-agent element. Entries in this field must follow the Text Format.

carriers—Enter the 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.

allow-next-hop-lp—Enable or disable the 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) that are 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: 2^{32}-1

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: 2^{32}-1

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: 2^{32}-1

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: 2^{32}-1

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: 2^{32}-1

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: 2^{32}-1

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: 2^{32}-1

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: 2^{32}-1

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: 10 / Max: 2^{32}-1

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 carrier determined by the local policy element should be added to the outgoing message

Default	None
Values	• None—Carrier information will not be added to the outgoing message • uri-param—Adds a parameter to the Request-URI (e.g., cic-XXX) • prefix—Adds 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 element is also empty, the default is proxy.

Values	• proxy—If the Net-Net SBC is an 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 a Net-Net SBC, system will behave as a B2BUA when forwarding the request. • redirect—System will send a SIP 3xx reDIRECT response with contacts (found in the local-policy) to the previous hop • record-route—The Net-Net SBC forwards requests with a record-route

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 system uses the redirect action defined in the sip-interface.

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

send-media-session—Enable or disable the inclusion of a media session description in the INVITE sent by the Net-Net SBC. The only instance in which this field should be set to disabled is for a session agent that always redirects requests, meaning that it returns an error or 3xx response instead of forwarding an INVITE message. Setting this field to disabled prevents the Net-Net SBC from establishing flows for that INVITE message until it recurses the 3xx response.

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—Set how often to ping a session agent in seconds

Default	0
Values	Min: 0 / Max: 999999999

ping-send-mode—Set the mode with which you want to send ping messages to session agents

Default	keep-alive
Values	keep-alive | continuous

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	diabled
Values	enabled | disabled

options—Establish customer-specific features and/or parameters. This value can be a comma separated list of “feature=<value>" or "feature" parameters.

media-profiles—Start up an outgoing call as a Fast Start call with the information in the media profile used for the logical channels when the incoming call is slow start for an H.323 operation. This list is used to determine if a source and/or destination of a call is a session agent on that list. If a media profiles list is configured in the matching session-agent element, then the frame and codec information in the corresponding media profile will be used for the outgoing call. If the media-profiles list in the session-agent element is empty, the h323-stack > media-profiles list will be consulted. This field should reference the codec that you expect the gatekeeper/gateway to use. This media-profiles entry must correspond to at least one valid name field entry in a media profile element that has already been configured.

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 privacy features

Default	enabled
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

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.

trunk-group—Enter trunk group names and trunk group contexts to match in either IPTEL or custom format; one session agent can accommodate 500 trunk groups. 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. You can add and delete single entries from the list using plus (+) and minus (-) signs without having to overwrite the whole list.'

Entries for this list must one of the following formats: `tgrp:context` or `tgrp.context`.

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: 4294967295

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%

early-media-allow— Select the early media suppression for the session agent

Values	• none—No early media allowed • reverse—Allow early media in the direction of calling endpoint • both—Allow early media in both directions

invalidate-registrations—Enable or disable the invalidation of all the registrations going to this SA when its state transitions to "out of service"

Default	disabled
Values	enabled | disabled

rfc2833-mode— Select whether 2833/UII negotiation will be transparent to the Net-Net SBC (pre-4.1 behavior), or use 2833 for DTMF

Default	none
Values	• none—The 2833-UII interworking will be decided based on the h323-stack configuration. • 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.

rfc2833-payload—Enter the payload type used by the SA in preferred rfc2833-mode

Default	0
Values	Valid Range: 0, 96-127

> **Note:** When this value is zero, the global "rfc2833-payload" configured in the H323 configuration element will be used instead. For SIP SA, the payload defined in the SIP Interface will be used, if the SIP-I is configured with rfc2833-mode as "preferred".

max-inbound-sessions—Enter the maximum number of inbound sessions allowed from this session agent

Default	0
Values	Min: 0 / Max: 999999999

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-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

codec-policy—Enter the codec policy you want to apply to this session agent

enforcement-profile—Enter the enforcement policy set of allowed SIP methods you want to use for this session agent

Default	None
Values	Name of a valid enforcement-profile element

refer-call-transfer—Enable or disable the refer call transfer feature for this session agent

Default	disabled
Values	enabled | disabled

reuse-connections—Enter the SIP TCP connection reuse mode. The presence of "reuse-connections" in the options field of the sip-interface will cause the Net-Net SBC to reuse all inbound TCP connections for sending rquests to the connected UA.

Default	tcp
Values	tcp | sctp | none

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

tcp-reconn-interval—Set the amount of time in seconds before retrying a TCP connection.

Default	0
Values	0, 2-300

register-burst-window—Enter the window size in seconds for the maximum number of allowable SIP registrations.

Default	0
Values	Min: 0 / Max: 999999999

rate-constraints—Access the **rate-constraints** subelement

max-register-burst-rate—Enter the maximum number of new registrations you want this session agent to accept within the registration burst rate window. When this threshold is exceeded, the Net-Net SBC responds to new registration requests with 503 Service Unavailable messages.

Default	0
Values	Min: 0 / Max: 999999999

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 or any dialog-creating request.

Default	None
Values	SIP Response codes

manipulation-string—Enter a value to references the $HMR_STRING variable used to populate SIP headers and elements using HMR

manipulation-string—Enter a string you want used in the header manipulation rules for this session-agent.

manipulation-pattern—Enter the regular expression to be used in header manipulation rules for this session-agent.

sip-profile—Enter the name of the **sip-profile** you want to add to the **session-agent.**

sip-isup-profile—Enter the name of the **sip-isup-profile** you want to add to the **session-agent.**

Notes	N/A
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: 1.0 / Most recent update: S-C6.2.0
RTC Status	Supported
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 **method** 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 **method** 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 **method** 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 **method** 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

session-agent> rate-constraints is an element of the **session-router path**. The full path from the topmost ALCI prompt is: **configure terminal > session-router > session-agent > rate-constraints**.

Release

First appearance: 5.1.1

RTC Status

Supported

session-agent-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 | state | app-protocol |
strategy | dest | trunk-group | sag-recursion | stop-sag-recurse
| 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 it must be unique.

description—Describe the session agent group element

state—Enable or disable the session-agent-group element

Default	enabled
Values	enabled | disabled

app-protocol—Distinguish H.323 session agent groups from SIP session agent groups

Default	SIP
Values	H323 | SIP

strategy—Select the session agent allocation options for the session-agent-group. Strategies determine how session agents are chosen by this session-agent-group element.

Default Hunt

Values

- Hunt—Selects session agents in the order in which they are listed
- RoundRobin—Selects 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—Selects 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

dest—Enter one or more destinations (i.e., next hops) available for use by this session-agent group. The destination value(s) must correspond to a valid IP address or hostname.

trunk-group—Enter 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. Multiple entries are surrounded in parentheses and separated from each other with spaces.

Entries for this list must one of the following formats: `tgrp:context` or `tgrp.context`.

sag-recursion—Enable or disable SIP SAG recursion for this SAG

Default	disabled
Values	enabled | disabled

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

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: 1.0 / Most recent update: 1.2.1

RTC Status

Supported

Notes

This is a multiple instance configuration element.

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 | ttr-no-response | in-service-period |
burst-rate-window | sustain-rate-window | rate-constraints |
select | no | show | done | exit>
```

Parameters

name—Enter the name for this session constraint. This must be a unique identifier that you use when configuring a SIP interface on which you are applying it. This is a required parameter.

state—Enable or disable this session constraint

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

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 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: 1 / Max: 999999999

min-asr—Enter the minimum ASR in percentage

Default	0
Values	Min: 0 / Max: 100

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 taken out of service because of excessive transaction timeouts

Default	0
Values	Min: 0 / Max: 999999999

ttr-no-response—Enter the time delay in seconds to wait before changing the status of an element (like a session agent) after it has been taken out of service because of excessive transaction timeouts

Default	0
Values	Min: 0 / Max: 999999999

in-service-period—Enter the time in seconds that elapses before an element (like a session agent) can return to active service after being placed in the standby state

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

Default	0
Values	Min: 0 / Max: 999999999

sustain-rate-window—Enter the time in seconds used to measure the sustained rate

Default	0
Values	Min: 10 / Max: 999999999

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.***

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: 4.1.1

RTC Status Supported

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>
```

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 **method** 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 **method** 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 **method** 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 **method** 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 **session-constraints> rate-constraints** is an element of the **session-router path**. The full path from the topmost ALCI prompt is: **configure terminal > session-router > session-constraints > rate-constraints**.

