Reference Guide

AudioCodes Gateway & Session Border Controller Series

Command-Line Interface (CLI)

Version 7.6

Notices

Information contained in this document is believed to be accurate and reliable at the time of publishing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of published material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: May-11-2025

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

Stay in the Loop with AudioCodes

Notes and Warnings

⚠ The device is an indoor unit and therefore, must be installed only **INDOORS**.

Configuration and usage of this device must be in accordance with your local security regulations, telephony regulations, or any other related regulations.

The scope of this document does not fully cover security aspects for deploying the device in your environment. Security measures should be done in accordance with your organization's security policies. For basic security guidelines, refer to the *Recommended Security Guidelines* document.

OPEN SOURCE SOFTWARE. Portions of the software may be open source software and may be governed by and distributed under open source licenses, such as the terms of the GNU General Public License (GPL), the terms of the Lesser General Public License (LGPL), BSD and LDAP. If any open source software is provided in object code, and its accompanying license requires that it be provided in source code as well, the Buyer may receive such source code by contacting AudioCodes.

- This device includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
- This device includes cryptographic software written by Eric Young (eay@cryptsoft.com).

Related Documentation

Document Name
SBC-Gateway Series Release Notes for Latest Release (LR) Versions
Installation Manuals
MP-1288 Analog Media Gateway Hardware Installation Manual
MP-1288 High-Density Analog Media Gateway Quick Guide
Mediant 500 E-SBC Hardware Installation Manual
Mediant 500L Gateway & E-SBC Hardware Installation Manual
Mediant 800 Gateway & E-SBC Hardware Installation Manual
Mediant 1000B Gateway and E-SBC Hardware Installation Manual
Mediant 3100 SBC and Media Gateway Hardware Installation Manual
Mediant 2600 E-SBC Hardware Installation Manual

Document Name
Mediant 4000B SBC Hardware Installation Manual
Mediant 9000 Series SBC Hardware Installation Manual
Mediant Cloud Edition SBC for Amazon AWS Installation Manual
Mediant Cloud Edition SBC for Microsoft Azure Installation Manual
Mediant Cloud Edition SBC for Google Cloud Installation Manual
Mediant Cloud Edition SBC for OpenStack-VMware-Private Cloud Installation Manual
Mediant Virtual Edition SBC for Amazon AWS Installation Manual
Mediant Virtual Edition SBC for Microsoft Azure Installation Manual
Mediant Virtual Edition SBC for Google Cloud Installation Manual
Mediant Virtual Edition SBC for VMware-KVM-HyperV Installation Manual
Mediant Virtual Edition SBC for Container Environments Installation Manual
Stack Manager for Mediant VE-CE SBC User's Manual
User's Manuals
MP-1288 High-Density Analog Media Gateway User's Manual
Mediant 500 Gateway & E-SBC User's Manual
Mediant 500L Gateway & E-SBC User's Manual
Mediant 800 Gateway & E-SBC User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 3100 Gateway and E-SBC User's Manual
Mediant 2600 E-SBC User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual

Document Revision Record

LTRT	Description
18039	Initial document release for Version 7.6 (7.60A.100.022) ■ New commands: a-secured-connectivity; encrypt-private-key-files; tls-subject-name (Local Users table); certificate create set-authority-information-access-ocsp; bfcp-ip-from-audio; emerg-alert-info-uri; reload-timeout-for-emergency-call; ha-file-transfer-port; ha-secure-file-transfer-port; alarm-raise-threshold; alarm-clear-threshold; password-expired-alarm; copy ext-core-dumps; erase ext-core-dumps ■ Updated commands: sshkex-algorithms-string (more cipher algorithms); write factory (new clear-keys-and-certs); certificate create signing-request (send to URL); show users (new option all); show debug-file reset-info (displays uptime); ro-community-string-psw (removed); rw-community-string-psw (removed); delete-ro-community-string (removed); delete-rw-community-string (removed); trusted-managers (removed); manager-ipv6-host-name removed); manager-host-name (removed); auto-send-keep-alive (removed); reset-community-string (removed); snmp-acl (removed); backup-server (removed); alt-rte-tel2ip-method (removed) ■ Miscellaneous: valid range displayed in error message for out-of-range value; SNMP configuration tables; command renames (as-subs-ipgroupname, notification-ip-group-name, presence-publish-ip-group-name, pstn-bus-local-reference; obsolete IP Profile commands (coders-group-id, sce, remote-base-udp-port, sbc-ext-coders-group-id, sbc-fax-coders-group-id, sbc-allowed-coders-group-id)

Table of Contents

1 Introduction

This document describes the Command-Line Interface (CLI) commands for configuring, monitoring and diagnosing AudioCodes Media Gateways and Session Border Controllers (SBC).

- For a detailed description of each command concerned with configuration, refer to the device's *User's Manual*.
- Some AudioCodes products referred to in this document may not have been released in this version. Therefore, ignore commands that are applicable only to these specific products. For a list of the products released in this version, refer to the *Release Notes* of the SBC and Media Gateway series, which can be downloaded from AudioCodes website.

Part I

Getting Started

2 Typographical Conventions

This document uses the following typographical conventions:

Table 2-1: Typographical Conventions

Convention	Description
bold font	Bold text indicates commands and keywords, for example: `ping 10.4.0.1 timeout 10`
< ... >	Text enclosed by angled brackets indicates Command for which you need to enter a value (digits or characters), for example: `ping <IP Address> timeout <Duration>`
|	The pipeline (or vertical bar) indicates a choice between commands or keywords, for example: `# reload {if-needed|now|without-saving}`
[...]	Keywords or command enclosed by square brackets indicate optional commands (i.e., not mandatory). This example shows two optional commands, size and repeat: `ping <IP Address> timeout <Duration> [size <Max Packet Size>] [repeat <1-300>]`
{...}	Keywords or command enclosed by curly brackets (braces) indicate a required (mandatory) choice, for example: `# reload {if-needed|now|without-saving}`

3 Accessing the CLI

You can access the device's CLI using the following methods:

- **RS-232:** Device's that are appliances (hardware) can be accessed through RS-232 by connecting a VT100 terminal to the device's console (serial) port or using a terminal emulation program (e.g., HyperTerminal®) with a PC. Once you have connected via a VT100 terminal and started the emulation program, set the program settings as follows:

  - 115200 baud rate
  - 8 data bits
  - No parity
  - 1 stop bit
  - No flow control

  For cabling your device's RS-232 interface (console port), refer to the device's *User's Manual* or *Hardware Installation Manual*.

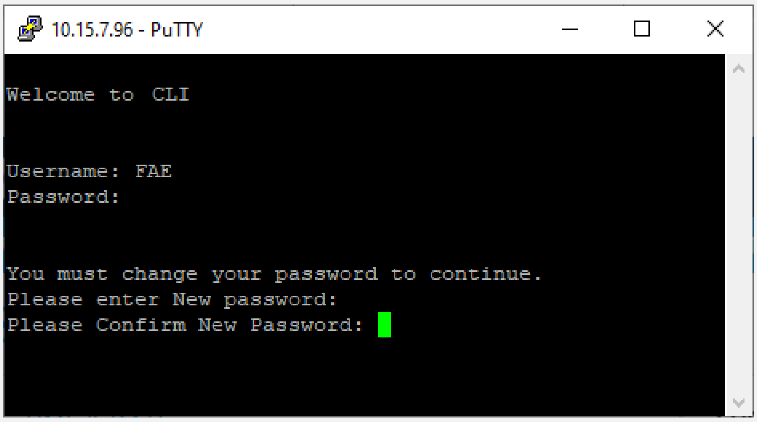
- **SSH:** For remote access, the device can be accessed through the SSH protocol using third-party SSH client software. A popular freeware SSH client software is PuTTY. By default, SSH access is disabled. To enable SSH, enter the following command set:

  ```
  # configure system
   (config-system)# cli-settings
   (cli-settings)# ssh on
  ```

- **Telnet:** For remote access, the device can be accessed through the Telnet protocol using third-party Telnet client software (e.g., PuTTY). Most Windows® computers come with a program called Telnet, which can be activated via the Windows command line:

  ```
  > telnet <Device's OAMP IP Address>
  Welcome to ...
  Username: <Username>
  Password: <Password>
  ```

- When accessing the device's CLI, you are prompted to enter your management username and password. The credentials are common to all the device's management interfaces (e.g., Web).
- If your 'Status' in the Local Users table is **New**, after entering your username and current password, you're prompted to change your password:



```
Welcome to CLI


Username: FAE
Password:


You must change your password to continue.
Please enter New password:
Please Confirm New Password:
```

After entering a new password in the 'New password' and 'Confirm New Password' fields, you're CLI session automatically closes and you need to log in again with your new password.

- The default username and password of the Administrator user level is **Admin** and **Admin**, respectively.
- The default username and password of the Monitor user level is **User** and **User**, respectively.
- You can enforce password complexity, using the `enforce-password-complexity` command. For a description of password complexity, refer to the User's Manual (WebUsers_Password).

4 CLI Command Modes

Before you begin your CLI session, it is recommended that you familiarize yourself with the CLI command modes. Each mode provides different levels of access to commands, as described below.

Basic User Mode

The Basic User command mode is accessed upon a successful CLI login authentication. Any user level can access the mode. The commands available under this mode are limited and only allow you to view information (using the show commands) and activate various debugging capabilities.

```
Welcome to ...
Username: Admin
Password: <Password>
>
```

The Basic User mode prompt is ">".

⚠ You can enforce password complexity, using the `enforce- password-complexity` command. For a description of password complexity, refer to the User's Manual (WebUsers_Password).

Privileged User Mode

The Privileged User command mode is the high-level tier in the command hierarchy, one step up from the Basic User mode. A password is required to access the mode **after** you have accessed the Basic User mode. The mode allows you to configure all the device's settings. Once you have logged in to the device, the Privileged User mode is accessed by entering the following commands:

> enable

```
Password: <Privileged User mode password>
#
```

The Privileged User mode prompt is "**#**".

- Only management users with Security Administrator or Master user levels can access the Privileged User mode.
- The default password for accessing the Privileged User mode is **Admin** (case-sensitive). To change this password, use the `privilege-password` command.
- If you enable RADIUS- or LDAP-based user login authentication, when users with Security Administrator privilege level log in to the device's CLI, they are automatically given access to the Privileged User mode.
- You can enforce password complexity, using the `enforce-password-complexity` command. For a description of password complexity, refer to the User's Manual (WebUsers_Password).

The Privileged User mode groups the configuration commands under the following configuration command sets:

Configuration Command Sets	Description
Network	Contains IP network-related commands (e.g., interface and dhcp-server). To access this command set: # configure network (config-network)#
System	Contains system-related commands (e.g., clock, snmp settings, and web). To access this command set: # configure system (config-system)#
Troubleshoot	Contains troubleshooting-related commands (e.g., syslog, logging and test-call). To access this command set: # configure troubleshoot (config-troubleshoot)#
VoIP	Contains voice-over-IP (VoIP) related commands (e.g., ip-group, sbc, and media). To access this command set: # configure voip (config-voip)#

Switching Command Modes

To switch between command modes, use the following commands on the root-level prompt:

- Switching from Basic User to Privileged User mode:

```
> enable
Password: <Password>
#
```

- Switching from Privileged User to Basic User mode:

```
# disable
>
```

5 CLI Shortcut Keys

The device's CLI supports the following shortcut keys to facilitate configuration.

Table 5-1: CLI Shortcut Keys

Shortcut Key	Description
↑↓↑	(Up and down arrow keys) Retypes the previously entered command (stored in the command history buffer). Continuing to press the key cycles through all commands entered, starting with the most recent command.
Tab	Pressing the key after entering a partial, but unique command automatically completes the command name.

?	(Question mark) Can be used for the following:
	■ To display commands pertaining to the command set, for example:
	`(config-network)# ?`
	`access-list Network access list`
	`dhcp-server     DHCP server configuration`
	`dns             DNS configuration`
	`...`
	■ To display commands beginning with certain letters. Enter the letter followed by the "?" mark (no space), for example:
	`(config-network)# d?`
	`dhcp-server     DHCP server configuration`
	`dns             DNS configuration`
	■ To display a description of a command. Enter the command followed by the "?" mark (no space), for example:

Shortcut Key	Description
	(config-network)#dns srv2ip? srv2ip SRV to IP internal table ■ To display all subcommands for the current command. Enter the command, a space, and then the "?" mark, for example: (config-network)# dns srv2ip ? [0-9] index If one of the listed items after running the "?" mark is "<cr>", a carriage return (Enter) can be entered to run the command, for example: show active-alarms ? <cr>
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 + U	Deletes all characters on the command line.
Space Bar	When pressed after "--MORE--" that appears at the end of a displayed list, the next items are displayed.

6 Common CLI Commands

The table below describes common CLI commands.

Table 6-1: Common CLI Commands

Command	Description

`| <filter>`	Filters a command's output by matching the filter string or expression, and thereby displaying only what you need. The syntax includes the command, the vertical bar (|) and then the filter expression:
	`<command>|<filter string or expression>`
	The filter expression can be any of the following:
	■ **include <string>:** Filters the output to display only lines with the string, for example:
	`# show running-config|include sbc routing ip2ip-routing 1`
	`sbc routing ip2ip-routing 1`
	■ **exclude <string>:** Filters the output to display all lines except the string.
	■ **egrep <expression>:** Filters the output according to common options of the "egrep" Unix utility.
	■ **begin <string>:** Filters the output to display all lines starting with the matched string, for example:
	`# show running-config|begin troubleshoot`
	` configure troubleshoot`
	`  syslog`
	`   syslog on`
	`   syslog-ip 10.8.94.236`
	`   activate`
	`  exit`
	`  activate`
	` exit`
	■ **between <string 1> <string 2>:** Filters the output to display only lines located between the matched string 1 (top line) and string 2 (last line). If a string contains a

Command	Description

	space(s), enclose the string in double quotes. For example, the string, sbc malicious-signature-database 0 contains spaces and is therefore enclosed in double quotes:
	# show running-config|between "sbc malicious-signature-database 0" exit
	  sbc malicious-signature-database 0
	   name "SIPVicious"
	   pattern "Header.User-Agent.content prefix 'friendly-scanner'"
	   activate
	  exit
	■ **count:** Displays the number of output lines.

`| tail <number of lines>`	Filters the command output to display a specified number of lines from the end of the output. The syntax includes the command of whose output you want to filter, the vertical bar (|) followed by the tail command, and then the number of lines to display:
	<command> | tail <number of lines (1-1000) to display>
	Below shows an example where the last five lines of the show running-config command output are displayed:
	# show running-config | tail 5
	    testcall-id "555"
	    activate
	   exit
	   activate
	  exit

`activate`	Applies (activates) the command setting. **Note:** ■ Offline configuration changes require a restart of the device. A restart can be performed at the end of your configuration changes. A required restart is indicated by an asterisk (*) before the command prompt, as shown

Command	Description

	in the following example.
	`(sip-def-settings)# user-inf-usage on`
	`(sip-def-settings)*#`
	To restart the device, use the `reload now` command (restarting the device by powering it off-on or by pressing the reset pinhole button doesn't preserve new configuration).
	- The command is applicable to SBC and Gateway functionality.

`defaults`	Restores the configuration of the currently accessed command set to factory default settings. For example, the below restores the Automatic Update configuration to factory defaults: `(auto-update)# defaults`
`descending`	Displays the command output in descending order, for example: `# show voip calls active descending` **Note:** Currently, this filter is supported only by certain show commands.
`display`	Displays the configuration of current configuration set.

`do`	Runs a command from another unrelated command without exiting the current command set. For example, the command to display all active alarms is run from the current command set for clock settings:
	`(clock)# do show active-alarms`
	The example below runs the `show running-config` command (which displays device configuration) from the current command set for clock settings:
	`(clock)# do show running-config`

Command	Description

`exit`	Leaves the current command-set and returns one level up. For online parameters, if the configuration was changed and no **activate** command was entered, the **exit** command applies the **activate** command automatically. If entered on the top level, the session ends.
	`(config-system)# exit`
	`# exit`
	`Connection to host lost.`

`first <x>`	Filters the command output to display only the first x number of entries. For example, the following displays only the first two entries: `# show voip calls history sbc first 2` **Note:** Currently, this filter is supported only by certain show commands.
`help`	Displays a short help how-to string.
`history`	Displays a list of previously run commands in the current CLI session in the command history buffer. You can also clear the command history buffer, using the `clear history` command.
`last <x>`	Filters the command output to display only the last x number of entries. For example, the following displays only the last four entries: `# show voip calls active last 4` **Note:** Currently, this filter is supported only by certain show commands.
`list`	Displays a list of the available commands list of the current command-set.
`match`	Filters the command output to display only entries with the matched string. For example, the following filters currently active SBC calls that contain the string "abc": `# show voip calls active sbc match abc`

Command	Description
	Note: Currently, this filter is supported only by certain show commands.

`no`	Undoes an issued command, disables a feature, or deletes a table row. Enter the **no** form before the command, for example:
	- Disables the debug log feature:
	`# no debug log`
	- Deletes the table row at Index 2:
	`<config-voip># no sbc routing ip2ip-routing 2`

`pwd`	Displays the full path to the current CLI command, for example:
	`(auto-update)# pwd`
	`/config-system/auto-update`

`quit`	Terminates the CLI session.
`range <x-y>`	Filters the command output to display only a specific range of entries from x to y. For example, the following only displays entries 1 to 4: `# show voip calls active range 1-4` **Note:** Currently, this filter is supported only by specific `show` commands.

`where`	Searches a table for a row index that contains a specific value for a specific table column. Use the following format:
	`<Table> where <Column Name> <Value>`
	The following example searches the IP Groups table for a row index whose table column 'name' contains the value "ITSP":
	`(config-voip)# ip-group where name ITSP`
	`(ip-group-1)#`

7 Working with Tables

This section describes general commands for configuring tables in the CLI.

Adding New Rows

When you add a new row to a table, it is automatically assigned to the next consecutive, available index.

Syntax

```
# <table name> new
```

Command Mode

Privileged User

Example

If the Accounts table is configured with three existing rows (account-0, account-1, and account-2) and a new row is added, account-3 is automatically created and its configuration mode is accessed:

```
(config-voip)# sip-definition account new
(account-3)#
```

Adding New Rows to Specific Indices

You can add a new row to any specific index number in the table, even if a row has already been configured for that index. The row that was assigned that index is incremented to the next consecutive index number, as well as all the index rows listed below it in the table.

Syntax

```
# <table name> <row index> insert
```

Note

The command is applicable only to the following tables:

- Firewall table (`access-list`)
- Message Manipulations table (`message-manipulations`)

- (SBC Only) IP-to-IP Routing table (`ip2ip-routing`)
- (SBC Only) Classification table (`classification`)
- (SBC Only) Message Conditions table (`condition-table`)
- (SBC Only) Inbound Manipulations table (`ip-inbound-manipulation`)
- (SBC Only) Outbound Manipulations table (`ip-outbound-manipulation`)
- (Gateway Only) Destination Phone Number Manipulation for IP-to-Tel Calls table (`dst-number-map-ip2tel`)
- (Gateway Only) Destination Phone Number Manipulation for Tel-to-IP Calls table (`dst-number-map-tel2ip`)
- (Gateway Only) Source Phone Number Manipulation for IP-to-Tel Calls table (`src-number-map-ip2tel`)
- (Gateway Only) Source Phone Number Manipulation for Tel-to-IP Calls table (`src-number-map-tel2ip`)
- (Gateway Only) Calling Name Manipulation for Tel-to-IP Calls table (`calling-name-map-tel2ip`)
- (Gateway Only) Calling Name Manipulation for IP-to-Tel Calls table (`calling-name-map-ip2tel`)
- (Gateway Only) Redirect Number Tel-to-IP table (`redirect-number-map-tel2ip`)

Command Mode

Privileged User

Example

If the IP-to-IP Routing table is configured with three existing rows (ip2ip-routing-0, ip2ip-routing-1, and ip2ip-routing-2) and a new row is added at Index 1, the previous ip2ip-routing-1 becomes ip2ip-routing-2, the previous ip2ip-routing-2 becomes ip2ip-routing-3, and so on:

```
(config-voip)# sbc routing ip2ip routing 1 insert
(ip2ip-routing-1)#
```

Changing Index Position of Rows

You can change the position (index) of a table row, by moving it one row up or one row down in the table.

Syntax

```
# <table name> <row index> move-up|move-down
```

Note

The command is applicable only to certain tables.

Command Mode

Privileged User

Example

Moving row at Index 1 down to Index 2 in the IP-to-IP Routing table:

```
<config-voip># sbc routing ip2ip-routing 1 move-down
```

Deleting Table Rows

You can delete a specific table row, by using the no command.

Syntax

```
# no <table name> <row index to delete>
```

Command Mode

Privileged User

Example

This example deletes a table row at Index 2 in the IP-to-IP Routing table:

```
<config-voip># no sbc routing ip2ip-routing 2
```

8 CLI Error Messages

The table below lists and configures common error messages given in the CLI.

Table 8-1: CLI Error Messages

Message	Helpful Hints
"Invalid command"	The command may be invalid in the current command mode or you may not have entered sufficient characters for the command to be recognized.
"Incomplete command"	You may not have entered all of the pertinent information required to make the command valid. To view available Command associated with the command, enter a question mark (?) on the command line.

"Invalid argument"	You have entered an invalid value (argument) for the command.
	For commands that require an integer within a specific range, the error message displays the valid range when you enter a value outside of it, for example:
	`(cli-settings)# window-height 70000`
	`Invalid argument "70000". Value must be in range [0-65535]`

9 Running Multiple Non-Interactive SSH Commands from Command Line

You can configure the device with multiple, non-interactive SSH (CLI) commands from a command-line connection, instead of using a terminal emulator program (e.g., PuTTY). Unlike terminal emulator programs, the command line has no user prompts and is similar to Unix SSH. This feature may be useful, for example, if you want to run a batch of SSH commands via automated connections.

As an SSH client, you can run the command-line connection tool (e.g., PuTTY Link or Plink) from a computer's command prompt. For computers running Windows, this can be done using the Command Prompt command-line app. When you enter a command, it's executed on the device instead of through a login shell.

You can enter multiple commands on the **single** command line, including standalone commands and command sequences. Separate each command with a semicolon (;).

The command-line syntax depends on the command-line connection tool that you are using to connect to the device. The following are examples using the Plink command-line connection tool:

- To display network interfaces and CPU status (i.e., `show` commands):

```
C:\projects\tftp>plink.exe -no-antispoof -ssh 10.4.30.11 -l Admin -pwd Admin
"sh run ne int; sh sys util"
```

- To configure the syslog server's IP address:

```
C:\projects\tftp>plink.exe -no-antispoof -ssh 10.4.30.11 -l Admin -pwd Admin
"conf tr; sys; syslog-ip 10.4.2.11; act"
```

- To configure commands that are located in two different CLI paths:

```
C:\projects\tftp>plink.exe -no-antispoof -ssh 10.4.30.11 -l Admin -pwd Admin
"conf voip; sip-definition settings; 100-to-18x-timeout 100; exit; exit; show
system utilization"
```

- This feature is applicable only to non-interactive commands.
- This feature is not supported for async commands (e.g., `ping`).
- You can enter up to 8,000 characters on the command line (input).
- When using the command line, no other SSH connections (sessions) can be established with the device.
- The device's Activity Log (see Reporting Management User Activities) also logs the commands executed from the command line (which are indicated in syslog as "Activity Log: Executing multiple CLI commands").

10 CLI Configuration Wizard

AudioCodes CLI Wizard provides a quick-and-easy tool for configuring your device with basic, initial management settings:

- Login passwords for the Security Administrator (**Admin**) and User Monitor user accounts for accessing the device's embedded Web and CLI servers.
- IP network of the operations, administration, maintenance, and provisioning (OAMP) interface
- SNMP community strings (read-only and read-write)

The utility is typically used for first-time configuration of the device and is performed through a direct RS-232 serial cable connection with a computer. Configuration is done using the device's CLI. Once configured through the utility, you can access the device's management interface through the IP network.

Prerequisites for CLI Wizard

To use the CLI Wizard, you must be connected to the device through a direct serial connection and the device must be running with factory defaults. If you have performed any device configuration prior to using the CLI Wizard, follow the procedure below to restore the device to factory defaults.

➢ **To restore device to factory defaults:**

1. At the CLI prompt #, type the following, and then press Enter; the device starts the restoring-to-factory defaults process. This may take a few minutes.

```
# write factory
Writing factory default and restarting ...
```

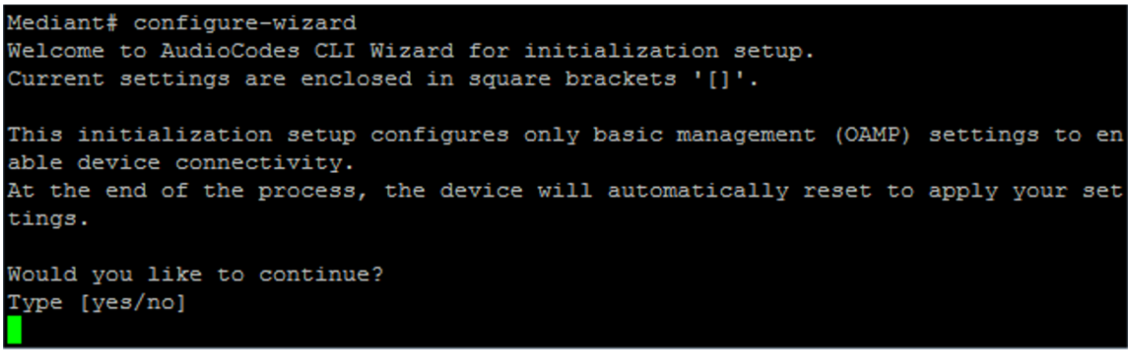
2. When the device has restored to factory defaults, you are prompted to log in to the CLI. Log in to the CLI, and then continue with the procedure for accessing the CLI Wizard (see Starting CLI Wizard below).

Starting CLI Wizard

Once you have met the prerequisites (see Prerequisites for CLI Wizard above), you can start the CLI Wizard.

➢ **To start the CLI Wizard:**

1. At the root-prompt level #, type the `configure-wizard` command, and then press Enter; the CLI Wizard mode is accessed and you are prompted to confirm continuation of the wizard:



```
Mediant# configure-wizard
Welcome to AudioCodes CLI Wizard for initialization setup.
Current settings are enclosed in square brackets '[]'.

This initialization setup configures only basic management (OAMP) settings to en
able device connectivity.
At the end of the process, the device will automatically reset to apply your set
tings.

Would you like to continue?
Type [yes/no]
```

2. Type the following to continue, and then press Enter:

```
yes
```

If you type no, the CLI Wizard closes and you are returned to the "privileged" mode (indicated by the # prompt).

Configuring Device through CLI Wizard

Once you have accessed the CLI Wizard, the wizard prompts you along to configure the device's management settings in the following order:

1. Web/CLI users' login passwords
2. OAMP network settings
3. SNMP community strings

As you complete a configuration topic (listed above), the wizard prompts you for the next topic. You can skip a specific configuration topic and accept default settings by typing the no command when prompted. Within each configuration topic, you can accept the default value of a parameter and skip to the next parameter, by simply pressing the Enter key.

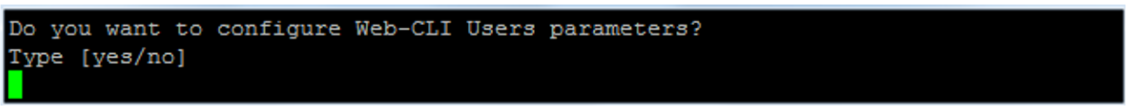
- For each parameter, the CLI wizard displays the current setting enclosed in square brackets [...].
- If you do not make any changes to parameter values in the CLI Wizard, at the end of the last configuration stage (i.e., SNMP settings), the CLI Wizard quits and returns you to the initial CLI prompt.

Configuring Web and CLI Login Password

The first configuration stage prompted by the wizard concerns Web/CLI users' login passwords. These passwords are for the Security Administrator (**Admin**) user account and User Monitor user account (read-only).

➢ To configure Web/CLI users' login password:

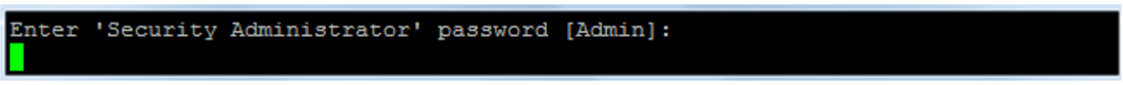
1. When you first access the CLI Wizard and have confirmed to continue, you are prompted to configure the login passwords:



```
Do you want to configure Web-CLI Users parameters?
Type [yes/no]
```

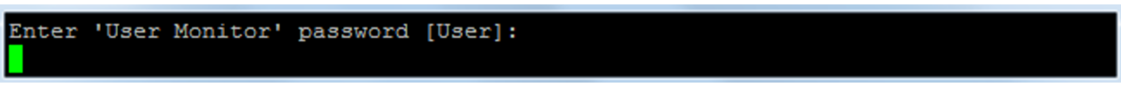
Type `yes` to begin this configuration stage, and then press Enter. Otherwise, if you want to leave the settings at default values, type `no` to skip this stage and continue with the next stage.

2. At the prompt, type the new password for the Administrator user account, and then press Enter:



```
Enter 'Security Administrator' password [Admin]:
```

3. At the prompt, type the new password for the Monitor user account, and then press Enter:



```
Enter 'User Monitor' password [User]:
```

4. The wizard prompts you for configuring the OAMP network settings. Continue with the OAMP network configuration stage, as described in Configuring OAMP Network Interface below.

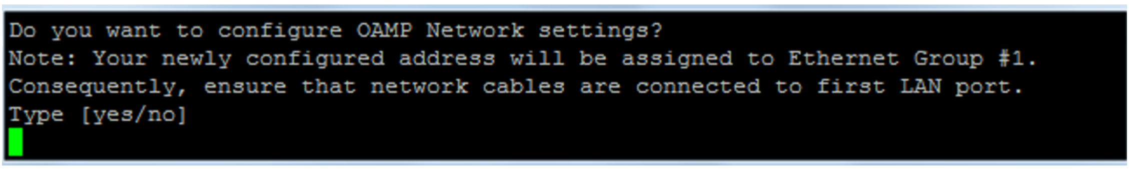
Configuring OAMP Network Interface

The second configuration stage prompted by the wizard concerns OAMP network settings. This is the interface used for accessing the device's management platform over the IP network and includes the following configuration:

- IP address
- Prefix length
- VLAN ID
- Default Gateway
- Primary and secondary Domain Name Server (DNS) addresses

➢ To configure OAMP network settings:

1. When the Web/CLI users' login passwords configuration stage is complete, you are prompted to configure the OAMP network settings:

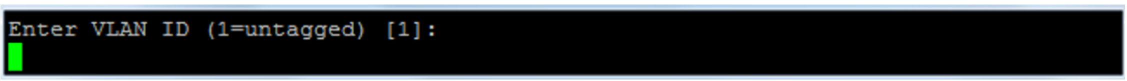


```
Do you want to configure OAMP Network settings?
Note: Your newly configured address will be assigned to Ethernet Group #1.
Consequently, ensure that network cables are connected to first LAN port.
Type [yes/no]
```

Before continuing, make a note of the Ethernet port mentioned in the screen above with which this OAMP interface is associated. When you later cable the device to the IP network after the wizard has applied your settings, you must use this port.

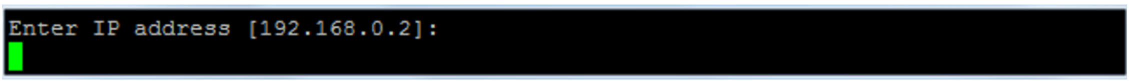
Type `yes` to begin this configuration stage, and then press Enter. Otherwise, if you wish to leave the settings at default values, type `no` to skip this stage and continue with the next stage as described in Configuring SNMP Community Strings below.

2. At the prompt, type the VLAN ID, and then press Enter:



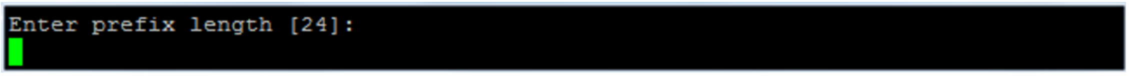
```
Enter VLAN ID (1=untagged) [1]:
```

3. At the prompt, type the IP address, and then press Enter:



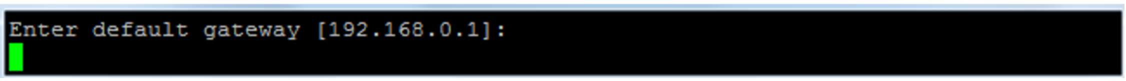
```
Enter IP address [192.168.0.2]:
```

4. At the prompt, type the prefix length (in CIDR notation), and then press Enter:



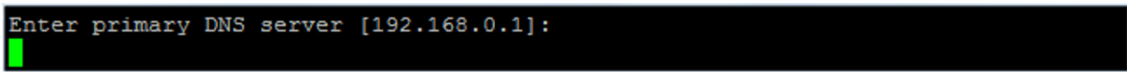
```
Enter prefix length [24]:
```

5. At the prompt, type the Default Gateway address, and then press Enter:



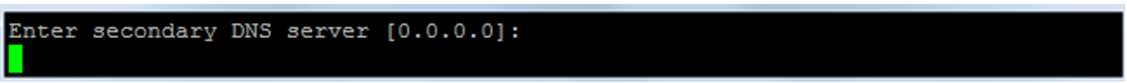
```
Enter default gateway [192.168.0.1]:
```

6. At the prompt, type the primary DNS address, and then press Enter:



```
Enter primary DNS server [192.168.0.1]:
```

7. At the prompt, type the secondary DNS address, and then press Enter:



```
Enter secondary DNS server [0.0.0.0]:
```

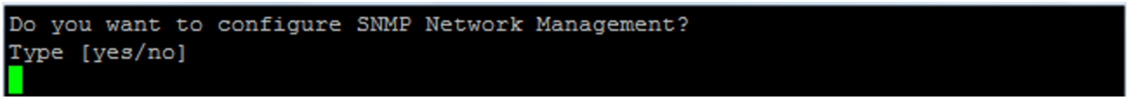
8. The wizard prompts you for configuring the SNMP settings. Continue with the SNMP configuration stage, described in Configuring SNMP Community Strings below.

Configuring SNMP Community Strings

The last configuration stage prompted by the wizard concerns SNMP settings. This concerns SNMP read-only and read-write community strings.

➢ To configure SNMP settings:

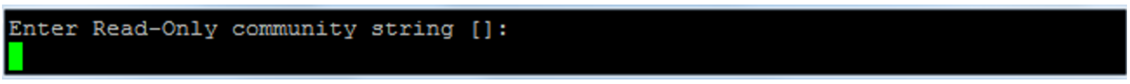
1. When the OAMP network configuration stage is complete, you are prompted to configure the SNMP settings:



```
Do you want to configure SNMP Network Management?
Type [yes/no]
```

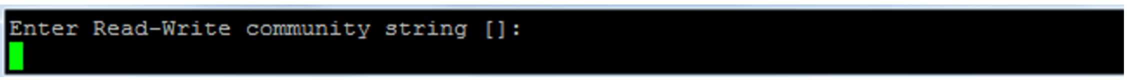
Type `yes` to begin the SNMP configuration stage, and then press Enter. Otherwise, if you wish to leave the settings at default values, type `no` to skip this stage and continue with the final stage of confirming your settings as described in Confirming Configuration Settings below.

2. At the prompt, type the read-only SNMP community string, and then press Enter:



```
Enter Read-Only community string []:
```

3. At the prompt, type the read-write SNMP community string, and then press Enter:



```
Enter Read-Write community string []:
```

4. The wizard prompts you to confirm all your configuration settings done in the CLI Wizard. Continue with the procedure for confirming configuration, described in Confirming Configuration Settings below.

Confirming Configuration Settings

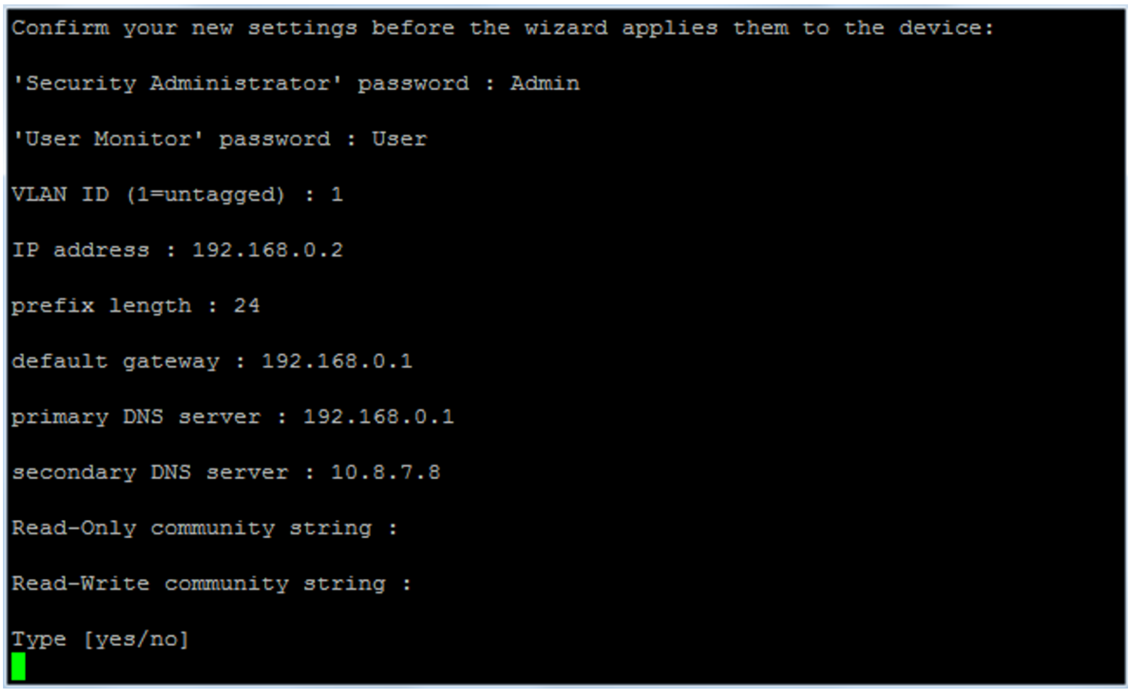
Once you have completed the last configuration stage (i.e., SNMP settings described in Configuring SNMP Community Strings on the previous page), you are prompted by the CLI Wizard to confirm all your configuration settings. Once confirmed, the CLI Wizard applies your settings to the device's flash memory (with a device restart).

⚠

- After you have confirmed your settings and the CLI Wizard has applied them to your device, you cannot use the CLI Wizard again unless you restore the device to factory defaults, as described in Prerequisites for CLI Wizard on page 22.
- If you did not make any changes in the CLI Wizard, after the last stage in the CLI Wizard, you are exited from the wizard and returned to the enable mode prompt `#`.

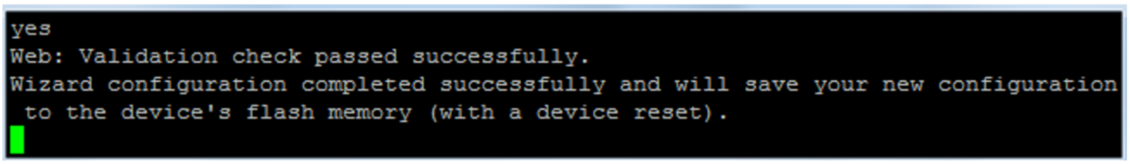
➢ To confirm and apply your settings:

1. When the last configuration stage is complete, the wizard prompts you to confirm your settings. The CLI Wizard displays all its configurable parameters with their values (default or user-defined), as shown in the example below:



```
Confirm your new settings before the wizard applies them to the device:

'Security Administrator' password : Admin

'User Monitor' password : User

VLAN ID (1=untagged) : 1

IP address : 192.168.0.2

prefix length : 24

default gateway : 192.168.0.1

primary DNS server : 192.168.0.1

secondary DNS server : 10.8.7.8

Read-Only community string :

Read-Write community string :

Type [yes/no]
```

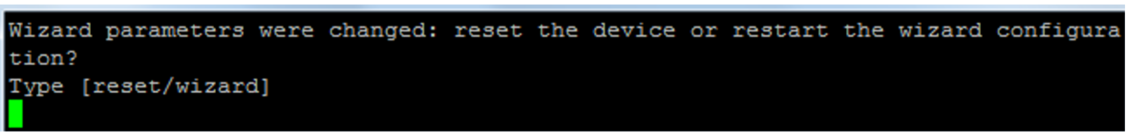
2. To confirm your settings, type `yes`, and then press Enter; the CLI Wizard checks that your configuration is valid and if yes, saves the configuration to the device's flash memory with a device restart. This may take a few minutes. (Otherwise, `type` no to skip this step and continue with Step 3.)



```
yes
Web: Validation check passed successfully.
Wizard configuration completed successfully and will save your new configuration
 to the device's flash memory (with a device reset).
```

When the CLI Wizard finishes saving your configuration, you are exited from the CLI Wizard and returned to the CLI prompt that appears when CLI sessions are initially established.

3. If you typed `no` in Step 2 above, the wizard prompts you with two options:



```
Wizard parameters were changed: reset the device or restart the wizard configura
tion?
Type [reset/wizard]
```

- `reset`: Restarts the device without applying your settings (i.e., remains at default settings) and quits the CLI Wizard, returning you to the initial CLI prompt.
- `wizard`: Returns you to the beginning of the CLI Wizard (i.e., Web/CLI users' password configuration stage), allowing you to start your configuration from scratch. Your previous settings in the CLI Wizard are ignored and remain at default.

Part II

Root-Level Commands

11 Introduction

This part describes commands located at the root level, which includes the following main commands:

Command	Description
`debug`	See Debug Commands on page 30
`show`	See Show Commands on page 56
`clear`	See Clear Commands on page 123
Maintenance commands	See General Root Commands on page 132

12 Debug Commands

This section describes the debug commands.

Syntax

```
# debug
```

This command includes the following commands:

Command	Description
`auxilary-files`	See debug auxilary-files on the next page
`capture`	See debug capture on page 33
`cli`	See debug cli delayed-command on page 39
`debug-recording`	See debug debug-recording on page 40
`dial-plan`	See debug dial plan on page 42
`exception-info`	See debug exception-info on page 43
`exception-syslog-history`	See debug exception-syslog-history on page 44
`fax`	See debug fax on page 44
`ha`	See debug ha on page 45
`log`	See debug log on page 46
`pstn`	See pstn-debug on page 262
`reset-history`	See debug reset-history on page 48
`reset-syslog-history`	See debug reset-syslog-history on page 49
`sip`	See debug sip on page 49
`speedtest`	See debug speedtest on page 50
`syslog`	See debug syslog on page 51
`syslog-server`	See debug syslog-server on page 51
`test-call`	See debug test-call on page 52

Command	Description
`usb`	See debug usb on page 54
`voip`	See debug voip on page 55

debug auxilary-files

This command debugs loaded Auxiliary files.

Syntax

```
# debug auxilary-files {dial-plan|user-info}
```

Command	Description
`dial-plan`	Debugs the dial plan (see debug auxilary-files dial-plan below).
`user-info`	Debugs the User Info file (see debug auxilary-files user-info on the next page).

Command Mode

Privileged User

debug auxilary-files dial-plan

This command debugs the Dial Plan file.

Syntax

```
# debug auxilary-files dial-plan {info|match-number <Dial Plan Number> <Prefix Number>}
```

<table>
<tr><th>Command</th><th colspan="2">Description</th></tr>
<tr><td><code>info</code></td><td colspan="2">Displays the loaded Dial Plan file and lists the names of its configured Dial Plans.</td></tr>
<tr><td rowspan="2"><code>match-number</code></td><td colspan="2">Checks whether a specific prefix number is configured in a specific Dial Plan number. If the Dial Plan is used for tags, the command also shows the tag name.</td></tr>
<tr><td>Dial Plan Number</td><td>Defines the Dial Plan in which to search for the</td></tr>
</table>

Command	Description	
		specified prefix number.
	Prefix Number	Defines the prefix number to search for in the Dial Plan.

Note

The index number of the first Dial Plan is 0.