Release First appearance: 5.1.1

RTC Status Supported

session-router-config

The **session-router-config** element allows you to configure whether or not session-related functionality is enabled within your network, whether it contains a Net-Net SBC SR or SD.

Syntax

```
session-router <state | system-number-type | sr-primary-name |
sr-primary-address | sr-secondary-name | sr-secondary-address |
divide-resources | match-lp-src-parent-realms | nested-realm-
stats | reject-message-threshold | reject-message-window |
session-directors | holidays | force-report-trunk-info |
additional-lp-lookups | max-routes-per-lookup | total-lp-routes |
select | no | show | done | exit>
```

Parameters

state—Enable or disable this session-related functionality on the system

Default	enabled
Values	enabled | disabled

system-number-type—Define the telephone number format used in local policy and local policy lookups

Default	Pots
Values	• Pots—Telephone numbers are in Decimal routing number format (0-9). This is the default and recommended setting. • E164—Telephone numbers are in E.164 format as defined by the global-number format of the tel URI defined in RFC 3966 • Routing—Telephone numbers are in Penta Decimal routing numbers (0-9, A-F). This value is not currently used but reserved for future enhancements.

sr-primary-name—Enter the name of the primary session router; must match the target name in the boot parameters of the primary SR

sr-primary-address—Enter the IP Address of the maintenance interface of the primary session router; must match the "inet on ethernet" address in the boot parameters of the primary SR

sr-secondary-name—Enter the name of the secondary session router; must match the target name in the boot parameters of the secondary SR

sr-secondary-address—Enter the IP Address of the maintenance interface of the secondary session router. This must match the "inet on ethernet" address in the boot parameters of the secondary SR.

divide-resources—Indicate whether or not resources are divided by the number of configured session directors. This includes:

- realm-config bandwidth
- session-agent max-sessions
- session-agent max-outbound-sessions

- session-agent max-burst-rate
- session-agent max-sustain-rate

Default disabled

Values enabled | disabled

match-lp-src-parent-realms—Enable or disable local policy parent realm matching based on a parent realm

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: 2^{32}-1

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: 2^{32}-1

force-report-trunk-info—Enable or disable generation of VSAs for trunk group information even when you are not using trunk-group routing; VSAs 65-68 to report originating and terminating trunk group information

Default disabled

Values enabled | disabled

session-directors—Access the session-directors subelement.

holidays—Access the session-router-holidays subelement.

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-config** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-router.**

Release First appearance: 1.0 / Most recent update: S-C6.2.0

RTC Status Supported

Notes This is a single instance configuration element.

session-router > holidays

The **session-router-holidays** configuration subelement establishes the holiday schedule to which the Net-Net SBC conforms.

Syntax

```
holidays <date | description | select | no | show | done | exit>
```

Parameters **date**—Enter the date of a holiday in YYYY-MM-DD format. A session router holidays entry will not function properly unless it is a valid date.

description—Describe the holiday

Path **session-router-holidays** is a subelement under the session-router-config element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-router > holidays**.

Release First appearance: 1.0

RTC Status Supported

Notes This is a multiple instance configuration element.

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

rules-called—Enter the rule(s) defined in the translation rules element applied to the called number

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: 1.0

RTC Status

Supported

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 | acct-stop-on-challenge | enum-sag-match | options
| registration-cache-limit | register-use-to-for-lp | refer-src-
routing | 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 SIP dialog transparency service 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—Enter the 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	none
Values	• none—No SIP-NAT is necessary • private—Indicates 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—Indicates 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: 1024 / Max: 65535; 0

register-service-route—Select the service-route usage for REGISTER requests

Default	always
Values	• never—Never use service-route for REGISTER • always—Always user service-route for REGISTER • removal—Use service-route for de-registration • session—Use service-route when the UA has a session • session+removal—Use service-route for de-registration and for when the UA has a session

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: 0 / 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: 0 / 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: 0 / 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: 0 / Max: 999999999

inactive-dynamic-conn—Enter the time limit in seconds for inactive dynamic connections

Default	32
Values	Min: 1 / Max: 999999999

red-sip-port—Enter the port for sending or receiving SIP checkpoint messages. Setting this to 0 disables SIP HA on the Net-Net SBC.

Default	1988
Values	Min: 1024 / Max: 65535; 0

Notes This parameter is not RTC supported.

red-max-trans—Enter the size of the SIP signaling transaction list in entries stored in memory

Default	10000
Values	Min: 0 / Max: 999999999

Notes This parameter is not RTC supported.

red-sync-start-time—Enter the time in milliseconds before the HA Net-Net SBC begins SIP signaling state checkpointing. As long as this HA Net-Net SBC is healthy and active, it remains in a constant cycle of (re)setting this field's timer and checking to see if it has become standby.

Default	5000
Values	Min: 0 / Max: 999999999

Notes This parameter is not RTC supported.

red-sync-comp-time—Enter the time in milliseconds the standby Net-Net SBC waits before checkpointing with the active Net-Net SBC to obtain the latest SIP signaling transaction information once the initial checkpointing process is complete

Default	1000
Values	Min: 0 / Max: 999999999

Notes This parameter is not RTC supported.

options—Enter customer-specific features and/or parameters. This optional field allows for a comma separated list of "feature=<value>" or "feature" parameters for the sip-config element.

sip-message-len—Set the size constraint in bytes on a SIP message

Default	4096
Values	Min: 0 / Max: 65535

add-reason-header—Enable or disable adding the reason header for rfc 3326 support

Default	disabled
Values	enabled | disabled

enum-sag-match—Enable or disable matching this SAG's group name to hostname portions of ENUM NAPTR or LRT replacement URIs**.**

Default	disabled
Values	enabled | disabled

extra-method-stats—Enable or disable the expansion SIP Method tracking feature.

Default	disabled
Values	enabled | disabled

nsep-user-sessions-rate—Set the CPS for call rates on a per user basis for NSEP. A value of 0 disables the call admission control on a per user basis.

Default	50
Values	0-999999999

rph-feature—Set the state of NSEP support for the global SIP configuration

Default	disabled
Values	enabled | disabled

enforcement-profile—Enter the name of the enforcement profile (SIP allowed methods).

registration-cache-limit—Set the maximum number of SIP registrations that you want to keep in the registration cache. A value of 0 means there is no limit on the registration cache, therefore disabling this feature.

Default	0
Values	Min: 0 / Max: 999999999

add-ucid-header—Enable or disable the using the UCID to correlate replicated SIP message information when you use SRR.

Default	disabled
Values	enabled | disabled

nsep-sa-sessions-rate—Enter maximum acceptable number of SIP INVITES (NSEP sessions) per second to allow for SIP session agents. 0 means there is no limit.

Default	0
Values	Min: 0 / Max: 999999999

register-use-to-for-lp—Enable or disable the use of an ENUM query to return the SIP URI of the Registrar for a SIP REGISTER message for routing purposes

Default	disabled
Values	enabled | disabled

refer-src-routing—Enable or disable the use of the referring party's source realm lookup policy to route subsequent INVITEs after static or dynamic REFER handling has been terminated. When disabled, the system derives the lookup from the source realm of the calling party.

Default	disabled
Values	enabled | disabled

pass-gruu-contact—Enable or disable the **sip-config** to parse for GR URI parameter in the contact header in non-registered endpoints' messages.

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: 1.0 / Most recent update: S-C6.2.0

RTC Status Supported

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 | required-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 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.

required-mode-inbound—Select the treatment of 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 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 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 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 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: 1.0 / Most recent update: 2.0

RTC Status

Supported

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 a SIP interface for your 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 | 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 | manipulation-pattern |
sip-isup-profile | 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 of the **sip-interface** configuration element

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.

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.

Default Recurse

Values

- Proxy—Send the response back to the previous hop
- Recurse—Recurse on the contacts in the response

contact-mode—Select the contact header routing mode

Default none

Values

- none
- maddr
- strict
- loose

nat-traversal—Select the type of HNT functionality for SIP

Default none

Values

- none—NAT Traversal is disabled
- always—Performs HNT when SIP-Via and transport addresses do not match
- rport—Performs 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: 999999999

registration-caching—Enable or disable registration cache used for all UAs rather than those behind NATs

Default	disabled
Values	enabled | disabled

min-reg-expire—Enter the minimum registration expiration time in seconds for HNT registration caching

Default	300
Values	Min: 1 / Max: 999999999

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: 1 / Max: 999999999

route-to-registrar—Indicate whether or not the SD should forward a request 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

teluri-scheme—Enable or disable the conversion of SIP URIs to Tel URIs

Default	disabled
Values	enabled | disabled

uri-fqdn-domain—Change the host part of the URIs to the FQDN value set here. This applies to the Request-URI, From header, and To header in non-dialog requests sent from the SIP interface.

options—Enter optional features and/or parameters

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

sip-dynamic-hnt—Enable or disable adaptive HNT

Default	disabled
Values	enabled | disabled

max-nat-interval—Enter the amount of time in seconds that testing should not exceed for adaptive HNT. The Net-Net SBC will keep the expires interval at this value.

Default	3600
Values	Min: 0 / Max: 999999999

nat-int-increment—Enter the amount of time in seconds to use as the increment in value in the SIP expires header for adaptive HNT

Default	10
Values	Min: 0 / Max: 999999999

nat-test-increment—Enter the amount of time in seconds that will be added to the test timer for adaptive HNT

Default	30
Values	Min: 0 / Max: 999999999

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

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: 1025 / 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: 1025 / Max: 65535

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—Enter the name of the SIP header manipulations configuration to apply 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

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.

anonymous-priority—Set the policy priority parameter for this SIP interface. It is used to facilitate emergency sessions from unregistered endpoints. This value is compared against a policy priority parameter in a local policy configuration element.

Default	none
Values	• none • normal • non-urgent • urgent • emergency

network-id—Set the value that will be inserted into the P-Visited-Network-ID header

ext-policy-server—Enter the name of external policy server used as the CLF for this SIP interface

default-location-string—Set a default location string to insert into P-Access-Network-Info header when the CLF does not return this value

term-tgrp-mode—Select the mode for routing 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

charging-vector-mode—Set the state of P-Charging-Vector header handling

Default	pass
Values	• none—Pass the P-Charging-Vector header received in an incoming SIP message untouched as the message is forwarded out of the Net-Net SBC, not extracting RADIUS information • 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, extracting RADIUS information • delete—Delete the P-Charging-Vector header received in an incoming SIP message before it is forwarded out of the Net-Net SBC • insert—Inserts 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—Removes the P-Charging-Vector from incoming requests for a session and store it. Then the Net-Net SBC inserts it into outbound responses related to that session in a P-Charging-Vector header.

Notes

Note that the default setting for the **charging-vector-mode** is `pass` for new SIP interface configurations. If you are upgrading and there are pre-existing SIP interfaces in your (upgraded) configuration, the default becomes `none`.

charging-function-address-mode—Set the state of P-Charging-Function-Address header handling

Default	pass
Values	• none—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, not extracting RADIUS information • 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, extracting RADIUS information • 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—Inserts 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—To be configured on the SIP interface facing the UE, configures the Net-Net SBC to replace the PCFA with the most recently cached values rather than the **ccf-address** and **ecf-address** you set to be static in your configuration. The cached values come from one of the following that the Net-Net SBC has received most recently: request, response, registration, or local configuration. • delete-and-respond—To be configured on the SIP interface facing the S-CPCF, configures the Net-Net SBC to strip out the latest cached PCFA.

Notes

Note that the default setting for the **charging-function-address-mode** is `pass` for new SIP interface configurations. If you are upgrading and there are pre-existing SIP interfaces in your (upgraded) configuration, the default becomes `none`.

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

secured-network—Enable or disable sending messages on unsecured transport

Default	disabled
Values	enabled | disabled

max-incoming-conns—Enter the maximum number of TCP/TLS connections for this sip interface

Default	0
Values	Min: 0 / Max: 40000; setting a value of 0 disables this parameter

per-scr-ip-max-incoming-conns—Enter the maximum number of TCP/TLS connections per peer IP address

Default	0
Values	Min: 0 / Max: 40000; setting a value of 0 disables this parameter.

inactive-conn-timeout—Enter the timeout, measured in seconds for idle TCP/TLS connections

Default	0
Values	Min: 0 / Max: 999999999; setting a value of 0 disables the timer.

implicit-service-route—Enable or disable the implicit service route behavior

Default	disabled
Values	• enabled • disabled • strict

rfc2833-payload—Enter the payload type used by the SIP interface in preferred rfc2833-mode

Default	101
Values	Min: 96 / Max: 127

rfc2833-mode—Choose whether the SIP interface will behave exactly the same way as before and the 2833or 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 | preferred | dual

trans-expire—Set the transaction expiration timer in seconds

Default	0
Values	Min: 0 / Max: 999999999

invite-expire—Set the INVITE transaction expiration timer in seconds

Default	0
Values	Min: 0 / Max: 999999999

tcp-nat-interval—Enter the TCP NAT traversal registration interval in seconds

Default	90
Values	Min: 0 / Max: 999999999

constraint-name—Enter the name of the constraint being applied to this interface

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

max-redirect-contacts—Enter the maximum number of contact and route attempts in case of a redirect

Default	0
Values	Min: 0 / Max: 10

untrusted-conn-timeout—Enter the timeout time, in seconds, for untrusted endpoints on TCP/TLS connections

Default	0
Values	Min: 0 (disabled) / Max: 999999999

enforcement-profile—Enter the name of the enforcement profile associated with this SIP interface

refer-call-transfer—Enable or disable the refer call transfer feature.

Default	disabled
Values	enabled | disabled

route-unauthorized-calls—Enter the name of the SA or SAG you want to route unauthorized calls

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—Enable or disable this SIP interface inserting an SDP into either an INVITE or a REINVITE

Default	disabled
Values	• disabled—Do not insert an SDP • invite—Insert an SDP in the invite • reinvite—Insert an SDP in the reinvite

add-sdp-profile—Enter a list of one or more media profile configurations you want to use when the Net-Net SBC inserts SDP into incoming INVITEs that have no SDP. The media profile contains media information the Net-Net SBC inserts in outgoing INVITE.

ims-aka-feature—Enable or disable IMS-AKA use for a SIP interface

Default	disabled
Values	enabled | disabled

manipulation-pattern—Enter the regular expression used in header manipulation rules for this sip-interface.

manipulation-string—Enter the string used in header manipulation rules for this sip-interface.

sip-profile—Enter the name of the **sip-profile** to apply to this interface.

sip-isup-profile—Enter the name of the **sip-isup-profile** to apply to this interface.