Command Mode

Privileged User

Example

Checking if the called prefix number 2000 is configured in Dial Plan 1, which is used for obtaining the destination IP address (tag):

```
# debug auxilary-files dial-plan match-number PLAN1 2000
Match found for 4 digits
Matched prefix: 2000
Tag: 10.33.45.92
```

Displaying the loaded Dial Plan file and listing its configured Dial Plans:

```
# debug auxilary-files dial-plan info
  File Name: dialPlan.txt
  Plans:
  Plan #0 = PLAN1
  Plan #1 = PLAN2
```

debug auxilary-files user-info

This command displays the name of the User-Info file installed on the device.

Syntax

```
# debug auxilary-files user-info info
```

Command Mode

Privileged User

Example

Displaying the name of the User-Info file installed on the device:

```
# debug auxilary-files user-info info
User Info File Name UIF_SBC.txt
```

debug capture

This command captures network traffic.

Syntax

```
# debug capture {rpcap-server|trim|voip}
```

Command	Description
rpcap-server	See debug capture rpcap-server below
trim	See debug capture trim on the next page
voip	See debug capture voip on page 35

Command Mode

Privileged User

debug capture rpcap-server

This command starts the device's embedded rpcap server for capturing packets on the network, so that Wireshark clients can start/stop packet capturing, collect the captured packets, and filter them for analysis.

This command also configures the first and second port of the rpcap server. The first port is an always-open listening port for initial connections (by default, 2002). The second port (by default, dynamically allocated) is sent to the client during the initial connection to open a new TCP connection for the captured packets

Syntax

```
# debug capture rpcap-server {start [<First Port>]}
```

```
# debug capture rpcap-server {start [<Second Port>]}
# debug capture rpcap-server stop
```

Command	Description
`start <First Port>`	Starts the rpcap server. Optionally, you can also configure the first port for the remote packet capture sessions with Wireshark. By default, the device uses port 2002.
`start <First Port Already Configured> <Second Port>`	(Optional) Configures the second port of the device's rpcap server. By default, the device dynamically allocates the port number. **Note:** Configure the first port before the second port.
`stop`	Stops packet capturing by the rpcap server.

Command Mode

Privileged User

Example

This example starts the rpcap server and configures the first port to 2000 and the second port to 2004:

```
# debug capture rpcap-server start 2000
rpcap server started successfully on port 2000

# debug capture rpcap-server start 2000 2004
```

or

```
# debug capture rpcap-server start 2000 2004
```

debug capture trim

This command trims captured network traffic for USB captures.

Syntax

```
# debug capture trim {in-file <File>|offset <Time>}
```

Command	Description
`in-file`	Trims captured traffic. Uses the existing file on USB storage.
`offset`	After a capture has been saved on an attached USB stick, you can trim the capture to include only a relevant time-slice. The command is useful when fetching a large capture file via SSH over a slow network connection. Offset is from the start of the capture, in hours:minutes:seconds.

Command Mode

Privileged User

Example

Offsetting 1 hour 20 minutes from start of capture in order to trim captured USB traffic:

```
debug capture trim offset 00:01:20
```

debug capture voip

This command captures network traffic on VoIP network interfaces.

Syntax

```
# debug capture voip {interface|physical}
```

Command	Description
`interface`	Captures network traffic on one of the VoIP sub-system network interfaces. See debug capture voip interface below
`physical`	Captures traffic on the wire. See debug capture voip physical on page 37

debug capture voip interface

This command defines and starts debug capturing (recording) of network traffic on a specific VoIP network interface.

The debug capture starts when you run the command. To stop the capture, press Ctrl+C. When stopped and a server is defined, the device then sends the captured traffic (.pcap file) to the server.

Syntax

```
# debug capture voip interface {kernel-dev <Name>|vlan <VLAN ID>} proto
<Protocol Filter> host <Host Filter> port <Port Filter>
[tftp-server <TFTP Server IPv4 or IPv6 Address>|ftp-server <FTP Server IPv4 or
IPv6 Address>]
```

Command	Description
`kernel-dev`	Defines an interface on which to debug capture by its kernel name (e.g., `eth0`, `eth1`, `lo`, or `tun0`) instead of by VLAN. You can use this option, for example, to record packets on the interface used for WebSocket tunneling. To specify all kernels, type `any`.
`vlan`	Defines the VLAN ID (instead of kernel interface) of the network interface on which to debug capture.
`proto`	Defines the protocol filter: ■ `all` (all protocols) ■ `arp` (ARP packets) ■ `icmp` (ICMP packets) ■ `ip` (IP packets) ■ `ipv6` (IPv6 packets) ■ `tcp` (TCP packets) ■ `udp` (UDP packets)
`host`	Defines the host (IP address) from/to which the packets are captured. To specify all hosts, type `any`.
`port`	(Optional) Defines the port filter (1-65535 or `any` for all ports). When using `arp` or `icmp` as the protocol filter, port filter can't be used and the only valid value is `any`.
`ftp-server`	(Optional) Defines the IP address of the FTP server to which the captured traffic file (.pcap) is sent. If not specified, captured traffic is displayed in the CLI console. After running the command, press Ctrl+C when you want the capture to end and the captured traffic file to be sent to the server. **Note:** The FTP server's IP address must be accessible from one

Command	Description
	of the VoIP network interfaces for the capture file to be successfully sent to the server. Ping the server to make sure it's accessible.
`tftp-server`	(Optional) Defines the IP address of the TFTP server to which the captured traffic file (.pcap) is sent. If not specified, captured traffic is displayed in the CLI console. After running the command, press Ctrl+C when you want the capture to end and the captured traffic file to be sent to the server. **Note:** The TFTP server's IP address must be accessible from one of the VoIP network interfaces for the capture file to be successfully sent to the server. Ping the server to make sure it's accessible.

Command Mode

Privileged User

Examples

Starting a debug capture on network interface VLAN 12, no host filter, and no port filter; the captured traffic is displayed in the CLI console:

```
# debug capture voip interface vlan 12 proto all host any
```

Starting a debug capture on network interface VLAN 1 with a protocol filter (IP), no host filter, and a port filter (514); the captured traffic is saved to a temporary file and is sent (when you press Ctrl+C) to the TFTP server at address 171.18.1.21:

```
# debug capture voip interface vlan 1 proto ip host any port 514 tftp-server
171.18.1.21
```

debug capture voip physical

This command captures network traffic on a physical VoIP network interface.

Syntax

```
# debug capture voip physical {clear|cyclic-buffer|eth-lan|get_last_capture|insert-
pad|show|start|stop|target}
```

```
# debug capture voip physical target {ftp|tftp|usb}
# debug capture voip physical get_last_capture <TFTP/FTP Server IP Address>
```

- To start a capture:

```
# debug capture voip physical start
```

- To stop a capture:

```
# debug capture voip physical stop {<TFTP/FTP server IP Address>|usb}
```

Command	Description
clear	Deletes captured files from the device's RAM.
cyclic-buffer	Continuously captures packets in a cyclical buffer. Packets are continuously captured until the **Stop** command is entered.
eth-lan	Captures LAN frames.
get_last_capture	Retrieves the last captured PCAP file sent to a specified TFTP/FTP server IP address (IPv4 or IPv6). **Note:** The file is saved to the device's memory (not flash) and is erased after a device restart.
insert-pad	Before running this command, the debug capture must be started. Inserts a PAD packet. A marked packet is shown with black background regardless of the configured coloring rules. Benefit: A marked packet can easily be located later when analyzing in a large capture file.
show	Displays debug status and configured rules.
start	Starts the capture.
stop	Stops the capture and sends the capture file to the specified target (IPv4 or IPv6). The captured file is called "debug-capture-voip-<timestamp>.pcap".
target	Defines the capture storage target: ■ ftp ■ tftp ■ usb

Command	Description	
	user	(Only applicable if ftp is specified as the capture storage target) Defines the name of the FTP user.
	password	(Only applicable if ftp is specified as the capture storage target) Defines the password of the FTP user.

Command Mode

Privileged User

Note

- To free up memory on your device, it is recommended to delete the captured files when you no longer need them, using the following command: **debug capture voip physical clear**
- Capturing to USB is applicable only to devices providing USB port interfaces.
- The command is applicable only to MP-1288, Mediant 5xx, Mediant 8xx; Mediant 1000B, Mediant 2600 and Mediant 4000.

Examples

- Starting a physical VoIP debug capture:

```
# debug capture voip physical eth-lan
# debug capture voip physical start
```

- Retrieving the latest capture (PCAP file) saved on a specified server.

```
# debug capture voip physical get_last_capture 10.15.7.99
```

- Specifying USB as the destination to which to send the PCAP file:

```
# debug capture voip physical target usb
```

debug cli delayed-command

This command allows you to run a specified command after a user-defined interval.

Syntax

```
# debug cli delayed-command
```

Command	Description
`<Delay Time> {minutes|seconds} '<Command Name>'`	Configures how much time (in minutes or seconds) to wait before running a specific command. The entire command path must be specified and enclosed in apostrophe. To denote carriage returns in the path, use semi-colons (;).
`cancel <Command Number>`	Cancels the delayed timer for a specific command.
`show`	Displays configured delayed commands whose timers have not yet expired.

Command Mode

Privileged User

Example

This example performs a firmware upgrade after 10 minutes:

```
# debug cli delayed-command 10 minutes ‘copy firmware from
http://10.3.1.2:1400/tftp/SIP_F7.20A.150.001.cmp’
```

debug debug-recording

This command enables debug recording for all trunks.

To collect debug recording packets, use Wireshark open-source packet capturing program. AudioCodes' proprietary plug-in files are required. They can be downloaded from https://www.audiocodes.com/library/firmware. After starting Wireshark, type acdr in the 'Filter' field to view the debug recording messages. Note that the source IP address of the messages is always the device's OAMP IP address.

Syntax

```
# debug debug-recording <Destination IP Address> {ip-trace|port|pstn-
trace|signaling|signaling-media|signaling-media-pcm}
# debug debug-recording status
```

Command	Description
Destination IP Address	Defines the destination IP address (IPv4) to which to send the debug recording (i.e., debug recording server).
`ip-trace`	Defines the debug recording filter type. Filters debug recording for IP network traces, using Wireshark-like expression (e.g., udp && ip.addr==10.8.6.55). IP traces are used to record any IP stream according to destination and/or source IP address, or port and Layer-4 protocol (UDP, TCP or any other IP type as defined by http://www.iana.com). Network traces are typically used to record HTTP.
`port`	Defines the port of the debug recording server to which to send the debug recording.
`pstn-trace`	Defines the debug recording capture type as PSTN trace. The debug recording includes ISDN and CAS traces.
`signaling`	Defines the debug recording capture type as signaling. The debug recording includes signaling information such as SIP signaling messages, Syslog messages, CDRs, and the device's internal processing messages
`signaling-media`	Defines the debug recording capture type as signaling and media. The debug recording includes signaling, Syslog messages, and media (RTP/RTCP/T.38).
`signaling-media-pcm`	Defines the debug recording capture type as signaling, media and PCM. The debug recording includes SIP signalling messages, Syslog messages, media, and PCM (voice signals from and to TDM).
`status`	Displays the debug recording status.

Command Mode

Privileged User

Note

- To configure the PSTN trace level per trunk, use the following command: `configure voip > interface > trace-level`
- To send the PSTN trace to a Syslog server (instead of Wireshark), use the following command:`configure troubleshoot > pstn-debug`

- To configure and start a PSTN trace per trunk, use the following command: `configure troubleshoot > logging logging-filters`

Example

Displaying the debug recording status:

```
# debug debug-recording status
Debug Recording Configuration:
===============================
Debug Recording Destination IP: 10.33.5.231
Debug Recording Destination Port: 925
Debug Recording Status: Stop

Logging Filter Configuration (line 0):
=======================================
Filter Type: Any
Value:
Capture Type: Signaling
Log Destination: Syslog Server
Mode: Enable
```

debug dial plan

This command checks whether a specified Dial Plan contains specific digits.

Syntax

```
debug dial-plan <Dial Plan Name> match-digits <Digits to Match>
```

Command Mode

Basic and Privileged User

Example

Searching for digits "2000" in Dial Plan 1:

```
debug dial-plan 1 match-digits 2000
Match succeeded for dial plan 1 and dialed number 2000. Returned tag RmoteUser
```

debug exception-info

This command displays debug information about exceptions.

Syntax

```
# debug exception-info
```

Command	Description
`<Exception Number>`	Displays debug information of a specified exception number.

Command Mode

Privileged User

Example

This example shows how to display debug information related to exception 1:

```
# debug exception-info 1
There are 10 Exceptions
Exception Info of Exception 1:
Trap Message - Force system crash(0) due to HW Watchdog
Board Was Crashed: Signal 0, Task
BOARD MAC : 00908F5B1035
EXCEPTION TIME : 0.0.0 0.0.0
VERSION: Time 13.5.25, Date 16.12.16, major 720, minor 90, fix 485 Cmp
Name:ramESBC_SIP Board Type:77
RELATED DUMP FILE : core_E-SBC_ver_720-90-485_bid_5b1035-177_SIP
ZERO:00000000 AT:00000000 V0:00000000 V1:00000000 A0:00000000
A1:00000000 A2:00000000 A3:00000000
T0:00000000 T1:00000000 T2:00000000 T3:00000000 T4:00000000
T5:00000000 T6:00000000 T7:00000000
S0:00000000 S1:00000000 S2:00000000 S3:00000000 S4:00000000
S5:00000000 S6:00000000 S7:00000000
T8:00000000 T9:00000000 K0:00000000 K1:00000000 GP:00000000
SP:00000000 FP:00000000
stack_t - ss_sp:00000000 ss_size:00000000 ss_flags:00000000
PC:00000000            +0
RA:00000000            +0
```

debug exception-syslog-history

This command displays the syslog generated for exceptions.

Syntax

```
# debug exception-syslog-history <0-9>
```

Where *0* is the latest syslog generated due to an exception.

Command Mode

Privileged User

Example

This example shows how to display the last two syslog-related exceptions:

```
# debug exception-syslog-history 1
```

debug fax

This command debugs fax modem with a debug level.

Syntax

```
# debug fax
```

Command	Description
`basic`	Defines debug fax level to Basic. You can define the number of next sessions for debug.
`detail`	Defines debug fax level to Detail. You can define the number of next sessions for debug.

Note

- The command is applicable only to devices supporting FXS interfaces.
- To disable debug fax, type no debug fax.

Command Mode

Privileged User

Example

This example configures detailed fax debug for the next 10 sessions to be traced:

```
# debug fax detail 10
FaxModem debug has been activated in DETAIL mode. The 10 next FaxModem
sessions will be traced.
```

debug ha

This command debugs High Availability (HA).

Syntax

```
# debug ha
```

Command	Description
`clear-counters`	Clears the counters of sent and received HA keep-alive packets periodically sent between Active and Redundant devices.
`conn-to-red`	Connects to the Redundant device from the Active device through Telnet.
`disconnect-system <OAMP Address of Redundant Device>`	Disables HA mode and returns the two devices to stand-alone devices. In addition, the Redundant device is assigned the specified OAMP address.
`restart-tpncp-conn`	Restarts the HA control protocol between the Active and Redundant devices (for internal debug usage).

Note

The command is applicable only to devices supporting HA.

Command Mode

Privileged User

Example

This example accesses the Redundant device from the Active device, and then disconnects HA mode, assigning the Redundant device with a new OAMP address 212.4.55.7:

```
# debug ha conn-to-red

Username: Admin
Password:

> enable
Password:
# debug ha disconnect-system 212.4.55.7
```

debug log

This command displays debugging messages (e.g., Syslog messages). Also displays activities performed by management users in the devices' management interfaces (CLI and Web interface).

Syntax

```
debug log [full]
```

Command	Description
`full`	(Optional) Displays more information than the regular debug messages, for example, 'SID' (Session ID) and 'S' (Syslog message sequence). Useful (for example) in determining if there's a network problem resulting from a Loss of Packets.

Note

- When connected to the CLI through Telnet/SSH, the debug log command affects only the current CLI session.
- To disable logging, type **no debug log**.
  - When connected to the CLI through Telnet/SSH, the **no debug log** command affects only the current CLI session.
  - To cancel log display for all sessions, use the command **no debug log all**.

Command Mode

Basic and Privileged User

Example

Displaying debug messages:

```
debug log
Logging started
Jun 16 13:58:54  Resource SIPMessage deleted - (#144)
Jun 16 13:58:54  (#70) SBCRoutesIterator Deallocated.
Jun 16 13:58:54  (#283) FEATURE Deallocated.
```

Displaying debug messages (full):

```
debug log full
Logging started
Jun 16 13:59:55 local0.notice [S=707517] [SID:1192090812]
(sip_stack)(706869) Resource SIP Message deleted - (#79)
Jun 16 13:59:55 local0.notice [S=707518] [SID:1192090812]
(lgr_sbc)(706870)(#69) SBCRoutesIterator Deallocated.
Jun 16 13:59:55 local0.notice [S=707519] [SID:1192090812]
(lgr_sbc)(706871) (#282) FEATURE Deallocated.
```

debug os-util

This command enables the device to send CPU and memory utilization to the Syslog server. This is typically used for debugging only.

Syntax

```
debug os-util {cpu|memory} [interval]
```

Command	Description
`cpu [interval 0-1000 sec]`	Sends CPU utilization to syslog. You can optionally configure the interval for sending the utilization.
`memory [interval 0-1000 sec]`	Sends memory utilization to syslog. You can optionally configure the interval for sending the utilization.

Command Mode

Basic and Privileged User

Example

This example enables the sending of CPU utilization to syslog every 30 seconds:

```
debug os-util cpu 30
debug_os_util was enabled
```

debug reset-history

This command displays a history (last 20) of device restarts and the reasons for the restarts (for example, a restart initiated by the user through the Web interface).

Syntax

```
# debug reset-history
```

Command Mode

Privileged User

Example

This example shows restarts debug history:

```
# debug reset-history
Reset History :
Reset History [00]:
Reset Reason: an exception
Time : 6-1-2010 21:17:31
FIRMWARE: Time 12.3.20, Date 8.5.17, major 720, minor 140, fix 716
Reset Syslog Counter 214
************************************************
Reset History [01]:
Reset Reason: issuing of a reset from Web interface
Time : 1-1-2010 00:15:26
FIRMWARE: Time 12.3.20, Date 8.5.17, major 720, minor 140, fix 716
Reset Syslog Counter 213
************************************************
Reset History [02]:
Reset Reason: issuing of a reset from Web interface
Time : 3-1-2010 20:52:03
FIRMWARE: Time 12.3.20, Date 8.5.17, major 720, minor 140, fix 716
Reset Syslog Counter 212
************************************************
Reset History [03]:
 -- More -
```

debug reset-syslog-history

This command displays a history (last 20) of syslogs generated upon device restarts.

Syntax

```
# debug reset-syslog-history <0-19>
```

Where 0 is the latest syslog.

Command Mode

Privileged User

Example

This example debugs the latest syslog restart history:

```
# debug reset-syslog-history
```

debug sip

This command configures SIP debug level.

Syntax

```
# debug sip {[<Debug Level>]|status}
```

Command	Description
Debug Level	Defines the SIP debug level: ■ 0 = (No debug) Debug is disabled and Syslog messages are not sent. ■ 1 = (Basic) Sends debug logs of incoming and outgoing SIP messages. ■ 5 = (Detailed) Sends debug logs of incoming and outgoing SIP messages as well as many other logged processes.
`status`	Displays the current debug level.

Note

- If no level is specified, level 5 is used.
- Typing no debug sip configures the level to 0.

Command Mode

Privileged User

Example

Setting the SIP debug level to 5:

```
# debug sip 5
```

debug speedtest

This command tests the upload and download speed (in bps) to and from a specified URL, respectively.

Syntax

```
# debug speedtest set {upload|download} <URL>
# debug speedtest set upsize <Upload Transfer Bytes>
# debug speedtest {run|show|stop}
```

Command	Description
`upload`	Tests the upload speed to a URL (IP address or FQDN).
`upsize`	(Optional) Defines the number of bytes (1-10000000) to upload to the specified URL for testing the upload speed
`download`	Tests the download speed from a URL (IP address or FQDN).
`show`	Displays the test results.
`stop`	Stops the test.
`run`	Starts the test.

Example

Testing upload speed to speedy.com:

```
# debug speedtest set upload http://www.speedy.com/speedtest
  Upload URL  : http://www.speedy.com/speedtest
```

```
# debug speedtest run
Starting speed test. Check results using the command "debug speedtest show".
```

```
# debug speedtest show
Speed test results:
Upload  : Complete
URL: http://www.speedy.com/speedtest
            Bytes transferred: 1000000
            Speed: 9.8 Mbps
```

debug syslog

This command verifies that Syslog messages sent by the device are received by the Syslog server. After you run the command, you need to check the Syslog server to verify whether it has received your Syslog message.

Syntax

```
# debug syslog <String>
```

Command	Description
String	Configures any characters that you want to send in the Syslog message to the Syslog server.

Command Mode

Privileged User

Related Commands

debug syslog-server

Example

Verifying that a Syslog message containing "hello Joe" is sent to the Syslog server:

```
# debug syslog hello Joe
```

debug syslog-server

This command configures the IP address and port of the Syslog server.

Syntax

```
# debug syslog-server <IP Address> port <Port Number>
```

Command	Description
IP Address	Defines the IP address of the Syslog server.
`port`	Defines the port number of the Syslog server.

Note

To disable Syslog server debugging, use the following command:

```
# no debug syslog-server
```

Command Mode

Privileged User

Example

Enabling Syslog by configuring the Syslog server:

```
# debug syslog-server 10.15.1.0 port 514
Syslog enabled to dest IP Address: 10.15.1.0 Port 514
```

debug test-call

This command initiates and terminates a call from the device to a remote destination to test whether, for example, connectivity and media are correct. The device sends a SIP INVITE message and then manages the call with the call recipient.

Syntax

```
debug test-call ip
```

- Configures a test call:

```
debug test-call ip dial from {<Calling Number> to <Called Number> [dest-address <IP Address>] [sip-interface <SIP Interface ID>]|id <Test Call Table Index>}
```

- Configures a test call:

```
debug test-call ip set called-number <Called number> caller-id <Caller ID>
calling-number <Calling number>dest-address
<IP Address> play <Playback> sip-interfaces <SIP Interface ID> timeout
<Disconnection timeout> transport-type
```

- Terminates a test call:

```
debug test-call ip drop {<Calling Number>|id <Test Call Table Index>}
```

- Displays test call configuration:

```
debug test-call ip show
```

Command	Description
`ip`	Configures and initiates a test call to an IP address. ■ dial (Dials using specified parameters) ✓ from (Defines the calling number): ✓ [NUMBER] (Calling number) ✓ **id** (uses the Test Call Rules table entry) ■ **drop** (Terminates the latest outgoing test call): ✓ [Calling Number] (Terminates outgoing test call by number) ✓ id (Terminates outgoing test calls by table index) ■ **set** (Sets test options): ✓ **called-number** (Called number) ✓ **caller-id** (Caller ID) ✓ **calling-number** (Calling number) ✓ **dest-address** (Target host) ✓ **play** (Sets playback) ✓ **sip-interfaces** (Sets SIP interfaces to listen on)

Command	Description
	✓ **timeout** (Disconnection timeout (seconds)) ✓ **transport-type** (Transport type) ■ **show** (Displays test call configuration)

Command Mode

Basic and Privileged User

Note

- The command is applicable only to the SBC application.
- Test calls can be made with the following two recommended commands:
  - (Basic) Making a call from one phone number to another, without performing any configuration:

    ```
    debug test-call ip dial from * to * dest-address * [sip-interface *]
    ```

  - (Advanced) Configuring a row in the Test Call table, and then placing a call by the row index:

    ```
    debug test-call ip dial from id *
    ```

debug usb

This command debugs the USB stick connected to the device.

Syntax

```
# debug usb devices
```

Command	Description
`devices`	Displays information about the USB stick (e.g., manufacturer) connected to the device.

Command Mode

Privileged User

debug voip

This command debugs voice over IP channels.

```
# debug voip
```

Command	Description
`activate-channel {analog|digital|virtual} <Channel ID>`	Configures a specific channel.
`close-channels {analog|digital|virtual}`	Closes channels. To view the orientation of the device's hardware, use the command, show system assembly.
`dial-string {analog|digital|virtual}`	Sends a string of DTMF tones. To view the orientation of the device's hardware, use the command, show system assembly.
`open-and-activate {analog|digital|virtual}`	Opens and activates a channel. To view the orientation of the device's hardware, use the command, show system assembly.
`open-channel {analog|digital|virtual} <Channel ID>`	Opens a channel .
`wait-for-detection`	Waits for a digit detection event

Command Mode

Privileged User

13 Show Commands

This section describes the show commands.

Syntax

```
show
```

This command includes the following commands:

Command	Description
`activity-log`	See show activity-log on the next page
`alias`	See show alias on page 58
`admin state`	See show admin state on page 58
`cloud-manager-log`	See show cloud-manager-log on page 59
`debug-file`	See show debug-file on page 59
`high-availability`	See show high-availability on page 63
`ini-file`	See show ini-file on page 64
`kpi`	See show kpi on page 65
`last-cli-script-log`	See show last-cli-script-log on page 69
`network`	See show network on page 70
`running-config`	See show running-config on page 79
`sctp`	See show sctp on page 81
`startup-script`	See show startup-script on page 83
`storage-history`	See show storage-history on page 84
`system`	See show system on page 84
`users`	See show users on page 98
`voip`	See show voip on page 99

show activity-log

This command displays the device's Activity Log, which logs operations done in the device's management interfaces (e.g., CLI and Web interface).

Syntax

```
show activity-log
```

Command	Description
`(Carriage Return)`	Displays all logged message history.
`> <URL>`	Sends the logged activities to a remote server (TFTP or HTTP/S).

Command Mode

Basic and Privileged User

Note

If you have not enabled logging of user activities in the management interface, nothing is displayed in the output of this show command. To enable logging, see the following command:

```
configure troubleshoot > activity-log
```

Related Commands

- `configure troubleshoot > activity-log`: Enables logging of operations in the management interface.
- `password-history-visible`: Hides passwords in the Activity Log.

Example

This example displays the logged messages:

```
show activity log
activity-log 126: user 'Admin' via Telnet (10.13.2.3) time: 05/01/2023, 09:33:32 CLI:
'show activity-log ?'
activity-log 125: user 'Admin' via Telnet (10.13.2.3) time: 05/01/2023, 09:33:27 CLI:
'e'
activity-log 124: user 'Admin' via Telnet (10.13.2.3) time: 05/01/2023, 09:33:26
```

```
Successful user login
activity-log 121: user 'Admin' via Web (10.13.2.3) time: 05/01/2023, 09:31:47
Successful user login at 10.15.7.96:80
```

show admin state

This command displays the device's current administrative state (locked or unlocked).

Syntax

```
show admin state
```

Command Mode

Basic and Privileged User

Related Command

admin state – locks or unlocks the device.

Example

This example displays the administrative state of the device (which is unlocked):

```
# show admin state
current admin-state: unlock
```

show alias

This command displays the alias CLI commands, configured by the `cli-alias` command.

Syntax

```
show alias
```

Command Mode

Basic and Privileged User

Related Commands

`cli-alias`

Example

```
# show alias
Alias: conf | Command: show running-config
Alias: Copy | Command: copy from
```

show cloud-manager-log

This command displays the Cloud Manager logs .

Syntax

```
show cloud-manager-log
```

Command	Description
`(Carriage Return)`	Displays all logged message.

Command Mode

Basic and Privileged User

Related Command

`tail cloud-manager-log`

Note

The command is applicable only to Mediant VE/CE SBC (Cloud Manager).

Example

This example displays logged messages:

```
show cloud-manager-log
time="2022-04-27T11:30:40Z" level=info msg="*** init-db ***"
time="2022-04-27T11:30:40Z" level=debug msg="EXEC: command '/sbin/fw_
printenv [network_layout]' completed. output: network_layout=1\n"
time="2022-04-27T11:30:40Z" level=info msg="NW layout set to 1 from env (1)"
```

show debug-file

This command displays the debug file.

Syntax

```
show debug-file
```

Command	Description
`device-logs`	See show debug-file device-logs below
`reset-info`	See show debug-file reset-info on the next page

Command Mode

Basic and Privileged User

show debug-file device-logs

This command displays the device's debug file.

Syntax

```
show debug-file device-logs
```

Command	Description
`file <File Name>`	Displays the contents of a specified debug file (listed using the below command).
`list`	Displays a list of the debug files (e.g., ssbc-last-install.log and ssbc-rescue-install.log).

Command Mode

Basic and Privileged User

Example

This example displays the list of debug files:

```
show debug-file device-logs list
 DebugFile Device File: ssbc-last-install.log, ssbc-rescue-install.log,
```

show debug-file reset-info

This command displays logged device restarts in the debug file.

Syntax

```
show debug-file reset-info
```

Command	Description
list	Displays a list of logged device restarts. Each logged restart is numbered sequentially, displaying device uptime before the restart, reason for the restart, when the restart occurred, and the software version, for example: ** Current Reset Counter [84] ** ***** Reset ***** Reset Counter:83 Up Time (seconds): 237890 Reset Reason: a hardware reset Reset Time: 5.3.2025 2:24:18 SwVersion: ram_ESBC_SIP 760A-092-799 ************** If the restart was caused due to an error (i.e., crash), "Exception" (instead of "Reset") is displayed at the beginning of the logged restart, as shown in the following example: ***** Exception ***** Reset Counter:24 Exception Reason: CMX Kernel Panic EXCEPTION TIME : 4.9.2020 10.21.46 **************
reset-counter <Reset Counter> [file <File Name>]	Displays a logged device restart, specified by its Counter number (use the above command to view all the logged restarts and their Counter numbers). The output also shows any associated logged files. To view the file contents in the output, specify the file after the counter number, for example: M800B*# show debug-file reset-info reset-counter 83 Reset Files [syslog,no-sip]

Command	Description
	** Summary ** ***** Reset ***** Reset Counter:83 Up Time (seconds): 237890 Reset Reason: a hardware reset Reset Time: 5.3.2025 2:24:18 SwVersion: ramMP500_ESBC_SIP 760A-092-799 ************** `# show debug-file reset-info reset-counter 23 syslog`

Command Mode

Basic and Privileged User

Example

This example displays the list of logged device restarts:

```
M800B*# show debug-file reset-info list
** Current Reset Counter [84] **

***** Reset     *****
Reset Counter:83
Up Time (seconds): 237890
Reset Reason: a hardware reset
Reset Time: 5.3.2025 2:24:18
SwVersion: ramMP500_ESBC_SIP 760A-092-799
**************

***** Reset     *****
Reset Counter:82
Up Time (seconds): 436739
Reset Reason: a hardware reset
Reset Time: 2.3.2025 8:18:26
SwVersion: ramMP500_ESBC_SIP 760A-092-770
**************
```

show high-availability

This command displays network monitor status and HA status.

Syntax

```
show high-availability {network-monitor-status|status}
```

Command	Description
`network-monitor-status`	Displays HA Network Monitor status.
`status`	Displays HA status.

Related Commands

- debug ha on page 45
- ha
- high-availability

Command Mode

Basic and Privileged User

Example

- To display HA status:

```
# show high-availability status
HA Status:
Unit HA state is: Active
HA Connection with other unit State is: Connected
Last HA sync. action/state with other unit was: Sync. ended !
```

- To display HA Network Monitor status:

```
# show high-availability network-monitor-status
HA Network monitor is enabled
Number of unreachable table entries: 0
Entries status:
Table row 0: Reachability status is: Reachable, Destination peers status:
        Peer address 10.4.4.69: Reachability status is: Reachable, ping loss
```

```
percentage: 0%
Table row 1: Reachability status is: Reachable, Destination peers status:
        Peer address 10.5.5.5: Reachability status is: Reachable, ping loss
percentage: 0%
        Peer address 10.5.5.6: Reachability status is: Reachable, ping loss
percentage: 0%
Note - ping loss percentage refer to the last 5 minutes
```

show ini-file

This command displays the device's current configuration in ini-file format.

Syntax

```
show ini-file
```

Command Mode

Privileged User

Example

```
# show ini-file
;**************
;** Ini File **
;**************
;Board: M800B
;Board Type: 72
;Serial Number: 5967925
;Software Version: 7.40A.200.194
;DSP Software Version: 5014AE3_R => 724.12
;Board IP Address: 10.15.7.96
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;CPU: Cavium Networks Octeon V0.1 @ 500Mhz, total 2 core(s), 2 cpu(s), 1 socket
(s)
;Core(s) mapping:
;core #0, on cpu #0, on socket #0
;core #1, on cpu #1, on socket #0

--MORE--
```

show kpi

This command displays the 15-minute measurement intervals and values for the device's performance monitoring parameters.

Syntax

```
show kpi {current|interval}
```

Command	Description
`current`	See show kpi current below
`interval`	See show kpi interval on page 67

Command Mode

Basic and Privileged User

show kpi current

This command displays the current measured value (statistics) of performance monitoring parameters. The parameters are organized in a hierarchical tree (path), where the highest nodes include Gateway, Media, Network, SBC, and System. To view a performance monitoring parameter, simply drill down through the path of descendants to where the performance monitoring parameter is located.

Syntax

```
show kpi current {display|gateway|media|network|sbc|system}
```

Command	Description
`display`	Displays available descendants at the current path of the hierarchical tree of the performance monitoring parameters. To view all the performance monitoring parameters belonging to the last descendant in a path, enter a space and then question mark (?) at the end of the command line.
`gateway`	Displays the performance monitoring parameters related to the Gateway application.
`media`	Displays the performance monitoring parameters related to media.

Command	Description
`network`	Displays the performance monitoring parameters related to the network.
`sbc`	Displays the performance monitoring parameters related to the SBC application.
`system`	Displays the performance monitoring parameters related to the system.

Command Mode

Basic and Privileged User

Note

- A value of "null" indicates that the value of the performance monitoring parameter doesn't exist at the requested interval.

Example

- This example displays the next sub-nodes (descendants) under the path media/coderstats:

```
# show kpi current media coderstats display
 global                  (global)
 ipgroup                  (ipGroup)
```

- This example lists all the performance monitoring parameters under the path media/coderstats/global (using the ? at the end of the command line):

```
# show kpi current media coderstats global
coderg711               Shows Number of active channels with G.711 coder
current value
coderg711alaw             Shows Number of active channels with G.711alaw
coder current value
coderg711ulaw             Shows Number of active channels with G.711ulaw
coder current value
....
```

- This example displays the measured value of the performance monitoring parameter, memoryutilization:

```
# show kpi  current system systemstats global memoryutilization
Name                     Value
memoryUtilization      68
```

- This example displays the measured value of a specific index entity for the performance monitoring parameter, cpuutilization:

```
# show kpi current system cpustats cpu 0 cpuutilization

 Name                     Value
0
 cpuUtilization                27
```

show kpi interval

This command displays the measured values (statistics) of "historical" performance monitoring parameters for specific measured intervals (15-minute). These intervals are stored on the device - some up to four intervals and some up to 100 intervals. The interval is specified by its index number, which increments for each new interval.

Syntax

```
show kpi interval {<Interval Index>|all|last}
```

Command	Description
Interval Index	Displays the stored 15-minute interval of a specific interval index (start and end time). It can also be used to display the value of a specific 15-minute interval for a specific performance monitoring parameter. You can use the `all` option (see below) to view all available interval index numbers of a performance monitoring parameter. You can then calculate the index number that you want to view. For example, if you want to view the value of the second latest interval and the `all` option displayed interval indices 1 through 4, you would run the command with interval 3.
`all [gateway|media|network|sbc|system]`	Displays all the stored 15-minute intervals (interval index, and start and end time). It can also displays the values of all the stored 15-minute intervals for a specific performance monitoring

Command	Description
	parameter.
`last [gateway|media|network|sbc|system]`	Displays the last (latest) stored 15-minute interval (interval index, and start and end time). It can also display the value of the last stored 15-minute interval for a specific performance monitoring parameter.

Command Mode

Basic and Privileged User

Note

- If a specific interval doesn't exist or the interval is invalid (for whatever reason), "Item not found" is displayed.
- If there are no valid intervals (for whatever reason), no intervals are displayed when running the command `show kpi interval all`.

Example

- These examples display information of the stored 15-minute intervals (index and start and end times):
  - This example displays all the 15-minute intervals (interval indices, and start and end times):

```
# show kpi interval all
Interval Start Time         End Time            Status
  103     15/10/2020 15:15:00 15/10/2020 15:30:10 Valid
  102     15/10/2020 15:00:09 15/10/2020 15:15:00 Valid
  101     15/10/2020 14:45:10 15/10/2020 15:00:09 Valid
  100     15/10/2020 14:30:10 15/10/2020 14:45:10 Valid
  99      15/10/2020 14:15:10 15/10/2020 14:30:10 Valid
  98      15/10/2020 14:00:10 15/10/2020 14:15:10 Valid
  97      15/10/2020 13:45:00 15/10/2020 14:00:10 Valid
...
```

  - This example displays the last (most recently) stored 15-minute interval (interval index, and start and end time):

```
# show kpi interval last
Interval Index  103
```

```
Start Time     15/10/2020 15:15:00
End Time       15/10/2020 15:30:10
Interval Status Valid
```

- This example displays the specific 15-minute interval index #100 (start and end time):

```
# show kpi interval 100
Interval Index  100
Start Time     15/10/2020 14:30:10
End Time       15/10/2020 14:45:10
Interval Status Valid
```

- This example displays the values of all the 15-minute intervals for the performance monitoring parameter, memoryutilizationmax:

```
# show kpi interval all system systemstats global memoryutilizationmax
Name                          Interval   Value
memoryUtilizationMax
                                   16          68
                                   15          68
                                   14          62
                                   13          60
                                   12          60
....
```

- This example displays the value of the 15-minute interval index #11 for the performance monitoring parameter, memoryutilizationmax:

```
# show kpi interval 11 system systemstats global memoryutilizationmax

 Name                                Value
 memoryUtilizationMax                  68
```

show last-cli-script-log

This command displays the contents of the latest CLI Script file that was loaded (i.e., copy cli-script from) to the device. The device always keeps a log file of the most recently loaded CLI Script file.

Syntax

```
# show last-cli-script-log
```

Command Mode

Privileged User

Note

If the device restarts (or powers off), the logged CLI Script file is deleted.

Example

```
# show last-cli-script-log
---------------
# LOG CREATED ON: 26/04/2017   16:21:56
# Running Configuration
# IP NETWORK
# configure network
(config-network)# tls 0
(tls-0)# name default
(tls-0)# tls-version unlimited
...
```

show network

This command displays networking information.

Syntax

```
show network
```

Command	Description
`access-list`	See show network access-list on the next page
`arp`	See show network arp on the next page
`default-ca-bundle`	See show network default ca bundle on page 72
`dhcp clients`	See show network dhcp clients on page 73
`ether-group`	See show network ether-group on page 74
`http-proxy`	See show network http-proxy on page 74
`interface`	See show network interface on page 75

Command	Description
`network-dev`	See show network network-dev on page 77
`ovoc-tunnel`	See show network ovoc-tunnel on page 77
`physical-port`	See show network physical-port on page 78
`route`	See show network route on page 78
`tls`	See show network tls on page 79

Command Mode

Basic and Privileged User

show network access-list

This command displays the network access list (firewall) rules, which are configured in the Firewall table.

Syntax

```
show network access-list
```

Command Mode

Basic and Privileged User

Example

```
show network access-list
 L#  Source IP  /Pref SrcPort Port Range    Protocol  Action Count
---- --------------- ---- ------- ------------- --------  ------
0  10.6.6.7    /  0      0    0 - 65535  Any     ALLOW   616
Total 1 active firewall rules.
```

show network arp

This command displays the device's ARP entries. The 'Type' column in the command's output displays static ARP mappings as "permanent" and dynamic ARP mappings as "reachable".

Syntax

```
show network arp
```

Command Mode

Basic and Privileged User

Related Commands

`static-arp-table` - Defines the Static ARP table.

Example

```
show network arp
IP Address   MAC Address        Eth Device   Type
10.15.0.1    00:1c:7f:3f:a9:5d   vlan 1        reachable
10.15.2.1    00:1b:17:00:02:40   vlan 2          permanent

End of ARP table (2 entries displayed _
```

show network default ca bundle

This command displays the default certificate authorities (CA).

Syntax

```
show network default-ca-bundle {detail|status|summary}
```

Command	Description
`detail <CA index>`	Displays detailed information of a specific CA. The index number can be obtained from the command `show network default-ca-bundle summary`.
`status`	Displays if the device currently supports default CAs.
`summary`	Displays a summary of all the default CAs.

Command Mode

Basic and Privileged User

Example

This example displays the detailed information of the CA that is listed for index 30:

```
# show network default-ca-bundle detail 30
### Default CA Bundle Certificate 30
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 6643877497813316402 (0x5c33cb622c5fb332)
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN=Atos TrustedRoot 2011, O=Atos, C=DE
Validity
Not Before: Jul  7 14:58:30 2011 GMT
Not After : Dec 31 23:59:59 2030 GMT
Subject: CN=Atos TrustedRoot 2011, O=Atos, C=DE
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:95:85:3b:97:6f:2a:3b:2e:3b:cf:a6:f3:29:35:
be:cf:18:ac:3e:aa:d9:f8:4d:a0:3e:1a:47:b9:bc:
9a:df:f2:fe:cc:3e:47:e8:7a:96:c2:24:8e:35:f4:
a9:0c:fc:82:fd:6d:c1:72:62:27:bd:ea:6b:eb:e7:
8a:cc:54:3e:9
....
```

show network dhcp clients

This command displays DHCP server leases.

Syntax

```
show network dhcp clients
```

Command Mode

Basic and Privileged User

Example

```
show network dhcp clients
Total 0 leases.
```

show network ether-group

This command displays the Ethernet Groups, which are configured in the Ethernet Groups table.

Syntax

```
show network ether-group
```

Command Mode

Basic and Privileged User

Example

```
show network ether-group
G. Num  Group Name    Mode       State Uplinks     Group Members
 ------  --------------  -------------------  ----- -------
0     GROUP_1   REDUN_1RX_1TX/2  Up    1    GE_4_1  ,GE_4_2
1     GROUP_2   REDUN_1RX_1TX/2  Down  0    GE_4_3  ,GE_4_4
2     GROUP_3   GROUP_TYPE_NON/0 Up    0           ,
3     GROUP_4   GROUP_TYPE_NON/0 Up    0           ,
```

show network http-proxy

This command displays the NGINX configuration files for HTTP proxy services.

Syntax

```
show network http-proxy conf {active|errors|new}
```

Command	Description
`active`	Displays the nginx.conf file, which is the currently active HTTP Proxy configuration.
`errors`	Displays the nginx.errors file, which displays the errors in the temp_ nginx.conf file.
`new`	Displays the temp_nginx.conf file, which is the new configuration with invalid configuration.

Command Mode

Basic and Privileged User

Example

This example displays the NGINX errors:

```
show network http-proxy conf errors
nginx: [emerg] host not found in upstream "10.1.1.1.1:45" in /acBin/nginx/temp_n
 ginx.conf:34
nginx: configuration file /acBin/nginx/temp_nginx.conf test failed
```

show network interface

This command displays IP network Interfaces, which are configured in the IP Interfaces table, Including packet statistics per interface, for example, number of transmitted packets. The command also displays the status of the OSN module (supported only on certain devices).

Syntax

```
show network interface [description|osn]
```

Command	Description
Carriage Return	Displays all the IP Interfaces (IPv4 and IPv6) one after the other.
`description [ipv4|ipv6]`	Displays the IP Interfaces in table format: - `show network interface description`: Displays all IP Interfaces (IPv4 and IPv6). - `show network interface description ipv4`: Displays all IPv4 Interfaces. - `show network interface description ipv6`: Displays all IPv6 Interfaces.
`osn`	Displays the status of the OSN module. **Note:** This command is applicable only to devices that support the OSN module.