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: 1.0 / Most recent update: S-C6.2.0

RTC Status Supported

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 | tls-profile |
anonymous-connection | ims-aka-profile | select | no | show | done
| exit>
```

Parameters

address—Enter the IP address of the host associated with the sip-port entry.

port—Enter the port number for this sip-port

Default	5060
Values	Min: 1025 / Max: 65535

transport-protocol—Select the transport protocol associated for this sip-port

Default	UDP
Values	• TCP • UDP • TLS • SCTP

tls-profile—Enter the TLS profile name

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

ims-aka-profile—Enter the **name** value for the IMS-AKA profile configuration to use for a SIP port

Path **sip-ports** is a subelement is 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: 1.0 / Most recent update: 4.1

RTC Status Supported

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

The **sip-isup-profile** element allows you to set up a SIP ISUP format interworking. You can apply a configured SIP ISUP profile to a realm, session agent or SIP interface.

Syntax

```
sip-isup-profile <name | mode | isup-version | convert-isup-
format | select | no | show | done | exit>
```

Parameters

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-t926 | 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: S-C6.2.0

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.

Do not use a header rule name that is all capital letters. Capitals currently refer to predefined rules that are used as macros, and they might conflict with a name that uses capital letters; for example,

```
$IP_ADDRESS
```

Note: Acme Packet reserves the use of all capitals for future use.

Syntax

```
sip-manipulation <name | header-rules | mime-rules | mime-isup-
rules | import | export | description | select | no | show | done
| exit>
```

Parameters

name—Enter the name of this list of header rules.

header-rules—Access the header-rules subelement.

mime-rules—Access the mime-rules subelement.

mime-isup-rules—Access the mime-isup-rules-rules subelement.

import—Enter the complete file name, including .gz, of a previously exported sip-manipulation rule.

export—Enter the file name of a SIP manipulation to export configuration information a designated file.

description—Describe what the set of header rules is doing.

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: 4.0

RTC Status

Supported

sip-manipulation > header-rules

The **header-rules** subelement is used to define one action to perform on a given SIP header.

Do not use a header or element rule name that is all capital letters. Capitals currently refer to predefined rules that are used as macros, and they might conflict with a name that uses capital letters; for example,

```
$IP_ADDRESS
```

Note: Acme Packet reserves the use of all capitals for future use.

Syntax

```
header-rules <name | action | match-value | msg-type | methods |
element-rules | header-name | comparison-type | new-value |
select | no | show | done | exit>
```

Parameters

name—Enter the name of the header to which this rule applies. This name must match a header name.

action—Select 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 • store—Store this header • none—Take no action

match-value—Enter the exact value to be matched. The action you specify is only performed if the header value matches.

msg-type—Select the message type to which this header rule applies.

Default	any
Values	• any—Both Requests and Reply messages • request—Request messages only • reply— Reply messages only

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.

Default	none

element-rules—Access the element rules sub-subelement

header-name—Enter the header name for which the rules need to be applied

comparison-type—Select the comparison type that the match-value uses

Default	case-sensitive
Values	• case-sensitive • case-insensitive • pattern-rule • refer-case-sensitive • refer-case-insensitive • boolean

new-value—The new value to be used in add or manipulate actions. To clear the `new-value` enter an empty string.

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

First appearance: 4.0

RTC Status

Supported

sip-manipulation > header-rules > element-rules

The **element-rules** sub-subelement is used to define a list of actions to perform on a given SIP header.

Do not use an element rule name that is all capital letters. Capitals currently refer to predefined rules that are used as macros, and they might conflict with a name that uses capital letters; for example,

```
$IP_ADDRESS
```

Note: Acme Packet reserves the use of all capitals for future use.

Syntax

```
element-rules <name | type | action | match-val-type | match-
value | new-value | parameter-name | comparison-type | 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.

type—Select the type of element on which to perform the action

Default none

Values

- header-value—Full value of the header
- header-param-name—Header parameter name
- header-param—Parameter portion of the header
- uri-display—Display of the SIP URI
- 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-name—Name of the SIP URI param
- uri-param—Parameter included in the SIP URI
- uri-header-name—SIP URI header name
- uri-header—Header included in a request constructed from the URI
- uri-user-param—User parameter of the SIP URI
- status-code—Status code of the SIP URI
- reason-phrase—Reason phrase of the SIP URI
- uri-user-only—URI username without the URI user parameters
- uri-phone-number-only—User part of the SIP/TEL URI without the user parameters when the user qualifies for specific BNF

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
- store—Store the elements

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

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”

parameter-name—Enter the element parameter name for which the rules need to be applied

comparison-type—Select the type of comparison to be used for the match-value

Default	case-sensitive
Values	• case-sensitive • case-insensitive • pattern-rule

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: 4.0

RTC Status Supported

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 | gr-317 | etsi-356

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.

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 | 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, 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-headers—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: S-C6.2.0

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.

Do not use a header rule name that is all capital letters. Capitals currently refer to predefined rules that are used as macros, and they might conflict with a name that uses capital letters; for example,

```
$IP_ADDRESS
```

Note: Acme Packet reserves the use of all capitals for future use.

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: S-C6.2.0

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 ISUP message.

Syntax

```
sip-isup-param-rules <name | parameter-type | parameter-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.

parameter-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

parameter-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: S-C6.2.0

RTC Status

Supported

Notes

This is a multiple instance configuration element.

sip-manipulation>mime-rules

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.

Syntax

```
mime-rules <name | content-type | action | match-value |
comparison-type | msg-type | methods | new-value | mime-headers |
select | no | show | done | exit>
```

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-headers—Access the mime-headers subelement.

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: S-C6.2.0

RTC Status Supported

Notes This is a multiple instance configuration element.

sip-manipulation>mime-rules>mime-headers

The **mime-headers** configuration allows you to configure MIME headers, which operate on the specific headers in the match body part of the SIP message.

Do not use a header rule name that is all capital letters. Capitals currently refer to predefined rules that are used as macros, and they might conflict with a name that uses capital letters; for example,

```
$IP_ADDRESS
```

> *Note: Acme Packet reserves the use of all capitals for future use.*

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 name for this MIME header rule. This parameter is required and has no default.

mime-header-name—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 | 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-rules** element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-rules>mime-headers**.

Release First appearance: S-C6.2.0

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 | delete-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 default next-hop 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 default next-hop SIP element (a SIP proxy) in the external network

Default	5060
Values	Min: 1025 / Max: 65535

ext-address—Enter the IP address on the network interface in the external realm. This required entry must follow the IP address format. Changes to this parameter require a system reboot to take effect.

home-address—Enter the IP address on the network interface in the home realm. 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.

home-proxy-port—Enter the home realm proxy port number

Default	0
Values	Min: 0; 1025 / Max: 65535

route-home-proxy—Enable or disable requests being routed 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.

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 certain headers in a 3xx Response message being received and NATed when sent to the initiator of the SIP INVITE message

Default	disabled
Values	enabled | disabled

use-url-parameter—Select 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 type of 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>.

Default	Type `headers -d <enter>`

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 withSIP-NAT external address

delete-headers—Remove headers from the list of SIP headers configured in the headers field

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: 1.0 / Most recent update: 2.0

RTC Status Supported with exceptions - Changes to the sip-nat `ext-address` require reboot

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 | redirection | ingress-conditional-cac-admit |
egress-conditional-cac-admit | forked-cac-bw | cnam-lookup-server
| cnam-lookup-dir | cnam-unavailable-ptype | cnam-unavailable-
utype | select | no | show | done | exit>
```

Parameters

name—Enter a unique identifier for 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

redirection—Set this value to specify the redirection action, within the context of SIP Diversion interworking.

Default	none
Values	inherit | none | isup | diversion | history-info

ingress-conditional-cac-admit—Set this parameter to enabled to use conditional bandwidth CAC for media release on the ingress side of a call. Set this parameter to inherit for the value to be inherited from the realm-config, sip-interface, or sip-interface

Default	inherit
Values	enabled | disabled | inherit

egress-conditional-cac-admit—Set this parameter to enabled to use conditional bandwidth CAC for media release on the egress side of a call.

Default	inherit
Values	enabled | disabled | inherit

forked-cac-bw—Select the method for the CAC bandwidth to be configured between the forked sessions.

Default	inherit
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

cnam-lookup-server—Enter the name of an **enum-config** to query ENUM servers for CNAM data.

cnam-lookup-dir—Set this parameter to **ingress** or **egress** to identify where the Net-Net SBC performs a CNAM lookup with repsect to where the call traverses the system.

Default	egress
Values	ingress | egress

cnam-unavailable-ptype—Set this parameter to a string, no more than 15 characters, to indicate that the unavailable=p parameter was returned in a CNAM response.

cnam-unavailable-utype—Set this parameter to a string, no more than 15 characters, to indicate that the unavailable=u parameter was returned in a CNAM response.

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: S-C6.2.0

RTC Status

Supported

Notes

This is a multiple instance configuration element.

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 | delete | edit | select | no | show | done
| exit>
```

Parameters

entries—Enter the entries configuration subelement

delete—Delete a SIP to q850 mapping. Enter the SIP code.

edit—Edit a response map by number

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 > sip-q850-map**.

Release

First appearance: 4.0

RTC Status Supported

sip-q850-map > entries

The **entries** subelement is used to create the mapping of q850 cause to SIP reason code.

Syntax

```
entries <sip-status | q850-cause | q850-reason | select | no |
show | done | exit>
```

Parameters

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: 699

q850-reason—Describe text to accompany the mapped SIP response code

Path Entries is a subelement under the **sip-q850-map** configuration element, which is located under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-q850-map > entries**.

Release First appearance: 4.0

RTC Status Supported

sip-response-map

The **sip-response-map** element establishes SIP response maps associated with the upstream session agent.

Syntax

```
sip-response-map <name | entries | delete | edit | select | no |
show | done | exit>
```

Parameters

name—Name of SIP response map

entries—Access the entries subelement

delete—Remove the selected response-map entry

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: 1.1

RTC Status Supported

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 | 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 expires time.

Values Min: 0 / Max: 999999999

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: 1.1

RTC Status Supported

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 a particular NMS belongs. 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

Default	READ-ONLY
Values	• READ-ONLY—Allows GET requests • READ-WRITE—Allows both GET and SET requests

ip-addresses—Enter the IP address(es) for SNMP communities for authentication purposes. Entries must follow the IP Address Format.

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: 1.0

RTC Status Unsupported

Notes This is a multiple instance configuration element.

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 the **static-flow** configuration element

in-source—Enter the incoming source IP address and port of packets to match for static flow translation. 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
Values	Port: Min: 0 / Max: 65535

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

Values	Port: Min: 0 / Max: 65535

out-realm-id—Enter the egress 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
Values	Port: Min: 0 / Max: 65535

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
Values	Port: Min: 0 / Max: 65535

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

Default	none
Values	• none—No dynamic ALG functionality • NAPT—Configure as NAPT ALG • TFTP—Configure as TFTP ALG

average-rate-limit—Enter the maximum speed in bytes per second for this static flow

Default	0
Values	Min: 0 / Max: 125000000

start-port—Enter the internal starting ALG ephemeral port

Default	0

Values	Min: 1025 / Max: 65535

end-port—Enter the internal ending ALG ephemeral port

Default	0
Values	Min: 1025 / Max: 65535

flow-time-limit—Enter the time limit for a flow, measured in seconds

Values	Min: 0 / Max: 999999999

initial-guard-timer—Enter the initial flow guard timer, measured in seconds

Values	Min: 0 / Max: 999999999

subsq-guard-timer—Enter the subsequent flow guard timer, measured in seconds

Values	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: 1.0 / Most recent update: 4.1

RTC Status Supported

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: 0 / 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: 0 / 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 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.

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: 1.0 / Most recent update: 2.1

RTC Status Supported

Notes This is a multiple instance configuration element.

surrogate-agent

The **surrogate-agent** configuration element allows you to configure the Net-Net SBC for surrogate registration. This feature lets the Net-Net SBC explicitly register on behalf of Internet Protocol Branch Exchange (IP-PBX).

Syntax

```
surrogate-agent <register-host | register-user | state | realm-id
| description | customer-host | customer-next-hop | register-
contact-host | register-contact-user | password | register-
expires | replace-contact | route-to-registrar | aor-count |
auth-user | count-start | options | select | no | show | done |
exit>
```

register-host—Enter the registrar's hostname to be used in the Request-URI of the REGISTER request

register-user—Enter the user portion of the Address of Record

state—Enable or disable this surrogate agent

Default	enabled
Values	enabled | disabled

realm-id—Enter the name of the realm where the surrogate agent resides

description—Describe the surrogate agent. This parameter is optional.

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 parameter is optional.

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—Enter the password to be used for this agent

register-expires—Enter the expire time in seconds to be used in the REGISTER

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

Default	disabled
Values	enabled | disabled

route-to-registrar—Enable or disable requests coming from the surrogate agent being 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

Default	1
Values	Min: 0 / Max: 999999999

auth-user—Enter the authentication user name you want to use for the surrogate agent

max-register-attempt—Enter the number of times to attempt registration; a 0 value means registration attempts are unlimited

Default	3
Values	Min: 0 / Max: 10

register-retry-time—Enter the amount of time in seconds to wait before reattempting registration

Default	300
Values	Min: 10 / Max: 3600

count-start—Enter the number of registrations to do on behalf of this IP-PBX

Default	1
Values	Min: 0 / Max: 999999999

options—Enter non-standard options or features

Path **surrogate-agent** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > surrogate-agent.**

Release First appearance: 4.1; Last update: 5.1

system-access-list

The **system-access-list** configuration element allows you to configure system access control of the management interface on your 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 |
protocol | select | no | show | done | exit>
```

Parameters

source-address—Enter the network source address

netmask—Enter the source subnet mask

description—Provide a brief description of this **system-access-list** configuration.

protocol—Acess the **protocol** subelement.

Path **system-access-list** is an element of the system path. The full path from the topmost ACLI prompt is: **configure terminal > system> system-access-list**.

Release First appearance: 5.0 / Most recent update: S-C6.2.0

RTC Status Supported

system-access-list>protocol

protocol—Enter a specified protocol or the special value *all* that specifies by protocol the type of management traffic allowed to access the system.

The default value (all) matches all supported transport layer protocols.

Default	all
Values	all | ICMP | SCTP | TCP | UDP

Path **protocol** is a subelement of the **system-access-list** element. The full path from the topmost ACLI prompt is: **configure terminal > system> system-access-list>protocol**.

Release First appearance: S-C6.2.0

system-config

The **system-config** element establishes general system information and settings.

Syntax

```
system-config <hostname | 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 | syslog-servers | system-log-
level | process-log-level | process-log-ip-address | process-log-
port | collect | default-gateway | default-v6-gateway | restart |
call-trace | internal-trace | log-filter | remote-control |
alarm-threshold | exceptions | telnet-timeout | console-timeout |
link-redundancy-state | cli-audit-trail | source-routing | cli-
more | terminal-height | debug-timeout | trap-event-lifetime |
ipv6-support | options | select | no | show | done | exit>
```

Parameters

hostname—Enter the main hostname that identifies the Net-Net SBC. Entries must follow either the Hostname (or FQDN) Format or the IP Address Format.

description—Describe the Net-Net SBC. 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. This value has no relation to the **system-config > hostname** field. 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 is enabled. 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 the SNMP authentication traps

Default	disabled
Values	enabled | disabled

enable-snmp-syslog-notify—Enable or disable sending 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—Determine whether traps are sent 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—Determine whether the environmental monitoring MIB is sent 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 I2C 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
Values	Min: 1 / Max: 500

snmp-syslog-level—Set the log severity levels that send syslog notifications to an NMS via SNMP if 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	• emergency • critical • major • minor • warning • notice • info • trace| • debug • detail

syslog-servers—Access the syslog-servers subelement

system-log-level—Set the system-wide log severity levels write to the system log

Default	warning

Values
- emergency
- critical
- major
- minor
- warning
- notice
- info
- trace
- debug
- detail

process-log-level—Set the default log level that processes running on the Net-Net SBC start

Default notice

Values
- emergency
- critical
- major
- minor
- warning
- notice
- info
- trace
- debug
- detail

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: 0; 1025 / Max: 65535

default-gateway—Enter the IP address of the gateway to use when IP traffic sent by the Net-Net SBC is destined for a network other than one of the LANs on which the 10/100 Ethernet interfaces could be. Entries must follow the IP Address Format. A value of 0.0.0.0 indicates there is no default gateway.

Default 0.0.0.0

default-v6-gateway—Set the IPv6 default gateway for this Net-Net SBC. This is the IPv6 egress gateway for traffic without an explicit destination. The application of your Net-Net SBC determines the configuration of this parameter.

restart—Enable or disable the Net-Net SBC rebooting when a task is suspended. When set to enabled, this field causes the Net-Net SBC to reboot automatically when it detects a suspended task. When this field is set to disabled and a task is suspended, the Net-Net SBC does not reboot.