Command Mode

Basic and Privileged User

Example

- Displays all IPv4 interfaces:

```
show network interface description ipv4
Index  Application Type  IP Address     Prefix  Gateway     VlanID     Interface Name
  Interface Mode      status
0        O+M+C              10.15.7.96       16       10.15.0.1      1           O+M+C
   IPv4 Manual         Up
```

- Displays all IP interfaces:

```
show network interface
 Name: vlan 1
 Vlan ID: 1
 Underlying Interface: GROUP_1
 Hardware address is: 00-90-8f-5b-10-35

   Name: O+M+C
   Application Type: O+M+C
   IP Address: 10.15.7.96/16
   Gateway: 10.15.0.1
   Interface Mode: IPv4 Manual

 Name: IPv6-Interface
   Application Type: OAMP
   IP Address: 2001:db8:85a3::8a2e:370:7334/16
   Gateway: 2001:db8:85a3::8a2e:370:7334
   Interface Mode: IPv6 Manual

Name: SIP
   Application Type: CONTROL
   IP Address: ::/0
   Interface Mode: IPv6 Auto

 Uptime:  91:15:43
 rx_packets 8559313    rx_bytes 485973245   rx_dropped 0   rx_errors 0
 tx_packets 14412       tx_bytes 6476742       tx_dropped 0    tx_errors 0
```

- This example displays the OSN status (which is down):

```
show network interface osn
OSN is Down
Port Mode  :FORWARDING
txFrames    0000000000
rxFrames    0000000000
```

show network network-dev

This command displays the Ethernet Devices, which are configured in the Ethernet Devices table.

Syntax

```
show network network-dev
```

Command Mode

Basic and Privileged User

Example

```
show network network-dev
 D.Num  Device Name  VlanID  MTU   GroupName
 ------  ------------------  ---------  ------  ----------------
 0      vlan 1       1      1400 GROUP_1 # show network interface
```

show network ovoc-tunnel

This command displays the status of the WebSocket tunnel between the device and OVOC, and the IP address allocated to the device by OVOC.

Syntax

```
show network ovoc-tunnel
```

Command Mode

Basic and Privileged User

Example

```
show network ovoc-tunnel
OVOC Tunnel is Connected
OVOC Tunnel Ip Address is 169.254.7.52
OVOC Tunnel Ip Prefix is 18
```

show network physical-port

This command displays the Ethernet ports, which are configured in the Physical Ports table.

Syntax

```
show network physical-port
```

Command Mode

Basic and Privileged User

Example

```
show network physical-port

 Port Num   Port Name    MAC Address    Speed    Duplexity  Link Status  Native
VLAN
 1        GE_4_1     00:90:8f:5b:10:35  1Gbps   FULL     UP   1
 2        GE_4_2     00:90:8f:5b:10:35                DOWN 1
 3        GE_4_3     00:90:8f:5b:10:35                DOWN 1
 4        GE_4_4     00:90:8f:5b:10:35                DOWN 1
```

show network route

This command displays the status of the static routes, which are configured in the Static Routes table.

Syntax

```
show network route
```

Command Mode

Basic and Privileged User

Example

```
show network route
Codes: C - connected, S - static

C  169.253.0.0/16  is directly connected, InternalIf 2, Active
```

```
C  10.15.0.0/16  is directly connected, vlan 1, Active
S  0.0.0.0/0  [1] via 10.15.0.1, vlan 1, Active
```

show network tls

This command displays TLS security information (TLS Context), which is configured in the TLS Contexts table.

Syntax

```
show tls
```

Command	Description
`certificate`	Displays certificate information.
`contexts`	Displays TLS security context information.
`trusted-root {detail <Index>|summary}`	Displays trusted certificates. ■ detail (Displays a specific trusted certificate) ■ summary (Displays all trusted certificates)

Command Mode

Basic and Privileged User

Example

```
show tls contexts
Context #  Name
---------  ---------------------------
0        default
2        ymca

Total 2 active contexts.
Total certificate file size: 4208 bytes.
```

show running-config

This command displays the device's current configuration.

Syntax

```
show running-config
```

Command	Description
(Carriage Return)	Displays the device's full configuration in the format of a CLI command script. You can copy and paste the displayed output in a text-based file (e.g., using Notepad), and then upload the file to another device, or the same device if you want to make configuration changes, as a CLI script file.
`> <URL Destination>`	Sends the device's configuration in CLI script format, as a file to a remote destination defined by a URL (TFTP, HTTP or HTTPS).
`full [> <URL Destination>]`	Displays the device's configuration as well as default configuration settings that were not actively set by the user. In regular mode, only configuration that is not equal to the default is displayed. Can also send the configuration in CLI script format, as a file to a remote destination defined by a URL (TFTP, HTTP or HTTPS).
`network`	Displays the device's network configuration (config-network).
`system`	Displays the device's system configuration (config-system).
`troubleshoot`	Displays the device's troubleshoot configuration (config-troubleshoot).
`voip`	Displays the device's VoIP configuration (config-voip).

Command Mode

Basic and Privileged User

Note

- The Local Users table (in which management users are configured, as described in user on page 231) is included in the output of this command only if you are in Privileged User command mode.

- You can also run this command from any other command, using the `do` command, for example:

```
(clock)# do show running-config
```

Example

This example sends the device's configuration to an HTTP server:

```
show running-config> http://10.9.9.9
```

show sctp

This command displays Stream Control Transmission Protocol (SCTP) information.

Syntax

```
show sctp
```

Command	Description
`connections`	See show sctp connections below
`statistics`	See show sctp statistics on the next page

Command Mode

Basic and Privileged User

show sctp connections

This command displays SCTP socket associations status.

Syntax

```
show sctp connections
```

Command Mode

Basic and Privileged User

Note

SCTP is applicable only to Mediant 90xx and Mediant Software.

Related Commands

```
(config-network)# sctp
```

Example

The example below displays the local SCTP endpoint (i.e., device) titled "Association #1", and the SCTP association status with the remote SCTP endpoint (proxy) titled "Association #2).

```
show sctp connections
------------------------------------------------------------------
Association #1
Type:              SERVER
State:             LISTEN
Local Addresses:      10.55.3.80, 10.55.2.80
Local Port:        5060
------------------------------------------------------------------
```

```
Association #2
Type:              CLIENT
State:             ESTABLISHED
Local Addresses:      10.55.3.80, 10.55.2.80
Local Port:        50226
Remote Addresses      Configured     State
10.55.1.100:5060      Yes         INACTIVE - Primary
10.55.0.100:5060      Yes         ACTIVE - Secondary
```

show sctp statistics

This command displays statistics for all SCTP socket associations.

Syntax

```
show sctp statistics
```

Command Mode

Basic and Privileged User

Note

SCTP is applicable only to Mediant 90xx and Mediant Software.

Related Commands

```
(config-network)# sctp
```

Example

The example below displays statistics for all SCTP associations (only a partial output is shown below).

```
show sctp statistics
MIB according to RFC 3873:
discontinuity.sec = 1547641112, discontinuity.usec = 169612, currestab = 3,
activeestab = 2
restartestab = 0, collisionestab = 0, passiveestab = 1, aborted = 1
shutdown = 0, outoftheblue = 0, checksumerrors = 0, outcontrolchunks = 248438
outorderchunks = 1769, outunorderchunks = 349601, incontrolchunks = 243466,
inorderchunks = 1769
inunorderchunks = 466146, fragusrmsgs = 0, reasmusrmsgs = 0, outpackets =
302051, inpackets = 306499
```

```
input statistics:
recvpackets = 306499, recvdatagrams = 306499, recvpktwithdata = 281264,
recvsacks = 241804, recvdata = 467915
recvdupdata = 6, recvheartbeat = 828, recvheartbeatack = 826, recvecne = 0,
recvauth = 1
recvauthmissing = 0, recvivalhmacid = 0, recvivalkeyid = 0, recvauthfailed = 0,
recvexpress = 467914
recvexpressm = 0, recv_spare = 0, recvswcrc = 301493, recvhwcrc = 5006
```

```
output statistics:
sendpackets = 302051, sendsacks = 246385, senddata = 351370, sendretransdata
= 75
sendfastretrans = 0, sendmultfastretrans = 0, sendheartbeat = 1210, sendecne = 0
sendauth = 0, senderrors = 0, send_spare = 0, sendswcrc = 297046, sendhwcrc =
5005
...
```

show startup-script

This command displays the Startup Script file log.

Syntax

```
# show startup-script
```

Commands	Description
`recovery-log`	Displays the logs generated during the failed Startup Script process. If the startup process fails, the device is rolled back to its previous configuration.
`startup-log`	Displays the Startup Script log.

Command Modes

Privileged User

show storage-history

This command displays the CDRs and SDRs stored on the device.

Syntax

```
show storage-history {services|unused}
```

Command	Description
`services`	Displays registered storage services (e.g., `cdr-storage-history` and `sdr-storage-history`).
`unused`	Displays stored files that are not used.

Command Mode

Basic and Privileged User

Related Command

`clear storage-history`

show system

This command displays system information.

Syntax

```
show system
```

Command	Description
`alarms`	See show system alarms below
`alarms-history`	See show system alarms-history on the next page
`assembly`	See show system assembly on page 87
`clock`	See show system clock on page 87
`cpu-util`	See show system cpu-util on page 88
`fax-debug-status`	See show system fax-debug-status on page 88
`feature-key`	See show system feature-key on page 89
`floating-license`	See show system floating-license on page 90
`floating-license reports`	See show system floating-license reports on page 90
`log`	See show system log on page 91
`ntp-status`	See show system ntp-status on page 92
`radius servers status`	See show system radius servers status on page 92
`security status`	See show system security status on page 93
`temperature`	See show system temperature on page 94
`uptime`	See show system uptime on page 95
`utilization`	See show system utilization on page 95
`version`	See show system version on page 96

Command Mode

Basic and Privileged User

show system alarms

This command displays active alarms.

Syntax

```
show system alarms
```

Command Mode

Basic and Privileged User

Examples

```
show system alarms
Seq. Source                  Severity   Date                 Description
1. Board#1/EthernetLink#2         minor     11.6.2010 , 14:19:42   Ethernet link
alarm. LAN port number 2 is down.
2. Board#1/EthernetGroup#2        major     11.6.2010 , 14:19:46   Ethernet Group
alarm. Ethernet Group 2 is Down.
```

show system alarms-history

This command displays the system alarms history.

Syntax

```
show system alarms-history
```

Command Mode

Basic and Privileged User

Example

```
show system alarms-history
Seq. Source                  Severity   Date                 Description
1. Board#1                   major     24.2.2011 , 20:20:32   Network element admin
  state change alarm. Gateway is locked.
3. Board#1/EthernetLink#2       minor     24.2.2011 , 20:20:34   Ethernet link alarm.
LAN
  port number 2 is down.
4. Board#1/EthernetLink#3       minor     24.2.2011 , 20:20:34   Ethernet link alarm.
LAN
  port number 3 is down.
```

show system assembly

This command displays information about the device's hardware assembly (slots, ports, module type, fan tray and power supply). It also displays virtual NICs for Mediant CE/VE.

Syntax

```
show system assembly
```

Command Mode

Basic and Privileged User

Example

```
show system assembly
Board Assembly Info:
|Slot No.        | Ports    |Module Type          |
| 1           | 1      | E1/T1             |
| 2           | 1-4     | FXS              |
| 3           | 0      | Empty             |
| 4           | 1-4     | LAN-GE              |
| 5           | 0      | Empty             |

USB Port 1: Empty
USB Port 2: Empty
```

show system clock

This command displays the device's time and date.

Syntax

```
show system clock
```

Command Mode

Basic and Privileged User

Example

```
show system clock
14:12:48  01/02/2017  (dd/mm/yyyy)
```

show system cpu-util

This command displays the voice CPU utilization (in percentage).

Syntax

```
show system cpu-util
```

Command	Description
refreshing	(Optional) Refreshes the displayed voice CPU utilization information. Press CTRL+C to stop the refresh.
history voice	Displays CPU utilization in the last 72 hours, 60 minutes, and 60 seconds.

Command Mode

Basic and Privileged User

Example

```
show system cpu-util
 Voice CPU utilization 20%%%
```

show system fax-debug-status

This command displays fax debug status (off or on).

Syntax

```
show system fax-debug-status
```

Command Mode

Basic and Privileged User

Example

```
show system fax-debug-status
The fax debug is OFF. # show fax-debug-status
```

show system feature-key

This command displays the device's License Key.

Syntax

```
show system feature-key
```

Command Mode

Basic and Privileged User

Example

```
show system feature-key

Key features:
Board Type: Mxx
DATA features:
IP Media: Conf
DSP Voice features: RTCP-XR
Channel Type: DspCh=30
HA
Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP
G727 ILBC EVRC-B AMR-WB G722 EG711 MS_RTA_NB MS_RTA_WB SILK_NB
SILK_WB SPEEX_NB SPEEX_WB OPUS_NB OPUS_WB
Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
E1Trunks=2
T1Trunks=2
FXSPorts=1
FXOPorts=1
BRITrunks=2
QOE features: VoiceQualityMonitoring MediaEnhancement
Control Protocols: MGCP SIP SBC=30 TRANSCODING=5 TestCall=6 SIPRec=10
CODER-TRANSCODING=2 SIPRec-Redundancy=2
Default features:
Coders: G711 G726
```

show system floating-license

This command displays information on the Floating License. This includes whether it is enabled, and if so, connection status with OVOC, OVOC Product Key, and SBC allocation resources.

Syntax

```
show system floating-license
```

Command Mode

Basic and Privileged User

Example

```
show system floating-license
Floating License is on
OVOC IP address: 10.8.6.250
OVOC Connection status: Connected
OVOC product ID: 384
Allocation profile: SIP Trunking
Allocation - FEU (Far End Users): 0
Allocation - signaling sessions: 6000
Allocation - media sessions: 6000
Allocation - transcoding sessions: 1536
User Limit - FEU (Far End Users): No limit
User Limit - signaling sessions: No limit
User Limit - media sessions: No limit
User Limit - transcoding sessions: No limit)
```

show system floating-license reports

This command displays the Floating License reports that the device sends to OVOC. The report contains the device's SBC resource consumption (signaling sessions, media sessions, transcoding sessions, and far-end user registrations).

Syntax

```
show system floating-license reports
```

Command Mode

Basic and Privileged User

Example

```
show system floating-license reports
[2018-09-04 17:17:56] Signaling Sessions: (2111), Media Sessions: (2109),
Transcoding Sessions: (2029), Far End Users: (0)
[2018-09-04 17:16:55] Signaling Sessions: (2032), Media Sessions: (0),
Transcoding Sessions: (0), Far End Users: (0)
[2018-09-04 17:15:54] Signaling Sessions: (0), Media Sessions: (0), Transcoding
Sessions: (0), Far End Users: (0)
```

show system log

This command displays the device's logged event messages.

Syntax

```
show system log
```

Command	Description
`(Carriage Return)`	Displays all logged message history.
`-h`	Displays the log history in a readable format.
`no-sip`	Displays all non-SIP related logged messages (in chronological order).
`persistent [0-9]`	Displays all persistent log history or optionally, a specific persistent log file (0 to 9, where 0 is the latest file).

Command Mode

Basic and Privileged User

Note

- The `persistent` command is applicable only to Mediant 9000 and Mediant VE/SE.
- Persistent Logging is always enabled (cannot be disabled).

Related Commands

- `system-log-size`: Configures the maximum file size of the system log that is saved on the device, use the command . This determines the amount of logged information displayed when the `show system log` command is run.

- `system-persistent-log-size`: Configures the maximum file size of each persistent log.
- `system-persistent-log-period`:Configures the maximum file age of each persistent log.
- `copy system-log-persistent`: Sends persistent log files to a remote server.
- `tail system log`: Shows the tail-end (last lines) of the output.

Example

This example displays the persistent logged messages stored in logged file #0 (latest):

```
show system log persistent 0
Sep  9 04:53:28 local0.notice [S=5165] [BID=20d56a:101]  !!! Repeated 31528
times : CDR/SDR (SDR-STORAGE-HISTORY): send to '10.8.5.150' failed: Failed
to connect to host [Time:09-09@04:53:28.592]
Sep  9 01:10:19 local0.notice [S=3877] [BID=20d56a:101]  !!! Repeated 23908
times : CDR/SDR (SDR-STORAGE-HISTORY): send to '10.8.5.150' failed: Failed
to connect to host [Time:09-09@01:10:19.165]
```

show system ntp-status

This command displays NTP information.

Syntax

```
show system ntp-status
```

Command Mode

Basic and Privileged User

Example

```
show system ntp-status
Configured NTP server #1 is 0.0.0.0
NTP is not synchronized.
Current local time: 2010-01-04 00:50:52
```

show system radius servers status

This command displays the status of the RADIUS severs.

Syntax

```
show system radius servers status
```

Command Mode

Basic and Privileged User

Example

```
show system radius servers status
servers 0
ip-address 10.4.4.203
auth-port 1812
auth-ha-state "ACTIVE"
acc-port 1813
acc-ha-state "ACTIVE"
servers 1
ip-address 10.4.4.202
auth-port 1812
auth-ha-state "STANDBY"
acc-port 1813
acc-ha-state "STANDBY"
```

This example shows the following fields per server:

- If the authentication port is 0, the server is not part of the redundancy server selection for authentication.
- If the accounting port is 0, the server is not part of the redundancy server selection for accounting.
- Server authentication redundancy (HA) status. ACTIVE = the server was used for the last sent authentication request.
- Server accounting redundancy (HA) status. ACTIVE = the server was used for the last sent accounting request.

show system security status

This command displays if the device is operating in FIPS mode.

Syntax

```
show system security status
```

Command Mode

Basic and Privileged User

Note

FIPS is supported only by Mediant 4000B and Mediant 9080.

Example

This example displays the FIPS mode (which is disabled):

```
show system security status
FIPS mode: Disabled
```

show system temperature

This command displays the temperature of the device's CPU as well as DSPs (in the Media Processing Module / MPM).

Syntax

```
show system temperature
```

Command Mode

Basic and Privileged User

Note

The command is applicable only to Mediant 4000B SBC.

Example

```
show system temperature
Last Updated Temperature (in Celsius):
    CSM (GA #3 ASM #1): 42
    DSM (GA #7 ASM #0): 59
    DSM (GA #7 ASM #3): 62
```

Where "CSM" is the CPU, "DSM" the DSP module, and "GA" the slot.

show system uptime

This command displays the device's uptime (time since last restarted).

Syntax

```
show system uptime
```

Command Mode

Basic and Privileged User

Example

```
show system uptime
Uptime: 3 days, 0 hours, 55 minutes, 46 seconds
```

show system utilization

This command displays the device's CPU and memory utilization (in percentage).

Syntax

```
show system utilization
```

Command	Description
`history {at-start|voice}`	■ `at-start`: Displays CPU utilization (in percentage) measured five minutes after the device restarts. ■ `voice`: Displays CPU utilization (in percentage) of voice: ✓ Utilization per hour in the last 72 hours. ✓ Utilization per minute in the last hour (60 minutes).
`refreshing <Refresh Rate>`	Displays CPU and memory utilization (in percentage) every user-defined refresh rate. To stop the display, press the Ctrl+C key combination.

Command Mode

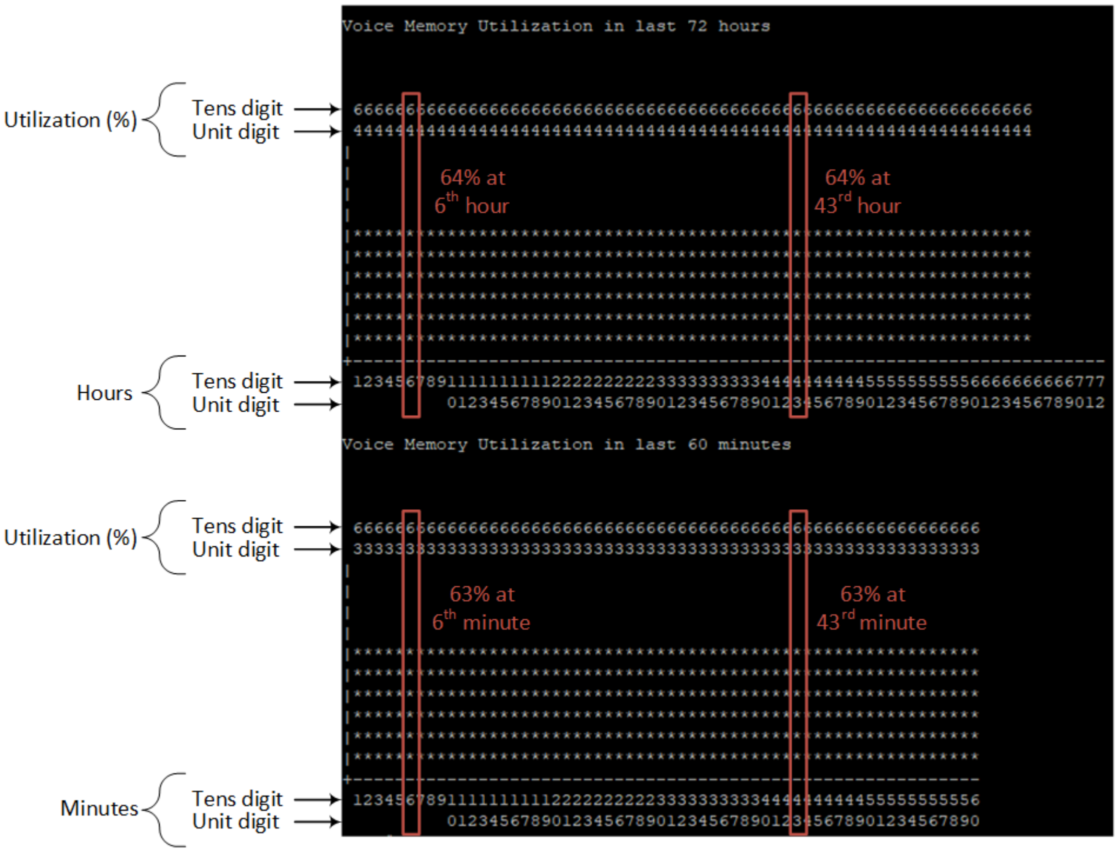
Basic and Privileged User

Example

This example displays system utilization, which is refreshed every 5 seconds:

```
show system utilization refreshing 5
CPUs utilization: Data 0% Voice 19%
CPUs Used Memory: Data 0% Voice 56%
System Time 00:58:1
```

The example below displays CPU utilization in the last 72 hours and 60 minutes, using the command, `show system utilization history voice`:



```
Voice Memory Utilization in last 72 hours


 66666666666666666666666666666666666666666666666666666666666666666
 44444444444444444444444444444444444444444444444444444444444444444
|
|
|
|
|*****************************************************************
|*****************************************************************
|*****************************************************************
|*****************************************************************
|*****************************************************************
|*****************************************************************
+------------------------------------------------------------------------
 123456789111111111122222222223333333333444444444455555555556666666666777
          012345678901234567890123456789012345678901234567890123456789012
Voice Memory Utilization in last 60 minutes


 666666666666666666666666666666666666666666666666666666666666
 333333333333333333333333333333333333333333333333333333333333
|
|
|
|
|************************************************************
|************************************************************
|************************************************************
|************************************************************
|************************************************************
|************************************************************
+------------------------------------------------------------
 123456789111111111122222222223333333333444444444455555555556
          012345678901234567890123456789012345678901234567890
```

show system version

This command displays the current running software and hardware version.

Syntax

```
show system version
```

Command Mode

Basic and Privileged User

Example

```
show system version

Version info:
--------------
;Board: Mxx
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 5967925
;Slot Number: 1
;Software Version: 7.20A.140.652
;DSP Software Version: 5014AE3_R => 721.09
;Board IP Address: 10.15.7.96
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 512M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 3  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;;;Key features:;Board Type: M800B ;DATA features: ;IP Media: Conf ;DSP Voice
features: RTCP-XR ;Channel Type: DspCh=30 ;HA ;Coders: G723 G729 G728
NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-
WB G722
 EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB
OPUS_NB OPUS_WB ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;E1Trunks=2 ;T1Trunks=2 ;FXSPorts=1 ;FXOPorts=1
;BRITrunks=2 ;QOE
 features: VoiceQualityMonitoring MediaEnhancement ;Control Protocols: MGCP
SIP SBC=30 TRANSCODING=5 TestCall=6 SIPRec=10 CODER-
TRANSCODING=2 SIPRec-Redundancy=2 ;Default features:;Coders: G711
G726;

;------  HW components------
;
; Slot # : Module type : # of ports
;----------------------------------------------
;      1 : FALC56      : 1
;      2 : FXS         : 4
;      3 : Empty
;----------------------------------------------
```

show users

This command displays users that are currently logged into the device's management interfaces (CLI and Web) and optionally, all configured users.

Syntax

```
show users {all}
```

Command	Description
Enter	Displays currently logged-in users. For each logged-in user, the command displays the following: ■ Type of management interface (console, Telnet, SSH, or Web). ■ User's username. ■ Remote IP address from where the user has logged in. ■ Duration (days and time) of the session. ■ Unique index (session ID).
`all`	Displays currently active logged-in users and all configured users in the Local Users table. For each configured user, the command displays the following: ■ Index row of user in the Local Users table. ■ User's username. ■ Date and time that the password was last changed. ■ Date and time when the password will expire ("Unlimited" if no expiration date). ■ Status of the password (e.g., "Unlimited" or "Valid").

Command Mode

Basic and Privileged User

Note

- The current session from which the `show` command is run is displayed with an asterisk (*).
- The device can display management sessions of up to 24 hours. After this time, the duration counter is reset.

Example

- Displays currently logged-in users:

```
# show users
[0]*   ssh      Admin    10.11.2.2        0d00h17m55s
[0]    WEB      Admin    10.11.2.2        0d00h01m44s
```

- Displays currently logged-in users and all users configured in the Local Users table:

```
M800B# show users all
[Active Sessions]:
[0]*   ssh     Admin    10.11.2.2        0d00h05m16s
[0]    WEB     Admin    10.11.2.2        0d00h02m40s

[All Users]:
Index       Username      PW Last Change           PW Expr. Date        Status
[0]         Admin         2025-02-23 07:25:05      Unlimited
   Unlimited
[1]         User          2025-02-23 07:25:05      Unlimited
    Unlimited
```

show voip

This command displays VoIP-related information.

Syntax

```
show voip
```

Command	Description
`calls`	See show voip calls on the next page
`channel-stats`	See show voip channel-stats on page 105
`coders-stats`	See show voip coders-stats on page 106
`cpu-stats`	See show voip cpu-stats on page 107
`dsp`	See show voip dsp on page 107
`e911`	See show voip e911 on page 109

Command	Description
`ids`	See show voip ids on page 109
`interface`	See show voip interface on page 111
`ip-group`	See show voip ip-group on page 112
`ldap`	See show voip ldap on page 113
`other-dialog`	See show voip other-dialog statistics on page 115
`proxy`	See show voip proxy sets status on page 115
`realm`	See show voip realm on page 116
`register`	See show voip register on page 116
`subscribe`	See show voip subscribe on page 119
`voip tags-cac`	See show voip tags-cac on page 120
`tdm`	See show voip tdm on page 121

Command Mode

Basic and Privileged User

show voip calls

This command displays active VoIP call information.

Syntax

```
show voip calls {active|history|statistics}
```

Command	Description
`active`	See show voip calls active on the next page
`history`	See show voip calls history on page 102
`statistics`	See show voip calls statistics on page 103

Command Mode

Basic and Privileged User

show voip calls active

This command displays active calls.

Syntax

```
show voip calls active [<Filter>|<Session ID>|descending|gw|sbc|siprec|summary]
```

Command	Description
(Carriage Return)	Displays the total number of active calls and detailed call information.
Filter	Filters the displayed output, using one of the following filter commands: `first`, `last`, `match`, or `range`. For more information on these filters, see Common CLI Commands on page 11.
Session ID	Displays detailed call information for a specific SIP session ID.
`descending`	Displays currently active calls, listed in descending order by call duration.
`gw`	Displays call information of currently active Gateway calls, listed in ascending order by call duration.
`sbc`	Displays call information of currently active SBC calls, listed in ascending order by call duration.
`siprec`	Displays call information of currently active SIPRec calls, listed in ascending order by call duration.
`summary`	Displays the total number of currently active calls (Gateway and SBC)

Command Mode

Basic and Privileged User

Related Commands

To hide (by displaying an asterisk) the values of the Caller and Callee CDR fields, use the `cdr-history-privacy` command.

Example

Displaying all active calls:

```
show voip calls active sbc
Total Active Calls: 1000
| Session ID   |    Caller       |    Callee       | Origin |     Remote IP     |End Point
Type |Duration|Call State

=================================================================
=================================================================
=
|314380675    |1129@10.3.3.194    |100@10.3.91.2     |Incoming|10.3.3.194
(IPG-1)  |SBC         |00:05:12|Connected
|314380675    |1129@10.3.3.194    |100@10.3.91.2     |Outgoing|10.3.3.194
(IPG-2)  |SBC         |00:05:12|Connected
|314380674    |1128@10.3.3.194    |100@10.3.91.2     |Incoming|10.3.3.194
(IPG-1)  |SBC         |00:05:12|Connected
```

show voip calls history

This command displays CDR history information.

Syntax

```
show voip calls history {gw|sbc|siprec} [<Filter>|<Session ID>]
```

Command	Description
`gw`	Displays historical Gateway CDRs.
`sbc`	Displays historical SBC CDRs.
`siprec`	Displays historical SIPRec CDRs.
Filter	Filters the displayed output, using one of the following filter commands: `first`, `last`, `match`, or `range`. For more information on these filters, see Common CLI Commands on page 11.
Session ID	(Optional) Displays historical SBC or Gateway CDRs of a specified SIP session ID.

Command Mode

Basic and Privileged User

Related Commands

To hide (by displaying an asterisk) the values of the Caller and Callee CDR fields, use the `cdr-history-privacy` command.

Example

Displaying CDR history information:

```
show voip calls history sbc
```

show voip calls statistics

This command displays call statistics.

Syntax

```
show voip calls statistics {gw|ipgroup|sbc|siprec}
```

Command	Description	
`gw [ip2tel|tel2ip]`	Displays all Gateway call statistics or per call direction:	
	`ip2tel`	Displays statistics of IP-to-Tel calls
	`tel2ip`	Displays statistics of Tel-to-IP calls
`ipgroup <IP Group ID>`	Displays call statistics per IP Group (ID).	
`sbc [media]`	Displays SBC call statistics (see the example below) or optionally, SBC media statistics (Active Media legs and Active Transcoding Sessions).	
`siprec`	Displays the total number of currently active SIPRec signalling sessions with the SIPRec server (SRS).	

Command Mode

Basic and Privileged User

Example

- The examples display various SIPRec sessions:

- Eight recorded calls (Gateway and/or SBC) without SRS redundancy:

```
show voip calls statistics siprec
SIPRec number of active sessions: 8 (redundant sessions: 0)
```

- Eight recorded SBC calls with SRS redundancy (active-standby):

```
show voip calls statistics siprec
SIPRec number of active sessions: 8 (redundant sessions: 8)
```

- Eight recorded SBC calls with SRS redundancy (active-active):

```
show voip calls statistics siprec
SIPRec number of active sessions: 16 (redundant sessions: 0)
```

- The example displays SBC call statistics:

```
show voip calls statistics sbc
SBC Call Statistics:
Active INVITE dialogs: 0
Active incoming INVITE dialogs: 0
Active outgoing INVITE dialogs: 0
Average call duration [min:sec]: ---
Call attempts: 0
Incoming call attempts: 0
Outgoing call attempts: 0
Call Attempted Rate for Incoming Calls (CAPS): 0
Call Attempted Rate for Outgoing Calls (CAPS): 0
Average number of seconds from invite to response (PDD): ---
Established calls: 0
Incoming established calls: 0
Outgoing established calls: 0
Establishment Rate for Incoming Calls (established calls per second): 0
Establishment Rate for Outgoing Calls (established calls per second): 0
Answer Seizure Ratio (ASR): ---
Network Effectiveness Ratio (NER): ---
Total sum in minutes of call duration: 0
Calls terminated due to busy line: 0
Incoming calls terminated due to busy line: 0
Outgoing calls terminated due to busy line: 0
Calls terminated due to no answer: 0
Incoming calls terminated due to no answer: 0
Outgoing calls terminated due to no answer: 0
```

```
Calls terminated due to forward: 0
Incoming calls terminated due to forward: 0
Outgoing calls terminated due to forward: 0
Calls terminated due to resource allocation failure: 0
Incoming calls terminated due to resource allocation failure: 0
Outgoing calls terminated due to resource allocation failure: 0
Calls terminated due to media negotiation failure: 0
Incoming calls terminated due to media negotiation failure: 0
Outgoing calls terminated due to media negotiation failure: 0
Calls terminated due to general failure: 0
Incoming calls terminated due to general failure: 0
Outgoing calls terminated due to general failure: 0
Calls abnormally terminated: 0
Incoming calls abnormally terminated: 0
Outgoing calls abnormally terminated: 0
Incoming calls terminated due to no routing failure: 0
Incoming calls terminated due to classification failure: 0
Not Established Incoming Calls which are configured as Success: 0
Not Established Outgoing Calls which are configured as Success: 0
Not Established Incoming Calls which are configured as Failed: 0
Not Established Outgoing Calls which are configured as Failed: 0
```

show voip channel-stats

This command displays statistics associated with a specific VoIP channel.

Syntax

```
show voip channel-stats {analog|channel-count|digital|jitter-threshold|pl|pl-
threshold|rtt-threshold|virtual}
```

Command	Description
`analog`	Displays an analog channel's statistics (FXS or FXO). ■ channel number (0-255; run the command show system assembly to facilitate defining this command) ■ number of channels (1-256)
`channel-count`	Displays the number of active voice channels.
`digital`	Displays a digital channel's statistics (E1/T1 or BRI). ■ channel number (0-255; run the command show

Command	Description
	system assembly to facilitate defining this command) ■ number of channels (1-256)
`jitter-threshold`	Displays the number of analog channels, digital channels, and virtual channels on which jitter occurred that exceeded the threshold you configured (in the range 0-65535).
`pl`	Displays the number of analog channels, digital channels, and virtual channels on which PL (packet loss) occurred.
`pl-threshold`	Displays the number of analog channels, digital channels, and virtual channels on which PL (packet loss) occurred that exceeded the threshold you configured (in the range 0-65535).
`rtt-threshold`	Displays the number of analog channels, digital channels, and virtual channels on which the RTT (Round Trip Time) exceeded the threshold you configured (in the range 0-65535).
`virtual`	Displays a virtual channel's statistics of active calls. ■ channel number (0-255; run the command show system assembly to facilitate defining this command) ■ number of channels (1-256)

Command Mode

Basic and Privileged User

show voip coders-stats

This command displays the number and percentage of active channels using each audio coder.

Syntax

```
show voip coders-stats
```

Command Mode

Basic and Privileged User

Example

Showing that 67 channels (25.18%) of the 266 active channels are using the G.729e coder, 76 (28.57%) are using the G.726 coder, and 123 (46.24%) are using the G.722 coder:

```
show voip coders-stats
There are 266 active channels.
Coder    Number of Channels     Percentage
---------------------------------------------
G729e        67             25.18
G726        76             28.57
G722        123             46.24
```

show voip cpu-stats

This command displays the device's CPU percentage use.

Syntax

```
show voip cpu-stats
```

Command Mode

Basic and Privileged User

Example

Displaying CPU percentage use:

```
show voip cpu-stats
CPU percentage: 47%
```

show voip dsp

This command displays DSP information.

Syntax

```
show voip dsp
```

Command	Description
`perf`	See show voip dsp perf below
`status`	See show voip dsp status below

Command Mode

Basic and Privileged User

show voip dsp perf

This command displays performance monitoring of DSP data.

Syntax

```
show voip dsp perf
```

Command Mode

Basic and Privileged User

Example

Displaying performance monitoring of DSP data:

```
show voip dsp perf

DSP Statistics (statistics for 144 seconds):
Active DSP resources: 0
Total DSP resources: 76
DSP usage : 0
```

show voip dsp status

This command displays the current DSP status.

Syntax

```
show voip dsp status
```

Command Mode

Basic and Privileged User

Example

Displaying the current DSP status:

```
show voip dsp status

Group:0 DSP firmware:624AE3 Version:0660.07 - Used=0 Free=72 Total=72
  DSP device  0:  Active   Used= 0  Free= 6  Total= 6
  DSP device  1:  Active   Used= 0  Free= 6  Total= 6
  DSP device  2:  Active   Used= 0  Free= 6  Total= 6
  DSP device  3:  Active   Used= 0  Free= 6  Total= 6
  DSP device  4:  Active   Used= 0  Free= 6  Total= 6
  DSP device  5:  Active   Used= 0  Free= 6  Total= 6
  DSP device  6:  Active   Used= 0  Free= 6  Total= 6
  DSP device  7:  Active   Used= 0  Free= 6  Total= 6
  DSP device  8:  Active   Used= 0  Free= 6  Total= 6
  DSP device  9:  Active   Used= 0  Free= 6  Total= 6
  DSP device 10:  Active   Used= 0  Free= 6  Total= 6
  DSP device 11:  Active   Used= 0  Free= 6  Total= 6
Group:1 DSP firmware:204IM Version:0660.07 - Used=0 Free=8 Total=8
  DSP device 12:  Active   Used= 0  Free= 4  Total= 4
  DSP device 13:  Active   Used= 0  Free= 4  Total= 4
Group:2 DSP firmware:204IM Version:0660.07 - Used=0 Free=4 Total=4
  DSP device 14:  Active   Used= 0  Free= 4  Total= 4
Group:4 DSP firmware:204IM Version:0660.07 - Used=4 Free=0 Total=4
  DSP device 15:  Active   Used= 4  Free= 0  Total= 4
```

show voip e911

This command displays the ELIN number per E911 caller and the time of call.

Syntax

```
show voip e911
```

Command Mode

Basic and Privileged User

show voip ids

This command displays the Intrusion Detection System (IDS) blacklist of remote hosts (IP addresses / ports) considered malicious.

Syntax

```
# show voip ids {blacklist active|active-alarm}
# show voip ids active-alarm {all|match <ID> rule <ID>}
```

Command	Description
`active-alarm`	Displays all active blacklist alarms: - all (Displays all active alarms) - match (Displays active alarms of an IDS matched ID and rule ID)
`blacklist active`	Displays blacklisted hosts.

Command Mode

Privileged User

Related Commands

- ids policy
- ids rule
- clear voip ids blacklist

Example

- Displaying the IDS blacklist:

  ```
  # show voip ids blacklist active
  Active blacklist entries:
  10.33.5.110(NI:0) remaining 00h:00m:10s in blacklist
  ```

  Where SI is the SIP Interface, and NI is the Network interface.

- Displaying the blacklist of all active IDS alarms:

  ```
  # show voip ids active-alarm all
  IDSMatch#0/IDSRule#1: minor alarm active.
  ```

- Displaying details regarding an active IDS alarm of the specified match and rule IDs:

```
# show voip ids active-alarm match 0 rule 1
IDSMatch#0/IDSRule#1: minor alarm active.
- Scope values crossed while this alarm is active:
   10.33.5.110(SI0)
```

show voip interface

This command displays information (basic configuration, status and Performance Monitoring) of a specified telephony interface (E1/T1, BRI or FXS/FXO).

Syntax

```
show voip interface {e1-t1|bri|fxs-fxo} <Trunk ID|Module/Port>
```

Command	Description
`e1-t1`	Displays information on a specified E1/T1 interface.
`bri`	Displays information on a specified BRI interface.
`fxs-fxo`	Displays the current status, main PM parameters and main configuration parameters to a specific analog interface (FXS or FXO
Trunk ID	Defines the E1/T1 Trunk ID. **Note:** This is applicable only to Mediant 3100.
Module	Defines the module slot index as shown on the front panel. **Note:** This is not applicable to Mediant 3100.
Port	Defines the module's analog port number (FXS/FXO) or trunk port number (E1/T1 or BRI) to display. **Note:** This is not applicable only to Mediant 3100.

Command Mode

Basic and Privileged User

Note

- Parameters displayed depend on the PSTN protocol type.
- The command is applicable to devices supporting analog and/or digital PSTN interfaces.

Example

Displaying information of the E1/T1 interface of trunk port 1 of trunk module 3:

```
show voip interface e1-t1 3/1
 show voip interface e1-t1 3/1
-------------------------------
module/port:      3/1
trunk number:     0
protocol:         t1_transparent
state:            not active
alarm status:     LOS 1,  LOF 0,  RAI 0,  AIS 0,  RAI_CRC 0
loopback status:   no loop
send alarm status: no alarm
main performance monitoring counters collected in the last 470 seconds:
     BitError:          0          EBitErrorDetected:      0
     CRCErrorReceived:   0          LineCodeViolation:      0
     ControlledSlip:     0          ControlledSlipSeconds:  0
     ErroredSeconds:     0          BurstyErroredSeconds:   0
     UnAvailableSeconds: 470        PathCodingViolation:    0
     LineErroredSeconds: 0          SeverelyErroredSeconds: 0
     SeverelyErroredFramingSeconds: 0

   basic configuration:
     framing:       T1_FRAMING_ESF_CRC6
     line-code:      B8ZS
     clock-master:   CLOCK_MASTER_OFF
     clock-priority: 0
     trace-level:    no-trace
```

show voip ip-group

This command displays the following QoS metrics per IP Group:

- QoE profile metrics per IP Group and its associated Media Realm on currently established calls such as MOS, jitter, packet loss, and delay. Metrics are displayed as average amounts.
- Bandwidth Profile (BW) metrics for Tx and Rx traffic per IP Group and/or Media Realm. Metrics are displayed with a status color for each specific port.
- QoE profile metrics for the remote (far-end) such as MOS, jitter, packet loss, and delay. Each metric is displayed with a specific color.
- Group MSA metrics for the IP Group and the Media Realm. Metrics are displayed as an aggregated value.

Syntax

```
show voip ip-group <IP Groups Table Index> media-statistics
```

Command Mode

Basic and Privileged User

Example

Displaying QoS metrics of IP Group configured in row index 0:

```
show voip ip-group 0 media-statistics
IPGroup 0. BWProfile: -1, QoEProfile: -1
-------------------------------------
MSA: 0
Averages: MOS 0  Remote MOS 0 Delay 0 Remote Delay 0 Jitter 0 Remote Jitter 0
Fraction loss  tx 0 Fraction loss rx 0
Packet sent 0 Packet received 0
Audio Tx BW 0, Audio Tx Status Green
Audio Rx BW 0, Audio Rx Status Green
Total Tx BW 0, Total Tx Status Green
Total Rx BW 0, Total Rx Status Green
Video Tx BW 0, Video Tx Status Green
Video Rx BW 0, Video Rx Status Green
MSA color Gray MSA remote color Gray
MOS color Gray remote MOS color Gray
Delay color Gray  remote Delay color Gray
PL color Gray  remote PL color Gray
Jitter color Gray  remote Jitter color Gray
color is not relevant
Media Realm -1. BWProfile -1, QoEProfile: -1
```

show voip ldap

This command displays the number of 'internal AD search requests', i.e., routings requiring information from the AD, including requests answered via the cache and directly from the AD. Routing requests are stored every 15 minutes. The last 96 intervals (24h) are stored.

Syntax

```
show voip ldap {cache-hits-pm|print-cache} {group <Group Matrix Index>}|print-
cache-entry {group <Group Index>}|print-cache-nums|searches-pm|timeout-pm
```

Command	Description
`cache-hits-pm`	Displays the number of responses answered by the cache in each interval.
`print-cache`	Displays the cache (by group).
`print-cache-entry`	Displays a cache entry (by key and group).
`print-cache-nums`	Displays the number of entries and aged entries in the cache.
`searches-pm`	Displays performance monitoring results for searches.
`timeout-pm`	Displays performance monitoring results for searches.