Default enabled

Values	enabled | disabled

call-trace—Enable or disable protocol message tracing for sipmsg.log for SIP and alg.log for MGCP

Default	disabled
Values	enabled | disabled

internal-trace— Enable or disable internal ACP message tracing for all processes

Default	disabled
Values	enabled | disabled

log-filter—Set to `logs` or `all` to send the logs to the log server

Default	all
Values	• none • traces • traces-fork • logs • log-fork • all • all-fork

remote-control—Enable or disable listening for remote ACP config and control messages before disconnecting

Default	enabled
Values	enabled | disabled

alarm-threshold — Accesses the alarm-threshold subelement.

exceptions—Select system tasks that have no impact on system health or cause the system to restart. This field contains the name(s) of the task(s) surrounded by quotation marks. If there are multiple entries, they should be listed within quotation marks, with each entry separated by a <Space>.

telnet-timeout—Enter the time in seconds the Net-Net SBC waits when there is no Telnet activity before an administrative telnet session, or SSH connection, is terminated. A value of 0 disables this functionality, meaning no time-out is being enforced.

Default	0
Values	Min: 0 / Max: 65535

console-timeout—Enter the time in seconds the Net-Net SBC waits when there is no activity on an ACLI administrative session before it terminates the session. The ACLI returns to the User Access Verification login sequence after it terminates a console session. A value of 0 disables this functionality.

Default	0
Values	Min: 0 / Max: 65535

link-redundancy-state—Enable or disable the link redundancy

Default disabled

Values enabled | disabled

collect—Accesses the collect subelement

cli-audit-trail—Enable or disable the ACLI command audit trail. The **cli-audit-trail** outputs to cli.audit.log.

Default enabled

Values enabled | disabled

source-routing—Enable or disable source routing egress HIP packets based on source IP addresses. This parameter is used to route packets based on their source address, and not on the system's routing table. This feature is only used for management applications within the Net-Net SBC that utilitze HIP interfaces.

A few things to note:

- This feature only affects media-network interfaces.
- The bootparam flag (0x80008) does not work in C-Series 5.x and D-Series 5.x and up. You must use the system-config source-routing parameter.
- The source-routing parameter is not RTC-supported. You must reboot after enabling it.

Default disabled

Values enabled | disabled

cli-more—Enable this parameter to have the ACLI "more" paging feature working consistently across console, Telnet, or SSH sessions with the Net-Net SBC. When this parameter is disabled, you must continue to set this feature on a per session basis.

Default disabled

Values enabled | disabled

terminal-height—Set the Net-Net SBC terminal height when the **more** prompt option is enabled

Default 24

Values Minimum: 5 / Maximum: 1000

debug-timeout—Enter the time, in seconds, you want to the Net-Net SBC to timeout log levels for system processes set to **debug** using the ACLI **notify** and **debug** commands. A value of 0 disables this parameter.

Default 0

Values Min: 0 / Max: 65535

trap-event-lifetime—Set this parameter to the number of days you want to keep the information in the alarm synchronization table; 0 turns alarm synchronization off

Default 0

Values Min: 0 / Max: 7

ipv6-support—Set this parameter to **enabled** if you want to use IPv6 on your system. Otherwise, you can leave this parameter set to **disabled** (default).

Default	disabled
Values	enabled | disabled

options—Enter any customer-specific features and/or parameters for this global system configuration. This parameter is optional.

Notes Under the **system-config** element, options are not RTC supported.

Path **system-config** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config.**

Release First appearance: 1.0 / Most recent update: 5.1

RTC Status Supported

Notes This is a single instance configuration element.

system-config > alarm-threshold

The alarm-threshold configuration element allows you to configure custom alarms for certain system conditions based on those conditions reaching defined operating levels.

Syntax

```
alarm-threshold <type | volume | severity | value | select | no |
show | done | exit>
```

Parameters

type — The type of custom alarm-threshold this object creates.

Values
- cpu — Alarm based on CPU usage
- space — Alarm based on used space on an identified disk volume
- memory — Alarm based on memory usage
- sessions — Alarm based on percentage of licensed sessions in use
- rfactor — unused

volume — Identifies the disk volume that this alarm threshold monitors. This parameter is only configured when the type parameter is set to space.

severity — The system severity of this alarm.

Default	minor
Values	major | minor | critical

value — The percentage usage of the resource identified in the type parameter that triggers this alarm.

Default	2
Values	1 - 100

Path **alarm-threshold** is a subelement of the system-config element. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > alarm-threshold**.

RTC Status Supported

system-config>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 | red-collect-state | red-max-trans | red-sync-
start-time | red-sync-comp-time | push-receiver | group-settings
| push-success-trap-state | select | no | show | done | exit>
```

Parameters

sample-interval—Enter the data collection sampling interval, in minutes

Default	0
Values	Min: 1 / Max: 120

push-interval—Enter the data collecting push interval, in minutes

Default	0
Values	Min: 0 / 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

boot-state—Enable or disable group collection on reboot

Default	disabled
Values	enabled | disabled

Notes

This parameter is not RTC supported.

red-collect-state—Enable or disable HA support for the collection function

Default	disabled
Values	enabled | disabled

red-max-trans—Enter the maximum number of redundancy sync transactions to keep on active

Default	1000
Values	Min: 0 / Max: 999999999

red-sync-start-time—Enter the time to start redundancy sync timeout, in milliseconds.

Default	5000
Values	Min: 0 / Max: 999999999

red-sync-comp-time—Enter the time to complete a redundancy sync, in milliseconds.

Default	1000
Values	Min: 0 / Max: 999999999

push-receiver—Access the `push-receiver` subelement

group-settings—Access the `group-settings` subelement

push-success-trap-state—Enable this parameter if you want the Net-Net SBC to send a trap confirming successful data pushes to HDR servers

Default	disabled
Values	enabled | disabled

Path **collect** is a subelement of the system-config element. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > collect**.

Release First appearance: 5.0

RTC Status Supported

system-config>collect>push-receiver

The **push-receiver** configuration 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 hostname or IP 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—Set the protocol with which to send HDR collection record files.

Default	FTP
Values	FTP | SFTP

Path **push-receiver** is a subelement of the system-config>collect subelement. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > collect > push-receiver**.

Release First appearance: 5.0

RTC Status Supported

system-config>collect>group-settings

The **group-settings** subelement allows you to configure and modify collection parameters for specific groups.

Syntax

```
group-settings <group-name | sample-interval | start-time | end-
time | boot-state | select | no | show | done | exit>
```

Parameters

group-name—Enter the name of the object the configuration parameters are for. There can only be one object per group.

Values

- system
- interface
- session-agent
- session-realm
- voltage
- fan
- temperature
- sip-sessions
- sip-ACL-oper
- sip-ACL-status
- sip-client
- sip-server
- sip-policy
- sip-errors
- sip-status
- algd-state
- mgcp-trans
- mgcp-media-events
- mgcp-ACL
- algd-ACL
- h323-stats

Values

- system
- interface
- session-agent
- session-realm
- voltage
- fan
- temperature
- sip-sessions
- sip-ACL-oper
- sip-ACL-status
- sip-client
- sip-server
- sip-policy
- sip-errors
- sip-status
- algd-state
- mgcp-trans
- mgcp-media-events
- mgcp-ACL
- algd-ACL
- h323-stats

sample-interval—Enter the group data collection sampling interval, in minutes

Default	0
Values	Min: 0 / 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=hour; m=minute; s=second)

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=hour; m=minute; s=second)

boot-state—Enable or disable data collection for this group.

Default	disabled
Values	enabled | disabled

Path

group-settings is a subelement of the system-config>collect subelement. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > collect > group-settings**.

Release

First appearance: 5.0

RTC Status

Supported

system-config > syslog-servers

The **syslog-servers** subelement configures multiple syslog servers.

Syntax