Command Mode

Basic and Privileged User

Example

- Displaying the the number of responses answered by the cache in each interval:

```
show voip ldap cache-hits-pm
server 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 server 1
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

- Displaying the cache (by group):

```
show voip ldap print-cache
print cache
servers' group number 0 Hash size 0 aged 0
servers' total Hash size 16384
servers' group number 1 Hash size 0 aged 0
```

- Displaying the cache (by key and group):

```
show voip ldap print-cache-entry
servers' group number 0 Hash size 0 aged 0
```

```
servers' total Hash size 16384
servers' group number 1 Hash size 0 aged 0
```

show voip other-dialog statistics

This command displays the number of current incoming and outgoing SIP dialogs (e.g., REGISTER), except for INVITE and SUBSCRIBE messages.

Syntax

```
show voip other-dialog statistics
```

Command Mode

Basic and Privileged User

Note

The command is applicable only to the SBC application.

Example

```
show voip other-dialog statistics
SBC other Dialog Statistics:
Active other dialogs: 0
Incoming other dialogs Rate (dialogs per second): 0
Outgoing other dialogs Rate (dialogs per second): 0
Average incoming other dialogs Rate (dialogs per second): 0
Average outgoing other dialogs Rate (dialogs per second): 0
Maximum incoming other dialogs Rate (dialogs per second): 0
Maximum outgoing other dialogs Rate (dialogs per second): 0
```

show voip proxy sets status

This command displays the information of Proxy Sets including their status. The status ("OK" or "FAIL") indicates IP connectivity with the proxy server.

Syntax

```
show voip proxy sets status
```

Command Mode

Basic and Privileged User

Example

Displaying status of Proxy Sets:

```
show voip proxy sets status
 Active Proxy Sets Status
ID  NAME   MODE    KEEP ALIVE   ADDRESS      PRIORITY  WEIGHT
SUCCESS COUNT  FAILED COUNT  STATUS
0   ITSP–1  Parking   Disabled    NOT RESOLVED
1   ITSP-2  Homing    Enabled     10.8.6.31(10.8.6.31)                    OK
```

show voip realm

This command displays statistics relating to Media Realms and Remote Media Subnets.

Syntax

- Displaying Media Realms:

```
show voip realm <Media Realm Table Index> statistics
```

- Displaying Remote Media Subnets:

```
show voip realm <Media Realm Table Index> remote-media-subnet <Remote
Media Subnet Table Index> statistics
```

Command Mode

Basic and Privileged User

Note

The command is especially useful when Quality of Experience Profile or Bandwidth Profile is associated with the Media Realm or Remote Media Subnets.

show voip register

This command displays registration status of users.

Syntax

```
show voip register {account|board|db sbc|ports|suppserv gw|user-info}
```

Command	Description
`account {gw|sbc}`	Displays registration status of user Accounts (Accounts table). - `gw`: Gateway accounts - `sbc`: SBC accounts)
`board`	Displays registration status for the entire gateway.
`db sbc {list|user}`	Displays SBC users registered with the device: - `list`: Displays the status of all registered SBC users, showing their AOR and Contact - `user` <AOR>: Displays detailed information about a specific registered SBC user (AOR) The output displays the following: - "UserInfo Contact" if the contact is configured in the device's User information table - "Not-Active" if user currently not registered - "IPG" - IP Group to which user is classified - "SI" - SIP Interface associated with user - "ID" - internal identification number used for debugging - MOS measurements: ✓ "LastMOS" - last call MOS score, timestamp and color ("N/A" means no calls during intervals) ✓ "AvgMOS" - average MOS over 12 intervals and color ("N/A" means no calls during intervals) ✓ "MinMOS" - minimum MOS over 12 intervals and color ("N/A" means no calls during intervals) **Note:** The command is applicable only to the SBC application.
`ports`	Displays registration status of the devices' ports. **Note:** The command is applicable only to the Gateway application.
`suppserv gw [list]`	Displays the number of users in the Supplementary Services table. - `list`: Displays detailed information about users, including registration status (REGISTERED / NOT REGISTERED. **Note:** The command is applicable only to the Gateway application.
`user-info`	Displays registration status of users in the User Info table.

Command	Description

`{gw|sbc}`
`[list]`
	■ `gw`: Displays total number of Gateway users.
	✓ `list`: Displays detailed information about users, including registration status - REGISTERED / NOT REGISTERED.
	■ `sbc`: Displays total number of SBC users.
	✓ `list`: Displays detailed information about users, including registration status - REGISTERED / NOT REGISTERED.

Command Mode

Basic and Privileged User

Example

- Displaying registration status of SBC users of AOR "1111":

```
show voip register db sbc user 1111

*** SBC Registered Contacts for AOR 1111 ***

============================================================
=====
UserInfo Contact | Not-Active | IPG:3 | SI:-1 | ID:19 | LastMOS:N/A |
AvgMOS:N/A | MinMOS:N/A
*** All SBC AORs for AOR 1111:
1111
```

- Displaying registration status of SBC users of AOR 12345@audiocodes.com enabled for MOS calculations:

```
 show voip register db sbc user 12345@audiocodes.com

*** SBC Registered Contacts for AOR 12345@audiocodes.com ***

============================================================
=====
<sip:12345@6t0ow5277pca.invalid;transport=ws>;+sip.ice;reg-
id=1;+sip.instance="<urn:uuid:eae4b222-cae4-40a3-abbe-
a384b87980fa>";expires=600 | IPG:0 | SI:0 | ID:0 | LastMOS:27(Gray) @
00:00:00.000 | AvgMOS:N/A(Gray) | MinMOS:N/A(Gray)
*** All SBC AORs for AOR 12345@audiocodes.com:
```

```
12345@audiocodes.com, 12345, 12345^urn:uuid:eae4b222-cae4-40a3-
abbe-a384b87980fa
```

- Displaying port registration status:

```
show voip register ports

*** Ports Registration Status ***

Gateway     Port           Status
==================================================
Module 3    Port 1    FXO    REGISTERED
------------------------------------------------
Module 3    Port 2    FXO    REGISTERED
------------------------------------------------
Module 3    Port 3    FXO    REGISTERED
------------------------------------------------
Module 3    Port 4    FXO    NOT REGISTERED
------------------------------------------------
Module 5    Port 1    FXS    NOT REGISTERED
------------------------------------------------
Module 5    Port 2    FXS    NOT REGISTERED
------------------------------------------------
Module 5    Port 3    FXS    NOT REGISTERED
------------------------------------------------
Module 5    Port 4    FXS    REGISTERED
```

- Displaying detailed information about users in the Supplementary Services table:

```
show voip register suppserv gw list

*** GW Supp Serv Users Registration Status ***

Index  Type        Status       Contact
==================================================
1      EndPoint     NOT REGISTERED  sip:4000@10.15.7.96:5060
```

show voip subscribe

This command displays active SIP SUBSCRIBE dialog sessions.

Syntax

```
show voip subscribe {list|statistics}
show voip subscribe list [<Session ID>|descending|summary]
```

Command	Description
`list`	Displays SUBSCRIBE dialog information. One of three options can be selected: ■ <Session ID> (Displays detailed information for the specified Session ID). ■ descending(Displays SUBSCRIBE dialogs sorted in descending order by call duration). ■ summary (Displays a summary of SUBSCRIBE dialogs).
`statistics`	Displays SUBSCRIBE dialog statistics including incoming and outgoing SUBSCRIBEs.

Command Mode

Basic and Privileged User

Example

Displaying a summary of active SUBSCRIBE dialogs:

```
show voip subscribe statistics
SBC SUBSCRIBE Dialog Statistics:Active SUBSCRIBE dialogs: 0
Incoming SUBSCRIBE Rate (dialogs per second): 0
Outgoing SUBSCRIBE Rate (dialogs per second): 0
Average incoming SUBSCRIBE Rate (dialogs per second): 0
Average outgoing SUBSCRIBE Rate (dialogs per second): 0
Maximum incoming SUBSCRIBE Rate (dialogs per second): 0
Maximum outgoing SUBSCRIBE Rate (dialogs per second): 0
```

show voip tags-cac

This command displays list of 'cac' keys for maximum concurrent calls per user and their current value out of the maximum call limit.

Syntax

```
show voip tags-cac
show voip tags-cac key {<Phone number or IP address>}
```

Command	Description
`show voip tags-cac`	Displays a list of 'cac' keys and their concurrent calls out of the maximum allowed concurrent calls.
`show voip tags-cac key {<Phone number or IP address>}`	Displays the current concurrent calls out of the maximum allowed concurrent calls for a specific user (specified by phone number or IP address).

Command Mode

Basic and Privileged User

Example

This example displays the current number of concurrent calls out of the maximum concurrent calls for a user with phone number 12345678:

```
show voip tags-cac key +12345678
```

show voip tdm

This command displays TDM status.

Syntax

```
show voip tdm
```

Command Mode

Basic and Privileged User

Example

The command is applicable only to devices supporting PSTN interfaces.

Example

```
show voip tdm
Clock status:
    TDM Bus Active Clock Source Internal
Configuration:
    PCM Law Select 3
    TDM Bus Clock Source 1
    TDM Bus Local Reference 0
    TDM Bus Type 2
    Idle ABCD Pattern 15
    Idle PCM Pattern 255
    TDM Bus PSTN Auto Clock Enable 0
    TDM Bus PSTN Auto Clock Reverting Enable 0
```

14 Clear Commands

This section describes the clear commands.

Syntax

```
# clear
```

This command includes the following commands:

Command	Description
`alarms-history`	See clear alarms-history below
`debug-file`	See clear debug-file on the next page
`clear history`	See clear history on the next page
`qos`	See clear qos counters on page 125
`security-files`	See clear security-files on page 125
`storage-history`	See clear storage-history on page 126
`system-log`	See clear system-log on page 127
`user`	See clear user on page 127
`voip`	See clear voip on page 128

Command Mode

Privileged User

clear alarms-history

This command deletes the Alarms History table.

Syntax

```
# clear alarms-history
```

Command Mode

Privileged User

clear debug-file

This command deletes the debug file (and core dump).

Syntax

```
# clear debug-file
```

Command Mode

Privileged User

clear history

This command deletes the CLI's command history buffer. The buffer stores all commands that you have run in the current CLI session. Typically, if you want to recall a previously typed command, which is stored in the history buffer, you press the up and down arrow keys.

Syntax

```
# clear history [<index>]
```

Command	Description
`clear history`	Deletes all commands from the command history buffer.
`clear history <index>`	Deletes a specific command (by index) from the command history buffer.

Related Commands

`history` - displays all commands in the command history buffer (by index).

Command Mode

Privileged User

Example

This example clears the historical command that is stored in the buffer at index 5 (i.e., `ignore-auth-stale`):

```
# history
  1  e
  2  history
  3  configure voip
  4  sip-definition settings
  5  ignore-auth-stale
  6  ex
  7  ex

# clear history 5
```

clear qos counters

This command deletes counter data related to quality of service.

Syntax

```
# clear qos counters
```

Command Mode

Privileged User

clear security-files

This command manually triggers zeroization (which is automatically done when enabling FIPS mode). Zeroization completely wipes out all sensitive content residing on the device:

- Security secrets (e.g., TLS private keys, certificates, and root certificates)
- Core dump files
- System Snapshot files

Syntax

```
# clear security-files
```

Command Mode

Privileged User

Related Commands

`fips` (enables FIPS mode)

Note

For products supporting FIPS mode, please contact AudioCodes.

Example

This example triggers zeroization:

```
# clear  security-files
```

clear storage-history

This command deletes the locally stored CDRs or SDR files.

Syntax

```
# clear storage-history <Service Name> {all|unused}
```

Command	Description
Service Name	The name of the service. To view services, run the `show storage-history services` command. Currently supported services: - `cdr-storage-history` - `sdr-storage-history`
`all`	Deletes all stored CDR or SDR files.
`unused`	Deletes unused locally stored CDR or SDR files.

Command Mode

Privileged User

Related Commands

`show storage-history services`

Example

- Deleting all stored CDR files:

```
# clear storage-history cdr-storage-history all
```

- Deleting all unused stored CDR files:

```
# clear storage-history cdr-storage-history unused
```

clear system-log

This command deletes the system log. This clears the Syslog messages in the CLI, and on the Web interface's Message Log page (Troubleshoot menu > Troubleshoot tab > Message Log) where it does the same as clicking the **Clear** button.

Syntax

```
# clear system-log
```

Command Mode

Privileged User

Related Commands

`show system log`

clear user

This command terminates CLI users who are currently logged in through RS-232 (console), Telnet, or SSH. When run, the command drops the Telnet/SSH session or logs out the RS-232 session, and displays the login prompt.

Syntax

```
# clear user <Session ID>
```

Command	Description
Session ID	Unique identification of each currently logged in CLI user. Allows you to end the active CLI session of a specific CLI user. You can view session IDs by running the `show users` command.

Note

The CLI session from which the command is run cannot be terminated.

Command Mode

Privileged User

Related Commands

`show users`

Example

Ending the CLI session of a specific user:

```
# clear user 1
```

clear voip

This command deletes VoIP-related information and disconnects calls.

Syntax

```
# clear voip {calls|ids|register}
```

Command	Description
`calls`	See clear voip calls below
`ids blacklist`	See clear voip ids blacklist on the next page
`register`	See clear voip register db sbc on page 130

Command Mode

Privileged User

clear voip calls

This command disconnects active calls.

Syntax

```
# clear voip calls [<Session ID>|tag]
```

Command	Description
(Carriage Return)	Disconnects all calls.
Session ID	(Optional) Disconnects the call with the specified Session ID.
`tag`	Disconnects calls that match the specified Dial Plan tag (name=value).

Command Mode

Privileged User

Related Commands

show voip calls active

Example

- Displaying and then disconnecting a call based on Session ID:

```
# show voip calls
Total Active Calls: 1
| Session ID  |    Caller       |    Callee       | Origin |    Remote IP    |End Point
Type |Duration|Call State

=============================================================
=============================================================
=========
|326433737    |3005            |2000            |Outgoing|10.8.6.36        |FXS-3/3
 |00:00:06|Connected

# clear voip calls 326433737
1 Active Calls were Manually disconnected
```

- Disconnecting calls whose Dial Plan tag is "region=usa":

```
# clear voip calls tag region=usa
```

clear voip ids blacklist

This command deletes active blacklisted remote hosts in the IDS Active Black List table.

Syntax

```
# clear voip ids blacklist {all|entry <Removal Key>}
```

Command	Description
`all`	Deletes all blacklisted entries in the IDS Active Black List table.
`entry <Removal Key>`	Deletes a blacklisted entry in the IDS Active Black List table, specified by its Removal Key.

Command Mode

Privileged User

Related Commands

show voip ids

Example

This example deletes a blacklisted entry whose Removal Key is 776-854-3:

```
# clear voip ids blacklist entry 776-854-3
```

clear voip register db sbc

This command deletes SBC users registered from the device's registration database.

Syntax

```
# clear voip register db sbc user <AOR>
# clear voip register db sbc ip-group <ID or Name>
```

Command	Description
AOR	Defines the Address of Record (AOR) of the user (user part or user@host).
ID or name	Configures an IP Group (i.e., deletes all registered users belonging to the IP Group).

Command Mode

Privileged User

Note

The command is applicable only to the SBC application.

Example

Clearing John@10.33.2.22 from the registration database:

```
# clear voip register db sbc user John@10.33.2.22
```

15 General Root Commands

This section describes general root commands. These commands are entered at root level.

Command	Description
admin	See admin below
copy	See copy on page 136
dir	See dir on page 143
erase	See erase on page 144
fips	See fips on page 145
ha	See ha on page 145
history	See history on page 146
nslookup	See nslookup on page 147
output-format	See output-format on page 148
ping	See ping on page 149
pstn	See pstn on page 151
reload	See reload on page 151
srd-view	See srd-view on page 154
system-snapshot	See system-snapshot on page 154
tail	See tail on page 156
telnet	See telnet on page 157
traceroute	See traceroute on page 158
usb	see usb on page 159
write	See write on page 159
write-and-backup	See write-and-backup on page 161

admin

This command provides various administration-related operations.

Syntax

```
admin
```

Command	Description
`register`	See admin register|unregister below
`state`	See admin state on the next page
`streaming`	See admin streaming on page 136
`unregister`	See admin register|unregister below

admin register|unregister

This command registers (or unregisters) users with a proxy server.

Syntax

```
admin register|unregister {accounts|gw|ports|suppserv|userinfo}
```

Command	Description
`accounts <Account Index>`	Registers user Accounts, configured in the Accounts table.
`gw`	Registers the device as a single entity (Gateway).
`ports <Module Number> <Port Number>`	Registers the device's ports. You need to specify the module number and port number.
`suppserv <Extension Number>`	Registers an FXS endpoint by phone number and BRI line extensions configured in the Supplementary Services table.
`userinfo {gw|sbc} <Local User>`	Registers users configured in the User Info table.

Command Mode

Basic and Privileged User

Example

This example registers Port 1 located on Module 3:

```
admin register ports 3 1
Registering module 3 port 1 (200)
```

admin state

This command locks and unlocks the device.

Syntax

- Locks the device:

```
# admin state lock {graceful <timeout>|no-graceful} [disconnect-client-connections]
```

- Unlocks the device:

```
# admin state unlock
```

Command	Description
`lock graceful <timeout>|forever`	Gracefully locks the device after a user-defined interval (seconds), during which new calls are rejected and existing calls continue. If the existing calls do not end on their own accord during the interval, the device terminates (disconnects) them when the

Command	Description
	timeout expires. To wait until all calls end on their own before locking the device (no timeout), use the `forever` option. During this time, no new calls are accepted.
`lock no-graceful`	Immediately ends (disconnects) all active calls (if any exist) and locks the device.
`disconnect-client-connections`	Closes existing TLS/TCP client connections and rejects incoming TLS/TCP client connections when the device is in locked state.
`unlock`	Unlocks the device.

Command Mode

Privileged User

Related Commands

show admin state – displays the current administrative state

Example

This example locks the device after 50 seconds and closes existing TLS/TCP connections:

```
# admin state lock graceful 50 disconnect-client-connections
```

admin streaming

This command stops or starts audio streaming of Music on Hold (MoH) from an external media player connected to an FXS port.

Syntax

```
admin streaming {start|stop}
```

Command	Description
`start {<FXS Port>|all}`	Starts audio streaming on a specific FXS port or all FXS ports.
`stop {<FXS Port>|all}`	Stops audio streaming on a specific FXS port or all FXS ports.

Command Mode

Basic and Privileged User

Example

This example starts audio streaming on FXS port 1:

```
admin streaming start 1
```

copy

This command downloads and uploads files from and to the device, respectively.

Syntax

```
# copy <File Type> from|to {<URL>|console|usb:///<Filename>} [interface <IP Interface name>]
```

Command	Description
File Type	
`aux-package`	Defines the file type as an auxiliary package file, allowing you to download or upload a batch of auxiliary files, using a TAR (Tape ARchive) file (.tar). The TAR file can contain any number and type of Auxiliary files, for example, a Dial Plan file and a CPT file.
`call-progress-tones from`	Defines the file type as a Call Progress Tones (CPT) file. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`cas-table from`	Defines the file type as a Channel Associated Signaling (CAS) table file. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`cli-script {from|to}`	Defines the file type as a CLI script file.

`configuration-pkg {from|to}`	Defines the file type as a Configuration Package file (.7z), which includes all files.
	For uploading a Configuration File that is password-protected, use the `encrypted` option to specify the password:
	`copy configuration-pkg from <URL> encrypted <Password>`
	For downloading the Configuration File, if you want to password-protect it and include the TLS certificates, use the `encrypted` and `certificates` options, respectively:
	`copy configuration-pkg from <URL> encrypted <Password> certificates`

`debug-file to`	Defines the file type as a debug file and copies the file from the device to a destination. The debug file contains the following information: ■ Exception information, indicating the specific point in the code where the crash occurred and a list of up to 50 of the most recent SNMP alarms that were raised by the device before it crashed. ■ Latest log messages that were recorded prior to the crash.

Command	Description
	- Core dump. The core dump is included only if core dump generation is enabled, no IP address has been configured, and the device has sufficient memory on its flash memory. May include additional application-proprietary debug information. The debug file is saved as a zipped file with the following file name: "debug_<device name>_ver_<firmware version>_mac_<MAC address>_<date>_<time>". For example, debug_acMediant_ver_700-8-4_mac_ 00908F099096_1-03-2015_3-29-29.
`dial-plan from`	Defines the file type as a Dial Plan file. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`ext-core-dumps to`	Defines the file type as a logged app process (TPApp) crash file (in Core Dump file). **Note:** The file can only be downloaded from the device (see the command `to` below).
`firmware from`	Defines the file type as a firmware file (.cmp). **Note:** After the .cmp file is loaded to the device, it's automatically saved to the device's flash memory with a device restart.
`incremental-ini-file from`	Defines the file type as an ini file, whereby parameters that are not included in the ini file remain at their current settings. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`ini-file {from|to}`	Defines the file type as an ini file, whereby parameters that are not included in the ini file are restored to default values. **Note:** The file can be uploaded to or downloaded from the device.
`mt-firmware`	Defines the file type as a firmware file (.cmp) for Media Transcoders (MT) in the Media Transcoding Cluster feature.
`nginx-conf-files to`	Defines the file type as an NGINX configuration file (for HTTP Proxy services). The following files are copied: - /acBin/nginx/nginx.conf: Contains the currently active

Command	Description
	configuration ■ /acBin/nginx/temp_nginx.conf: Contains the new configuration that has errors, which is not applied to the device ■ /acBin/nginx/nginx.errors: Contains error messages relating to the new configuration
`prerecorded-tones from`	Defines the file type as a Prerecorded Tones (PRT) file. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`redundant-debug-file to`	Defines the file type as a debug file of the Redundant device in the High-Availability (HA) system, and copies the file from the device to a destination. **Note:** The file can only be downloaded from the device (see the command 'from' below).
`sbc-wizard from`	Defines the file type as a SBC Wizard Configuration Template file, which is used by the Configuration Wizard. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`startup-script from`	Defines the file type as a Startup CLI script file.
`storage-history`	Defines the file type as a locally stored Call Detail Record (CDR) file. Define the name of the service. To view services, run the command `show storage-history services`. Currently supported services: `cdr-storage-history` and `sdr-storage-history`
`system-log`	Defines the file type as a system log file. **Note:** The file can only be downloaded from the device (see the command `to` below).
`system-log-no-sip`	Defines the file type as a system log file without SIP messages. **Note:** The file can only be downloaded from the device (see the command `to` below).
`system-log-persistent`	Defines the file type as a persistent system log file. **Note:** ■ The file can only be downloaded from the device (see

Command	Description
	the command `to` below). - The command is applicable only to Mediant 9000 and Mediant VE/CE.
`tls-cert from`	Defines the file type as a TLS certificate file. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`tls-private-key from`	Defines the file type as a TLS private key file. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`tls-root-cert from`	Defines the file type as a TLS trusted root certificate file. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`user-info from`	Defines the file type as a User Info file. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`vmc-firmware`	Defines the file type as a firmware file (.cmp) for Media Components (MC) in the Media Cluster feature.
`voice-prompts`	Defines the file type as a Voice Prompts (VP) file. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`web-favicon from`	Defines the file type as an icon file associated with the device's URL saved as a favorite bookmark on your browser's toolbar when using the device's Web interface. **Note:** The file can only be uploaded to the device (see the command 'from' below).
`web-logo from`	Defines the file type as an image file, which is displayed as the logo in the device's Web interface. **Note:** The file can only be uploaded to the device (see the command 'from' below).
Download or Upload	
`from`	Uploads the file to the device.
`to`	Sends the file from the device to a specified destination.

Command	Description
File Location	

URL	Defines the URL from/to which to upload/send the file.
	The file transfer protocol can be one of the following:
	■ HTTP
	■ HTTPS
	■ SCP
	■ TFTP
	Note: The URL for HTTP/S and SCP can include the authentication username and password, using the following syntax (e.g., HTTPS):
	`https://<Username>:<Password>@<IPv4 or IPv6>/<Path>`
	For example:
	`copy firmware from https://sue:1234@10.4.10.0/firmware.cmp`

`console`	Displays the current .ini configuration file on the CLI console. **Note:** The command is applicable only to the .ini configuration file (copy ini-file to).
`usb:///<file name>`	Uploads the file from a USB stick that is connected to the device, or downloads the file from the device to a USB stick connected to the device. **Note:** The command is applicable only to devices that provide a USB port interface.
IP Interface	
`interface <IP Interface>`	Defines the IP Interface by name (configured in the IP Interfaces table) to use for the copy process. By default (i.e., `interface`not configured), the device uses the IPv4 OAMP or IPv6 OAMP interface (in the IP Interfaces table) for the copy process for IPv4 or IPv6 servers, respectively. If there is no OAMP IP Interface with the same IP version (IPv4 or IPv6) as the remote server, the copy process fails.

Command Mode

Privileged User

Related Commands

- `erase`
- `dir`
- `write`

Note

- When you upload a file to the device, you must run the `write` command to save the file to flash memory; otherwise, the file is deleted when the device restarts or powers off.
- For more information on the different file types, refer to the User's Manual.
- During firmware file (.cmp) upload, a message is displayed showing uploaded progress information. The message is also displayed in the console of all other users that are currently connected to the device through CLI. The message forcibly stops the users from performing further actions, preventing them from interrupting the uploaded process. Below shows an example of such a message:

```
# copy firmware from http://10.3.1.2:1400/tftp/SIP_F7.20A.140.226.cmp
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload   Total   Spent    Left  Speed
100 40.7M  100 40.7M    0     0  1288k      0  0:00:32  0:00:32 --:--:-- 1979k
Firmware file http://10.3.1.2:1400/tftp/SIP_F7.20A.140.226.cmp was loaded.
(user: Admin, IP local)
The system will reboot when done
DO NOT unplug/reset the device
.............................................................
Firmware process done. Restarting now...
Restarting......
```

  The displayed information includes:

  - %: Percentage of total bytes downloaded and uploaded; downloaded is displayed only when downloading a file (i.e., copy from command)
  - Total: Total bytes downloaded and uploaded.
  - %: Percentage of downloaded bytes (copy from command only).
  - Received: Currently downloaded bytes (copy from command only).
  - %: Percentage of uploaded bytes (copy to command only).
  - Xferd: Currently uploaded bytes (copy to command only).
  - Average Dload: Average download speed in bytes/sec (copy from command only).
  - Speed Upload: Average upload speed in bytes/sec (copy to command).

- Time Spent: Elapsed time.
- Time Left: Time remaining for the file upload/download to complete.
- Current Speed: Current upload/download speed in bytes/sec.

Example

- Uploading firmware file from an HTTP server and using IP Interface "MyOAMP":

```
# copy firmware from http://192.169.11.11:80/SIP_F7.20A.260.002.cmp
interface MyOAMP
```

- Displaying (copying) the ini configuration file to the CLI console:

```
# copy ini-file to console
```

- Uploading Auxilliary file batch from an HTTP server:

```
# copy myauxfiles.tar from http://www.exmaple.com/auxiliary
```

- Uploading CLI-based configuration from a TFTP server:

```
# copy cli-script from tftp://192.168.0.3/script1.txt
```

- Upgrading the device’s firmware from an HTTP server:

```
# copy firmware from http://www.exmaple.com/firmware.cmp
```

- Uploading Dial Plan file:

```
copy dial-plan from http://10.4.2.2/MyHistoryFiles/
```

- Downloading logged DTLS app process crash (in Core Dump file):

```
copy ext-core-dumps to http://10.4.2.2/Logs/ interface MyOAMP name DTLS
```

dir

This command displays the device’s current auxiliary files directory.

Syntax

```
# dir
```

Command Mode

Privileged User

Example

Displaying the device’s current auxiliary files directory:

```
# dir
directory listing:
call-progress-tones [usa_tones_13.dat]  9260 Bytes
cas-table [Earth_Calling.dat]   43852 Bytes
tls-private-key [pkey.pem]      940 Bytes
tls-cert [server.pem]   643 Bytes
```

erase

This command deletes a file from the device's memory.

Syntax

```
# erase <File Name>
```

Note

- View files using the `dir` command.
- To make sure the file type is correctly entered, copy it from the `dir` command output.
- The `erase` command only deletes the file from the device's RAM (and from the device’s current usage). To delete the file permanently (from flash memory), run the `dir` command, and then run the `write` command.

Command Mode

Privileged User

Related Commands

- `copy`
- `dir`
- `write`

Example

- Viewing files:

```
# dirdirectory listing:
/cert/1/pkey    2488 Bytes
/cert/1/cert    1318 Bytes
debug-file [core_MP500_E-SBC_ver_760A-92-882_bid_5b1035-89_SIP_
TPApp-WEBS_18-3-2                          025_11-25-25.lzma]     5380710
Bytes   Storage Type: internal-flash
```

- Erasing the CPT file from flash memory:

```
# erase debug-file
# write
```

fips

This command enables the device to operate in FIPS mode to fully comply with Federal Information Processing Standards (FIPS) 140-2 Level 1, which is a security standard specified by the United States Government that is used to validate cryptographic modules (i.e., the device).

Syntax

```
# fips on|off
```

Command Mode

Privileged User

Note

FIPS is supported only by Mediant 4000B and Mediant 9080.

Related Commands

`clear security-files` (manually triggers zeroization)

ha

This command performs various High-Availability (HA) maintenance operations.

Syntax

```
# ha
```

Command	Description
`manual-switch-over`	Forces an HA switchover from active to redundant unit.
`reset-redundant-unit`	Restarts the redundant unit.

Note

The command is applicable only to HA-supporting devices.

Command Mode

Privileged User

history

This command displays the CLI's command history buffer. The buffer stores all commands that you have run in the current CLI session. Typically, if you want to recall a previously typed command, which is stored in the history buffer, press the up and down arrow keys. The command history buffer is automatically cleared of all stored commands when you close the session.

Syntax

```
# history
```

Related Commands

- `clear history` - deletes the stored commands in the command history buffer.
- `password-history-visible` - hides passwords in the command history buffer.

Command Mode

Privileged User

Example

This example displays the commands in the command history buffer:

```
# history
 e
 2  conf voip
 3  sip-definition account 1
 4  password *******
 5  ex
```

nslookup

This command queries the Domain Name System (DNS) to obtain domain name mapping or IP address mapping, using the name server look up tool.

Syntax

```
nslookup <Hostname> {force|source|type}
```

Command	Description
Hostname	Defines the host name.
`force`	Enables the device to use the default DNS servers (primary and secondary) for nslookup. It only uses the default DNS servers when all other DNS servers fail as described in chronological order: 1. The device uses the DNS server configured for the associated IP Interface. 2. If no DNS server was configured for the associated IP Interface or no IP Interface was associated, the device uses the DNS server configured for the default OAMP IP Interface. 3. If no DNS server was configured for the OAMP IP interface, only then does the device uses the default DNS servers.
`source voip interface {name|vlan} {force|type}`	(Optional) Defines an IP interface name or VLAN ID (1 - 3999).
`type {a|aaaa|cname |naptr|srv}`	(Optional) Defines the type of DNS query.

Note

The DNS server must be configured for this command to function. The DNS server can be configured using:

- Internal DNS table: configure network > dns dns-to-ip
- Internal SRV table: configure network > dns srv2ip
- IP Interfaces table: configure network > interface network-if
- Default DNS servers: configure network > dns settings > dns-default-primary-server-ip

Command Mode

Basic and Privileged User

Example

- This example looks up the IP address of Google:

```
nslookup google.com
google.com resolved to 216.58.213.174
```

output-format

This command enables the output of certain show commands to be displayed in JSON format.

Syntax

```
output-format
```

Command	Description
`json`	Displays the output in JSON format.
`plain`	Displays the output in regular plain text format.

Note

The JSON format is supported only by certain show commands. For filtering the output, see the first, last, range and descending commands in Section Common CLI Commands on page 11.

Command Mode

Basic User and Privileged User

Example

The example displays only the first two calls and in JSON format:

```
output-format json
show voip calls history sbc first 2
{
"History" : [
{
   "CallEndTime": "08:21:41.376  UTC Wed Mar 28 2018",
   "IpGroup": "Linux",
   "Caller": "sipp",
   "Callee": "service",
   "Direction": "Incoming",
   "Duration": "00:00:17",
   "RemoteIP": "10.33.5.141",
   "TermReas": "NORMAL_CALL_CLEAR",
   "SessionId": "3c71d9:152:621"
},
{
   "CallEndTime": "08:21:41.366  UTC Wed Mar 28 2018",
   "IpGroup": "Linux",
   "Caller": "sipp",
   "Callee": "service",
   "Direction": "Outgoing",
   "Duration": "00:00:17",
   "RemoteIP": "10.33.5.141",
   "TermReas": "NORMAL_CALL_CLEAR",
   "SessionId": "3c71d9:152:621"
}
]
}
```

ping

This command sends (pings) ICMP echo request messages to a remote destination (IP address or FQDN) to check connectivity. Pings have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of "pad" bytes used to fill out the packet. Ping works with both IPv4 and IPv6.

Syntax

```
ping {<IPv4 Address>|ipv6 <IPv6 Address>|<Hostname>} [source voip interface
{vlan <VLAN ID>|name <Interface Name>}] [repeat <Echo Requests>] [size
<Payload Size>] [tos|traffic-class <0-254>]
```

Command	Description
<IPv4 Address>	Configures an IPv4 IP address in dotted-decimal notation.
`ipv6 <IPv6 Address>`	Configures an IPv6 address as X:X::X:X.
<Hostname>	Configures a hostname or FQDN (.g., abc.com).
`source voip interface`	(Optional) Defines the interface from where you want to ping. This can be one of the following: ■ vlan (configures the VLAN ID) ■ name (configures the IP network interface name)
`repeat`	(Optional) Defines the number (1-300) of echo requests.
`size`	(Optional) Defines the payload size (0-max packet size).
`tos|traffic-class`	(Optional) Defines the QoS of the ping packets by setting a value (0-254) in the IPv4 (tos) or IPv6 (traffic-class) header.

Command Mode

Basic and Privileged User

Note

To terminate the ping, use the key combination Ctrl+C.

Example

- Sending 3 ICMP packets with 555 bytes payload size to 10.4.0.1 via interface VLAN 1:

```
ping 10.4.0.1 source voip interface vlan 1 repeat 3 size 555
PING 10.4.0.1 (10.4.0.1): 555 data bytes
563 bytes from 10.4.0.1: icmp_seq=0 ttl=255 time=1.3 ms
563 bytes from 10.4.0.1: icmp_seq=1 ttl=255 time=1.1 ms
563 bytes from 10.4.0.1: icmp_seq=2 ttl=255 time=1.2 ms
--- 10.4.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0 packet loss
round-trip min/avg/max = 1.1/1.2/1.3 ms
```

- Pinging an FQDN:

```
ping corp.abc.com source voip interface vlan 1
```

- Pinging an IPv6 destination address with QoS definition:

```
ping ipv6 2001:15::300 traffic-class 100
```

pstn

This command initiates a manual switchover between D-channels (primary and backup) pertaining to the same Non-Facility Associated Signaling (NFAS) group.

Syntax

```
# pstn nfas-group-switch-activity <NFAS Group Number>
```

Note

The command is applicable only devices supporting digital PSTN interfaces.

Command Mode

Privileged User

Example

```
# pstn nfas-group-switch-activity 2
```

reload

This command restarts the device, with or without saving configuration to flash memory.

A required device restart is indicated by an asterisk (*) before the command prompt, as shown in the following example:

```
(sip-def-settings)# user-inf-usage on
(sip-def-settings)*#
```

Syntax

```
# reload {if-needed|now|without-saving}
```

Command	Description
`if-needed [graceful]`	Restarts the device only if you have configured parameters that require a device restart for their new settings to take effect. The restart can be done immediately or upon certain conditions: ■ `reload if-needed`: Restarts the device immediately. ■ `reload if-needed graceful <seconds>`: Restarts the device only after the user-defined period (in seconds) elapses.
`now [graceful]`	Restarts the device immediately and saves configuration (including Auxiliary files) to flash memory (before restart). The restart can be done immediately or upon certain conditions: ■ `reload now` : Restarts the device immediately. ■ `reload now graceful <seconds>`: Restarts the device only after the user-defined period (in seconds) elapses. ■ `reload now graceful if-no-calls`: ✓ If calls exist, the device doesn't restart and displays "Not Good (In Call)".

Command	Description
	✓ If no calls exist, the device restarts immediately and displays "OK". ✓ If the device is unable to restart (for whatever reason), it displays "Not Good".
`without-saving [in <Minutes>|graceful <Seconds>]`	Restarts the device without saving configuration to flash memory. (Optional) You can configure a delay time before restart occurs: ■ `in`: Restarts the device only after a user-defined period (in minutes). Use this before making changes to sensitive settings. If your changes cause the device to lose connectivity, wait for the device to restart with the previous working configuration. ■ `graceful`: Restarts the device within a user-defined graceful period (in seconds) to allow currently active calls (if any) to end. During this graceful period, no new calls are accepted. If all currently active calls end before the graceful period expires, the device restarts immediately (instead of waiting for the graceful period to expire). If there are active calls when the graceful period expires, the device terminates the calls and restarts. To cancel the delayed restart, use the `no reload` command.

Command Mode

Privileged User

Related Commands

- `write`
- `reload-timeout-for-emergency-call`

Example

This example restarts the device immediately only if there are parameters that have been modified which require a restart to take affect:

```
# reload if-needed
```

srd-view

This command access a specific SRD (tenant) view. To facilitate configuration of the Multi-Tenancy feature through the CLI, the administrator can access a specific tenant view. Once in a specific tenant view, all configuration commands apply only to that specific tenant and the tenant's name (SRD name) forms part of the CLI prompt. Only table rows (indexes) belonging to the viewed tenant can be modified. New table rows are automatically associated with the viewed tenant (i.e., SRD name).

Syntax

```
srd-view <SRD Name>
```

Command Mode

Basic and Privileged User

Note

To exit the tenant view, enter the following command:

```
no srd-view
```

Example

Accessing the 'itsp' tenant view:

```
srd-view itsp
(srd-itsp)#
```

system-snapshot

This command is for managing snapshots that are can be used for system recovery. The device can maintain up to 10 snapshots. If 10 snapshots exist and you create a new one, the oldest snapshot is removed to accommodate the newly created snapshot.

Syntax

```
# system-snapshot
```

Command	Description
`create <Snapshot Name> [force]`	Creates a snapshot of the system. If no name is defined, a default name is given to the snapshot. If you enter the force command, the device overrides the oldest snapshot with this one if the maximum number of system snapshots has been reached. The final snapshot name is in the following format: <Snapshot Name>-<Version>-<Creation Time> The device's version is automatically added as well as the date and time of the snapshot creation.
`default <Snapshot Name>`	Defines the default rescue snapshot. If no name is specified, the current snapshot is made default.
`delete <Snapshot Name>`	Deletes a snapshot.
`load <Snapshot Name>`	Recovers the device by loading a snapshot. If no name is entered, the default snapshot is loaded.
`rename <existing name> <new name>`	Modifies the name of a snapshot.
`show`	Displays all saved snapshots. The default system snapshot is shown with an asterisk (*).

Command Mode

Privileged User

Note

The command is applicable only to Mediant 9000 and Mediant SE/VE.

Example

This example creates a snapshot of the system with the name "My-Snapshot":

```
# system-snapshot create My-Snapshot
```

tail

This command displays the last lines (tail end) of the output of certain show log commands. The number of lines to show can optionally be specified. If not specified, the last 100 lines are shown by default. This is useful for long outputs where you need to scroll all the way down to view the last lines.

Syntax

```
# tail {cloud-init-log|cloud-manager-log|aws-manager-log|system log} [<lines>]
```

Command	Description
`tail cloud-init-log [<lines>]`	Shows cloud-init logs (Mediant Software SBC only).
`tail cloud-manager-log [<lines>]`	Shows Cloud Manager logs (Mediant Software CE/VE SBC only.
`tail aws-manager-log [<lines>]`	Shows AWS manager logs (Mediant Software SBC on AWS only).
`tail system log [<lines>]`	Shows system logs.
`tail system log no-sip [<lines>]`	Shows system logs without SIP messages.
`tail system log persistent [<lines>]`	Shows persistent system logs.

Command Mode

Privileged User

Example

This example displays the last 8 lines of the `system log` output:

```
# tail system log 8
To: <sip:2000@10.8.5.92>;tag=1c1941351400
Call-ID: 15310103972732022122059@10.8.5.92
CSeq: 11341 REGISTER
```

```
Reason: SIP ;cause=500 ;text="IPGroup Registration Mode Configuration"
Content-Length: 0

 [Time:04-04@15:31:48.705]
Apr  4 15:31:48.705 local3.notice [S=783984] [SID=5f4b8a:231:39752]  (N
694002) (#34257)gwSession[Deallocated] [Time:04-04@15:31:48.706]
```

telnet

This command invokes a Telnet session from the device towards a remote host for remote management. A remote administrator can access the device's CLI from the WAN leg while performing the full authentication process. The administrator can then invoke Telnet sessions towards other devices in the LAN to manage them. No special pin-holes or forwarding rules need be declared to manage them.

Syntax

```
# telnet <Address> <Port> interface vlan <VLAN ID>
```

Command	Description
Address	Remote host IP address.
Port	(Optional) Remote host port number.
`interface vlan`	(Optional) Device's VLAN ID from where you want to create the Telnet session.

Command Mode

Privileged User

Example

Invoking a Telnet session:

```
# telnet 10.4.4.25
```

- Invoking a Telnet session to a device located on the LAN:

```
# telnet 11.11.11.201 23  interface vlan 1
```

traceroute

This command performs a traceroute and displays the route (path) and packet transit delays across an IP network, for diagnostic purposes.

Syntax

```
traceroute {<IPv4 Address or Hostname>|ethernet|ipv6}
```

```
traceroute ethernet mpid <Endpoint Identifier> domain <Domain Name>
```

```
traceroute {ipv6 <IPv6 Address>|<IPv4 Address or Hostname>}
```

```
traceroute {ipv6 <IPv6 Address>|<IPv4 Address or Hostname>} interface {name
<Interface Name>|vlan <VLAN ID>} [proto udp|icmp]
```

```
traceroute {ipv6 <IPv6 Address>|<IPv4 Address or Hostname>} proto udp|icmp
```

Command	Description
IPv4 Address or Hostname	The IPv4 address or hostname to which the trace is sent.
`interface {name|vlan}`	Name of the IP Interface or VLAN ID.
`proto {icmp|udp}`	Defines the protocol type. The default is UDP. IPv4 traceroute also supports icmp protocol type.

Note

- Supports both IPv4 and IPv6 addresses.
- In IPv4, it supports hostname resolution as well.
- Sends three requests to each hop on the way to the destination.

Command Mode

Basic and Privileged User

Example

Examples of using this command:

- IPv6:

```
traceroute ipv6 2014:6666::dddd
1  2014:7777::aa55 (2014:7777::aa55)  2.421 ms  2.022 ms  2.155 ms
2  2014:6666::dddd (2014:6666::dddd)  2.633 ms  2.481 ms  2.568 ms
Traceroute: Destination reached
```

- IPv4:

```
traceroute 10.3.0.2
1  1 (10.4.0.1)  2.037 ms  3.665 ms  1.267 ms
2  1 (10.3.0.2)  1.068 ms  0.796 ms  1.070 ms
Traceroute: Destination reached
```

usb

This command allows maintenance on USB sticks plugged into the device.

Syntax

```
# usb
```

Command	Description
`list`	Displays files located on the USB.
`remove`	Safely removes a USB stick that is plugged into the device.

Command Mode

Privileged User

Note

The command is applicable only devices that provide USB port interfaces.

write

This command saves the device's current configuration to flash memory or optional, restores the device to factory defaults.

Syntax

```
# write
```

Command	Description
(Carriage Return)	Saves configuration to flash memory .
`factory [clear-keys-and-certs|keep-network-and-users-configuration]`	Restores the device's configuration to factory defaults. You can also use the following options: ■ `clear-keys-and-certs`: Restores configuration to factory defaults and deletes all TLS-related files (TLS certificates, root certificates and public keys) used by the TLS Contexts. ■ `keep-network-and-users-configuration`: Restores configuration to factory defaults, except network settings, which ensures that the device’s management interfaces can be accessed using the current OAMP network interface address after the device is restored to default.

Command Mode

Privileged User

Note

- The `write` command does not restart the device. For parameters that require a restart for their settings to take effect, use the `reload now` command instead, or use it after the `write` command.
- The `write factory` command (without `keep-network-and-users-configuration)` erases all current network configuration and thus, remote connectivity to the device (Telnet/SSH) may fail immediately after you run this command.
- The `write factory` command also erases the Auxiliary files.

Related Commands

reload now

Example

Saving the configuration to flash memory:

```
# write
Writing configuration…done
```

write-and-backup

This command saves the device's configuration file to flash memory and uploads it to a specified destination. The feature provides a method to back up your saved configuration.

Syntax

```
# write-and-backup to {<URL>|usb}
```

Command	Description
`URL`	Defines the destination as a URL (TFTP or HTTP/S) to a remote server.
`usb`	Defines the destination to a folder on a USB storage stick plugged in to the device.

Command Mode

Privileged User

Note

- The USB option applies only to devices with USB interfaces.
- The configuration of the backed-up file is based only on CLI commands.
- The device first saves the configuration file to flash memory and then sends the file to the configured destination.

Related Commands

write

Example

- Saving a device's configuration to flash memory and sends it to a HTTP remote server:

```
# write-and-backup to http://www.example.com/configuration.txt
```

- Saving a device's configuration to flash memory and sends it to the plugged-in USB stick:

```
# write-and-backup to usb:///configuration.txt
```

Part III

System-Level Commands

16 Introduction

This part describes the commands located on the System configuration level. The commands of this level are accessed by entering the following command at the root prompt:

Syntax

```
# configure system
(config-system)#
```

This level includes the following commands:

Command	Description
automatic-update	See automatic-update on page 165
cli-settings	See cli-settings on page 175
clock	See clock on page 181
configuration-version	See configuration-version on page 183
feature-key	See feature-key on page 184
floating-license	See floating-license on page 185
http-services	See http-services on page 187
hw	See hw on page 192
hostname	See hostname on page 193
kpi alarm-thresholds	See kpi alarm-thresholds on page 197
ldap	See ldap on page 200
login-oauth-servers	See login-oauth-servers on page 206
metering-client	See metering-client on page 207
management-access-list	See management-access-list on page 208
mgmt-auth	See mgmt-auth on page 209
ntp	See ntp on page 211
oauth-servers	See oauth-servers on page 213

Command	Description
`packetsmart`	See packetsmart on page 215
`performance-profile`	See performance-profile on page 216
`radius`	See radius on page 218
`sbc-performance-settings`	See sbc-performance-settings on page 221
`snmp`	See snmp on page 222
`user`	See user on page 231
`user-defined-failure-pm`	See user-defined-failure-pm on page 234
`users-settings`	See users-settings on page 235
`web`	See web on page 236
`welcome-msg`	See welcome-msg on page 240

Command Mode

Privileged User

17 automatic-update

This command configures the Automatic Update feature.

Syntax

```
(config-system)# automatic-update
(auto-update)#
```

Command	Description
<Files to Upload>	For commands under `automatic-update` that specify the files to upload for the Automatic Update feature, see Files to Upload on page 167.
`aupd-graceful-shutdown <Seconds>`	Enables the graceful lock period for Automatic Update and defines the period.
`aupd-interface`	Assigns an IP Interface (configured in the IP Interfaces table) for the Auto-Update mechanism.
`crc-check {off|regular|voice-conf-ordered}`	Enables the device to run a Cyclic Redundancy Check (CRC) on the downloaded configuration file to determine whether the file content (regardless of file timestamp) has changed compared to the previously downloaded file. Depending on the CRC result, the device installs or discards the downloaded file. regular: CRC considers order of lines in the file (i.e., same text must be on the same lines). voice-conf-ordered: CRC ignores the order of lines in the file (i.e., same text can be on different lines).
`credentials`	Defines the username and password for digest (MD5 cryptographic hashing) and basic access authentication with the HTTP server on which the files to download are located for the Automatic Update feature.
`default-configuration-package-password <password>`	Defines the password used to protect (encrypt) the Configuration Package file when it's uploaded to the device using the Automatic Update feature (see the `configuration-pkg` command). If the file is not password-protected, then ignore this command. **Note:** The password configured by this command is also used for protecting (encrypting) the Configuration

Command	Description
	Package file when downloading it from the device through SFTP.
`http-user-agent`	Defines the information sent in the HTTP User-Agent header. For more information, see http-user-agent on page 170.
`max-transfer-time`	Defines the file transfer timeout (minutes) for downloading a file from the provisioning server for automatic updates.
`predefined-time`	Defines the time of day in the format hh:mm (i.e., hour:minutes).
`predefined-random-time`	Defines the maximum randomization interval (in seconds) for the daily scheduled automatic update.
`run`	Triggers the Automatic Update feature. **Note:** The command does not replace the activate command
`run-on-reboot {off|on}`	Enables the Automatic Update feature to run when the device restarts (or powers up).
`template-files-list`	Defines the type of files in the file template to download from a provisioning server for the Automatic Update process. For more information, see template-files-list on page 171.
`template-url`	Defines the URL address of the provisioning server on which the file types, specified in the file template using the template-files-list command are located for download for the Automatic Update process. For more information, see template-url on page 172.
`tftp-block-size`	Defines the TFTP block size according to RFC 2348.
`update-firmware {off|on}`	Enables automatic update of the device's software file (.cmp).
`update-frequency-sec`	Defines the interval (in minutes) between subsequent Automatic Update processes.
`verify-certificate {off|on}`	Enables verification of the server certificate over HTTPS. The device authenticates the certificate against the

Command	Description
	trusted root certificate store of the associated TLS Context. Only if authentication succeeds does the device allow communication.
`verify-cert-subject-name {off|on}`	Enables verification of the SSL Subject Name (Common Name) in the server's certificate when using HTTPS. If the server's URL contains a hostname, the device validates the server's certificate subject name (CN/SAN) against this hostname (and not IP address); otherwise, the device validates the server's certificate subject name against the server's IP address

Command Mode

Privileged User

Files to Upload

This command automatically uploads specified files to the device from a remote server.

Syntax

```
(config-system)# automatic-update
(auto-update)#
```

Command	Description
`auto-firmware`	Defines the URL path to a remote server from where the software file (.cmp) can be uploaded. This is based on timestamp.
`call-progress-tones`	Defines the URL path to a remote server from where the Call Progress Tone (CPT) file can be uploaded.
`cas-table`	Defines the URL path to a remote server from where the Channel Associated Signaling (CAS) file can be uploaded.
`cli-script`	Defines the URL path to a remote server from where the CLI Script file can be uploaded.
`configuration-pkg`	Defines the URL path to a remote server from where the Configuration Package file can be uploaded.

Command	Description
	Note: If the file is password-protected (encrypted), define the password using the `default-configuration-package-password` command.
`dial-plan`	Defines the URL path to a remote server from where the Dial Plan file can be uploaded.
`dial-plan-csv`	Defines the URL path to a remote server from where the Dial Plan file (.csv) can be uploaded.
`feature-key`	Defines the URL path to a remote server from where the License Key file can be uploaded.
`firmware`	Defines the URL path to a remote server from where the software file (.cmp) file can be uploaded. **Note:** This is a one-time file update; once uploaded, the device does not uploaded it again.
`gw-user-info`	Defines the name of the Gateway User Information file and the URL address (IP address or FQDN) of the server where the file is located.
`incremental-ini-file`	Defines the name of the incremental *ini* file (configuration) and the URL address (IP address or FQDN) of the server where the file is located. Parameters that are not included in the ini file remain at their current settings.
`ini-file`	Defines the URL path to a remote server from where the voice configuration file can be uploaded.
`mt-firmware`	Defines the URL path to a remote server from where the software file (.cmp) for the MT device, participating in the Media Transcoding Cluster, can be uploaded.
`prerecorded-tones`	Defines the URL path to a remote server from where the Prerecorded Tone file can be uploaded.
`sbc-user-info`	Defines the name of the SBC User Information file and the URL address (IP address or FQDN) of the server where the file is located.
`sbc-wizard`	Defines the URL path to a remote server from where

Command	Description
	the SBC Wizard configuration template file can be uploaded.
`startup-script`	Defines the URL path to a remote server from where the Startup Script file can be uploaded.
`tls-cert`	Defines the URL path to a remote server from where the TLS certificate file can be uploaded.
`tls-private-key`	Defines the URL path to a remote server from where the TLS private key file can be uploaded.
`tls-root-cert`	Defines the URL path to a remote server from where the TLS root CA file can be uploaded (replaces existing files).
`tls-root-cert-incr`	Defines the URL path to a remote server from where the TLS root CA file can be uploaded (incremental file uploaded).
`user-info`	Defines the URL path to a remote server from where the User Info file can be uploaded.
`vmc-firmware`	Defines the URL path to a remote server from where the software file (.cmp) for the Media Component (MT), participating in the Media Cluster, can be uploaded.
`vmt-firmware`	Defines the URL path to a remote server from where the software file (.cmp) for the vMT device, participating in the Media Transcoding Cluster, can be uploaded.
`voice-prompts`	Defines the URL path to a remote server from where the Voice Prompts file can be uploaded.
`web-favicon`	Defines the URL path to a remote server from where the favicon image file for the favorite bookmark on your Web browser's toolbar associated with the device's URL, can be uploaded.
`web-logo`	Defines the URL path to a remote server from where the logo image file for the Web interface can be uploaded.

Command Mode

Privileged User

Note

The URL can be IPv4 or IPv6. If IPv6, enclose the address in square brackets:

- URL with host name (FQDN) for DNS resolution into an IPv6 address:

```
http://[FQDN]:<port>/<filename>
```

- URL with IPv6 address:

```
http://[IPv6 address]:<port>/<filename>
```

Example

Automatic update of a CLI script file:

```
# configure system
(config-system)# automatic-update
(auto-update)# cli-script "http://192.168.0.199/cliconf.txt"
Note: Changes to this parameter will take effect when applying the
'activate' or 'exit' command
(automatic-update)# activate
```

http-user-agent

This command configures the information sent in the HTTP User-Agent header in HTTP Get requests.

Syntax

```
(config-system)# automatic-update
(auto-update)# http-user-agent <String>
```

Command Mode

Privileged User

Note

Refer to the User's Manual for detailed information on configuring the string using placeholders (e.g., "<NAME>", "<MAC>", "<VER>", and "<CONF>").

Example

Configuring HTTP User-Agent header using placeholders:

```
(config-system)# automatic-update
(auto-update)# http-user-agent ITSPWorld-<NAME>;<VER>(<MAC>)
```

Above configuration may generate the following in the header:

```
User-Agent: ITSPWorld-Mediant;7.20.200.001(00908F1DD0D3)
```

template-files-list

This command configures which type of files in the file template to download from a provisioning server for the Automatic Update process. For more information on file templates, refer to the User's Manual.

Syntax

```
(config-system)# automatic-update
(auto-update)# template-files-list <File Types>
```

Command	Description
<File Types>	Defines the file types: `ini`: ini file `init`: ini template file `cli`: CLI Script file `clis`: CLI Startup Script file `acmp`: CMP file based on timestamp `vp`: Voice Prompts (VP) file (applies only to Mediant 1000B) `usrinf`: User Info file `cmp`: CMP file `fk`: Feature Key file `cpt`: Call Progress Tone (CPT) file

Command	Description
	■ prt: Prerecorded Tones (PRT) file ■ cas: CAS file (applies only to Digital PSTN supporting devices) ■ dpln: Dial Plan file ■ amd: Answering Machine Detection (AMD) file ■ sslp: SSL/TLS Private Key file ■ sslr: SSL/TLS Root Certificate file ■ sslc: SSL/TLS Certificate file

Command Mode

Privileged User

Note

The file types must be separated by commas, but without spaces.

Related Commands

template-url

Example

Specifying the ini, License Key, and CPT file types to download:

```
(config-system)# automatic-update
(auto-update)# template-files-list ini,fk,cpt
```

template-url

This command configures the URL address of the provisioning server on which the file types, specified in the file template using the template-files-list command are located for download during the Automatic Update process. For more information on file templates, refer to the User's Manual.

Syntax

```
(config-system)# automatic-update
(auto-update)# template-url <URL>/<File Name <FILE>>
```

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>&lt;URL&gt;</td><td>Defines the URL address of the provisioning server (HTTP/S, FTP, or TFTP).</td></tr>
<tr><td>File Name
&lt;FILE&gt;</td><td>Defines the file name using the <FILE> placeholder. The placeholder is replaced by the following hard-coded strings, depending on file type as configured by the template-files-list command:
<table>
<tr><th>File Type (template-files-list)</th><th>Hard-coded String</th></tr>
<tr><td><code>ini</code></td><td>device.ini</td></tr>
<tr><td><code>init</code></td><td>deviceTemplate.ini</td></tr>
<tr><td><code>cli</code></td><td>cliScript.txt</td></tr>
<tr><td><code>clis</code></td><td>cliStartupScript.txt</td></tr>
<tr><td><code>acmp</code></td><td>autoFirmware.cmp</td></tr>
<tr><td><code>vp</code></td><td>vp.dat
(applies only to Mediant 1000B)</td></tr>
<tr><td><code>usrinf</code></td><td>userInfo.txt</td></tr>
<tr><td><code>cmp</code></td><td>firmware.cmp</td></tr>
<tr><td><code>fk</code></td><td>fk.ini</td></tr>
<tr><td><code>cpt</code></td><td>cpt.dat</td></tr>
<tr><td><code>prt</code></td><td>prt.dat</td></tr>
<tr><td><code>cas</code></td><td>cas.dat
(applies only to Digital PSTN devices)</td></tr>
<tr><td><code>dpln</code></td><td>dialPlan.dat</td></tr>
<tr><td><code>amd</code></td><td>amd.dat</td></tr>
<tr><td><code>sslp</code></td><td>pkey.pem</td></tr>
<tr><td><code>sslr</code></td><td>root.pem</td></tr>
<tr><td><code>sslc</code></td><td>cert.pem</td></tr>
</table>
</td></tr>
</table>

Command Mode

Privileged User

Related Commands

template-files-list

Example

Specifying the URL of an HTTP server at 10.8.8.20 from which the files specified in the file template can be downloaded:

```
#(config-system)# automatic-update
(auto-update)# template-url http://10.8.8.20/Site1_<FILE>
```

If the template file list is configured as follows:

```
(auto-update)# template-files-list ini,fk,cpt
```

the device sends HTTP requests to the following URLs:

- http://10.8.8.20/Site1_device.ini
- http://10.8.8.20/Site1_fk.ini
- http://10.8.8.20/Site1_cpt.data

18 cli-settings

This command configures various CLI settings.

Syntax

```
(config-system)# cli-settings
(cli-settings)#
```

Command	Description
`cli-alias`	Defines the CLI Aliases table (see cli-alias on page 178).
`default-window-height`	Defines the number (height) of output lines displayed in the CLI terminal window. This applies to all new CLI sessions and is preserved after device restarts. The valid value range is -1 (default) and 0-65535: ■ A value of -1 means that the parameter is disabled and the settings of the CLI command `window-height` is used. ■ A value of 0 means that all the CLI output is displayed in the window. If the window is too small to display all the lines, the window displays all the lines by automatically scrolling down the lines until the last line (i.e., the "—MORE—" prompt is not displayed). ■ A value of 1 or greater displays that many output lines in the window and if there is more output, the “—MORE—" prompt is displayed. For example, if you configure the parameter to 4, up to four output lines are displayed in the window and if there is more output, the “—MORE—" prompt is displayed (at which you can press the spacebar to display the next four output lines). **Note:** You can override this parameter for a specific CLI session and configure a different number of output lines, by using the window-height CLI command in the currently active CLI session.
`idle-timeout`	Defines the maximum duration (in minutes) that a CLI session can remain idle, before being disconnected.

Command	Description
`password-obscurity {off|on}`	Displays passwords in encrypted (obscured) format in the output of the `show running-config` command. The word "obscured" is also shown to indicate that it's an encrypted password. Below shows an example of an obscured password configured for a Remote Web Service (`http-remote-services`): `rest-password 8ZybmJHExMTM obscured`
`password-history-visible {off|on}`	Hides passwords (default - `off`) by replacing them with asterisks (*) in the CLI's command history buffer (see history on page 146).
`privilege-password`	Defines the password for the privilege (Enable) mode.
`ssh {off|on}`	Enables secure access using SSH.
`ssh-acl`	Assigns an Access List entry (client) permitted to access the SSH interface. The Access List is configured by the access-list command.
`ssh-admin-key`	Defines the RSA public key (hexadecimal) for SSH client login.
`ssh-ciphers-string`	Defines the SSH cipher string.
`ssh-if`	Defines SSH interfaces (see ssh-if on page 179).
`ssh-kex-algorithms-string`	Defines the SSH Key Exchange Algorithms.
`ssh-last-login-message {off|on}`	Enables the display of the last address from which the user logged into the SSH server.
`ssh-macs-string`	Defines the SSH MAC algorithms.
`ssh-max-binary-packet-size`	Defines the maximum SSH binary packet size.
`ssh-max-login-attempts`	Defines the maximum number of SSH login attempts.
`ssh-max-payload-size`	Defines the maximum size of the SSH payload (in bytes).

Command	Description
`ssh-max-sessions`	Defines the maximum number of SSH sessions.
`ssh-port`	Defines the local port for SSH.
`ssh-require-public-key {off|on}`	Enables SSH authentication via RSA public key.
`ssh-red-device-port`	Defines the proxy SSH port number on the active device for accessing the redundant device's embedded SSH server from the active device for downloading files from the redundant device. **Note:** The command is applicable only to device's in HA mode.
`telnet-mode {disable|enable|ssl-only}`	Enables Telnet access to the device.
`telnet-acl`	Assigns an Access List entry (client) permitted to access the Telnet interface. The Access List is configured by the access-list command.
`telnet-if`	Defines Telnet interfaces (see telnet-if on page 180).
`telnet-port`	Defines the local port number for Telnet.
`telnet-max-sessions`	Defines the maximum number of Telnet sessions.
`verify-telnet-cert {disable|require}`	Enables or disables verification of peer (client) certificate by Telnet server.
`window-height {0|1-65535|automatic}`	Defines the height of the CLI terminal window for the current CLI session **only**: ■ 0: All the CLI output lines are displayed. If the window is too small to display all the lines, the window displays all the lines by automatically scrolling down the lines until the last line (i.e., the "—MORE—" prompt is not displayed). ■ 1-65535: Defines the number of lines to display in the window. ■ automatic: Whenever you manually change the height of the window (i.e., by dragging with the mouse), the new size is automatically saved.

Command	Description
	Note: The window height can be configured for all sessions using the CLI command, default-window-height.

Command Mode

Privileged User

Example

The example configures the CLI terminal window height to 15 lines:

```
(config-system)# cli-settings
(cli-settings)# window-height 15
```

cli-alias

This command configures the CLI Aliases table, which lets you define aliases that act as shortcuts for CLI commands.

Syntax

```
(config-system)# cli-settings
(cli-settings)# cli-alias <Index>
(cli-alias-<Index>)#
```

Command	Description
Index	Defines the table row index.
`alias-command`	Defines the command for which you want to create an alias.
`alias-name`	Defines the alias for the command. **Note:** The value is case-sensitive and cannot include spaces.

Command Mode

Privileged User

Related Commands

`show alias`

Example

This example configures the alias "CopyF" for the command `copy firmware from`:

```
(config-system)# cli-settings
(cli-settings)# cli-alias 0
(cli-alias-0)# alias-command 'copy firmware from'
(cli-alias-0)# alias-name CopyF
```

ssh-if

This command configures the SSH Interfaces table, which lets you define IP interfaces for the SSH application.

Syntax

```
(config-system)# cli-settings
(cli-settings)# ssh-if <Index>
(ssh-if-<Index>)#
```

Command	Description
Index	Defines the table row index.
`interface-name`	Assigns an IP Interface from the IP Interfaces table for communication with the embedded SSH server.
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`port`	Defines the local port to use for SSH application.

Command Mode

Privileged User

Example

This example configures the SSH interface on VRF "vrf05":

```
(config-system)# cli-settings
(cli-settings)# ssh-if 0
(ssh-if-0)# network-source vrf05
(ssh-if-0)# port 23
```

This example configures the SSH interface on interface "MyIfx":

```
(config-system)# cli-settings
(cli-settings)# ssh-if 0
(ssh-if-0)# interface-name MyIfx
(ssh-if-0)# port 23
```

telnet-if

This command configures the Telnet Interfaces table, which lets you define IP interfaces for the Telnet application.

Syntax

```
(config-system)# cli-settings
(cli-settings)# telnet-if <Index>
(telnet-if-<Index>)#
```

Command	Description
Index	Defines the table row index.
`interface-name`	Assigns an IP Interface from the IP Interfaces table for communication with the embedded Telnet server.
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`port`	Defines the local port to use for Telnet application.

Command Mode

Privileged User

Example

This example configures the Telnet interface on interface "MyIfx":

```
(config-system)# cli-settings
(cli-settings)# telnet-if 0
(telnet-if-0)# interface-name MyIfx
(telnet-if-0)# port 23
```

19 clock

This command configures the date and time of the device.

Syntax

```
(config-system)# clock
(clock)#
```

Command	Description
`date`	Defines the date in the format dd/mm/yyyy (i.e., day/month/year).
`date-header-time-sync {off|on}`	Enables the device to obtain its date and time for its internal clock from the SIP Date header in 200 OK messages received in response to sent REGISTER messages.
`date-header-time-sync-interval`	Defines the minimum time (in seconds) between synchronization updates using the SIP Date header method for clock synchronization.
`ptp-time-sync {off|on}`	Enables the device (virtual machine) to obtain its date and time from the host's virtual PTP (Precision Time Protocol) device. **Note:** The parameter is applicable only to Mediant CE/VE deployed on Azure or Hyper-V.
`summer-time`	Configures daylight saving time.
`time`	Defines the current time in the format hh:mm:ss (i.e., hour:minutes:seconds).
`utc-offset`	Defines the time zone (offset from UTC) in seconds. The value must be a multiple of 60 (seconds). For example, to set an offset of 2 hours, configure the parameter to 7200 (i.e., 2 hours is 7200 seconds). If the value is not a multiple of 60, the device automatically rounds it to the nearest multiple of 60 and logs this adjustment in a syslog message. For example, if you enter 7195, the device rounds it to 7200.

Command Mode

Privileged User

Example

This example configures the date of the device.

```
(config-system)# clock
(clock)# date 23/11/2016
```

20 configuration-version

This command configures the ini file version number when saving the device's configuration to an ini file. The version number appears in the file as: "INIFileVersion = <number>"

Syntax

```
(config-system)# configuration-version <Number>
```

Command Mode

Privileged User

Example

This example configures the ini file version to 72101:

```
(config-system)# configuration-version 72101
```

21 feature-key

This command updates the License Key.

Syntax

```
(config-system)# feature-key <"License Key">
```

Command Mode

Privileged User

Note

You must enclose the License Key string in quotes ("...").

Example

This example updates the License Key:

```
(config-system)# feature-key
"r6wmr5to25smaB12d21aiSl94yMCf3lsfjBjagcch1kq9AZ9MJqqCOw44ywFcMIlbi
BaeNcsjh878ld1f2wKbY3IXJj1SOIcbiBfc6FBj1fROIJ9XvAw8k1IXdoFcOpeQJp2e
0sti1s0blNecypomhgU5yTIPREPQtl2e1wpiNgx7IRfeyXV?2s9@coFcOhdayWjWh
QuJelgb5VbfyENc2w46O6OG3lf7NJnbkF5mxkka5xccyoVedYq1gMc"
```

22 floating-license

This command enables the Floating License or Flex License model and configures an Allocation Profile for the model.

Syntax

```
(config-system)# floating-license
(floating-license)#
```

Command	Description
`allocation-media-sessions`	Defines media session capacity for the customized Allocation Profile.
`allocation-profile {custom|registered-users|sip-trunking}`	Defines the Allocation Profile type.
`allocation-registered-users`	Defines registered user capacity for the customized Allocation Profile.
`allocation-signaling-sessions`	Defines SIP signaling capacity for the customized Allocation Profile.
`allocation-siprec-sessions`	Defines SIPRec capacity for the customized Allocation Profile.
`allocation-webrtc-sessions`	Defines WebRTC capacity for the customized Allocation Profile.
`floating-license {off|on}`	Enables the Floating License or Flex License.
`limit-media-sessions`	Defines a media session limit for the customized Allocation Profile.
`limit-registered-users`	Defines a registered user limit for the customized Allocation Profile.
`limit-signaling-sessions`	Defines a signaling capacity limit for the customized Allocation Profile.
`limit-siprec-sessions`	Defines a SIPRec session limit for the customized Allocation Profile.

Command	Description
`limit-transcoding-sessions`	Defines a transcoding session limit for the customized Allocation Profile.
`limit-webrtc-sessions`	Defines a WebRTC session limit for the customized Allocation Profile.

Command Mode

Privileged User

Example

This example enables the Floating License or Flex License and configures it for the factory default Allocation Profile that is suited for SIP Trunking applications:

```
(config-system)# floating-license
(floating-license)# floating-license on
(floating-license)# allocation-profile sip-trunking
```

23 http-services

This command configures Web (HTTP) services.

Syntax

```
(config-system)# http-services
(http-client-services)#
```

Command	Description
http-remote-services	Defines the HTTP Remote Services table for REST. For more information, see http-remote-services on the next page.
remote-monitoring {off|on}	Enables the device to send monitoring reports to a remote monitoring server when the device is located behind NAT.
remote-monitor-alarms	Enables the device to send a remote monitoring report of currently active alarms to the monitoring server.
remote-monitor-kpi	Enables the device to send a remote monitoring report of performance monitoring statistics to the monitoring server.
remote-monitor-registration	Enables the device to send a remote monitoring report of users registered with the device to the monitoring server.
remote-monitor-reporting-period	Defines the time interval (in seconds) between each remote monitoring report that is sent to the monitoring server.
remote-monitor-status	Enables the device to send a remote monitoring report of its status to the monitoring server.
rest-debug-mode {0-3}	Defines the level of debug messages of HTTP services, which are sent to Syslog. 0 blocks all messages; 3 is the most detailed level.
routing-qos-status {disable|enable}	Enables QoS-based routing by the routing server.
routing-qos-status-rate	Defines the rate (in sec) at which the device sends QoS reports to the routing server.
routing-server-group-status {disable|enable}	Enables the reporting of the device's topology status (using the REST TopologyStatus API command) to HTTP remote hosts.

Command	Description
`routing-server-registration-status`	Enables the synchronization of the device's registration database with remote HTTP hosts.

Command Mode

Privileged User

http-remote-services

This command configures the Remote Web Services table, which lets you define Web-based (HTTP/S) services provided by third-party, remote HTTP/S hosts.

Syntax

```
(config-system)# http-services
(http-client-services)# http-remote-services <Index>
(http-remote-services-<Index>)#
```

Command	Description
Index	Defines the table row index.
`http-login-needed {disable|enable}`	Enables the use of AudioCodes proprietary REST API Login and Logout commands for connecting to the remote host.
`http-num-connections`	Defines the number of sockets that the device opens per HTTP remote host.
`http-persistent-connection {disable|enable}`	Configures whether the HTTP connection with the host remains open or is only opened per request.
`http-policy {round-robin|sticky-next|sticky-primary}`	Defines the mode of operation when you have configured multiple remote hosts (in the HTTP Remote Hosts table) for a specific remote Web service.
`http-policy-between-groups {sticky-primary|sticky-next}`	Defines the mode of operation between groups of hosts, which are

Command	Description
	configured in the HTTP Remote Hosts table for the specific remote Web service.
`http-remote-hosts`	Defines the HTTP Remote Hosts table, which lets you define remote HTTP hosts per Remote Web Service. The table is a "child" of the Remote Web Services table. For more information, see http-remote-hosts on the next page.
`rest-ka-timeout`	Defines the duration (in seconds) in which HTTP-REST keep-alive messages are sent by the device if no other messages are sent.
`rest-message-type {call-status|general|qos|registration-status|remote-monitoring|routing|topology-status}`	Defines the type of service provided by the HTTP remote host.
`rest-name`	Defines the name to easily identify the row.
`rest-password`	Defines the password for HTTP authentication.
`rest-path`	Defines the path (prefix) to the REST APIs.
`rest-timeout`	Defines the TCP response timeout (in seconds) from the remote host.
`rest-tls-context`	Assigns a TLS context (if HTTPS).
`rest-user-name`	Defines the username for HTTP authentication.
`rest-verify-certificates {disable|enable}`	Enables certificate verification when connection with the host is based on HTTPS.
`verify-cert-subject-name`	Enables the verification of the TLS

Command	Description
{disable|enable}	certificate subject name (Common Name / CN or Subject Alternative Name / SAN) when connection with the host is based on HTTPSthat is used in the incoming connection request from the OVOC server.

Command Mode

Privileged User

Example

This example configures an HTTP service for routing:

```
(config-system)# http-services
(http-client-services)# http-remote-services 0
(http-client-services-0)# rest-message-type routing
(http-client-services-0)# rest-name ARM
```

http-remote-hosts

This command configures the HTTP Remote Hosts table, which lets you define remote HTTP hosts per Remote Web Service. The table is a "child" of the Remote Web Services table.

Syntax

```
(config-system)# http-services
(http-client-services)# http-remote-services <Index>
(http-client-services-<Index>)# http-remote-hosts <Index>
(http-remote-hosts-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
group-id <0-4>	Defines the host's group ID.
host-priority-in-group	Defines the priority level of the host within the assigned group.

Command	Description
<0-9>	
rest-address	Defines the IP address or FQDN of the remote HTTP host.
rest-interface	Defines the IP network interface to use.
rest-port	Defines the port of the remote HTTP host.
rest-name	Configures an arbitrary name to identify the host.
rest-transport-type {rest-http|rest-https}	Defines the HTTP protocol.

Command Mode

Privileged User

Example

This example configures an HTTP remote host "ARM" at 10.15.7.8:

```
(config-system)# http-services
(http-client-services)# http-remote-services 0
(http-client-services-0)# http-remote-hosts 1
(http-remote-hosts-0/1)# rest-address 10.15.7.8
(http-remote-hosts-0/1)# rest-interface 0
(http-remote-hosts-0/1)# rest-servers ARM
(http-remote-hosts-0/1)# rest-transport-type rest-http
```

24 hw

This command configures hardware-related settings.

Syntax

```
(config-system)# hw
(hw)#
```

Command	Description
`dual-powersupply-supported {no|yes}`	Enables the device to send an SNMP alarm (acPowerSupplyAlarm) for one or both Power Supply modules if a module is removed from the chassis or not operating correctly (failure).

Command Mode

Privileged User

Note

The command is applicable only to Mediant 800, Mediant 9000, AND mp-1288.

Example

This example enables sending an alarm if a Power Supply module is removed or fails.

```
(config-system)# hw
(hw)# dual-powersupply-supported yes
```

25 hostname

This command configures the product name, which is displayed in the management interfaces (as the prompt in CLI, and in the Web interface).

Syntax

```
(config-system)# hostname <String>
```

Command Mode

Privileged User

Example

This example configures the product name from "Mediant" to "routerABC":

```
(config-system)# hostname routerABC
```

26 kpi

This command configures Key Performance Indicators (KPI).

Syntax

```
(config-system)# kpi
(kpi)#
```

Command	Description
`graphs`	Defines KPI Layouts. For more information, see graphs on the next page.
`layouts`	Defines KPI Layout For more information, see layouts on page 196.
`alarm-thresholds`	Defines the Alarm Thresholds table. For more information, see kpi alarm-thresholds on page 197.

kpi-data

This command plots performance monitoring parameters on a KPI Layout graph.

Syntax

```
(config-system)# kpi
(kpi)# graphs <Index>
(graphs-<Index>)# kpi-data <Index>
(kpi-data-<Index>/<Index>)
```

Command	Description
Index	Defines the table row index.
`kpi-data-color`	Defines the color (in Hex color code) of the plotted line on the graph for the performance monitoring parameter.
`kpi-data-title`	Defines the name of the plotted line for the performance monitoring parameter, which is displayed as a legend below the graph.
`kpi-data-url`	Defines the REST URL path to the performance monitoring parameter that you want to plot.

Command Mode

Privileged User

Example

This example configures a graph for the performance monitoring parameter cpuUtilization:

```
(config-system)# kpi
(kpi)# graphs 0
(graphs-0)#  kpi-data 0
(kpi-data-0/0)# kpi-data-color #FF0000
(kpi-data-0/0)# kpi-data-title CPU
(kpi-data-0/0)# kpi-data-url
/api/v1/kpi/current/system/cpuStats/cpu/0/cpuUtilization
(kpi-data-0/0)# activate
```

graphs

This command configures graphs of KPI Layouts.

Syntax

```
(config-system)# kpi
(kpi)# graphs <Index>
(graphs-<Index>)#
```

Command	Description
Index	Defines the table row index.
`kpi-data`	Defines the performance monitoring parameter to plot on the graph. For more information, see kpi-data on the previous page.
`graphs-subtitle`	Defines the name of the performance monitoring parameter for which this alarm threshold rule applies.
`graphs-title`	Defines a label for the graph, which is displayed above the graph.
`graphs-tooltip-text {No}`	Defines text that is displayed in the tooltip with the plotted values.

Command	Description
`graphs-tooltip {Disable|Enable}`	Enables a tooltip that appears when you hover your mouse over a point on the plotted line of the graph.
`graphs-xtitle`	Defines a label for the graph's x axis, which is displayed horizontally below the x axis.
`graphs-ytitle`	Defines a label for the y axis, which is displayed vertically alongside the y axis.

Command Mode

Privileged User

Example

This example configures a graph of a KPI layout and titles it "System Monitoring":

```
(config-system)# kpi
(kpi)# graphs 0
(graphs-0)#  graphs-title System Monitoring
(graphs-0)# graphs-xtitle TIME
(graphs-0)# graphs-ytitle %
(graphs-0)# activate
```

layouts

This command configures the KPI Layouts table, which defines graph layout pages for the device's performance monitoring parameters.

Syntax

```
(config-system)# kpi
(kpi)# layouts <Index>
(layouts-<Index>)#
```

Command	Description
Index	Defines the table row index.
`layouts-description`	Defines an arbitrary name to easily identify the layout.

Command	Description
layouts-graph1 layouts-graph2 layouts-graph3 layouts-graph4	Defines the graph for the layout.
layouts-layout {1x1|1x2|2x1|2x2}	Defines the layout, regarding number and positioning of graphs.
layouts-title	Defines a name for the layout.

Command Mode

Privileged User

Example

This example configures a KPI Layout with a 1x1 layout:

```
(config-system)# kpi
(kpi)# layouts 0
(layouts-0)#  layouts-title SBC
(layouts-0)# layouts-layout 1x1
(layouts-0)# activate
```

kpi alarm-thresholds

This command configures the Alarm Thresholds table, which lets you define alarm thresholds for performance monitoring parameters.

Syntax

```
(config-system)# kpi alarm-thresholds <Index>
(alarm-thresholds-<Index>)#
```

Command	Description
Index	Defines the table row index.
entity-index	Defines a specific index row of the entity with which the performance monitoring parameter is associated.

Command	Description
`kpi-name`	Defines the name of the performance monitoring parameter for which this alarm threshold rule applies.
`pm-path`	Defines the path (application name, group name and element name) to the performance monitoring parameter.
`threshold-clear-message`	Defines the alarm text that is displayed when the alarm is cleared.
`threshold-clear-watermark`	Defines a value that if crossed by the performance monitoring parameter, clears the raised alarm.
`threshold-direction {down|up}`	Defines the direction of crossing the threshold values (watermarks) for which the alarm is raised or cleared.
`threshold-mode {disabled|enabled}`	Enables (activates) the Alarm Threshold rule.
`threshold-raise-message`	Defines the alarm text that is displayed when the alarm is raised.
`threshold-raise-watermark`	Defines a value that if crossed by the performance monitoring parameter, raises the alarm.
`threshold-severity {critical|default|indeterminate|major|minor|warning}`	Defines the severity level of the alarm.

Command Mode

Privileged User

Example

This example configures an alarm threshold rule for performance monitoring parameter licenseFeuUsage:

```
(config-system)# kpi alarm-thresholds 0
(alarm-thresholds-0)# kpi-name licenseFeuUsage
(alarm-thresholds-0)# pm-path system/licensestats/global
(alarm-thresholds-0)# threshold-direction up
(alarm-thresholds-0)# threshold-raise-watermark 50
(alarm-thresholds-0)# threshold-clear-watermark 40
(alarm-thresholds-0)# threshold-raise-message The %PM% parameter value
(%VALUE%) has exceeded the high threshold (%RAISEWM%).
(alarm-thresholds-0)# threshold-clear-message The %PM% parameter value
(%VALUE%) has returned to normal levels.
(alarm-thresholds-0)# threshold-severity warning
(alarm-thresholds-0)# enabled
```

27 ldap

This command configures LDAP and includes the following subcommands:

Syntax

```
(config-system)# ldap
```

Command	Description
`ldap-configuration`	See ldap-configuration below
`ldap-server-groups`	See ldap ldap-server-groups on page 203
`settings`	See ldap settings on page 204

Command Mode

Privileged User

ldap-configuration

This command configures the LDAP Servers table, which lets you define LDAP servers.

Syntax

```
(config-system)# ldap-configuration <Index>
(ldap-configuration-<Index>)#
```

Command	Description
Index	Defines the table row index.
`bind-dn`	Defines the LDAP server's bind Distinguished Name (DN) or username.
`domain-name`	Defines the domain name (FQDN) of the LDAP server.
`interface`	Defines the interface on which to send LDAP queries.
`ldap-servers-search-dns`	Defines the LDAP Search DN table, which lets you define LDAP base paths per LDAP Servers table. For more information, see ldap ldap-servers-search-dns on page 202.

Command	Description
`max-respond-time`	Defines the duration (in msec) that the device waits for LDAP server responses.
`mgmt-attr`	Defines the LDAP attribute name to query, which contains a list of groups to which the user is a member of.
`mgmt-ldap-groups`	Defines the Management LDAP Groups table, which lets you define an access level per management groups per LDAP Servers table. For more information, ldap mgmt-ldap-groups on the next page.
`password`	Defines the user password for accessing the LDAP server during connection and binding operations.
`server-group`	Assigns the LDAP server to an LDAP Server Group, configured in the LDAP Server Groups table.
`server-ip`	Defines the LDAP server's IP address.
`server-port`	Defines the LDAP server's port.
`tls-context`	Assigns a TLS Context if the connection with the LDAP server is TLS.
`use-tls {no|yes}`	Enables the device to encrypt the username and password (for Control and Management related queries) using TLS when sending them to the LDAP server.
`verify-certificate {no|yes}`	Enables certificate verification when the connection with the LDAP server uses TLS.
`verify-subject-name`	Enables the verification of the TLS certificate subject name (Common Name / CN or Subject Alternative Name / SAN) that is used in the incoming connection request from the LDAP server.

Command Mode

Privileged User

Example

This example configures an LDAP server with IP address 10.15.7.8 and password "itsp1234":

```
(config-system)# ldap-configuration 0
(ldap-configuration-0)# server-ip 10.15.7.8
(ldap-configuration-0)# password itsp1234
```

ldap ldap-servers-search-dns

This command configures the LDAP Search DN table, which lets you define LDAP base paths, per LDAP Servers table.

Syntax

```
(config-system)# ldap-configuration <Index>
(ldap-configuration-<Index>)# ldap-servers-search-dns <Index>
(ldap-servers-search-dns-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`base-path`	Defines the base path Distinguished Name (DN).

Command Mode

Privileged User

Example

This example configures the LDAP base path "OU=NY,DC=OCSR2,DC=local":

```
(config-system)# ldap-configuration 0
(ldap-configuration-0)# ldap-servers-search-dns 1
(ldap-servers-search-dns-0/1)# base-path OU=NY,DC=OCSR2,DC=local
```

ldap mgmt-ldap-groups

This command configures the Management LDAP Groups table, which lets you define an access level per management groups per LDAP Servers table.

Syntax

```
(config-system)# ldap-configuration <Index>
(ldap-configuration-<Index>)# mgmt-ldap-groups <Index>
(mgmt-ldap-groups-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`groups`	Defines the Attribute names of the groups in the LDAP server.
`level`	Defines the access level of the group(s).

Command Mode

Privileged User

Example

This example configures the LDAP server with monitor access level:

```
(config-system)# ldap-configuration 0
(ldap-configuration-0)# mgmt-ldap-groups 1
(mgmt-ldap-groups-0/1)# level monitor
```

ldap ldap-server-groups

This command configures the LDAP Server Groups table, which lets you define LDAP Server Groups. An LDAP Server Group is a logical configuration entity that contains up to two LDAP servers.

Syntax

```
(config-system)# ldap ldap-server-groups <Index>
(ldap-server-groups-<Index>)#
```

Command	Description
Index	Defines the table row index.
`cache-entry-removal-timeout`	Defines the cache entry removal timeout.
`cache-entry-timeout`	Defines the cache entry timeout.
`search-dn-method {parallel|sequentialy}`	Defines the method for querying the DN objects within each LDAP server.
`server-search-method`	Defines the method for querying between the two

Command	Description
`{parallel|sequentialy}`	LDAP servers in the group.
`server-type {control|management}`	Configures whether the servers in the group are used for SIP-related LDAP queries (Control) or management login authentication-related LDAP queries (Management).

Command Mode

Privileged User

Example

This example configures the LDAP Server Group for management-login authentication LDAP queries and where the search between the servers is done one after the other:

```
(config-system)# ldap ldap-server-groups 0
(ldap-server-groups-0)# server-type management
(ldap-server-groups-0)# server-search-method sequentialy
```

ldap settings

This command configures various LDAP settings.

Syntax

```
(config-system)# ldap settings
(ldap)#
```

Command	Description
`auth-filter`	Defines the filter (string) to search the user during the authentication process.
`cache {clear-all|refresh-entry}`	Configures LDAP cache actions.
`enable-mgmt-login {off|on}`	Enables the device to use LDAP for authenticating management interface access.
`entry-removal-timeout`	Defines the duration (in hours) after which an entry is removed from the LDAP cache.

Command	Description
`entry-timeout`	Defines the duration (minutes) an entry in the LDAP cache is valid.
`ldap-cache-enable {off|on}`	Enables the LDAP cache.
`ldap-numeric-attr`	Defines up to five LDAP Attributes (separated by commas) for which the device uses for LDAP query searches in the AD for numbers that may have characters between the digits.
`ldap-search-server-method {parallel|sequentialy}`	Defines the search method in the LDAP servers if more than one LDAP server is configured.
`ldap-service {off|on}`	Enables the LDAP service.
`search-dns-in-parallel {parallel|sequentialy}`	Configures whether DNs should be checked in parallel or sequentially when there is more than one search DN.

Command Mode

Privileged User

Example

This example enables the LDAP cache and sets the valid duration of a cached entry to 1200 minutes.

```
(config-system)# ldap settings
(ldap)# ldap-cache-enable on
(ldap)# entry-timeout 1200
```

28 login-oauth-servers

This command configures the Login OAuth Servers table, which configures an OAuth 2.0 server entity for OAuth-based user-login authentication.

Syntax

```
(config-system)# login-oauth-servers <Index>
(login-oauth-servers-<Index>)#
```

Command	Description
Index	Defines the table row index.
max-resp-time	Defines the maximum time (in seconds) that the device waits for a response from the OAuth server.
oauth-server	Assigns an OAuth server, which is configured in the OAuth Servers table (oauth-servers).
server-name	Defines an arbitrary name to easily identify the row.
service-activation	Enables this OAuth-based authentication login rule.

Command Mode

Privileged User

Example

This example configures a login OAuth server:

```
(config-system)# login-oauth-servers 0
(login-oauth-servers-0)# server-name Azure AD for Login
(oauth-servers-0)# oauth-server AZURE
```

29 metering-client

This command configures the network interface (e.g., eth1) that is associated with the Elastic IP address for the Metered License model (pay-as-you-go) when the device is deployed in the Amazon Web Services (AWS) cloud.

Syntax

```
(config-system)# metering-client <Index>
(metering-client-<Index>)#
```

Command	Description
Index	Defines the table row index.
`network-interface`	Defines the network interface associated with the Elastic IP address.

Command Mode

Privileged User

Note

The command is applicable only to Mediant VE.

Example

This example configures network interface "eth1" as associated with the Elastic IP address:

```
(config-system)#  metering-client 0
(metering-client-0)# eth1
```

30 management-access-list

This command configures the Management Access List table, which lets you restrict access to the device's management interfaces (Web, REST API, SSH, or Telnet).

Syntax

```
(config-system)# management-access-list <Index>
(management-access-list-<Index>)#
```

Command	Description
`ip-address`	Defines the management station (client) as an IP address (IPv4 or IPv6) that can access the specified management interface type.
`type {all|rest|ssh|telnet|web}`	Defines the type of management interface that the client is allowed to access.

Command Mode

Privileged User

Example

This example allows access from a client at IP address 10.11.12.120 to the device's REST interface:

```
(config-system)# management-access-list 0
(management-access-list-0)# ip-address 10.11.12.120
(management-access-list-0)# type rest
```

31 mgmt-auth

This command configures various management settings.