```
syslog-servers <address | port | facility | select | no | show |
done | exit>
```

Parameters

address—Enter the syslog server's IP address

port—Enter the port number on the syslog server that the Net-Net SBC sends log

Default	514

facility—Enter the user-defined facility value sent in every syslog message from the Net-Net SBC to the syslog server. This value must conform to IETF RFC 3164.

Default	4

Path

syslog-servers is a subelement under the system-config element. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > syslog-servers.**

Release

First appearance: 1.2.1

RTC Status

Supported

Notes

We recommend configuring no more than 8 syslog-config subelements.
This is a multiple instance configuration subelement.

test-pattern-rule

The **test-pattern-rule** configuration element allows you to test the regular expression that you might use in SIP manipulation rules to see if it yields the results you require. This element is useful for testing the regex values that you devise because it will tell you whether that value is valid or not.

Syntax

```
test-pattern-rule <expression | string | show | exit>
```

Parameters

expression—Enter the regular expression that you want to test. The Net-Net SBC will inform you whether or not there is a match.

string—Enter the string against which you want to compare the regular expression

show—Show the test pattern you entered, whether there was a match, and the number of matches

Path

test-pattern-rule is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > test-pattern-rule**.

Release

First appearance: 5.0

RTC Status

Supported

Notes

The **test-pattern-rule** element can also be configured in Superuser mode as a command.

test-policy

The **test-policy** element tests and displays local policy routes from the ACLI.

Syntax

```
test-policy <source-realm | from-address | to-address | time-of-
day | carriers | media-profiles | show | exit>
```

Parameters

source-realm—Enter the name set in the source-realm field of a configured local policy. Entering an "*" in this field matches for any source realm. Leaving the field empty indicates that only the "global" realm will be tested.

from-address—Enter the "from" address of the local policy to look up/test. From addresses should be entered as SIP-URLs in the form of `sip:19785551212@netnetsystems.com`.

to-address—Enter the "to" address of the local policy to look up/test. To addresses should be entered as SIP-URLs in the form of `sip:19785551212@netnetsystems.com`.

time-of-day—Enable or disable use of the time of day value set in the start-time and end-time fields you set in configured local-policy elements

Values enabled | disabled

carriers—Enter the names of permitted carriers set in the carriers fields set in configured local-policy elements. This field is formatted as a list of comma-separated text strings enclosed in quotation marks.

media-profile—Enter a list of media profiles

show—Show the next hop and the associated carrier information for all routes matching the "from" and "to" addresses entered

Path

Type **test-policy** at the topmost ACLI prompt.

Release First appearance: 1.0 / Most recent update: 1.2.1

RTC Status Supported

Notes Type the show command to perform the actual test lookup after parameters have been entered.

The **test-policy** element can also be configured in Superuser mode as a command.

test-translation

The **test-translation** element tests translation rules configured for the Address Translation feature.

Syntax

```
test-translation <called-address | calling-address | translation-
id | exit | show>
```

Parameters

called-address—Enter the address on which the called rules will be applied. This entry is required.

calling-address—Enter the address on which the calling rules will be applied. This entry is required.

translation-id—Enter the translation rules to test. This entry is required.

show—Show results of translation

Path Type **test-translation** at the topmost ACLI prompt.

Release First appearance: 1.3

RTC Status Supported.

Notes The **test-translation** element can also be configured in Superuser mode as a command.

tls-global

The **tls-global** 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 (disabled) / Max: 24

Path **tls-global** is an element of the security path. The full path from the topmost ACLI prompt is: **configure terminal > security> tls-global**.

Release First appearance: 5.0

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 |
tls-version | options | cert-status-check | cert-status-profile-
list | select | no | show | done | exit>
```

name—Enter the name of the TLS profile

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 the default `ALL`, or enter a list of supported ciphers which you can find in the TLS section of the *Net-Net 4000 ACLI Configuration Guide*'s *Security* chapter. As of Release S-C6.1.0, TLSv1 and SSLv3 have been removed made redundant by the **tls-version** parameter).

Default	all

verify-depth—Enter the maximum depth of the certificate chain that will be verified

Default	10
Values	Min: 0 / Max: 10

mutual-authenticate—Enable or disable mutual authentication on the Net-Net SBC

Default	disabled
Values	enabled | disabled

tls-version—Enter the TLS version you want to use with this TLS profile

Default	compatability
Values	TLSv1 | SSLv3 | compatability

cert-status-check—Enable or disable OCSP in conjunction with an existing TLS profile.

Default	disabled
Values	enabled | disabled

cert-status-profile-list—Select an object from the **cert-status-profile** parameter. In order to enable this parameter, this list must not be empty. If multiple **cert-status-**

profile objects are assigned to **cert-status-profile-list**, the Net-Net SBC will use a hunt method beginning with the first object on the list.

Values	Any valid certificate status profile from cert-status-profile parameter

Mode Superuser

Path **tls-profile** is an element under the security path. The full path from the topmost prompt is: **configure terminal > security > tls-profile**.

Release First appearance: 4.1 / Most recent update S-C6.2.0

RTC Status Supported

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 | 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.

type—Select the address translation type to be performed

Default	none
Values	• add—Adds a character or string of characters to the address • delete—Deletes a character or string of characters from the address • replace—Replaces a character or string of characters within the address • none—Translation rule is disabled

add-string—Enter the 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: 999999999

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. This 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: 999999999

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: 1.3

RTC Status

Supported

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.

filter-level—Set the filter level for the NMS identified within this trap-receiver element

Default	critical
Values	• All—All alarms, syslogs, and other traps will be trapped out. That is, the corresponding NMS will receive informational, warning, and error events.

- Minor—All syslogs generated with a severity level greater than or equal to MINOR and all alarms generated with a severity level greater than or equal to MINOR will be trapped out
- Major—All syslogs generated with a severity level greater than or equal to MAJOR and all alarms generated with a severity level greater than or equal to MAJOR will be trapped out
- Critical—Syslogs generated with a severity level greater than or equal to CRITICAL and all alarms generated with a severity level greater than or equal to CRITICAL will be trapped out

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: 1.0 / Most recent update: 1.3

RTC Status

Unsupported

Notes

This is a multiple instance configuration element.

tunnel-orig-params

The **tunnel-orig-params** configuration element defines a single remote IKEv2 peer.

Syntax

```
tunnel-orig-params < name | remote-addr | retry-limit |
retry-time | batch | select | no | show | done | exit >
```

Parameters

name—Enter the name of this instance of the **tunnel-orig-params** configuration element.

Default	None
Values	A valid configuration element name, that is unique within the **tunnel-orig-params** namespace

remote-addr—Enter the IPv4 address of a remote IKEv2 peer.

Default	None
Values	Any valid IPv4 address

retry-limit—Set the number of times IKEv2 tries to initiate the tunnel. If this value is exceeded, IKEv2 abandons the initiation attempt and issues an SNMP trap.

Default	3
Values	Min: 1 | Max: 5

retry-time—Set the interval (in seconds) between initiation attempts.

Default	10 seconds
Values	Min: 5 | Max: 60

Path **tunnel-orig-params** is a subelement under the ike element. The full path from the topmost ACLI prompt is: **configure-terminal>security>ike>tunnel-orig-params**.

Release First appearance: S-C6.2.0

RTC Status Supported

Notes This is a multiple instance configuration element.

6 ACLI Command Summary

ACLI Commands

Command	Mode	Notes
acl-show	Superuser	
acquire-config	Superuser	
activate-config	Superuser	
archives	User	multi-parameter
arp-add	Superuser	
arp-check	Superuser	
arp-delete	Superuser	
backup-config	Superuser	
check-space-remaining	Superuser	
check-stack	Superuser	
clear-alarm	Superuser	
clear-cache	Superuser	multi-parameter
clear-deny	Superuser	
clear-sess	Superuser	multi-parameter
clear-trusted	Superuser	
cli	User	
configure	Superuser	
delete-backup-config	Superuser	
delete-config	Superuser	
delete-import	Superuser	
delete-status-file	Superuser	
display-alarms	User	
display-backups	User	
display-current-cfg-version	User	
display-logfiles	User	
display-running-cfg-version	User	
enable	User	

Command	Mode	Notes
exit	User	
generate-certificate-request	User	
generate-key	User	
format	Superuser	
import-certificate	User	
ipv6	Superuser	
kill	Superuser	
load-image	Superuser	
log-level	Superuser	
management	Superuser	
monitor	User	
notify	Superuser	
packet-capture	Superuser	
packet-trace	Superuser	multi-parameter
password-secure-mode	Superuser	
ping	User	
prompt-enabled	Superuser	
realm-specifics	User	
reboot	Superuser	
request	Superuser	multi-parameter
reset	Superuser	
restore-backup-config	Superuser	
save-config	Superuser	
secret	Superuser	
set-system-state	Superuser	
show	User	multi-parameter
ssh-password	Superuser	
ssh-pub-key	Superuser	
stack	Superuser	
stop-task	Superuser	
switchover-redundancy-link	Superuser	
systime-set	Superuser	
tail-logfile-close	Superuser	
tail-logfile-open	Superuser	

Command	Mode	Notes
tcb	Superuser	
test-audit-log	Superuser	
test-pattern-rule	User	multi-parameter
test-policy	User	multi-parameter
test-translation	User	multi-parameter
timezone-set	Superuser	
verify-config	Superuser	
watchdog	User	

Multi-parameter ACLI Commands

The archives, test-policy, test-translation, and show commands are multi-parameter commands. This means that the command's functionality is dependent on the first argument you pass to it.