Syntax

```
(config-system)# mgmt-auth
(mgmt-auth)#
```

Command	Description
`default-access-level {no-access|monitor|administrator|security-administrator}`	Defines the device's default access level when the LDAP/RADIUS response doesn't include an access level attribute for determining the user's management access level.
`local-cache-mode {absolute-expiry-timer|reset-expiry-upon-access}`	Defines the password's local cache timeout to reset after successful authorization.
`local-cache-timeout`	Defines the locally stored login password's expiry time, in seconds. When expired, the request to the Authentication server is repeated.
`obscure-password-mode {off|on}`	Enables the device to enforce obscured (i.e., encrypted) passwords whenever you create a new management user or modify the password of an existing user (Local Users table) through CLI (`configure system > user`). For more information, see the command `configure system > user > password`.
`oauth-web-login [disable| enable-with-`	Enables user login

Command	Description
`local|enable-without-local}`	authentication based on OAuth 2.0.
`password-expired-alarm`	Defines the number of days before login password expiration when the device sends the acExpiredPasswordAlarm SNMP alarm.
`timeout-behavior {VerifyAccessLocally|deny-access}`	Defines the device to search in the Local Users table if the Authentication server is inaccessible.
`use-local-users-db {always|always-before-auth-server|when-no-auth-server}`	Defines when to use the Local Users table in addition to the Authentication server.

Command Mode

Privileged User

Example

This example configures the device's default access level as 200:

```
(config-system)# mgmt-auth
(mgmt-auth)# default-access-level 200
```

32 ntp

This command configures Network Time Protocol (NTP) for updating the device's date and time.

Syntax

```
(config-system)# ntp
(ntp)#
```

Command	Description
`auth-key-id`	Defines the NTP authentication key identifier (string) for authenticating NTP messages.
`auth-key-md5`	Defines the authentication key (string) shared between the device (client) and the NTP server, for authenticating NTP messages.
`enable`	Enables the device to synchronize its local clock (date and time) with an NTP server.
`ntp-as-oam {off|on}`	Defines the location of the Network Time Protocol (NTP).
`ntp-network-interface`	Assigns an IP Interface from the IP Interfaces table for NTP communication.
`primary-server`	Defines the NTP server FQDN or IP address.
`secondary-server`	Defines the NTP secondary server FQDN or IP address.
`update-interval`	Defines the NTP update time interval (in seconds). The value must be a multiple of 60 (seconds). For example, to set an interval of 2 hours, configure the parameter to 7200 (i.e., 2 hours is 7200 seconds). If the value is not a multiple of 60, the device automatically rounds it to the nearest multiple of 60 and logs this adjustment in a syslog message. For example, if you enter 7195, the device rounds it to 7200.

Command Mode

Privileged User

Example

This example configures an NTP server with IP address 10.15.7.8 and updated every hour (3,600 seconds):

```
(config-system)# ntp
(ntp)# enable on
(ntp)# primary-server 10.15.7.8
(ntp)# update-interval 3600
```

33 oauth-servers

This command configures the OAuth Servers table, which configures an OAuth 2.0 server.

Syntax

```
(config-system)# oauth-servers <Index>
(oauth-servers-<Index>)#
```

Command	Description
Index	Defines the table row index.
`application-id`	Defines the Application (client) ID.
`authorization-endpoint`	Defines the authorization endpoint URL.
`base-url`	Defines the base URL.
`devicecode-endpoint`	Defines the device code endpoint URL.
`keys-endpoint`	Defines the key endpoint URL.
`keys-refresh-time`	Defines the endpoint key refresh time.
`logout-endpoint`	Defines the logout endpoint URL.
`network-interface`	Defines the local IP interface.
`rest-api-aud-prefix`	Defines the REST API 'aud' prefix.
`server-name`	Defines the OAuth server name.
`server-type {azure}`	Defines the OAuth server type.
`tls-context`	Defines the TLS Context.
`token-endpoint`	Defines the token endpoint URL.
`verify-certificate {disable|enable}`	Verifies the TLS certificate with the OAuth server.

Command Mode

Privileged User

Example

This example configures an OAuth server:

```
(config-system)# oauth-servers 0
(oauth-servers-0)# server-name Azure AD for SIP
(oauth-servers-0)# server-type azure
```

34 packetsmart

This command configures the device to send voice traffic data to BroadSoft's BroadCloud PacketSmart solution for monitoring and assessing the network in which the device is deployed.

Syntax

```
(config-system)# packetsmart
```

Command	Description
`enable`	Enables the PacketSmart feature.
`monitor voip interface-if`	Defines the IP network interface ID for voice traffic.
`network voip interface-if`	Defines the IP network interface ID for communication with PacketSmart.
`server address [port]`	Defines the PacketSmart server address and port.

Command Mode

Privileged User

Note

PacketSmart is applicable only to the Mediant 5xx and Mediant 8xx series.

Example

This example configures PacketSmart server IP address 10.15.7.8:

```
(config-system)# packetsmart enable
(config-system)# packetsmart monitor voip interface-if 0
(config-system)# packetsmart network voip interface-if 0
(config-system)# packetsmart server address 10.15.7.8
```

35 performance-profile

This command configures the Performance Profile table, which configures thresholds of performance-monitoring call metrics for Major and Minor severity alarms.

Syntax

```
(config-system)# performance-profile <Index>
(performance-profile-<Index>)#
```

Command	Description
Index	Defines the table row index.
entity {global|ip-group|srd}	Defines the entity.
hysteresis	Defines the amount of fluctuation (hysteresis) from the configured threshold in order for the threshold to be considered as crossed.
ip-group-name	Defines the IP Group (string).
major-threshold	Defines the Major threshold.
minimum-samples	Calculates the performance monitoring (only if at least 'minimum samples' is configured in the command 'window-size' (see below).
minor-threshold	Defines the Minor threshold.
pmtype {acd|asr|ner}	Defines the type of performance monitoring.
srd-name	Defines the SRD (string).
window-size	Configures how often performance monitoring is calculated (in minutes).

Command Mode

Privileged User

Example

This example configures a Performance Profile based on the ASR of a call, where the Major threshold is configured at 70%, the Minor threshold at 90% and the hysteresis for both thresholds at 2%:

```
(config-system)# performance-profile 0
(performance-profile-0)# entity ip-group
(performance-profile-0)# ip-group-name ITSP
(performance-profile-0)# pmtype asr
(performance-profile-0)# major-threshold 70
(performance-profile-0)# minor-threshold 90
(performance-profile-0)# hysteresis 2
```

36 radius

This command configures Remote Authentication Dial-In User Service (RADIUS) settings to enhance device security.

Syntax

```
(config-system)# radius
```

Command	Description
`radius servers`	See radius servers below
`radius settings`	See radius settings on the next page

radius servers

This command configures the RADIUS Servers table, which configures RADIUS servers.

Syntax

```
(config-system)# radius servers <Index>
(servers-<Index>)#
```

Command	Description
Index	Defines the table row index.
`acc-port`	Defines the RADIUS server's accounting port.
`auth-port`	Defines the RADIUS server's authentication port.
`ip-address`	Defines the RADIUS server's IP address.
`network-interface`	Assigns an IP Interface from the IP Interfaces table for RADIUS communication.
`shared-secret`	Defines the shared secret between the RADIUS client and the RADIUS server.

Command Mode

Privileged User

Example

This example configures a RADIUS server with IP address 10.15.7.8:

```
(config-system)# radius servers 0
(servers-0)# ip-address 10.15.7.8
```

radius settings

This command configures various RADIUS settings.

Syntax

```
(config-system)# radius settings
(radius)#
```

Command	Description
`double-decode-url {off|on}`	Enables an additional decoding of authentication credentials that are sent to the RADIUS server via URL.
`enable {off|on}`	Enables or disables the RADIUS application.
`enable-mgmt-login {off|on}`	Uses RADIUS for authentication of management interface access.
`local-cache-mode {0|1}`	Defines the capability to reset the expiry time of the local RADIUS password cache.
`local-cache-timeout`	Defines the expiry time, in seconds of the locally stored RADIUS password cache.
`nas-id-attribute`	Defines the RADIUS NAS Identifier attribute.
`rad-pap-req-msg-auth-tx {off|on}`	Enables the device to always include RADIUS attribute 80 (Message-Authenticator) when it sends RADIUS request messages (Access-Request packets) to the RADIUS server.
`rad-req-msg-auth-rx {off|on}`	Enables the requirement of RADIUS

Command	Description
	attribute 80 (Message-Authenticator) in incoming RADIUS messages from the RADIUS server.
`timeout-behavior`	Configures device behavior when RADIUS times out.
`vsa-access-level`	Defines the 'Security Access Level' attribute code in the VSA section of the RADIUS packet that the device should relate to.
`vsa-vendor-id`	Defines the vendor ID that the device should accept when parsing a RADIUS response packet.

Command Mode

Privileged User

Example

This example demonstrates configuring VSA vendor ID:

```
(config-system)# radius settings
(radius)# vsa-vendor-id 5003
```

37 sbc-performance-settings

This command defines a service for optimization of CPU core allocation.

Syntax

```
(config-system)# sbc-performance-settings
(sbc-performance-settings)# sbc-performance-profile {optimized-for-sip|optimized-for-srtp|optimized-for-transcoding}
```

Command Mode

Privileged User

Note

- For the command to take effect, a device restart with a burn to flash is required.
- The command is applicable only to Mediant 9000 and Mediant VE/SE.

Example

This example specifies CPU core allocation optimization for SRTP:

```
(config-system)# sbc-performance-settings
(sbc-performance-settings)# sbc-performance-profile optimized-for-srtp
```

38 snmp

This command configures Simple Network Management Protocol (SNMP).

Syntax

```
(config-system)# snmp
```

Command	Description
`alarm-customization`	See snmp alarm-customization below
`alarm-settings`	See snmp alarm-settings on the next page
`settings`	See snmp settings on page 224
`trap`	See
`v3-users`	See v3-users on page 229

Command Mode

Privileged User

snmp alarm-customization

This command configures the Alarms Customization table, which customizes the severity level of SNMP trap alarms.

Syntax

```
(config-system)# snmp alarm-customization <Index>
(alarm-customization-<Index>)#
```

Command	Description
Index	Defines the table row index.
`alarm-customized-severity {critical|indeterminate|major|minor|suppressed|warning}`	Defines the new (customized) severity of the alarm.
`alarm-original-severity`	Defines the original

Command	Description
`{critical|default|indeterminate|major|minor|warning}`	severity of the alarm according to the MIB.
`entity-id`	Defines the entity (e.g., IP Group 3) for which the alarm was sent.
`name <0-199>`	Defines the SNMP alarm that you want to customize. The alarm is configured using the last digits of the alarm's SNMP OID. For example, configure the parameter to "12" for the acActiveAlarmTableOverflow alarm (OID is 1.3.6.1.4.15003.9.10.1.21.2.0.**12**).

Command Mode

Privileged User

Example

This example customizes the acActiveAlarmTableOverflow alarm severity from major to warning level:

```
(config-system)# snmp alarm-customization 0
(alarm-customization-0)# name 1
(alarm-customization-0)# alarm-original-severity major
(alarm-customization-0)# alarm-customized-severity warning
```

snmp alarm-settings

This command configures the persistent Alarms History table feature.

Syntax

```
(config-system)# snmp alarm-settings
(alarm-settings)#
```

Command	Description
`alarms-persistent-history {off| on}`	Enables the device to store the alarms of the Alarms History table on its flash memory.
`persistent-history-save-interval`	Defines how often (in minutes) the device saves the alarms of the Alarms History table to its flash memory.

Command Mode

Privileged User

Example

This example enables the persistent Alarms History table feature:

```
(config-system)# snmp alarm-settings
(alarm-settings)# alarms-persistent-history on
```

snmp settings

This command configures various SNMP settings.

Syntax

```
(config-system)# snmp settings
(snmp)#
```

Command	Description
`access-groups`	Defines Access Groups (see access-groups).
`activate-keep-alive-trap [interval]`	Enables a keep-alive trap for the agent behind NAT.
`active-alarm-table-max-size`	Defines the maximum number of active alarms that can be displayed in the Active Alarms table.
`alarm-history-`	Defines the maximum number of historical alarms that can

Command	Description
`table-max-size`	be displayed in the Alarm History table.
`community-strings`	Defines SNMP community strings (see community-strings on the next page).
`disable {no|yes}`	Enables SNMP.
`enable-advanced-mode {off|on}`	Enables the SNMP advanced mode.
`enable-authentication-trap {off|on}`	Disables the sending of the Authentication Failure SNMP trap (authenticationFailure, OID 1.3.6.1.6.3.1.1.5.5).
`engine-id`	Defines the SNMP Engine ID. 12 HEX Octets in the format: xx:xx:...:xx
`interface-ipv6-name`	Assigns an IPv6 IP Interface (configured in the IP Interfaces table) to the SNMP application for SNMP over IPv6.
`interface-name`	Assigns an IPv4 IP Interface (configured in the IP Interfaces table) to the SNMP application for SNMP over IPv4.
`port`	Defines the port number for SNMP requests and responses.
`sys-contact`	Defines the contact person for this managed node (string) .
`sys-location`	Defines the physical location of the node (string).
`sys-name`	Defines the sysName as descibed in MIB-2 (string).
`trap-destination`	Defines SNMP trap destinations (see trap-destination on page 227).
`trusted-manager`	Defines SNMP Trusted Managers (see trusted-manager on page 227).
`v3-users`	Defines SNMPv3 users (see v3-users on page 229).
`view-tree-family`	Defines access authorization rules to MIB OIDs for the View Tree Family (see view-tree-family).

Command Mode

Privileged User

Example

This example enables SNMP functionality:

```
(config-system)# snmp settings
(snmp)# disable no
```

community-strings

This command configures the SNMP Community Strings table, which configures SNMP community strings.

Syntax

```
(config-system)# snmp settings
(snmp)# community-strings <Index>
(community-strings-<Index>)#
```

Command	Description
Index	Defines the table row index.
`group {read-only|read-write}`	Defines the access privilege of the SNMP community string.
`name`	Defines a descriptive name for the SNMP Community String.
`password`	Defines a password for the SNMP Community String.

Command Mode

Privileged User

Example

This example configures a read-only SNMP community string with password "Public-abc12_3":

```
(config-system)# snmp settings
(snmp)# community-strings 2
(community-strings-2)#  group read-only
(community-strings-2)#  name MonitorGroup
```

```
(community-strings-2)#  password Public-abc12_3
(community-strings-2)#  exit
```

trusted-manager

This command configures the SNMP Trusted Managers table, which configures SNMP Trusted Managers.

Syntax

```
(config-system)# snmp settings
(snmp)# trusted-manager <Index>
(trusted-manager-<Index>)#
```

Command	Description
Index	Defines the table row index.
ip-address	Defines the SNMP Trusted Manager's IPv4 address.
name	Defines a descriptive name for the SNMP Trusted Manager.

Command Mode

Privileged User

Example

This example configures an SNMP Trusted Manager with address 10.13.4.145:

```
(config-system)# snmp settings
(snmp)# trusted-manager 1
(trusted-manager-1)# name MyTrustedSNMP
(trusted-manager-1)# ip-address 10.13.4.145
(trusted-manager-1)# exit
```

trap-destination

Delete this text and replace it with your own content.

This command configures the SNMP Trap Destinations table, which configures SNMP trap destinations (managers).

Syntax

```
(config-system)# snmp settings
(snmp)# trap-destination <Index>
(trap-destination-<Index>)#
```

Command	Description
Index	Defines the table row index.
`address`	Defines the SNMP trap destination address (IP address or FQDN).
`enable {disable|enable}`	Enables the sending of traps to the SNMP trap destination.
`name`	Defines a descriptive name for the SNMP trap destination.
`port`	Defines the SNMP trap destination port.
`snmp-version {SNMPv2|SNMPv3}`	Defines the SNMP version of the SNMP trap manager (user).
`snmpv3-user`	Assigns an SNMPv3 user to this SNMP trap destination. **Note:** The command is applicable only if you configure `snmp-version` to `SNMPv3`.

Command Mode

Privileged User

Example

This example configures an SNMPv3 trap destination at 10.13.4.145:

```
(config-system)# snmp settings
(snmp)# trap-destinations 1
(trap-destinations-1)#  address 10.13.4.145
(trap-destinations-1)#  snmp-version SNMPv3
```

```
(trap-destinations-1)# snmpv3-user MyTrapManager
(trap-destinations-1)# exit
```

v3-users

This command configures the SNMPv3 Users table, which configures SNMPv3 users.

Syntax

```
(config-system)# snmp settings
(snmp)# v3-users <Index>
(v3-users-<Index>#
```

Command	Description
Index	Defines the table row index.
`auth-key`	Defines the authentication key. The hex string should be in xx:xx:xx... format (string).
`auth-protocol {md5|none|sha-1|sha-2-224| sha-2-256| sha-2-384| sha-2-512}`	Defines the authentication protocol.
`group {read-only|read-write|trap}`	Defines the group that this user is associated with.
`priv-key`	Defines the privacy key. The hex string should be in xx:xx:xx... format.
`priv-protocol {3des|aes-128|aes-192| aes-256|des|none}`	Defines the privacy protocol (string).
`username`	Defines the name of the SNMP user. Must be unique in the scope of SNMPv3 users and community strings.

Command Mode

Privileged User

Example

This example configures an SNMPv3 user:

```
(config-system)# snmp settings
(snmp)# v3-users 0
(v3-users-0)# username JaneD
```

39 user

This command configures the Local Users table, which configures management user accounts.

Syntax

```
(config-system)# user <Username>
(user-<Username>)#
```

Command	Description
`block-duration <Time>`	Defines the duration (in seconds) for which the user is blocked when the user exceeds a user-defined number of failed login attempts.
`cli-session-limit <Max. Sessions>`	Defines the maximum number of concurrent CLI sessions logged in with the same username-password.

`password <displayed password>|<Enter key for hidden password>`	Defines the user's password.
	- To show the password as you type, type the `password` command and then the password.
	- To hide the password as you type, type the `password` command, press the Enter key, and then type the password.
	Note:
	- For obscured (encrypted) passwords, do one of the following:
	✓ After typing the `password` command, paste (or type) the obscured password, and then type the `obscured` command, for example:
	`(config-system)# user John`
	`Configure new user John`
	`(user-John)#` **`password`**
	`db6bce85685c6634f61115456a083ea753f6d1`
	`7bc228ffa3ea306a4ec6f7f66e405b3904b`
	`8476465cca64 962af33cafd1` **`obscured`**
	To generate an encrypted password, configure the password through the Web interface, and then save the device's configuration to an ini file. As the ini file displays passwords in obscured format by default, simply copy-and-past the

Command	Description
	encrypted password from the ini file into the CLI. ✓ After typing the `password` command, press Enter, and then type the password, which is hidden when you type. This method is typically used when you don't have an obscured password; the device converts your typed password (e.g., "1234") into an obscured password. For example: (config-system)# user John Configure new user John (user-John)# password Please enter hidden password (press CTRL+C to exit): ■ To enforce password configuration in obscured format, use the command `obscure-password-mode on`. ■ The device displays all configured passwords as encrypted (obscured) in its CLI outputs.
`password-age <Days>`	Defines the validity duration (in days) of the password.
`privilege {admin|sec-admin|user}`	Defines the user's privilege level.
`public-key`	Defines a Secure Socket Shell (SSH) public key for RSA public-key authentication (PKI) of the remote user when logging into the device's CLI through SSH.
`session-limit <Max. Sessions>`	Defines the maximum number of concurrent Web sessions logged in with the same username-password.
`session-timeout <Number>`	Defines the duration (in minutes) of inactivity of a logged-in user, after which the user is automatically logged off the Web session.
`status {failed-login|inactivity|new|valid}`	Defines the status of the user.
`tls-subject-name`	Defines the Subject Name that should be in the certificate used

Command	Description
	for the TLS connection with the user.

Command Mode

Privileged User

Example

This example configures a new user "John" and hides the password when typed:

```
(config-system)# user John
Configure new user John
(user-John)# password

Please enter hidden password (press CTRL+C to exit):
New password successfully configured!
```

40 user-defined-failure-pm

This command configures the User Defined Failure PM table, which lets you configure user-defined Performance Monitoring (PM) SNMP MIB rules for SBC calls.

Syntax

```
(config-system)# user-defined-failure-pm <Index>
(user-defined-failure-pm-<Index>)#
```

Command	Description
Index	Defines the table row index.
`description`	Defines a descriptive name for the rule.
`internal-reason`	Defines the failure reason(s) that is generated internally by the device to count.
`method {invite|register}`	Defines the SIP method to which the rule is applied.
`sip-reason`	Defines the SIP failure reason(s) to count.
`user-defined-failure-pm {1-26}`	Defines the ID of the SNMP MIB group that you want to configure.

Command Mode

Privileged User

Example

This example configures a user- defined Performance Monitoring (PM) SNMP MIB group (#1)that counts SIP 403 responses due to INVITE messages:

```
(config-system)# user-defined-failure-pm 0
(user-defined-failure-pm-0)# method -invite
(user-defined-failure-pm-0)# sip-reason 403
(user-defined-failure-pm-0)# user-defined-failure-pm 1
```

40 users-settings

This command configures the enforcement of username and password complexity.

Syntax

```
(config-system)# users-settings
(users-settings)#
```

Command	Description
`enforce-password-complexity {off|on}`	Enables the enforcement of password complexity.
`enforce-username-complexity {off|on}`	Enables the enforcement of username complexity.
`password-complexity-check-by-regex`	Defines a password complexity policy by a regular expression (regex).
`username-complexity-check-by-regex`	Defines a username complexity policy by a regular expression (regex).

Command Mode

Privileged User

Example

This example enforces password complexity according to a regex:

```
(config-system)# users-settings
(users-settings)# enforce-password-complexity on
(users-settings)# password-complexity-check-by-regex ^(?!.*\\.\\.)[\\w.-]{1,40}$
```

41 web

This command configures various Web interface settings.

Syntax

```
(config-system)# web
(web)#
```

Command	Description
`blocking-duration-factor`	Defines the number to multiple the previous blocking time for blocking the IP address (management station) or user upon the next failed login scenario.
`check-password-history {off|on}`	Enables the device to enforce password history policy (reuse an old password), which prohibits a user from changing its password to any of the user's four previous passwords.
`check-weak-psw {off|on}`	Enables the weak password detection feature, which detects if a user in the Local Users table is configured with a weak password (listed in the Weak Passwords List table).
`csrf-protection {off|on}`	Enables cross-site request forgery (CSRF) protection of the device's embedded Web server.
`deny-auth-timer`	Defines the duration (in seconds) for which login to the Web interface is denied from a specific IP address (management station) for all users, when the number of failed login attempts has exceeded the maximum.
`deny-access-counting-valid-time`	Defines the maximum time interval (in seconds) between failed login attempts to be included in the count of failed login attempts for denying access to the user
`deny-access-on-fail-count`	Defines the maximum number of failed login attempts, after which the requesting IP address (management station) for all users is blocked.
`display-last-login-info {off|on}`	Enables the display of the user's login information upon each successful login attempt.
`enforce-password-complexity`	Enforces password complexity for users login and SNMP Community Strings.

Command	Description
`{off|on}`	
`enforce-web-host-name {off|on}`	Enforces access to the device's Web interface through a hostname only, and blocks any attempt to access the Web interface through the device's IP address.
`http-auth-mode {basic|digest-http-only|digest-when-possible}`	Selects HTTP basic (clear text) or digest (MD5) authentication for the Web interface.
`http-port`	Defines the device's LAN HTTP port for Web interface access.
`https-port`	Defines the device's LAN HTTPS port for secure Web interface access.
`invalid-login-report`	Defines how much information is provided in the logged error message when a user attempts to log in to the device with the wrong username or password (i.e., authentication failure).
`local-users-table-can-be-empty {off|on}`	Enables (allows) the deletion of all users in the Local Users table.
`min-web-password-len`	Defines the minimum length (number of characters) of the management user's login password when password complexity is enabled (using the [EnforcePasswordComplexity] parameter).
`req-client-cert {off|on}`	Enables requirement of client certificates for HTTPS Web interface connections.
`secured-connection {http-and-https|https-only|https-redirect}`	Defines the protocol (HTTP or HTTPS) for accessing the Web interface.
`session-timeout`	Defines the duration (in minutes) of inactivity of a logged-in user in the Web interface, after which the user is automatically logged off the Web session.
`user-inactivity-timeout`	Defines the duration (in days) for which a user has not logged in to the Web interface, after which the status of the user

Command	Description
	becomes inactive and can no longer access the Web interface.
`web-hostname`	Defines a hostname (FQDN) for accessing the device's Web interface.
`web-if`	Defines Web Interfaces (see web-if below).
`web-logo-enable {0|1}`	Enables the Web interface to display user-defined text instead of an image (logo).
`web-logo-text`	Defines the text that is displayed instead of the logo in the Web interface.
`web-password-change-interval`	Defines the minimum duration (in minutes) between login password changes.

Command Mode

Privileged User

Note

For more information on the commands, refer to the User's Manual.

Example

This example enables requirement of client certificates for HTTPS Web interface connections:

```
(config-system)# web
(web)# req-client-cert on
```

web-if

This command configures the Web Interfaces table, which lets you define additional interfaces for accessing the device's Web and REST management interfaces.

Syntax

```
(config-system)# web
(web)# web-if <Index>
(web-if-<Index>)#
```

Command	Description
Index	Defines the table row index.
`https-only-val {http-and-https|https-only}`	Defines the protocol required for accessing the management interface.
`http-port`	Defines the device's LAN HTTP port for management interface access.
`https-port`	Defines the device's LAN HTTPS port for management interface access.
`interface-name`	Assigns an IP Interface through which the management interface is accessed.
`require-client-certificate {no|yes}`	Enables requirement of client certificates for HTTPS management interface connections.
`tls-context-name`	Assigns a TLS Context (from the TLS Contexts table) to the management interface.

Command Mode

Privileged User

Example

This example configures a web interface on IP network interface "ITSP", using TLS certification and HTTPS:

```
(config-system)# web
(web)# web-if 0
(web-if-0)# interface-name ITSP
(web-if-0)# tls-context-name ITSP
(web-if-0)# https-only-val https-only
(web-if-0)# activate
```

42 welcome-msg

This command configures a banner message, which is displayed when you connect to the device's management interfaces (Web and CLI).

Syntax

```
(config-system)# welcome-msg <Index>
(welcome-msg-<Index>)# text <Message>
```

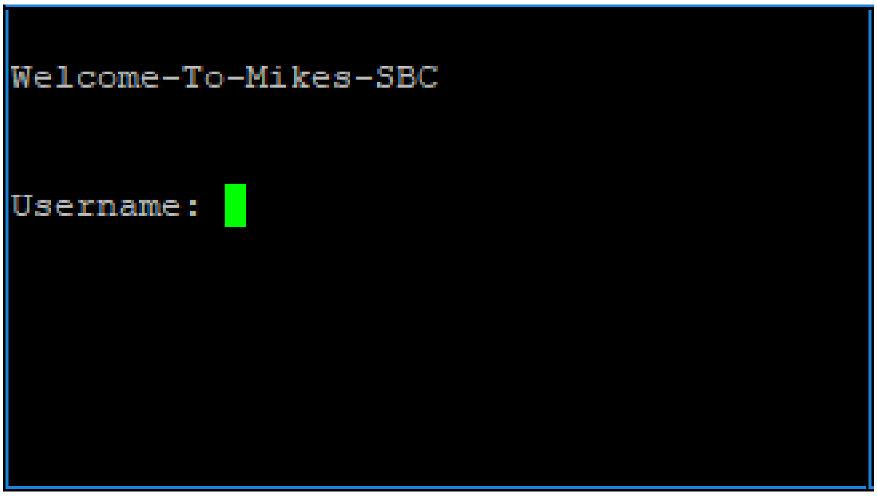
Command	Description
Index	Defines the table row index.
`text <Message>`	Defines the message (string) for the row.
`display`	Displays the banner message.

Command Mode

Privileged User

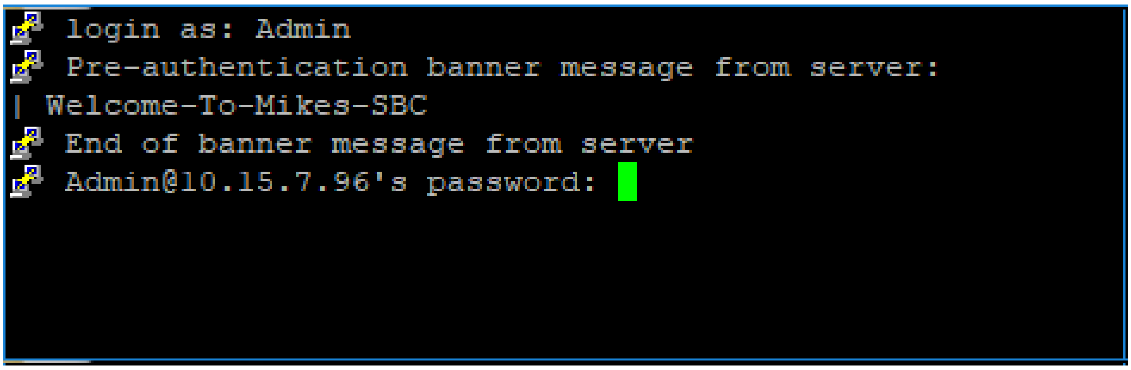
Note

- The message string must not contain spaces between characters. Use hyphens to separate words.
- The location of the displayed message depends on how you access the device:
  - **Web interface or Telnet CLI:** The message is displayed before you enter your login username, as shown in the following example for Telnet:



```
Welcome-To-Mikes-SBC

Username:
```

- **SSH CLI:** The message is displayed after you enter your login username (before the login password prompt), as shown in the following example:



```
login as: Admin
Pre-authentication banner message from server:
| Welcome-To-Mikes-SBC
End of banner message from server
Admin@10.15.7.96's password:
```

Example

- This example configures a banner message:

```
(config-system)# welcome-msg 0
(welcome-msg-0)# text Hello-World-of-SBC
(welcome-msg-0)# activate
(welcome-msg-0)# exit
(config-system)# welcome-msg 1
(welcome-msg-1)# text Configure-Me
(welcome-msg-1)# activate
```

- This example displays the message:

```
(config-system)# welcome-msg display
welcome-msg 0
 text "Hello-World-of-SBC"
welcome-msg 1
 text "Configure-Me"
```

- The message is displayed when you connect to the device's management interface:

```
Hello-World-of-SBC
Configure-Me
Username: Admin
```

Part IV

Troubleshoot-Level Commands

43 Introduction

This part describes the commands located on the Troubleshoot configuration level. The commands of this level are accessed by entering the following command at the root prompt:

Syntax

```
# configure troubleshoot
(config-troubleshoot)#
```

This level includes the following commands:

Command	Description
`activity-log`	See activity-log on page 245
`activity-trap`	See activity-trap on page 247
`cdr`	See cdr on page 248
`cdr-server`	See cdr-server on page 259
`debug-file`	See debug-file on page 261
`pstn-debug`	See pstn-debug on page 262
`fax-debug`	See fax-debug on page 263
`logging`	See logging on page 264
`max-startup-fail-attempts`	See max-startup-fail-attempts on page 269
`pool-thresholds settings`	See pool-thresholds settings on page 270
`pstn-debug`	See pstn-debug on page 271
`sdr`	See sdr on page 272
`sdr-server`	See sdr-server on page 278
`startup-n-recovery`	See startup-n-recovery on page 280
`syslog`	See syslog on page 281
`test-call`	See test-call

Command Mode

Privileged User

44 activity-log

This command configures event types performed in the management interface (Web and CLI) to report in syslog messages or in an SNMP trap.

Syntax

```
(config-troubleshoot)# activity-log
(activity-log)#
```

Command	Description
`action-execute {on|off}`	Enables logging notifications on actions executed events.
`cli-commands-log {on|off}`	Enables logging of entered CLI commands.
`config-changes {on|off}`	Enables logging changes in parameter values.
`device-reset {on|off}`	Enables logging notifications on device-restart events.
`files-loading {on|off}`	Enables logging notifications on auxiliary-files-loading events.
`flash-burning {on|off}`	Enables logging notifications on flash-memory-burning events.
`incremental-ini-log {on|off}`	Enables logging of changes in parameter values due to a loaded incremental ini file.
`login-and-logout {on|off}`	Enables logging notifications on login and logout events.
`sensitive-config-changes {on|off}`	Enables logging notifications on sensitive-parameters-value-change events.
`software-update {on|off}`	Enables logging notifications on device-software-update events.
`unauthorized-access {on|off}`	Enables logging notifications on non-authorized-access events.

Command Mode

Privileged User

Related Command

- activity-trap: enables an SNMP trap to report Web user activities
- show activity-log: displays logged activities
- max-ini-activity-logs: Defines the maximum lines in the incremental ini file to log when the command is set to incremental-ini-log.

Example

This example enables reporting of login and logout attempts:

```
(config-troubleshoot)# activity-log
(activity-log)# login-and-logout on
```

45 activity-trap

This command enables the device to send an SNMP trap to notify of Web user activities in the Web interface.

Syntax

```
(config-troubleshoot)# activity-trap {on|off}
```

Command Mode

Privileged User

Related Command

activity-log - configures the activity types to report.

Example

This example demonstrates configuring the activity trap:

```
(config-troubleshoot)# activity-trap on
```

46 cdr

This command provides sub-commands that configure various settings for CDRs.

Syntax

```
(config-troubleshoot)# cdr
(cdr)#
```

Command	Description
`aaa-indications {accounting-only|none}`	Configures which Authentication, Authorization and Accounting indications to use.
`call-duration-units {centi-seconds|deci-seconds|milliseconds|seconds}`	Defines the units of measurement for the call duration field in CDRs.
`call-end-cdr-sip-reasons-filter`	Defines SIP release cause codes that if received for the call, the devicedoes not sent Call-End CDRs for the call.
`call-end-cdr-zero-duration-filter {off|on}`	Enables the device to not send Call-End CDRs if the call's duration is zero (0).
`call-failure-internal-reasons`	Defines the internal response codes (generated by the device) that you want the device to consider as call failure, which is indicated by the optional 'Call Success' field in the sent CDR.
`call-failure-sip-reasons`	Defines the SIP response codes that you want the device to consider as call failure, which is indicated by the optional 'Call Success' field in the sent CDR.
`call-success-internal-reasons`	Defines the internal response codes (generated by the device) that you want the device to consider as call success, which is indicated by the optional 'Call Success' field in the sent CDR.
`call-success-sip-reasons`	Defines the SIP response code that you want the device to consider as call

Command	Description
	success, which is indicated by the optional 'Call Success' field in the sent CDR.
`call-transferred-after-connect`	Defines if the device considers a call as a success or failure when the internal response (generated by the device) "RELEASE_BECAUSE_CALL_TRANSFERRED" (807) is generated after call connect (SIP 200 OK).
`call-transferred-before-connect`	Defines if the device considers a call as a success or failure when the internal response (generated by the device) "RELEASE_BECAUSE_CALL_TRANSFERRED" (807) is generated before call connect (SIP 200 OK).
`cdr-file-name`	Defines the filename using format specifiers for locally stored CDRs.
`cdr-format`	Customizes the CDR format (see cdr-format on page 251).
`cdr-report-level {connect-and-end-call|end-call|none|start-and-end-and-connect-call|start-and-end-call}`	Defines the call stage at which media- and signaling-related CDRs are sent to a Syslog server.
`cdr-seq-num {off|on}`	Enables sequence numbering of SIP CDR syslog messages.
`cdr-servers-bulk-size`	Defines the maximum number of locally stored CDR files (i.e., batch of files) that the device sends to the remote server in each transfer operation.
`cdr-servers-send-period`	Defines the periodic interval (in seconds) when the device checks if a locally stored CDR file is available for sending to the remote CDR server.
`cdr-srvr-ip-adrr`	Defines the syslog server IP address for sending CDRs.
`compression-format`	Defines the file compression type for

Command	Description
`{gzip|none|zip}`	locally stored CDRs.
`enable {off|on}`	Enables or disables the RADIUS application.
`file-size`	Defines the maximum size per locally stored CDR file, in KB.
`files-num`	Defines the maximum number of locally stored CDR files.
`rotation-period`	Defines the interval size for locally stored CDR files, in minutes.
`media-cdr-rprt-level {end|none|start-and-end|start-end-and-update|update-and-end}`	Enables media-related CDRs of SBC calls to be sent to a Syslog server and configures the call stage at which they are sent.
`no-user-response-after-connect`	Defines if the device considers a call as a success or failure when the internal response (generated by the device) "GWAPP_NO_USER_RESPONDING" (18) is received after call connect (SIP 200 OK).
`no-user-response-before-connect`	Defines if the device considers a call as a success or failure when the internal response (generated by the device) "RELEASE_BECAUSE_CALL_TRANSFERRED" (807) is generated before call connect (SIP 200 OK).
`non-call-cdr-rprt {off|on}`	Enables creation of CDR messages for non-call SIP dialogs (such as SUBSCRIBE, OPTIONS, and REGISTER).
`radius-accounting {end-call|connect-and-end-call|start-and-end-call}`	Configures at what stage of the call RADIUS accounting messages are sent to the RADIUS accounting server.
`rest-cdr-http-servers`	Defines the REST server (by name) to where the device sends CDRs through REST API.
`rest-cdr-report-level {connect-and-end-call|connect-`	Enables signaling-related CDRs to be sent to a REST server and defines the call stage

Command	Description
`only|end-call|none|start-and-end-and-connect-call|start-and-end-call}`	at which they are sent.
`time-zone-format`	Defines the time zone string (only for display purposes).

Command Mode

Privileged User

Example

This example configures the call stage at which CDRs are generated:

```
(config-troubleshoot)# cdr
(cdr)# cdr-report-level start-and-end-call
```

cdr-format

This command customizes the format of CDRs for gateway (Gateway CDR Format table) and SBC (SBC CDR Format table) calls.

Syntax

```
(config-troubleshoot)# cdr
(cdr)# cdr-format
```

Command	Value
`gw-cdr-format`	See gw-cdr-format on the next page
`sbc-cdr-format`	See sbc-cdr-format on page 254
`show-title`	See show-title on page 257

Command Mode

Privileged User

gw-cdr-format

This command customizes the format of CDRs for gateway (Gateway CDR Format table) calls.

Syntax

```
(config-troubleshoot)# cdr
(cdr)# cdr-format gw-cdr-format <Index>
(gw-cdr-format-<Index>)#
```

Command	Value
Index	Defines the table row index.
`cdr-type {json-gw| local-storage-gw| radius-gw| syslog-gw}`	Defines the type of CDRs that you want customized.
`col-type {acct-stat-type|alert-time|amd-decision|amd-decision-prob|aoc-amount|aoc-currency|aoc-mult|b-channel|blank|call-duration|call-end-seq-num|call-id|call-orig|call-orig-radius|call-success|callee-display-id|caller-display-id|cdr-type|channel-id|coder-type|conn-id|connect-time|dst-host|dst-host-before-map|dst-ip|dst-num|dst-num-before-map|dst-num-plan|dst-num-type|dst-port|ep-type|fax-on-call|global-session-id|h323-id|ip-group-id|ip-group-name|ip-profile-id|ip-profile-name|isdn-line-type|latched-rtp-ip|latched-rtp-port|latched-t38-`	Defines the CDR field (column) that you want to customize.

<table>
<tr><th>Command</th><th>Value</th></tr>
<tr><td>ip|latched-t38-port|lcl-in-oct|lcl-in-pkt|lcl-jitter|lcl-mos-cq|lcl-out-oct|lcl-out-pkt|lcl-pkt-loss|lcl-r-factor|lcl-round-trip-delay|lcl-rtp-ip|lcl-rtp-port|lcl-ssrc-sender|leg-id|media-realm-id|media-realm-name|media-type|metering-pulses-generated|module-and-port|none|payload-type|pkt-interval|proxy-set-id|proxyset-name|pstn-term-reason|radius-call-id|redirect-num|redirect-num-before-map|redirect-num-plan|redirect-num-type|redirect-reason|release-time|report-type|rmt-in-oct|rmt-in-pkt|rmt-ip|rmt-jitter|rmt-mos-cq|rmt-out-oct|rmt-out-pkt|rmt-pkt-loss|rmt-port|rmt-r-factor|rmt-round-trip-delay|rmt-rtp-ip|rmt-rtp-port|rmt-ssrc-sender|rtp-ip-diffserv|session-id|setup-time|sig-ip-diffserv|sip-int-id|sip-local-tag|sip-remote-tag|sip-term-desc|sip-term-reason|sipinterface-name|src-dial-plan-tags|src-host|src-host-before-map|src-ip|src-num|src-num-before-map|src-num-plan|src-num-type|src-port|src-tags|srd-id|srd-name|term-reason|term-reason-cat|term-reason-val|term-side|term-side-radius|term-side-yes-no|transport-type|trigger|trunk-group-id|trunk-id|var-call-user-</td><td></td></tr>
</table>

Command	Value
`radius-id`	Defines the ID of the RADIUS Attribute.
`radius-type {standard|vendor-specific}`	Defines the RADIUS Attribute type.
`title`	Configures a new name for the CDR field name.

Command Mode

Privileged User

Example

This example changes the CDR field name "call-duration" to "Phone-Duration" for Syslog messages:

```
(config-troubleshoot)# cdr
(cdr)# cdr-format gw-cdr-format 0
(gw-cdr-format-0)# cdr-type syslog-media
(gw-cdr-format-0)# col-type call-duration
(gw-cdr-format-0)# title Phone-Duration
```

sbc-cdr-format

This command customizes the format of CDRs for SBC (SBC CDR Format table) calls.

Syntax

```
(config-troubleshoot)# cdr
(cdr)# cdr-format sbc-cdr-format <Index>
(sbc-cdr-format-<Index>)#
```

Command	Value
Index	Defines the table row index.
`cdr-type {local-storage-gw|radius-gw|syslog-gw}`	Defines the type of CDRs that you want customized.

Command	Value
`col-type {acct-stat-type|alert-time|blank|call-duration|call-end-seq-num|call-id|call-orig|call-orig-radius|call-success|callee-display-id|caller-display-id|cdr-type|channel-id|coder-transcoding|coder-type|connect-time|direct-media|dst-host|dst-host-before-map|dst-ip|dst-port|dst-tags|dst-uri|dst-uri-before-map|dst-username|dst-username-before-map|ep-type|global-session-id|h323-id|ip-group-id|ip-group-name|ip-profile-id|ip-profile-name|is-recorded|latched-rtp-ip|latched-rtp-port|latched-t38-ip|latched-t38-port|lcl-in-oct|lcl-in-pkt|lcl-jitter|lcl-mos-cq|lcl-out-oct|lcl-out-pkt|lcl-pkt-loss|lcl-r-factor|lcl-round-trip-delay|lcl-rtp-`	Defines the CDR field (column) that you want to customize.

Command	Value
`ip|lcl-rtp-port|lcl-ssrc-sender|leg-id|mc-index|mc-name|media-list|media-realm-id|media-realm-name|media-type|none|payload-type|pkt-interval|proxy-set-id|proxyset-name|radius-call-id|redirect-reason|redirect-uri|redirect-uri-before-map|release-time|released-from-ip|report-type|rmt-in-oct|rmt-in-pkt|rmt-ip|rmt-jitter|rmt-mos-cq|rmt-out-oct|rmt-out-pkt|rmt-pkt-loss|rmt-port|rmt-r-factor|rmt-round-trip-delay|rmt-rtp-ip|rmt-rtp-port|rmt-sip-user-agent|rmt-ssrc-sender|rtp-ip-diffserv|session-id|setup-time|sig-ip-diffserv|sip-int-id|sip-local-tag|sip-method|sip-remote-tag|sip-term-desc|sip-term-reason|sipinterface-name|src-dial-plan-tags|src-host|src-host-before-map|src-ip|src-port|src-tags|src-uri|src-uri-`	

Command	Value
`radius-id`	Defines the ID of the RADIUS Attribute.
`radius-type {standard|vendor-specific}`	Defines the RADIUS Attribute type.
`title`	Configures a new name for the CDR field name.

Command Mode

Privileged User

Example

This example changes the CDR field name "connect-time" to "Call-Connect-Time=" and the RADIUS Attribute to 281 for RADIUS messages:

```
(cdr)# cdr-format sbc-cdr-format 0
(sbc-cdr-format-0)# cdr-type radius-sbc
(sbc-cdr-format-0)# col-type connect-time
(sbc-cdr-format-0)# title Call-Connect-Time=
(sbc-cdr-format-0)# radius-type vendor-specific
(sbc-cdr-format-0)# radius-id 281
```

show-title

This command displays CDR column titles of a specific CDR type.

Syntax

```
(config-troubleshoot)# cdr
(cdr)# cdr-format show-title
```

Command	Value
`local-storage-gw`	Displays CDR column titles of locally stored Gateway CDRs.
`local-storage-sbc`	Displays CDR column titles of locally stored SBC CDRs.

Command	Value
`syslog-gw`	Displays CDR column titles of Syslog Gateway CDRs.
`syslog-media`	Displays CDR column titles of Syslog media CDRs.
`syslog-sbc`	Displays CDR column titles of Syslog SBC CDRs.

Command Mode

Privileged User

Example

This example displays column titles of Syslog Gateway CDRs:

```
(config-troubleshoot)# cdr
(cdr)# cdr-format show-title syslog-gw
|GWReportType   |Cid  |SessionId |LegId|Trunk|BChan|ConId|TG |EPTyp  |Orig
|SourceIp |DestIp |TON  |NPI  |SrcPhoneNum |SrcNumBeforeMap |TON  |NPI
|DstPhoneNum |DstNumBeforeMap |Durat|Coder |Intrv|RtpIp |Port
|TrmSd|TrmReason |Fax |InPackets |OutPackets|PackLoss
|RemotePackLoss|SIPCallId |SetupTime |ConnectTime |ReleaseTime |RTPdelay
|RTPjitter|RTPssrc |RemoteRTPssrc |RedirectReason |TON  |NPI
|RedirectPhonNum |MeteringPulses  |SrcHost |SrcHostBeforeMap |DstHost
|DstHostBeforeMap    |IPG (name) |LocalRtpIp |LocalRtpPort   |Amount |Mult
|TrmReasonCategory|RedirectNumBeforeMap|SrdId (name) |SIPInterfaceId
(name) |ProxySetId (name) |IpProfileId (name) |MediaRealmId
(name)|SigTransportType|TxRTPIPDiffServ |
TxSigIPDiffServ|LocalRFactor|RemoteRFactor|LocalMosCQ|RemoteMosCQ|SigS
ourcePort|SigDestPort|MediaType |AMD| % |SIPTrmReason|SIPTermDesc
|PstnTermReason|LatchedRtpIp |LatchedRtpPort |LatchedT38Ip |LatchedT38Port
|CoderTranscoding
```

47 cdr-server

This command configures the SBC CDR Remote Servers table, which configures remote SFTP servers to where the device sends the locally stored CDRs.

Syntax

```
(config-troubleshoot)# cdr-server
(cdr-server-<Index>)#
```

Command	Value
`Index`	Defines the table row index.
`address`	Defines the address of the server.
`connect-timeout <1-600>`	Defines the connection timeout (in seconds) with the server.
`interface-name`	Assigns an IP Interface from the IP Interfaces table for communication with the server.
`max-transfer-time <1-65535>`	Defines the maximum time (in seconds) allowed to spend for each individual CDR file transfer process.
`name`	Defines an arbitrary name to easily identify the rule.
`password`	Defines the password for authentication with the server.
`port`	Defines the SSH port number of the server.
`priority <0-10>`	Defines the priority of the server.
`remote-path`	Defines the directory path to the folder on the server where you want the CDR files to be sent.
`username`	Defines the username for authentication with the server.

Command Mode

Privileged User

Note

This command is applicable only to Mediant Software and Mediant 9000 SBCs.

Example

This example configures an SFTP server at index 0:

```
(config-troubleshoot)# cdr-server 0
(cdr-server-0)# name CDR-Server
(cdr-server-0)# address 170.10.2.5
(cdr-server-0)# password 1234
(cdr-server-0)# username sftp-my
(cdr-server-0)# remote-path /cdr
(cdr-server-0)# name CDR-Server
(cdr-server-0)# activate
```

48 debug-file

This command configures the Core Dump file feature.

Syntax

```
(config-troubleshoot)# debug-file
(debug-file)#
```

Command	Value
`attach-core-dump {off|on}`	Enables the Core Dump file to be included in the Debug file.
`core-dump-dest-ip`	Defines the IP address of the remote server where you want the device to send the Core Dump file.
`enable-core-dump {off|on}`	Enables the automatic generation of a Core Dump file upon a device crash.

Command Mode

Privileged User

Example

This example enables Core Dump file generation:

```
(config-troubleshoot)# debug-file
(debug-file)# enable-core-dump on
```

49 pstn-debug

This command enables PSTN debugging, which is sent to a Syslog server.

Syntax

```
# pstn-debug {off|on}
```

Note

To disable PSTN debugging, type **pstn-debug off**.

Command Mode

Privileged User

Related Commands

To configure the PSTN trace level, use the command: configure voip > interface > trace-level

Example

Enables PSTN debugging:

```
# pstn-debug on
```

50 fax-debug

This command configures fax / modem debugging.

Syntax

```
(config-troubleshoot)# fax-debug
```

Command	Description
`level {basic|detail}`	Defines the fax / modem debug level.
`max-sessions`	Configures debugging the maximum number of fax / modem sessions.
`off`	Disables fax / modem debugging.
`on`	Enables fax / modem debugging.

Command Mode

Privileged User

Example

This example configures fax / modem debug basic level:

```
(config-troubleshoot)# fax-debug level basic
(config-troubleshoot)# on
```

51 logging

This command configures logging and includes the following subcommands:

- logging-filters (see logging-filters below)
- settings (see settings on the next page)

logging-filters

This command configures the Logging Filters table, which configures filtering rules of debug recording packets, Syslog messages, and Call Detail Records (CDR). The table allows you to enable and disable configured Log Filter rules. Enabling a rule activates the rule, whereby the device starts generating the debug recording packets, Syslog messages, or CDRs.

Syntax

```
(config-troubleshoot)# logging logging-filters <Index>
(logging-filters-<Index>)#
```

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>Index</td><td>Defines the table row index.</td></tr>
<tr><td>filter-type {any|classification|fxs-fxo|ip-group| ip-group-tag| ip-to-ip-routing|ip-to-tel|ip-trace|sip-interface|srd|system-trace|tel-to-ip|trunk-bch|trunk-group-id|trunk-id|user}</td><td>Type of logging filter.</td></tr>
<tr><td>log-dest {debug-rec|local-storage|ovoc|syslog}</td><td>Log destination.</td></tr>
<tr><td>log-type {cdr| none| pstn-trace| signaling| signaling-media| signaling-media-pcm| sip-ladder| sip-only}</td><td>Log type.</td></tr>
<tr><td>mode {disable|enable}</td><td>Enables or disables the log rule.</td></tr>
<tr><td>value</td><td>Value of log filter (string).</td></tr>
</table>

Command Mode

Privileged User

Note

- To configure the PSTN trace level per trunk, use the following command: configure voip > interface > trace-level
- To configure PSTN traces for all trunks (that have been configured with a trace level), use the following command: debug debug-recording <Destination IP Address> pstn-trace
- To send the PSTN trace to a Syslog server (instead of Wireshark), use the following command: configure troubleshoot > pstn-debug

Example

This example configures a Logging Filter rule (Index 0) that sends SIP signaling syslog messages of IP Group 1 to a Syslog server:

```
(config-troubleshoot)# logging logging-filters 0
(logging-filters-0)# filter-type ip-group
(logging-filters-0)# log-dest syslog
(logging-filters-0)# log-type signaling
(logging-filters-0)# mode enable
(logging-filters-0)# value 1
```

settings

This command configures debug recording settings and logging of HTTP requests and responses received from HTTP clients.

Syntax

```
(config-troubleshoot)# logging settings
(logging-settings)#
```

Command	Description
`dbg-rec-blob-account-key`	Defines the SAS token key of the Azure Blob storage container for storing debug recording files. **Note:** This parameter is applicable only to Mediant 90xx and Mediant Software.
`dbg-rec-blob-container`	Defines the name of the Azure Blob storage container for storing debug recording files. **Note:** This parameter is applicable only to

Command	Description
	Mediant 90xx and Mediant Software.
`dbg-rec-blob-storage-url`	Defines the URL of the Azure Blob storage account for storing debug recording files. **Note:** This parameter is applicable only to Mediant 90xx and Mediant Software.
`dbg-rec-dest-ip`	Defines the destination IP address for debug recording.
`dbg-rec-dest-port`	Defines the destination UDP port for debug recording.
`dbg-rec-int-name`	Defines the IP Interface through which the device sends captured traffic to the debug server.
`dbg-rec-ip-trace-entity {all-physical-ports|group|physical-port|vlan-id}`	Defines the filtering of IP traces for log filtering rules (in the Logging Filters table) whose 'Filter Type' parameter is configured to **IP Trace**.
`dbg-rec-ip-trace-eth-group`	Filters IP traces by a specific Ethernet Group.
`dbg-rec-ip-trace-phy-port`	Filters IP traces by a specific Ethernet port.
`dbg-rec-ip-trace-vlan-id`	Filters IP traces by a specific VLAN ID.
`dbg-rec-status {start|stop|timer-restart}`	Displays current debug recording status (Started or Stopped), starts or stops debug recording, and resets the debug recording duration.
`dbg-rec-timeout`	Defines the maximum duration (in minutes) of the debug recording process, after which it automatically stops.
`dbg-rec-local-storage {disable|enable}`	Enables local storage of debug recording files.
`dbg-rec-local-storage-file-size`	Defines the maximum size (in megabytes) of the debug recording file (compressed) for local storage.
`dbg-rec-local-storage-files-count`	Defines the maximum number of debug recording files that can be stored locally.

Command	Description
`dbg-rec-local-storage-filename-prefix`	Defines a prefix for the debug recording file name.
`dbg-rec-local-storage-location {local-disk|azure-blob}`	Defines the type of storage for debug recording files.
`dbg-rec-local-storage-mode {cyclic|non-cyclic}`	Defines the file creation method when the number of maximum files is reached (as configured by the 'Number of Files' parameter), for local storage.
`dbg-rec-local-storage-recording {off|on}`	Starts debug recording file creation and local storage.
`dbg-rec-local-storage-rotation-period`	Defines the periodic duration (in minutes) of how often a debug recording file is created from the Current file (even if empty), for local storage.
`enable-http-client-dbg-msg {off|on}`	Enables the device to log (syslog) HTTP requests and responses (like CURL's verbose data) received from HTTP clients.
`http-log-filter`	Defines the HTTP clients whose requests and responses you want the device to log, based on the presence of specific strings within their URLs.

Command Mode

Privileged User

Example

This example configures the debug recoding server at 10.13.28.10 and starts the recording:

```
(config-troubleshoot)# logging settings
(logging-settings)# dbg-rec-dest-ip 10.13.28.10
(logging-settings)# dbg-rec-status start
```

52 max-ini-activity-logs

This command defines the maximum number of lines of parameters in the loaded incremental ini file to log for the Activity Types to Report feature. The parameter is applicable when you configure the command `activity-log` to `incremental-ini-log on`.

Syntax

```
(config-troubleshoot)# max-ini-activity-logs {0-2000}
```

Command Mode

Privileged User

Related Command

`activity-log`

Example

This example defines the maximum number of lines to log to 100:

```
(config-troubleshoot)# max-ini-activity-logs 100
```

53 max-startup-fail-attempts

This command defines the number of consecutive failed device restarts (boots), after which the device automatically restores its software and configuration based on (by loading) the default System Snapshot.

Syntax

```
(config-troubleshoot)# max-startup-fail-attempts {1-10}
```

Command Mode

Privileged User

Note

The command is applicable only to Mediant 9000 and Mediant SE/VE.

Example

This example defines automatic recovery to be triggered after three consecutive failed restart attempts:

```
(config-troubleshoot)# max-startup-fail-attempts 3
```

53 pool-thresholds settings

This command configures raise and clear thresholds for the acResourcePoolAlarm SNMP alarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.162), which indicates high resource pool utilization.

Syntax

```
(config-troubleshoot)# pool-thresholds settings
(pool-thresholds)
```

Command	Description
`alarm-clear-threshold`	Defines the threshold (in percentage) to clear the acResourcePoolAlarm SNMP alarm. The default is 90.
`alarm-raise-threshold`	Defines the threshold (in percentage) to raise the acResourcePoolAlarm SNMP alarm. The alarm is triggered (major severity level) when a specific resource pool utilization of the device reaches or exceeds this threshold. The default is 95.

Command Mode

Privileged User

Example

This example configures the raise threshold to 92% or more:

```
(config-troubleshoot)# pool-thresholds settings
(pool-thresholds)# alarm-raise-threshold 92
```

54 pstn-debug

This command enables or disables PSTN debugging.

Syntax

```
(config-troubleshoot)# pstn-debug {on|off}
```

Command Mode

Privileged User

Example

This example enables PSTN debugging:

```
(config-troubleshoot)# pstn-debug on
```

55 sdr

This command configures Session Detail Records (SDR).

Syntax

```
(config-troubleshoot)# sdr
```

Command	Description
`compression-format {gzip|none|zip}`	Defines the file compression format for locally stored SDR files.
`file-name`	Defines the filename for locally stored SDRs, using format specifiers.
`file-size`	Defines the size (in kilobytes) of each locally stored SDR file (before compression).
`files-num`	Defines the maximum number of locally stored SDR files.
`local-storage`	Enables the device to store generated SDRs locally.
`rest-sdr-http-servers`	Defines the name of the REST server (configured in the Remote Web Services table) to where the device sends SDRs.
`rest-sdr-record-type {stop|attempt-and-stop|attempt-intermediate-and-stop|intermediate-and-stop|attempt-start-stop|attempt-start-intermediate-stop}`	Defines the SDR types to generate and send to the REST server.
`rotation-period`	Defines how often (in minutes) the device creates a new file for locally stored SDRs.
`sdr-first-inter-interval`	Defines the time (in minutes) of the call at which the device generates the first Intermediate SDR.
`sdr-format {sbc-sdr-format|show-title}`	Defines SDR field customization and displays SDR field titles (see sdr-format sbc-sdr-format on the next page and sdr-format show-title on page 276).

Command	Description
`sdr-inter-interval`	Defines the time (in minutes) between each Intermediate SDR that the device generates during the call.
`sdr-record-type {attempt-and-stop| attempt-intermediate-and-stop| intermediate-and-stop stop}`	Defines the type of SDRs to generate.
`sdr-rest {off|on}`	Enables the device to send SDRs to an HTTP-based REST server, using its REST API.
`sdr-seq-num`	Enables the inclusion of a sequence number (S=) in SDR Syslog messages.
`sdr-servers-bulk-size`	Defines the maximum number of locally stored SDR files (i.e., batch of files) that the device sends to the remote server in each file transfer operation.
`sdr-servers-send-period`	Defines the periodic interval (in seconds) when the device checks if a locally stored SDR file is available for sending to the remote server.
`sdr-srvr-ip-adrr`	Defines the address (IPv4 or IPv6, or FQDN) of the Syslog server to where the device sends the SDRs.
`sdr-syslog {off|on}`	Enables the device to send SDRs to a Syslog server.

Command Mode

Privileged User

Example

This example enables SDR generation only for successfully established and terminated calls:

```
(config-troubleshoot)# sdr
(config-troubleshoot)# sdr-record-type stop
```

sdr-format sbc-sdr-format

This command configures SDR field customization.

Syntax

```
(config-troubleshoot)# sdr
(sdr)# sdr-format sbc-sdr-format <Index>
(sbc-sdr-format-<Index>)#
```

Command	Description
Index	Defines the table row index.
`sdr-type {json-sbc|local-storage|syslog-sbc}`	Defines the application type for which you want to customize SDRs.
`col-type {record-type|product-name|shelf-info|sequence-num|session-id|setup-time|connect-time|time-to-connect|release-time|call-duration|node-time-zone|ingress-calling-user|ingress-calling-host|egress-calling-user|egress-calling-host|ingress-dialed-user|ingress-dialed-host|egress-called-user|egress-called-host|redirectedby-user|redirectedby-host|referredby-user|referredby-host|ingress-call-source-ip|egress-call-dest-ip|ingress-term-reason|ingress-sip-term-reason|egress-term-reason|egress-sip-term-reason|ingress-ipgroup-name|egress-ipgroup-name|ingress-sipinterface-name|egress-sipinterface-name|media-list|route-attempt-num|direct-media|forking|ingress-src-tags|ingress-dst-tags|egress-src-tags|egress-dst-tags|inter-time|ingress-call-id|ingress-source-uri|ingress-dest-uri|ingress-source-uri-before-manipulation|ingress-destination-uri-before-manipulation|ingress-ip-profile-name|ingress-caller-display-id|ingress-callee-display-id|egress-call-id|egress-`	Defines the SDR field (column) that you want to customize.

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><code>source-uri|egress-destination-uri|egress-source-uri-before-manipulation|egress-destination-uri-before-manipulation|egress-ip-profile-name|egress-caller-display-id|egress-callee-display-id|is-success|ingress-sip-term-description|egress-sip-term-description|is-recorded|global-session-id|referredby-tags|ingress-call-orig|egress-call-orig|call-type|ingress-released-from-ip|egress-released-from-ip|ingress-var-call-user-def-1|ingress-var-call-user-def-2|ingress-var-call-user-def-3|ingress-var-call-user-def-4|ingress-var-call-user-def-5|egress-var-call-user-def-1|egress-var-call-user-def-2|egress-var-call-user-def-3|egress-var-call-user-def-4|egress-var-call-user-def-5|is-route-attempt|termination-side|ingress-codertype|egress-codertype|ingress-remote-input-packets|ingress-audio-packets-recvd|ingress-remote-packet-loss|ingress-packet-loss|egress-remote-input-packets|egress-audio-packets-recvd|egress-remote-packet-loss|egress-packet-loss|ingress-local-packets-loss|ingress-local-input-packets|ingress-local-output-packets|ingress-local-input-octets|ingress-local-output-octets|ingress-local-round-trip-delay|ingress-local-jitter|ingress-local-ssrc-sender|ingress-remote-output-packets|ingress-remote-input-octets|ingress-remote-output-octets|ingress-remote-round-trip-delay|ingress-remote-jitter|ingress-remote-ssrc-sender|egress-local-packets-loss|egress-local-input-packets|egress-local-output-packets|egress-local-input-octets|egress-local-output-octets|egress-local-round-trip-delay|egress-local-jitter|egressLocal-ssrc-sender|egress-</code></td><td></td></tr>
</table>

Command	Description
`title`	Defines a new name for the SDR field that you selected above.

Command Mode

Privileged User

Example

This example configures the SDR for sending to a REST server, with a single field whose name is "Phone Call Duration" for call duration:

```
(config-troubleshoot)# sdr
(sdr)# sdr-format sbc-sdr-format 0
(sbc-sdr-format-0)# sdr-type json-sbc
(sbc-sdr-format-0)# col-type call-duration
(sbc-sdr-format-0)# title Phone Call Duration
```

sdr-format show-title

This command displays the names (titles) of the SDR fields.

Syntax

```
(config-troubleshoot)# sdr
(sdr)# sdr-format show-title
```

Command	Description
`local-storage-sbc`	Displays the field titles for local storage SDRs.
`syslog-sbc`	Displays the field titles for SDRs in Syslog messages (sent to the Syslog server).

Command Mode

Privileged User

Example

This example displays the field titles for SDRs in Syslog messages:

```
(config-troubleshoot)# sdr
(sdr)# sdr-format show-title syslog-sbc
|RecordType|ProductName|ShelfInfo|SeqNum|SessionIdSetupTime|TimeToConn
ect|CallDuration|TimeZone|
IngressCallingUserName|EgressCallingUserName|IngressDialedUserName|Egre
ssCalledUserName|IngressCallSourceIp|
EgressCallDestIp|EgressTrmReason|EgressSIPTrmReason|IngressSipInterfaceN
ame|EgressSipInterfaceName|RouteAttemptNum
```

56 sdr-server

This command configures the SBC SDR Remote Servers table, which configures remote SFTP servers to where the device sends the locally stored SDR files.

Syntax

```
(config-troubleshoot)# sdr-server
(sdr-server-<Index>)#
```

Command	Value
`Index`	Defines the table row index.
`address`	Defines the address of the server.
`connect-timeout <1-600>`	Defines the connection timeout (in seconds) with the server.
`interface-name`	Assigns an IP Interface.
`max-transfer-time <1-65535>`	Defines the maximum time (in seconds) allowed to spend for each individual file transfer process.
`name`	Defines an arbitrary name to easily identify the rule.
`password`	Defines the password for authentication with the server.
`port`	Defines the SSH port number of the server.
`priority <0-10>`	Defines the priority of the server.
`remote-path`	Defines the directory path to the folder on the server where you want the files to be sent.
`username`	Defines the username for authentication with the server.

Command Mode

Privileged User

Example

This example configures an SFTP server at index 0:

```
(config-troubleshoot)# sdr-server 0
(sdr-server-0)# name SDR-Server
(sdr-server-0)# address 170.10.2.5
(sdr-server-0)# interface-name OAMP
(sdr-server-0)# password 1234
(sdr-server-0)# username sftp-my
(sdr-server-0)# remote-path /sdr
(sdr-server-0)# activate
```

57 startup-n-recovery

This command is for performing various management tasks.

Syntax

```
(config-troubleshoot)# startup-n-recovery
(startup-n-recovery)#
```

Command	Description
`enable-kernel-dump {core-dump|disable|exception-info}`	Enables kernel dump mode.
`startup-dark-mode {off|on}`	Hides the bootup log messages from being displayed in the CLI console during a device reset (boot up). However, if the device fails to load, serial darkening is disabled in the next bootup attempt.
`system-console-mode {rs232|vga}`	Defines the access mode for the console

Command Mode

Privileged User

Note

The command is applicable only to Mediant 9000 and Mediant SE/VE.

Example

This example configures the console mode to RS-232:

```
(config-troubleshoot)# startup-n-recovery
(startup-n-recovery)# system-console-mode rs232
(startup-n-recovery)# activate
```

58 syslog

This command configures syslog debugging.

Syntax

```
(config-troubleshoot)# syslog
(syslog)#
```

Command	Description
`debug-level {basic|detailed|no-debug}`	Defines the SIP media gateway's debug level.
`debug-level-high-threshold`	Defines the threshold for auto-switching of debug level.
`log-level {alert| critical| debug-not-recommended | error| emergency| info-not-recommended| notice| warning}`	Defines the minimum severity level of messages included in the Syslog message that is generated by the device. **Note:** It's strongly recommended to leave the syslog severity level at its default setting (i.e., `notice`) to prevent excessive utilization of the device's resources. Changing severity level is typically done only by AudioCodes Support for debugging.

Command	Description
`specific-debug-names-list`	Configures a specific debug names list (string).
`syslog {on|off}`	Enables or disables syslog messages.
`syslog-cpu-protection {on|off}`	Enables or disables downgrading the debug level when CPU idle is dangerously low.
`syslog-interface`	Assigns an IP Interface from the IP Interfaces table for communication with the primary syslog server.
`syslog-ip`	Defines the syslog server's address (IP address or FQDN).
`syslog-optimization {disable|enable}`	Enables or disables bundling debug syslog messages for performance.
`system-persistent-log-size`	Defines the maximum size (in KB) of each persistent system log file.
`system-persistent-log-period`	Defines the maximum age (in minutes) of each

Command	Description
	persistent system log file.
`syslog-port`	Defines the syslog server's port number.
`syslog-protocol {udp|tcp|tls}`	Defines the transport protocol for communicating with the primary Syslog server.
`syslog-servers`	Defines multiple secondary syslog servers. For more information, see syslog-servers on the next page.
`syslog-tls-context-name`	Assigns a TLS Context when the TLS transport protocol is used for communication with the Syslog server.
`system-log-size`	Defines the local system log file size (in Kbytes).

Command Mode

Privileged User

Note

The sequence number is per syslog destination and is reset whenever one of the parameters in the table above is modified. Therefore, it's recommended not to search logged messages by sequence number. Startup logs are indicated with the [Sup] tag.

Example

This example disables syslog:

```
(config-troubleshoot)# syslog
(syslog)# debug-level no-debug
```

syslog-servers

This command configures the Syslog Servers table, which allows you to configure multiple (up to four) secondary remote syslog servers to where the device sends syslog messages.

Syntax

```
(config-troubleshoot)# syslog
(syslog)# syslog-servers <Index>
(syslog-servers-<Index>)#
```

Command	Description
Index	Defines the table row index.
`info-type {All|CDR|SDR|Syslog}`	Defines the type of information (only CDRs, only SDRs, only syslog, or all) to send in the syslog.
`interface`	Defines the interface for syslog communication.
`ip-address`	Defines the syslog server's IP address (IPv4 or IPv6).
`kafka-connection-string`	Defines the authentication and encryption string

Command	Description
	(password) for connecting to the Kafka broker (topic).
`kafka-topic-name`	Defines the Kafka topic name. When the Kafka broker is hosted on Microsoft Azure, the topic name is the Event Hub name.
`mode {Disabled|Enabled}`	Activates or deactivates the syslog server.
`port`	Defines the syslog server's port number.
`protocol {KAFKA|TCP|TLS|UDP}`	Defines the transport protocol for communicating with the Syslog server.
`severity-level {Alert|Critical|Debug|Emergency|Error|Informational|Notice|Warning}`	Defines the minimum severity level of messages included in the Syslog message.

Command Mode

Privileged User

Niotes

- To configure the primary syslog server, see syslog on page 281.

- Duplicated secondary syslog servers configuration is invalid (i.e., cannot have the same IP address and port) and none can have the same IP address and port as the primary syslog server.
- The syslog sequence number resets if the device is restart.

Example

This example configures a secondary syslog server:

```
(config-troubleshoot)# syslog
(syslog)# syslog-servers 0
(syslog-servers-0)# ip-address 10.14.5.3
(syslog-servers-0)# mode Enabled
(syslog-servers-0)# severity-level Alert
```

59 settings

This command configures various test call settings.

Syntax

```
(config-troubleshoot)# test-call settings
(test-call)#
```

Command	Description
`testcall-dtmf-string`	Configures a DTMF string (tone) that is played for answered test calls.
`testcall-id`	Defines the incoming test call prefix that identifies it as a test call.

Command Mode

Privileged User

Example

This example configures a test call ID:

```
(config-troubleshoot)# test-call
(test-call)# testcall-id 03
```

60 test-call-table

This command configures the Test Call Rules table, which allows you to test SIP signaling (setup and registration) and media (DTMF signals) of calls between a simulated phone on the device and a remote IP endpoint.

Syntax

```
(config-troubleshoot)# test-call test-call-table <Index>
(test-call-table-<Index>)#
```

Command	Description
Index	Defines the table row index.
`allowed-audio-coders-group-name`	Assigns an Allowed Audio Coders Group, configured in the Allowed Audio Coders Groups table, which defines only the coders that can be used for the test call.
`allowed-coders-mode {not-configured|preference|restriction|restriction-and-preference}`	Defines the mode of the Allowed Coders feature for the Test Call.
`application-type {gw|sbc}`	Application type.
`auto-register {disable|enable}`	Automatic register.
`bandwidth-profile`	Bandwidth Profile.
`call-duration`	Call duration in seconds (-1 for auto, 0 for

Command	Description
	infinite).
`call-party {called|caller}`	Test call party.
`called-uri`	Called URI.
`calls-per-second`	Calls per second.
`dst-address`	Destination address and optional port.
`dst-transport {not-configured|sctp|tcp|tls|udp}`	Destination transport type.
`endpoint-uri`	Endpoint URI ('user' or 'user@host').
`ip-group-name`	IP Group.
`max-channels`	Maximum concurrent channels for session.
`media-security-mode {as-is|both|not-configured|rtp|srtp}`	Defines the handling of RTP and SRTP
`offered-audio-coders-group-name`	Assigns a Coder Group, configured in the Coder Groups table, whose coders are added to the SDP Offer in the outgoing Test Call.
`password`	Password for registration.
`play {disable|dtmf|prt}`	Playback mode.

Command	Description
`play-dtmf-method {inband|not-configured|rfc2833}`	Defines the method used by the devicefor sending DTMF digits that are played to the called party when the call is answered.
`play-tone-index`	Defines a tone to play from the installed PRT file.
`qoe-profile`	Quality of Experience (QOE) Profile.
`route-by {dst-address|ip-group}`	Routing method.
`schedule-interval`	0 disables scheduling, any positive number configures the interval between scheduled calls (in minutes).
`sip-interface-name`	SIP Interface.
`test-duration`	Test duration (minutes).
`test-mode {continuous|once}`	Test mode.
`user-name`	User name for registration.

Command Mode

Privileged User

Example

This example partially configures a test call rule that calls endpoint URI 101 at IP address 10.13.4.12:

```
(config-troubleshoot)# test-call test-call-table 0
(test-call-table-0)# called-uri 101
(test-call-table-0)# route-by dst-address
(test-call-table-0)# dst-address 10.13.4.12
```

Part V

Network-Level Commands

61 Introduction

This part describes the commands located on the Network configuration level. The commands of this level are accessed by entering the following command at the root prompt:

```
# configure network
(config-network)#
```

This level includes the following commands:

Command	Description
`access-list`	See access-list on page 295
`cloud-settings`	See cloud-settings on page 297
`custom-dns-server`	See custom-dns-server on page 299
`custom-mtu`	See custom-mtu on page 298
`dhcp-server`	See dhcp-server on page 300
`dns`	See dns on page 306
`dns-fallback-policy`	See dns-fallback-policy on page 311
`ether-group`	See ether-group on page 313
`eth-group-network-monitor`	See eth-group-network-monitor on page 314
`high-availability`	See high-availability on page 316
`http-proxy`	See http-proxy on page 320
`interface`	See interface on page 332
`mtc`	See mtc on page 335
`nat-translation`	See nat-translation on page 339
`network-dev`	See network-dev on page 341
`network-settings`	See network-settings on page 342
`ovoc-tunnel-settings`	See ovoc-tunnel-settings on page 345
`physical-port`	See physical-port on page 346

Command	Description
`qos`	See qos on page 347
`sctp`	See sctp on page 349
`security-settings`	See security-settings on page 351
`sni-to-tls-mapping`	See sni-to-tls-mapping on page 354
`static`	See static on page 355

Command Mode

Privileged User

62 access-list

This command configures the Firewall table, which lets you define firewall rules that define network traffic filtering rules.

Syntax

```
(config-network)# access-list <Index>
(access-list-<Index>)#
```

Command	Description
Index	Defines the table row index.
`allow-type {allow|block}`	Defines the firewall action if the rule is matched.
`byte-burst`	Defines the allowed traffic burst in bytes.
`byte-rate`	Defines the allowed traffic bandwidth in bytes per second.
`description`	Defines an arbitrary name to easily identify the row.
`dns-query-type {A|AAAA|CNAME-A|CNAME-AAAA|SRV-A|SRV-AAAA}`	Defines the DNS query (request) type used by the device to query the DNS server to resolve the domain name into an IP address(es) when the 'Source IP' parameter is configured with an FQDN.
`end-port`	Defines the destination ending port.
`network-interface-name`	Defines the IP Network Interface (string) for which the rule applies.
`packet-size`	Defines the maximum allowed packet size.
`prefixLen`	Defines the prefix length of the source IP address (defining a subnet).
`protocol`	Defines the IP user-level protocol.
`source-ip`	Defines the source IP address from where the packets are received.
`src-port`	Defines the source port from where the packets are received.
`start-port`	Defines the destination starting port.

Command	Description
`use-specific-interface {disable|enable}`	Use the rule for a specific interface or for all interfaces.

Command Mode

Privileged User

Example

This example configures a firewall rule allowing a maximum packet size of 1500 bytes on the "ITSP" network interface:

```
(config-network)# access-list
(access-list-0)# use-specific-interface enable
(access-list-0)# network-interface-name ITSP
(access-list-0)# allow-type allow
(access-list-0)# packet-size 1500
```

63 cloud-settings

This command enables the monitoring of scheduled maintenance events for virtual machines by the cloud platform and enables a switchover before events occur.

Syntax

```
(config-network)# cloud-settings
```

Command	Description
`monitoring-maintenance-events {disable|enable}`	Enables the device to monitor the cloud platform's scheduled maintenance events for virtual machines on which it's installed.
`treatment-maintenance-events {disable|enable}`	Enables the device to perform a switchover (active to standby for HA systems, or move sessions to a different Media Component for Mediant CE SBC's Elastic Media Cluster mode) before a scheduled maintenance event occurs on the virtual machine of the cloud platform.

Command Mode

Privileged User

Note

The command is applicable only to Mediant VE/CE deployed on Azure or Google Cloud Platform (GCP).

Example

This example enables switchover before a scheduled maintenance event occurs:

```
(config-network)# cloud-settings
(cloud-settings)# treatment-maintenance-events enable
```

64 custom-mtu

This command defines the Custom MTU table, which lets you define maximum transmission unit (MTU) size per IP Interface (listed in the IP Interfaces table). The MTU size is reflected in the Ethernet Devices table (`network-dev`).

Syntax

```
(config-network)# custom-mtu <Index>
(custom-mtu-<Index>)#
```

Command	Description
Index	Defines the table row index.
`mtu`	Defines the Maximum Transmission Unit (MTU) size.
`network-if`	Assigns an IP Interface (from the IP Interfaces table) for which the MTU size is applied.

Command Mode

Privileged User

Note

This command is applicable only to Mediant Software deployed on Azure or AWS.

Example

This example configures an MTU of 1,600 bytes for IP Interface eth0:

```
(config-network)# custom-mtu 0
(custom-mtu-0)# mtu 1600
(custom-mtu-0)# network-if eth0
```

65 custom-dns-server

This command defines the Custom DNS Servers table, which lets you define primary and secondary DNS servers per IP Interface (listed in the IP Interfaces table). This DNS configuration is then reflected in the read-only IP Interfaces table (`interface`).

Syntax

```
(config-network)# custom-dns-server <Index>
(custom-dns-server-<Index>)#
```

Command	Description
Index	Defines the table row index.
`network-if`	Assigns an IP Interface (from the IP Interfaces table) for which the DNS servers are defined.
`primary-address`	Defines the primary DNS server address.
`secondary-address`	Defines the secondary DNS server address.

Command Mode

Privileged User

Note

This command is applicable only to Mediant Software deployed on Azure or AWS.

Example

This example configures a primary DNS server for IP Interface eth0:

```
(config-network)# custom-dns-server 0
(custom-dns-server-0)# primary-address 152.1.3.4
(custom-dns-server-0)# network-if eth0
```

66 dhcp-server

This command configures DHCP and includes the following subcommands:

- delete-client (see dhcp-server delete-client below)
- option (see dhcp-server option on the next page)
- server (see dhcp-server server on the next page)
- static-ip (see dhcp-server static-ip on page 304)
- vendor-class (see dhcp-server vendor-class on page 305)

dhcp-server delete-client

This command removes IP addresses of DHCP clients leased from a DHCP server.

Syntax

```
(config-network)# dhcp-server delete-client
```

Command	Description
`all-dynamic`	Removes all dynamic leases.
`all-static`	Removes all static lease reservations.
`black-list`	Clears the blacklist of conflicting IP addresses.
`ip <IP Address>`	Removes a specified leased IP address.
`mac`	Removes a specified lease MAC address.

Command Mode

Privileged User

Example

This example removes the leased IP address 10.13.2.10:

```
(config-network)# dhcp-server delete-client ip 10.13.2.10
```

dhcp-server option

This command configures the DHCP Option table, which lets you define additional DHCP Options that the DHCP server can use to service the DHCP client. These DHCP Options are included in the DHCPOffer response sent by the DHCP server. The table is a "child" of the DHCP Servers table.

Syntax

```
(config-network)# dhcp-server option <Index>
(option-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dhcp-server-number`	Defines the index of the DHCP Servers table.
`expand-value {no|yes}`	Enables the use of the special placeholder strings, "<MAC>" and "<IP>" for configuring the value.
`option`	Defines the DHCP Option number.
`type {ascii|hex|ip}`	Defines the format (type) of the DHCP Option value.
`value`	Defines the DHCP option value.

Command Mode

Privileged User

Example

This example configures an additional DHCP Option 159 for the DHCP server configured in Index 0:

```
(config-network)# dhcp-server option 0
(option-0)# dhcp-server-number 0
(option-0)# option 159
```

dhcp-server server

This command configures the DHCP Servers table, which defines DHCP servers.

Syntax

```
(config-network)# dhcp-server server <Index>
(server-<Index>)#
```

Command	Description
Index	Defines the table row index.
`boot-file-name`	Defines the name of the boot file image for the DHCP client.
`dns-server-1`	Defines the IP address (IPv4) of the primary DNS server that the DHCP server assigns to the DHCP client.
`dns-server-2`	Defines the IP address (IPv4) of the secondary DNS server that the DHCP server assigns to the DHCP client.
`end-address`	Defines the ending IP address (IPv4 address in dotted-decimal format) of the IP address pool range used by the DHCP server to allocate addresses.
`expand-boot-file-name {no|yes}`	Enables the use of the placeholders in the boot file name, defined in 'boot-file-name'.
`lease-time`	Defines the duration (in minutes) of the lease time to a DHCP client for using an assigned IP address.
`name`	Defines the name of the DHCP server.
`netbios-node-type {broadcast|hybrid|mixed|peer-to-peer}`	Defines the NetBIOS (WINS) node type.
`netbios-server`	Defines the IP address (IPv4) of the NetBIOS WINS server that is available to a Microsoft DHCP client.
`network-if`	Assigns a network interface to the DHCP server.

Command	Description
`ntp-server-1`	Defines the IP address (IPv4) of the primary NTP server that the DHCP server assigns to the DHCP client.
`ntp-server-2`	Defines the IP address (IPv4) of the secondary NTP server that the DHCP server assigns to the DHCP client.
`override-router-address`	Defines the IP address (IPv4 in dotted-decimal notation) of the default router that the DHCP server assigns the DHCP client.
`sip-server`	Defines the IP address or DNS name of the SIP server that the DHCP server assigns the DHCP client.
`sip-server-type {dns|IP}`	Defines the type of SIP server address.
`start-address`	Defines the starting IP address (IPv4 address in dotted-decimal format) of the IP address pool range used by the DHCP server to allocate addresses.
`subnet-mask`	Defines the subnet mask (for IPv4 addresses) for the DHCP client.
`tftp-server-name`	Defines the IP address or name of the TFTP server that the DHCP server assigns to the DHCP client.
`time-offset`	Defines the Greenwich Mean Time (GMT) offset (in seconds) that the DHCP server assigns to the DHCP client.

Command Mode

Privileged User

Example

This example configures a DHCP server with a pool of addresses for allocation from 10.13.1.0 to 10.13.1.5 and a lease time of an hour:

```
(config-network)# dhcp-server server
(server-0)# start-address 10.13.1.0
(server-0)# end-address 10.13.1.5
(server-0)# lease-time 60
```

dhcp-server static-ip

This command configures the DHCP Static IP table, which lets you define static IP addresses for DHCP clients. The table is a "child" of the DHCP Servers table.

Syntax

```
(config-network)# dhcp-server static-ip <Index>
(static-ip-<Index<)#
```

Command	Description
Index	Defines the table row index.
`dhcp-server-number`	Associates the DHCP Static IP table entry with a DHCP server that you already configured.
`ip-address`	Defines the "reserved", static IP address (IPv4) to assign the DHCP client.
`mac-address`	Defines the DHCP client by MAC address (in hexadecimal format).

Command Mode

Privileged User

Example

This example configures the DHCP client whose MAC address is 00:90:8f:00:00:00 with a static IP address 10.13.1.6:

```
(config-network)# dhcp-server static-ip 0
(static-ip-0)# dhcp-server-number 0
(static-ip-0)# ip-address 10.13.1.6
(static-ip-0)# mac-address 00:90:8f:00:00:00
```

dhcp-server vendor-class

This command configures the DHCP Vendor Class table, which lets you define Vendor Class Identifier (VCI) names (DHCP Option 60).

Syntax

```
(config-network)# dhcp-server vendor-class <Index>
(vendor-class-<Index>)#
```

Command	Description
Index	Defines the table row index.
dhcp-server-number	Associates the DHCP Vendor Class entry with a DHCP server that you configured.
vendor-class	Defines the value of the VCI DHCP Option 60.

Command Mode

Privileged User

Example

This example configures the vendor class identifier as "product-ABC":

```
(config-network)# dhcp-server vendor-class 0
(vendor-class-0)# dhcp-server-number 0
(vendor-class-0)# vendor-class product-ABC
```

67 dns

This command configures DNS and includes the following subcommands:

- dns-to-ip (see dns dns-to-ip on the next page)
- override (see dns override on the next page)
- settings (see dns settings on page 308)
- srv2ip (see dns srv2ip on page 309)

Syntax

```
(config-network)# dns <Index>
```

Command	Description
Index	Defines the table row index.
`dns-to-ip`	Defines the internal DNS table for resolving host names into IP addresses.
`override`	Defines the DNS override interface.
`settings`	Configures DNS settings.
`srv2ip`	Defines the SRV to IP internal table. The table defines the internal SRV table for resolving host names into DNS A-Records. Three different A-Records can be assigned to a host name. Each A-Record contains the host name, priority, weight and port.

Command Mode

Privileged User

Example

This example configures the SRV to IP internal table:

```
configure network
 (config-network)# dns srv2ip 0
(srv2ip-0)#
```

dns dns-to-ip

This command configures the Internal DNS table, which lets you resolve hostnames into IP addresses.

Syntax

```
(config-network)# dns dns-to-ip <Index>
(dns-to-ip-<Index>)#
```

Command	Description
Index	Defines the table row index.
`domain-name`	Defines the host name to be translated.
`first-ip-address`	Defines the first IP address (in dotted-decimal format notation) to which the host name is translated.
`second-ip-address`	Defines the second IP address (in dotted-decimal format notation) to which the host name is translated.
`third-ip-address`	Defines the third IP address (in dotted-decimal format notation) to which the host name is translated.

Command Mode

Privileged User

Example

This example configures the domain name "proxy.com" with a resolved IP address of 210.1.1.2:

```
(config-network)# dns dns-to-ip 0
(dns-to-ip-0)# domain-name proxy.com
(dns-to-ip-0)# first-ip-address 210.1.1.2
```

dns override

This command configures the DNS override interface, which overrides the Internal DSN table settings.

Syntax

```
(config-network)# dns override interface <String>
```

Command Mode

Privileged User

Example

This example configures the DNS override interface:

```
configure network
(config-network)# dns override interface ITSP-1
```

dns settings

This command configures the default primary and secondary DNS servers.

Syntax

```
(config-network)# dns settings
(dns-settings)#
```

Command	Description
dns-default-primary-server-ip	Defines the IP address of the default primary IPv4 DNS server.
dns-default-secondary-server-ip	Defines the IP address of the default secondary IPv4 DNS server.
dns-default-primary-server-ipv6	Defines the IP address of the default primary IPv6 DNS server.
dns-default-secondary-server-ipv6	Defines the IP address of the default secondary IPv6 DNS server.

Command Mode

Privileged User

Example

This example configures the IP address of the default primary IPv4 DNS server to 210.1.1.2:

```
(config-network)# dns settings
(dns-settings)# dns-default-primary-server-ip 210.1.1.2
```

dns srv2ip

This command configures the Internal SRV table, which lets you resolve hostnames into DNS A-Records.

Syntax

```
(config-network)# dns srv2ip <Index>
(srv2ip-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dns-name-1`	Defines the first, second or third DNS A-Record to which the host name is translated.
`dns-name-2`	
`dns-name-3`	
`domain-name`	Defines the host name to be translated.
`port-1`	Defines the port on which the service is to be found.
`port-2`	
`port-3`	
`priority-1`	Defines the priority of the target host. A lower value means that it is more preferred.
`priority-2`	
`priority-3`	
`transport-type {udp|tcp|tls}`	Defines the transport type.
`weight-1`	Configures a relative weight for records with the same priority.
`weight-2`	
`weight-3`	

Command Mode

Privileged User

Example

This example configures DNS SRV to IP address 208.93.64.253:

```
(config-network)# dns srv2ip 0
(srv2ip-0)# domain-name proxy.com
(srv2ip-0)# transport-type tcp
(srv2ip-0)# dns-name-1 208.93.64.253
```

67 dns-fallback-policy

This command configures the DNS Fallback Policy table, which lets you configure up to two DNS fallback policies, each for a different traffic type (IPv4 or IPv6).