Command	Parameter
archives	create
	delete
	display
	exit
	extract
	get
	rename
	send
clear-cache	dns
	enum
	tls
	registration
clear-sess	h323d
	sipd
packet-trace	start
	stop
request	audit
	collection
test-pattern-rule	expression

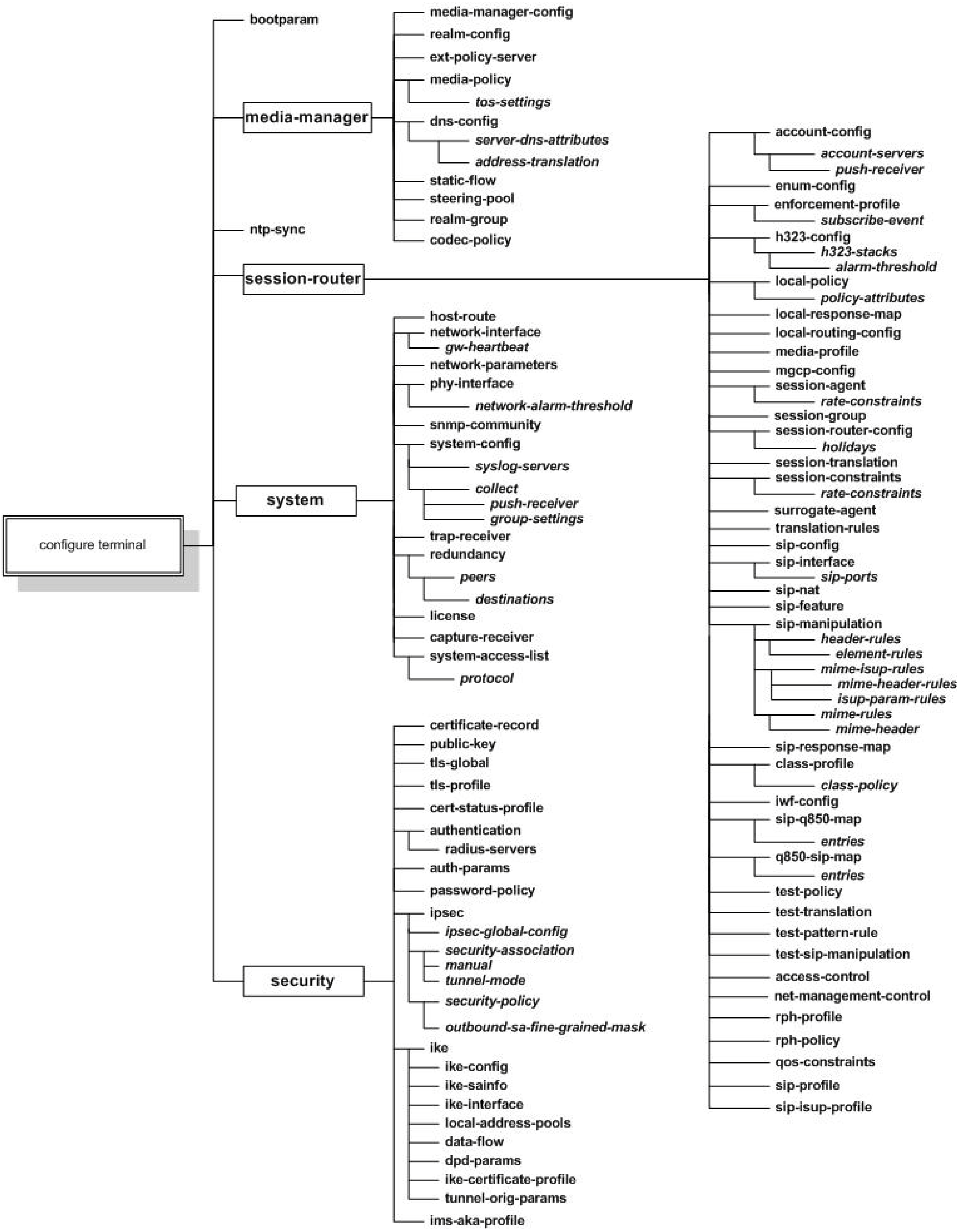
Command	Parameter
	string
	show
	exit
test-policy	carriers
	exit
	from-address
	media-profiles
	show
	source-realm
	time-of-day
	to-address
test-translation	called-address
	calling-address
	exit
	show
	translation-id
show	about
	acl
	algd
	arp
	backup-config
	buffers
	built-in-sip-manipulations
	call-recording-server
	certificates
	clock
	configuration
	directory
	dns
	enum
	ext-band-mgr
	ext-clf-svr
	features
	imports

	ip
	h323d
	health
	hosts
	interfaces
	ip
	logfile
	loglevel
	lrt
	mbcd
	media
	memory
	mgcp
	monthly-minutes
	nat
	net-management-control
	nsep
	packet-trace
	power

	privilege
	processes
	prom-info
	qos
	radius
	ramdrv
	realm
	redundancy
	registration
	route-stats
	routes
	running-config
	security
	sessions
	sipd
	snmp-community-table

	support-info
	system-state
	temperature
	trap-receiver
	uptime
	users
	version
	virtual-interfaces
	voltage

7 ACLI Configuration Element Tree


configure terminal
bootparam
media-manager
media-manager-config
realm-config
ext-policy-server
media-policy
tos-settings
dns-config
server-dns-attributes
address-translation
static-flow
steering-pool
realm-group
codec-policy
ntp-sync
session-router
system
host-route
network-interface
gw-heartbeat
network-parameters
phy-interface
network-alarm-threshold
snmp-community
system-config
syslog-servers
collect
push-receiver
group-settings
trap-receiver
redundancy
peers
destinations
license
capture-receiver
system-access-list
protocol
security
certificate-record
public-key
tls-global
tls-profile
cert-status-profile
authentication
radius-servers
auth-params
password-policy
ipsec
ipsec-global-config
security-association
manual
tunnel-mode
security-policy
outbound-sa-fine-grained-mask
ike
ike-config
ike-sainfo
ike-interface
local-address-pools
data-flow
dpd-params
ike-certificate-profile
tunnel-orig-params
ims-aka-profile
account-config
account-servers
push-receiver
enum-config
enforcement-profile
subscribe-event
h323-config
h323-stacks
alarm-threshold
local-policy
policy-attributes
local-response-map
local-routing-config
media-profile
mgcp-config
session-agent
rate-constraints
session-group
session-router-config
holidays
session-translation
session-constraints
rate-constraints
surrogate-agent
translation-rules
sip-config
sip-interface
sip-ports
sip-nat
sip-feature
sip-manipulation
header-rules
element-rules
mime-isup-rules
mime-header-rules
isup-param-rules
mime-rules
mime-header
sip-response-map
class-profile
class-policy
iwf-config
sip-q850-map
entries
q850-sip-map
entries
test-policy
test-translation
test-pattern-rule
test-sip-manipulation
access-control
net-management-control
rph-profile
rph-policy
qos-constraints
sip-profile
sip-isup-profile