Syntax

```
(config-network)# dns-fallback-policy <Index>
(dns-fallback-policy-<Index>)#
```

Command	Description
Index	Defines the table row index.
`rule1 {global-dns-ipv4|global-dns-ipv6|none|oam-if-ipv4|oam-if-ipv6}`	Defines the first DNS fallback rule.
`rule2 {global-dns-ipv4|global-dns-ipv6|none|oam-if-ipv4|oam-if-ipv6}`	Defines the second DNS fallback rule if rule 1 fails (or configured to `none`).
`rule3 {global-dns-ipv4|global-dns-ipv6|none|oam-if-ipv4|oam-if-ipv6}`	Defines the third DNS fallback rule if rule 2 fails (or configured to `none`).
`rule4 {global-dns-ipv4|global-dns-ipv6|none|oam-if-ipv4|oam-if-ipv6}`	Defines the fourth DNS fallback rule if rule 3 fails (or configured to `none`)
`type {ipv4|ipv6}`	Defines the type of traffic (IP version) for which you want to apply the DNS Fallback policy

Command Mode

Privileged User

Example

This example configures a DNS Fallback policy for IPv4 traffic with two rules - device tries the DNS server of the OAM IPv4 interface and if that fails, it tries the global IP v4 DNS servers:

```
(config-network)# dns-fallback-policy 0
(dns-fallback-policy-0)# type ipv4
(dns-fallback-policy-0)# oam-if-ipv4
(dns-fallback-policy-0)# global-dns-ipv4
(dns-fallback-policy-0)# exit
```

68 ether-group

This command configures the Ethernet Groups table, which lets you define Ethernet Groups by assigning them up to two Ethernet ports.

Syntax

```
(config-network)# ether-group <Index>
(ether-group-<Index>)#
```

Command	Description
Index	Defines the table row index.
member1	Assigns a port to the Ethernet Group.
member2	Assigns another port to the Ethernet Group.
mode {1rx-1tx|2rx-1tx|2rx-2tx|none|single}	Defines the mode of operation of the ports in the Ethernet Group. This applies only to Ethernet Groups containing two ports.

Command Mode

Privileged User

Example

This example configures Ethernet Group 0 with ports GE_4_1 and GE_4_1 and RX/TX mode:

```
(config-network)# ether-group 0
(ether-group-0)# member1 GE_4_1
(ether-group-0)# member2 GE_4_2
(ether-group-0)# mode 1rx-1tx
```

69 eth-group-network-monitor

This command configures the Ethernet Port Group Network Monitor table, which lets you define monitored destinations for determining port switchover for Ethernet port redundancy.

Syntax

```
(config-network)# eth-group-network-monitor <Index>
(eth-group-network-monitor-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dest-address`	Defines destination addresses (IP address or FQDN) of network hosts that you want monitored.
`ethernet-group`	Assigns an Ethernet Group through whose active port the device sends pings to monitor the reachability of destinations.
`ethernet-group-network-monitor-peers-status`	Displays the destinations of a selected monitored row (see ethernet-group-network-monitor-peers-status on the next page).
`network-interface`	Assigns a local IP network interface (listed in the IP Interfaces table) from where the device sends the ping requests.
`ping-count`	Defines the number of consecutive failed pings to the monitored entity, before the device considers the entity as unavailable.
`ping-timeout`	Defines the timeout (in milliseconds) for which the device waits for a reply from the monitored entity for its sent ping request.

Command Mode

Privileged User

Note

The command is applicable only to MP-1288 and Mediant 3100.

Example

This example configures a monitored row that pings IP address destinations 10.4.4.69 and 10.4.5.60 through the port of Ethernet Group 1:

```
(config-network)#  eth-group-network-monitor 0
(eth-group-network-monitor-0)# dest-address 10.4.4.69,10.4.5.60
(eth-group-network-monitor-0)# ethernet-group GROUP_1
(eth-group-network-monitor-0)# ping-timeout 1000
(eth-group-network-monitor-0)# ping-count 3
```

ethernet-group-network-monitor-peers-status

This command displays the reachability status of a specific destination in the Ethernet Port Group Network Monitor Peers Status table, per monitored row in the Ethernet Port Group Network Monitor table.

Syntax

```
(config-network)# eth-group-network-monitor <Index>
(eth-group-network-monitor-<Index>)# ethernet-group-network-monitor-peers-status <Index>
(ethernet-group-network-monitor-peers-status-<Index>/<Index>)# display
```

Command Mode

Privileged User

Note

The command is applicable only to MP-1288 and Mediant 3100.

Example

This example displays the reachability status of a destination of monitored row index 3:

```
(config-network)#  eth-group-network-monitor 3
(eth-group-network-monitor-3)# ethernet-group-network-monitor-peers-status 0
(ethernet-group-network-monitor-peers-status-3/0)# display
peer-dest-address (1.7.0.7)
is-peer-reachable (Reachability unverified)
ping-loss-percentage (100)
```

70 high-availability

This command configures the High Availability (HA) feature and includes the following subcommands:

Syntax

```
(config-network)# high-availability
```

Command	Description
`network-monitor`	See network-monitor below
`settings`	See settings on the next page

Command Mode

Privileged User

network-monitor

This command configures monitored network entities for the HA Network Monitor feature, whereby the device pings the entities and if a user-defined number of entities are offline, triggers an HA switchover.

Syntax

```
(config-network)# high-availability network-monitor <Index>
(network-monitor-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dest-address <IP Addresses>`	Defines the IP address of the destination to ping. You can configure multiple IP addresses, where each is separated by a comma or space.
`network-interface`	Assigns a local IP network interface (listed in the IP Interfaces table) from where the device sends the

Command	Description
	ping requests.
`ping-count`	Defines the number of consecutive failed pings to the monitored entity, before the device considers the entity as unavailable.
`ping-timeout`	Defines the timeout (in milliseconds) for which the device waits for a reply from the monitored entity for its sent ping request.

Command Mode

Privileged User

Example

This example configures a monitored entity with three destinations, pings sent from IP interface "OAMP", ping timeout for a response is 1000 ms, and HA switchover triggered after three failed pings:

```
(config-network)# high-availability network-monitor 0
(network-monitor-0#) dest-address 10.4.4.69,10.4.5.60
(network-monitor-0#) network-interface OAMP
(network-monitor-0#) ping-timeout 1000
(network-monitor-0#) ping-count 3
```

settings

This command configures various HA settings.

Syntax

```
(config-network)# high-availability settings
(ha)#
```

Command	Description
`ha-file-`	Defines the device's port for unsecured file transfer between active

Command	Description
`transfer-port`	and redundant devices in HA mode.
`ha-secure-file-transfer-port`	Defines the device's port for secured (HTTPS) file transfer between active and redundant devices in HA mode.
`ha-secured-connectivity {off|on}`	Enables secure (TLS) communication (HA Maintenance interface) between the active and redundant devices in the HA system.
`network-monitor-enabled {off|on}`	Enables the HA Network Monitor feature (see also the high-availability network-monitor command).
`network-monitor-threshold <1-10>`	Defines the number of failed (no ping responses) network monitored entries that trigger HA switchover.
operational-state-delay	Defines the duration (in seconds) to delay the transition from HA non-operational state, which occurs during HA synchronization between active and redundant devices, to HA operational state.
`priority <1-10>`	Defines the priority of the active device used in the HA Preempt mechanism.
`redundant-priority <1-10>`	Defines the priority of the redundant device used in the HA Preempt mechanism.
`redundant-unit-id-name <Name>`	Configures a name (string) for the redundant device.
`remote-address <IP Address>`	Defines the Maintenance interface address of the redundant device in the HA system. **Note:** For the parameter to take effect, a device restart is required.
`revertive-mode {off|on}`	Enables HA switchover based on HA priority. Note: For the parameter to take effect, a device restart is required.
`unit-id-name <Name>`	Configures a name (string) for the active device.

Command Mode

Privileged User

Example

This example enables the **HA Network Monitor feature**:

```
(config-network)# high-availability settings
(ha)# network-monitor-enabled on
```

71 http-proxy

This command configures HTTP proxy and includes the following subcommands:

Syntax

```
(config-network)# http-proxy
(http-proxy)#
```

Command	Description
`debug-level`	See http-proxy debug-level below
`directive-sets`	See http-proxy directive-sets on the next page
`dns-primary-server`	See http-proxy dns-primary-server on page 322
`dns-secondary-server`	See http-proxy dns-secondary-server on page 322
`http-proxy-app`	See http-proxy http-proxy-app on page 323
http-proxy-global-address	See http-proxy-global-address on page 323
`http-server`	See http-proxy http-server on page 324
`ovoc-serv`	See http-proxy ovoc-serv on page 326
`tcp-udp-server`	See http-proxy tcp-udp-server on page 328
`upstream-group`	See http-proxy upstream-group on page 329

Command Mode

Privileged User

http-proxy debug-level

This command configures the debug level for the HTTP proxy application.

Syntax

```
(config-network)# http-proxy
(http-proxy)# debug-level {alert|critical|emergency|error|info|no-debug|notice|warning}
```

Command Mode

Privileged User

Note

To disable debugging, use the no-debug option.

Example

This example configures the debug level to warning:

```
(config-network)# http-proxy
(http-proxy)# debug-level warning
```

http-proxy directive-sets

This command configures the HTTP Directive Sets table, which lets you define directive sets.

Syntax

```
(config-network)# http-proxy
(http-proxy)# directive-sets <Index>
(directive-sets-<Index>)#
```

Command	Description
Index	Defines the table row index.
`directives`	Defines directives. Once run, use the command directive to define the directive.
`set-description`	Defines a brief description for the HTTP Directive Set.
`set-name`	Defines a descriptive name, which is used when associating the row in other tables.

Command Mode

Privileged User

Example

This example configures an HTTP Directive Set called "ITSP-A" and configures a directive for it:

```
(config-network)# http-proxy
(http-proxy)# directive-sets 0
(directive-sets-0)# set-name ITSP-A
(directive-sets-0)# directives 0
(directives-0/0)# directive limit_rate 0;
```

http-proxy dns-primary-server

This command configures a primary DNS server for the HTTP Proxy.

Syntax

```
(config-network)# http-proxy
(http-proxy)# dns-primary-server <IP Address>
```

Command Mode

Privileged User

Example

This example configures a primary DNS server address of 100.1.10.2:

```
(config-network)# http-proxy
(http-proxy)# dns-primary-server 100.1.10.2
```

http-proxy dns-secondary-server

This command configures a secondary DNS server for the HTTP Proxy.

Syntax

```
(config-network)# http-proxy
(http-proxy)# dns-secondary-server <IP Address>
```

Command Mode

Privileged User

Example

This example configures a secondary DNS server address of 100.1.10.4:

```
(config-network)# http-proxy
(http-proxy)# dns-secondary-server 100.1.10.4
```

http-proxy-global-address

This command configures a public IP address for the device's NGINX server, which is used for the HTTP Proxy. This is used when the device is located behind NAT.

Syntax

```
(config-network)# http-proxy
(http-proxy)# http-proxy-global-address <IP Address>
```

Command Mode

Privileged User

Example

This example configures a public address of 89.50.10.4:

```
(config-network)# http-proxy
(http-proxy)# http-proxy-global-address 89.50.10.4
```

http-proxy http-proxy-app

This command enables the HTTP Proxy application.

Syntax

```
(config-network)# http-proxy
(http-proxy)# http-proxy-app {off|on}
```

Command Mode

Privileged User

Example

This example enables the HTTP Proxy application:

```
(config-network)# http-proxy
(http-proxy)# http-proxy-app on
```

http-proxy http-server

This command configures the HTTP Proxy Servers table, which lets you define HTTP proxy servers.

Syntax

```
(config-network)# http-proxy
(http-proxy)# http-server <Index>
(http-server-<Index>)#
```

Command	Description
Index	Defines the table row index.
`bind-to-device`	Enables the NGINX to bind the HTTP Proxy interface to a specific device network interface.
`directive-set`	Assigns a Directive Set.
`domain-name`	Defines a domain name (FQDN).
`http-port`	Defines the HTTP listening port, which is the local port for incoming packets for the HTTP service.
`https-port`	Defines the HTTPS listening port, which is the local port for incoming packets for the HTTP service.
`listen-interface`	Assigns an IP Interface from the IP Interfaces table to the HTTP Proxy service.
`location`	Configures HTTP locations (see location on the next page).
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`tls-context`	Assigns a TLS Context (TLS certificate) from the TLS Contexts table.
`verify-client-cert {disable|enable}`	Enables the verification of the client TLS certificate,

Command Mode

Privileged User

Example

This example configures an HTTP proxy server:

```
(config-network)# http-proxy
(http-proxy)# http-server 0
(http-server-0)# name ITSP-A
(http-server-0)# listen-interface Voice
(http-server-0)# http-port 5999
```

location

This command configures the HTTP Locations table, which lets you define HTTP locations per HTTP proxy servers.

Syntax

```
(config-network)# http-proxy
(http-proxy)# http-server <Index>
(http-server-<Index>)# locations <Index>
(location-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`cache {disable|enable}`	Enables the caching of files in this location.
`directive-set`	Assigns an NGINX directive set for the HTTP location.
`outbound-intfc`	Assigns a local, IP network interface for sending requests to the Upstream Group.
`tls-context`	Assigns a TLS Context for the TLS connection with the HTTP location.
`upstream-group`	Assigns a group of servers (Upstream

Command	Description
	Group) to handle the HTTP requests.
`upstream-path`	Defines a path to prepend to the URL before sending the request to the Upstream Group.
`upstream-scheme {HTTP| HTTPS}`	Defines the protocol for sending requests to the Upstream Group.
`url-pattern`	Defines the URL pattern.
`url-pattern-type {case-insensitive-regex|exact|prefix|prefix-ignore-regex|regex}`	Defines the type of URL pattern used for configuring the url-pattern parameter.
`verify-cert {disable|enable}`	Enables TLS certificate verification when the connection with the location is based on HTTPS.

Command Mode

Privileged User

Example

This example configures an HTTP location for an HTTP proxy server:

```
(http-proxy)# http-server 0
(http-server-0)# location 0
(location-0/0)# outbound-intfc Voice
(location-0/0)# upstream-group ITSP-UP
```

http-proxy ovoc-serv

This command configures the OVOC Services table, which lets you define an OVOC service.

Syntax

```
(config-network)# http-proxy
(http-proxy)# ovoc-serv <Index>
(ovoc-serv-<Index>)#
```

Command	Description
Index	Defines the table row index.
`device-interface-verify-cert {disable|enable}`	Enables the verification of the TLS certificate that is used in the incoming client connection request.
`device-login-interface`	Assigns an IP network interface (local, listening HTTP interface:port) for communication with the client.
`device-login-port`	Defines the login port of the requesting client.
`device-login-tls-context`	Assigns a TLS Context (TLS certificate) for the interface with the requesting client.
`device-scheme {http|https}`	Defines the protocol for communication with the requesting client.
`ovoc-interface`	Assigns an IP network interface (local, listening HTTP interface:port) for communication with OVOC.
`ovoc-interface-tls-context`	Assigns a TLS Context (TLS certificate) for the OVOC listening interface.
`ovoc-port`	Defines the listening port for the OVOC interface.
`ovoc-scheme {http|https}`	Defines the security scheme for the connection with OVOC.
`ovoc-verify-cert {disable|enable}`	Enables the verification of the TLS certificate that is used in the incoming connection request from OVOC.
`primary-server`	Defines the address of the primary OVOC server.
`service-name`	Defines a descriptive name, which is used when associating the row in other tables.

Command Mode

Privileged User

Example

This example configures an OVOC service with 222.1.5.6:

```
(config-network)# http-proxy
(http-proxy)# ovoc-serv 0
(ovoc-serv-0)# service-name OVOC-1
(ovoc-serv-0)# device-login-interface Voice
(ovoc-serv-0)# device-login-port 6011
(ovoc-serv-0)# ovoc-interface Voice
(ovoc-serv-0)# ovoc-port 6021
(ovoc-serv-0)# primary-server 222.1.5.6
```

http-proxy tcp-udp-server

This command configures the TCP/UDP Proxy Servers table, which lets you define TCP/UDP proxy servers.

Syntax

```
(config-network)# http-proxy
(http-proxy)# tcp-udp-server <Index>
(tcp-udp-server-<Index>)#
```

Command	Description
Index	Defines the table row index.
`directive-set`	Assigns an NGINX Directive Set for the HTTP service.
`listen-interface`	Assigns a local IP network interface for the listening (source) interface for communication with the TCP-UDP proxy server.
`listen-tls-context`	Assigns a TLS Context (TLS certificate) for the listening side.
`listen-use-ssl {disable|enable}`	Enables SSL on the listening side (i.e., listening to incoming connection requests).
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`outbound-interface`	Assigns a local, IP network interface for communicating with the Upstream Group.
`tcp-port`	Defines the TCP port of the listening interface.
`udp-port`	Defines the TCP port of the listening interface.

Command	Description
`upstream-group`	Assigns a group of servers (Upstream Group) to which to forward connection requests.
`upstream-tls-context`	Assigns a TLS Context for the TLS connection with the HTTP location.
`upstream-use-ssl {disable|enable}`	Enables SSL for securing connection requests with the Upstream Group.
`upstream-verify-cert {disable|enable}`	Enables TLS certificate verification of the Upstream Host on outgoing connection requests to the Upstream Group, when the connection is SSL.

Command Mode

Privileged User

Example

This example configures a TCP/UDP proxy server:

```
(config-network)# http-proxy
(http-proxy)# tcp-udp-server 0
(tcp-udp-server-0)# name TCP-Proxy
(tcp-udp-server-0)# listen-interface Voice
(tcp-udp-server-0)# tcp-port 5060
(tcp-udp-server-0)# outbound-interface Voice
(tcp-udp-server-0)# upstream-group TCP-UP
```

http-proxy upstream-group

This command configures the Upstream Groups table, which lets you define Upstream Groups.

Syntax

```
(config-network)# http-proxy
(http-proxy)# upstream-group <Index>
(upstream-group-<Index>)#
```

Command	Description
Index	Defines the table row index.
`load-balancing-mode {ip-hash|least-connections|round-robin}`	Defines the load-balancing of traffic method for the hosts belonging to the Upstream Group.
`max-connections`	Defines the maximum number of simultaneous active connections to the proxied upstream server.
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`protocol {HTTP\HTTPS|TCP\UDP}`	Defines the protocol.
`upstream-host`	Defines Upstream Hosts, which are hosts belonging to the Upstream Group (see http-proxy upstream-host below).

Command Mode

Privileged User

Example

This example configures an Upstream Group called Prov-Server:

```
(config-network)# http-proxy
(http-proxy)# upstream-group 0
(upstream-group-0)# name Prov-Server
```

http-proxy upstream-host

This command configures the Upstream Hosts table, which lets you define Upstream Hosts per Upstream Groups.

Syntax

```
(config-network)# http-proxy
(http-proxy)# upstream-group <Index>
(upstream-group-<Index>)# upstream-host <Index>
(upstream-host-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`backup {disable|enable}`	Enables the host to serve as a backup host.
`host`	Defines the address of the host as an FQDN or IP address (in dotted-decimal notation).
`port`	Defines the port number.
`weight`	Defines the weight for the load balancer.

Command Mode

Privileged User

Example

This example configures an Upstream Host for an Upstream Group:

```
(config-network)# http-proxy
(http-proxy)# upstream-group 0
(upstream-group-0)# upstream-host 0
(upstream-host-0/0)# host 10.6.7.8
```

72 interface

This command configures network interfaces and includes the following sub-commands:

- network-if (see interface network-if below)
- osn (see interface osn on page 334)

interface network-if

This command configures the IP Interfaces table, which lets you define local IP network interfaces.

Syntax

```
(config-network)# interface network-if <Index>
(network-if-<Index>)#
```

Command	Description
Index	Defines the table row index.
`application-type {cluster-media-control|control|maintenance|media|media-control|oamp|oamp-control|oamp-media|oamp-media-control}`	Defines the applications allowed on the IP interface.
`gateway`	Defines the IPv4/IPv6 address of the default gateway.
`ip-address`	Defines the IPv4/IPv6address in dotted-decimal notation of the network interface.
`mode {ipv4-dhcp|ipv4-manual| ipv6-dhcp| ipv6-manual| ipv6-manual-prefix| ipv6-stateless}`	Defines the method that the interface uses to acquire its IP address.
`name`	Configures a name for the network interface.
`overwrite-dynamic-dns-servers {disable|enable}`	Enables the device to use the DNS addresses

Command	Description
	obtained through DHCP for the 'Primary DNS' and 'Secondary DNS' parameters when dynamic IPv6 addressing is used.
`prefix-length`	Defines the prefix length of the IP address.
`primary-dns`	Defines the primary DNS server's IP address (in dotted-decimal notation), which is used for translating domain names into IP addresses for the interface.
`secondary-dns`	Defines the secondary DNS server's IP address (in dotted-decimal notation), which is used for translating domain names into IP addresses for the interface.
`underlying-dev`	Assigns an Ethernet Device (see network-dev on page 341) to the network interface.

Command Mode

Privileged User

Example

This example configures the OAMP, Media and Control network interface:

```
(config-network)# interface network-if 0
(network-if-0)# application-type oamp-media-control
(network-if-0)# mode ipv4-manual
(network-if-0)# ip-address 10.15.7.96
```

```
(network-if-0)# prefix-length 16
(network-if-0)# gateway 10.15.0.1
(network-if-0)# underlying-dev vlan1
```

interface osn

This command configures the Open Solutions Network (OSN) interface.

Syntax

```
(config-network)# interface osn
(conf-net-if-OSN)#
```

Command	Description
`native-vlan`	Defines the OSN Native VLAN ID. When set to 0 (default), the OSN uses the device's OAMP VLAN ID. When set to any other value, it specifies a VLAN ID configured in the Ethernet Devices table and which is assigned to a Media and/or Control application in the IP Interfaces table.
`shutdown`	Disables the Ethernet port of the internal switch that interfaces between the Gateway/SBC and OSN.

Command Mode

Privileged User

Example

This example configures the VLAN ID for the OSN:

```
(config-network)# interface osn
(conf-net-if-OSN)# native-vlan 1
```

73 mtc

This command configures the Media Cluster feature.

Syntax

```
(config-network)# mtc
```

Command	Description
`entity`	See entity below
`lock-mt`	See lock-mt on the next page
`reset-mt`	See reset-mt on the next page
`settings`	See settings on page 337
`unlock-mt`	See unlock-mt on page 338

entity

This command configures the Media Components table, which lets you define Media Components (MC) for the Media Cluster feature.

Syntax

```
(config-network)# mtc entity <Index>
(entity-<Index>)#
```

Command	Description
Index	Defines the table row index.
`interface`	Defines the Cluster interface of the Media Component.
`name`	Defines a name for the Media Component.
`oamp-ip-address`	Defines the IP address of the Media Component's OAMP interface.

Command Mode

Privileged User

Example

This example configures an MC:

```
(config-network)# mtc entity 0
(entity-0)# name MC-1
(entity-0)# oamp-ip-address 192.60.1.2
(entity-0)# interface MC-1-Cluster
```

lock-mt

This command locks a Media Component (MC) that is configured for the Media Cluster feature.

Syntax

```
(config-network)# mtc lock-mt <OAMP IP address of MC>
```

Command Mode

Privileged User

Example

This example locks the MC whose OAMP address is 192.60.1.2:

```
(config-network)# mtc lock-mt 192.60.1.2
```

reset-mt

This command restarts a Media Component (MC) that is configured for the Media Cluster feature.

Syntax

```
(config-network)# mtc reset-mt <OAMP IP address of MC>
```

Command Mode

Privileged User

Example

This example restarts the MC whose OAMP address is 192.60.1.2:

```
(config-network)# mtc reset-mt 192.60.1.2
```

settings

This command configures various Media Cluster settings.

Syntax

```
(config-network)# mtc settings
(mtc)#
```

Command	Description
`cluster-manager-ip-address`	Defines the IP address of the Cluster Manager.
`cluster-network-max-bandwidth`	Defines the maximum bandwidth allowed on each Cluster interface.
`graceful-timeout`	Defines a "grace" period (graceful timeout) before an action (e.g., lock, unlock, and restart) is done on an MC by the Cluster Manager.
`mc-profile`	Defines the operational mode (transcoding or no transcoding) of the Mediant CE SBC's Media Component (MC).
`redundancy-mode {best-effort|ha-mode}`	Defines the Cluster redundancy mode, which provides load-sharing and redundancy (in case of failure) between Media Components.
`sbc-cluster-mode {default|disabled|media-cluster|media-transcoding-cluster-(mtc)}`	Enables the specific Cluster feature (Media Cluster or Media Transcoding Cluster).
`sbc-device-role {default|media-component-(mc)|sbc-or-signaling-component-(sc)}`	Defines the role of the device in the Cluster – Signaling or Media Component.

Command Mode

Privileged User

Example

This example enables the Media Cluster feature:

```
(config-network)# mtc settings
(mtc)# sbc-cluster-mode media-cluster
```

unlock-mt

This command unlocks a locked Media Component (MC) that is configured for the Media Cluster feature.

Syntax

```
(config-network)# mtc unlock-mt <OAMP IP address of MC>
```

Command Mode

Privileged User

Example

This example unlocks the MC whose OAMP address is 192.60.1.2:

```
(config-network)# mtc unlock-mt 192.60.1.2
```

74 nat-translation

This command configures the NAT Translation table, which lets you define network address translation (NAT) rules for translating source IP addresses per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses (global - public) when the device is located behind NAT.

Syntax

```
(config-network)# nat-translation <Index>
(nat-translation-<Index>)#
```

Command	Description
Index	Defines the table row index.
`remote-interface-name`	Assigns a media IP interface (listed in the Remote Media Interface table) of the remote Media Component(s) operating under the Cluster Manager (Signaling Component). **Note:** This command is applicable only to Mediant CE SBC.
`source-ip-address`	Defines the source IP address (IPv4 or IPv6). Outgoing packets sent from this IP address are NAT'ed. **Note:** The parameter is applicable only to Mediant VE in HA mode that is deployed on the Azure cloud platform.
`src-end-port`	Defines the optional ending port range (0-65535) of the IP interface, used as matching criteria for the NAT rule.
`src-interface-name`	Assigns an IP network interface (configured in the IP Interfaces table) to the rule. Outgoing packets sent from the specified network interface are NAT'ed.
`src-start-port`	Defines the optional starting port range (0-65535) of the IP interface, used as matching criteria for the NAT rule.
`tar-ip-mode`	Defines the NAT IP address mode when the device is deployed in an Amazon Web Services (AWS) cloud-computing environment.
`target-end-port`	Defines the optional ending port range (0-65535) of the global address.
`target-ip-address`	Defines the global (public) IP address.

Command	Description
`target-start-port`	Defines the optional starting port range (0-65535) of the global address.

Command Mode

Privileged User

Example

This example configures a NATed IP address (202.1.1.1) for all traffic sent from IP network interface "voice":

```
# configure network
(config-network)# nat-translation 0
(nat-translation-0)# src-interface-name voice
(nat-translation-0)# target-ip-address 202.1.1.1
```

75 network-dev

This command configures the Ethernet Devices table, which lets you define Ethernet Devices. An Ethernet Device represents a Layer-2 bridging device and is assigned a unique VLAN ID and an Ethernet Group (Ethernet port group).

Syntax

```
(config-network)# network-dev <Index>
(network-dev-<Index>)#
```

Command	Description
Index	Defines the table row index.
mtu	Defines the Maximum Transmission Unit (MTU) size.
name	Configures a name for the Ethernet Device.
tagging {tagged|untagged}	Configures VLAN tagging for the Ethernet Device.
underlying-if	Assigns an Ethernet Group to the Ethernet Device.
vlan-id	Configures a VLAN ID for the Ethernet Device.

Command Mode

Privileged User

Related Commands

custom-mtu: Customizes the MTU (applicable only to Mediant Software deployed on Azure or AWS)

Example

This example configures an Ethernet Device with VLAN ID 2 for Ethernet Group 0 and untagged:

```
(config-network)# network-dev
(network-dev-0)# name VLAN 2
(network-dev-0)# vlan-id 2
(network-dev-0)# underlying-if 0
(network-dev-0)# tagging untagged
```

76 network-settings

This command configures the network settings.

Syntax

```
(config-network)# network-settings
(network-settings)#
```

Command	Description
`aws-ec2-endpoint`	Defines the Amazon Web Services (AWS) EC2 endpoint name: - Empty (default): The device automatically generates the AWS EC2 API endpoint based on the region in which it is deployed (e.g., "ec2.eu-central-1.amazonaws.com"). **Note:** High-Availability (HA) deployments in AWS environments use AWS EC2 API to implement IP failover. If two SBC instances are deployed in separate availability zones within the same region, the same AWS EC2 API endpoint will be used for both availability zones. In such a scenario, all traffic towards the AWS EC2 API endpoint will flow through the first availability zone, even for virtual machines deployed in the second availability zone. - Custom EC2 API endpoint FQDN (e.g., "vpce-0123456789.ec2.eu-central-1.vpce.amazonaws.com"). - Custom EC2 API endpoint FQDN followed by its IP address (e.g., "ec2.eu-central-1.amazonaws.com:10.1.2.3"). **Note:** The parameter is applicable only to Mediant VE/CE in AWS environments.
`dns-cache {disable|enable}`	Enables the device to cache (store) DNS-resolved IP addresses of the last successful DNS query of Proxy Sets configured with an FQDN.
`ethernet-redundancy {auto|disable|enable}`	Enables Ethernet port redundancy, configured in the Ethernet Groups table.

Command	Description
	Note: The parameter is applicable only to Mediant 90xx and Mediant Software.
`hostname`	Defines the device's hostname.
`icmp-disable-redirect {0|1}`	Enables sending and receiving of ICMP Redirect messages.
`icmp-disable-unreachable {0|1}`	Enables sending of ICMP Unreachable messages.
`interface-status-check {off|on}`	When the device is deployed in Azure cloud, it may experience intermittent problems in communication with virtual hosts that may cause the virtual network interface (NIC) to "freeze". To overcome this issue, the device can periodically check the status of all network interfaces to detect if this condition exists and mitigate it by performing a maintenance reboot. This feature is applicable only to Mediant VE/CE deployed on Azure cloud. **Note:** This feature is applicable only to Mediant VE/CE deployed on Azure cloud.
`interface-status-check-period`	Defines the period (in seconds) between each check of virtual network interface. **Note:** This feature is applicable only to Mediant VE/CE deployed on Azure cloud.
`interface-status-check-retries`	Defines the number of retries (ARP requests) if no change in the virtual network interface. **Note:** This feature is applicable only to Mediant VE/CE deployed on Azure cloud.
`limit-incoming-icmp-echo-requests`	Defines if the device limits the number of allowed incoming ICMP echo requests. **Note:** The parameter is applicable only to Mediant 90xx and Mediant Software.
`osn-internal-vlan {off|on}`	Enables a single management platform when the device is deployed as a Survivable Branch Appliance (SBA) in a Microsoft Skype for Business environment. It allows configuration and monitoring of the Gateway/SBC device through

Command	Description
	the SBA Management Interface.

Command Mode

Privileged User

Example

This example sending and receiving of ICMP Redirect messages:

```
(config-network)# network-settings
(network-settings)# icmp-disable-redirect 1
```

77 ovoc-tunnel-settings

This command configures WebSocket tunnel connection settings for communication between the device and OVOC.

Syntax

```
(config-network)# ovoc-tunnel-settings
(ovoc-tunnel-settings)#
```

Command	Description
`address`	Defines the address of the WebSocket tunnel server (OVOC).
`interface-name`	Defines the IP Interface for the WebSocket tunneling connection.
`password`	Defines the password for connecting the device to the WebSocket tunnel server (OVOC).
`path`	Defines the path of the WebSocket tunnel server.
`secured {off|on}`	Enables secured (HTTPS) WebSocket tunneling connection.
`username`	Defines the username for connecting the device to the WebSocket tunnel server (OVOC).
`verify-server {off|on}`	Enables the device to verify the TLS certificate that is used in the incoming WebSocket tunneling connection request from OVOC.

Command Mode

Privileged User

Example

This example configures the WebSocket server's address to 200.1.10.20:

```
(config-network)#  ovoc-tunnel-settings
(ovoc-tunnel-settings)# address 200.1.10.20
```

78 physical-port

This command configures the Physical Ports table, which lets you define the device's Ethernet ports.

Syntax

```
(config-network)# physical-port <Index>
(physical-port-<Index>)#
```

Command	Description
Index	Defines the table row index.
`port-description`	Configures a textual description of the port.
`speed-duplex {1000baset-full-duplex|1000baset-half-duplex|100baset-full-duplex|100baset-half-duplex|10baset-full-duplex|10baset-half-duplex|auto-negotiation}`	Defines the speed and duplex mode of the port.

Command Mode

Privileged User

Example

This example configures port 0 to auto-negotiation:

```
(config-network)# physical-port 0
(physical-port-0)# speed-duplex auto-negotiation
```

79 qos

This command configures Quality of Service (QoS) and includes the following subcommands:

- application-mapping (see qos vlan-mapping below)
- vlan-mapping (see qos application-mapping below)

qos vlan-mapping

This command configures the QoS Mapping table, which lets you define DiffServ-to-VLAN priority mapping (IEEE 802.1p) for Layer 3 and Layer-2 QoS.

Syntax

```
(config-network)# qos vlan-mapping <Index>
(vlan-mapping-<Index>)#
```

Command	Description
Index	Defines the table row index.
`diff-serv {0-63}`	Defines the DiffServ value.
`vlan-priority {0-7}`	Defines the VLAN priority level.

Command Mode

Privileged User

Example

This example maps DiffServ 60 to VLAN Priority (Class of Service) level 0:

```
(config-network)# qos vlan-mapping 0
(vlan-mapping-0)# diff-serv 60
(vlan-mapping-0)# vlan-priority 0
```

qos application-mapping

This command configures the QoS Settings table, which lets you define Layer-3 Class-of-Service QoS.

Syntax

```
(config-network)# qos application-mapping
(app-map)#
```

Command	Description
`bronze-qos {0-63}`	Defines the DiffServ value for the Bronze CoS content (OAMP applications).
`control-qos {0-63}`	Defines the DiffServ value for Premium Control CoS content (Call Control applications).
`gold-qos {0-63}`	Defines the DiffServ value for the Gold CoS content (Streaming applications).
`media-qos {0-63}`	Defines the DiffServ value for Premium Media CoS content.

Command Mode

Privileged User

Example

This example maps DiffServ 60 to VLAN Priority (Class of Service) level 0:

```
(config-network)# qos application-mapping
(app-map)# gold-qos 63
```

80 sctp

This command configures Stream Control Transmission Protocol (SCTP) settings.

Syntax

```
(config-network)# sctp
(sctp)#
```

Command	Description
`heartbeat-interval`	Defines the SCTP heartbeat Interval (in seconds), where a heartbeat is sent to an idle destination to monitor reachability every time the interval expires.
`initial-rto`	Defines the initial retransmission timeout (RTO) in msec for all the destination addresses of the peer.
`max-association-retransmit`	Defines the maximum number of consecutive association retransmissions before the peer is considered unreachable and the association is closed.
`max-data-chunks-before-sack`	Defines after how many received packets is Selective Acknowledgement (SACK) sent.
`max-data-tx-burst`	Defines the maximum number of DATA chunks (packets) that can be transmitted at one time (in a burst).
`max-path-retransmit`	Defines the maximum number of path retransmissions per remote transport address before it is considered as inactive.
`maximum-rto`	Defines the maximum retransmission timeout (RTO) in msec for all the destination addresses of the peer.
`minimum-rto`	Defines the minimum retransmission timeout (RTO) in msec for all the destination addresses of the peer.
`timeout-before-sack`	Defines the timeout (msec) since the packet was received after which SACK is sent (i.e., delayed SACK).

Command Mode

Privileged User

Note

SCTP is applicable only to Mediant 90xx and Mediant Software.

Related Commands

```
show sctp
```

Example

This example configures the SCTP heartbeat interval to 60 seconds:

```
(config-network)# sctp
(sctp)# heartbeat-interval 60
```

81 security-settings

This command configures various TLS certificate security settings.

Syntax

```
(config-network)# security-settings
(network-security)#
```

Command	Description
`encrypt-private-key-files {off|on}`	Enables the device to store all TLS private keys encrypted.
`encryption-key {assign|clear|display|generate}`	Defines password obfuscation using an encryption key (AES-256 algorithm with a 16-bit random CFB initialization vector). ■ `assign <key>`: Manually defines the key. ■ `clear`: Deletes the key. ■ `display`: Displays the key if configured, but only partially. The output of this command displays only the first four characters followed by three asterisks (e.g., %3 [-***). ■ `generate`: Device generates the key instead of manually.
`peer-hostname-verification-mode {0|1|2}`	Enables the device to verify the Subject Name of a TLS certificate received from SIP entities for authentication and establishing TLS connections: ■ 0 = Disable (default) ■ 1 = Verify Subject Name only when acting as a client for the TLS connection. ■ 2 = Verify Subject Name when acting as a server or client for the TLS connection.

Command	Description
`sips-require-client-certificate {off|on}`	Defines the device's mode of operation regarding mutual authentication and certificate verification for TLS connections. ■ off = Disable ✓ Device acts as a client: Verification of the server’s certificate depends on the VerifyServerCertificate parameter. ✓ Device acts as a server: The device does not request the client certificate. ■ on = Enable ✓ Device acts as a client: Verification of the server certificate is required to establish the TLS connection. ✓ Device acts as a server: The device requires the receipt and verification of the client certificate to establish the TLS connection. **Note:** For the parameter to take effect, a device reset is required.
`tls-expiry-check-period`	Defines the periodic interval (in days) for checking the TLS server certificate expiry date.
`tls-expiry-check-start`	Defines the number of days before the installed TLS server certificate is to expire when the device sends an SNMP trap event to notify of this.
`fips140mode {off|on}`	Enables FIPS 140-2 conformance mode for TLS. **Note:** Applicable only to specific products.

Command	Description
`tls-re-hndshk-int`	Defines the time interval (in minutes) between TLS Re-Handshakes initiated by the device.
`tls-rmt-subs-name`	Defines the Subject Name that is compared with the name defined in the remote side certificate when establishing TLS connections.
`tls-vrfy-srvr-cert {off|on}`	Enables the device, when acting as a client for TLS connections, to verify the Server certificate. The certificate is verified with the Root CA information.

Command Mode

Privileged User

Example

This example enables the device to verify the Server certificate with the Root CA information:

```
(config-network)# security-settings
(network-security)# tls-vrfy-srvr-cert on
```

82 sni-to-tls-mapping

This command configures the SNI To TLS Mapping table, which lets you define rules for mapping the 'server_name' in "client hello" messages to TLS Contexts (configured in the TLS Contexts table).

Syntax

```
(config-network)# sni-to-tls-mapping <Index>
(sni-to-tls-mapping-<Index>)#
```

Command	Description
Index	Defines the table row index.
`host-name`	Defines the 'server_name' in the "client hello" message (case-insensitive).
`tls-context`	Assigns a TLS Context, listed in the TLS Contexts table, to this rule (case-sensitive).

Command Mode

Privileged User

Example

This example configures an SNI-to-TLS Context mapping rule that maps "client hello" messages whose 'server_name' extension is "My-Server", to TLS Context "My TLS":

```
(config-network)# sni-to-tls-mapping 0
(sni-to-tls-mapping-0)# host-name 'My-Server'
(sni-to-tls-mapping-0)# tls-context 'My TLS'
```

83 static

This command configures the Static Routes table, which lets you define static IP routing rules.

Syntax

```
(config-network)# static <Index>
(static-<Index>)#
```

Command	Description
Index	Defines the table row index.
description	Configures a name for the rule.
destination	Defines the IP address of the destination host/network.
device-name	Associates an IP network interface through which the static route's Gateway is reached. The association is done by assigning the parameter the same Ethernet Device that is assigned to the IP network interface in the IP Interfaces table.
gateway	Defines the IP address of the Gateway (next hop) used for traffic destined to the subnet/host defined in 'destination' / 'prefix-length'.
prefix-length	Defines the Classless Inter-Domain Routing (CIDR)-style representation of a dotted-decimal subnet notation of the destination host/network.

Command Mode

Privileged User

Example

This example configures a static routing rule to specify the gateway (10.15.7.22) in order to reach 10.1.1.10:

```
(config-network)# static 0
(static-0)# destination 10.1.1.0
(static-0)# prefix-length 24
```

```
(static-0)# device-name vlan1
(static-0)# gateway 10.15.7.22
```

84 static-arp-table

This command configures the Static ARP table, which lets you define static Address Resolution Protocol (ARP) entries for mapping IP addresses to Media Access Control (MAC) addresses.

Syntax

```
(config-network)# static-arp-table <Index>
(static-arp-table-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dest-addr`	Defines the IP address of the destination host / network.
`eth-dev`	Assigns an Ethernet Device from the Ethernet Devices table, which is a VLAN that is associated with a specific IP interface in the IP Interfaces table.
`mac-addr`	Defines the MAC address that is mapped to the IP address specified by `dest-addr`.

Command Mode

Privileged User

Example

This example configures a static ARP rule that maps IP address 10.15.7.22 to MAC address 00-B0-D0-63-C2-26:

```
(config-network)# static-arp-table 0
(static-arp-table-0)# dest-addr 10.15.7.22
(static-arp-table-0)# mac-addr 00-B0-D0-63-C2-26
(static-arp-table-0)# eth-dev vlan1
```

85 tls

This command configures the TLS Contexts table, which lets you define TLS certificates, referred to as TLS Contexts.

Syntax

```
(config-network)# tls <Index>
(tls-<Index>)#
```

Command	Description
Index	Defines the table row index.
`certificate`	Certification actions - see certificate on page 361.
`ciphers`	Displays ciphers.
`ciphers-client`	Defines the supported cipher suite for TLS clients.
`ciphers-client-tls13`	Defines the supported cipher suite for TLS 1.3 clients.
`ciphers-server`	Defines the supported cipher suite for the TLS server (in OpenSSL cipher list format).
`ciphers-server-tls13`	Defines the supported cipher suite for the TLS 1.3 server (in OpenSSL cipher list format).
`dh-key-size {2048|3072}`	Defines the Diffie-Hellman (DH) key size (in bits).

Command	Description
	Note: ■ For supported key sizes, refer to the *User's Manual*. ■ 1024 is not recommended (it's not displayed as an optional value in the CLI, but it can be configured).
`dtls-version {dtls-v1.0| dtls-v1.2| unlimited}`	Defines the Datagram Transport Layer Security (DTLS) version, which is used to negotiate keys for WebRTC calls.
`key-exchange-groups`	Defines the groups that are supported for key exchange, ordered from most preferred to least preferred.
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`ocsp-default-response {allow|reject}`	Defines if the device allows or rejects peer certificates if it cannot connect to the OCSP server.
`ocsp-interface`	Assigns an IP Interface for communication with the OCSP server.
`ocsp-port`	Defines the OCSP

Command	Description
	server's TCP port number.
`ocsp-server {disable|enable}`	Enables or disables certificate checking using OCSP.
`ocsp-server-primary`	Defines the IP address (in dotted-decimal notation) of the primary OCSP server.
`ocsp-server-secondary`	Defines the IP address (in dotted-decimal notation) of the secondary OCSP server (optional).
`private-key {delete|generate|import}`	Private key actions - see private-key on page 364.
`public-key display`	Displays the public key of the certificate.
`require-strict-cert {off|on}`	Enables the validation of the extensions (keyUsage and extentedKeyUsage) of peer certificates.
`tls-renegotiation {disable|enable}`	Enables multiple TLS renegotiations (handshakes) initiated by the client (peer) with the device.
`tls-version {tls-v1.0|tls-v1.0_1.1|tls-v1.0_1.1_1.2|tls-v1.0_1.1_1.2_1.3|tls-v1.0_1.2|tls-v1.1|tls-v1.1_1.2|tls-v1.1_1.2_1.3||tls-v1.2|tls-v1.2_1.3|tls-v1.3 |unlimited}`	Defines the supported SSL/TLS protocol version. Clients attempting to communicate with the device using a different TLS version

Command	Description
	are rejected.
`trusted-root {clear-and-import|default-ca-bundle|delete|detail|export|import|summary}`	Trusted root certificate actions - see trusted-root on page 365.

Command Mode

Privileged User

Example

This example configures a TLS Context with TLS Ver. 1.2:

```
(config-network)# tls 1
(tls-1)# name ITSP
(tls-1)# tls-version tls-v1.2
(tls-1)# activate
```

certificate

This subcommand lets you do various actions on currently installed TLS certificates and lets you create certificates.

Syntax

```
(config-network)# tls <Index>
(tls-<Index>)#  certificate  {create|current-installed}
```

Command	Description
Index	Defines the table row index.
`create`	Creates a certificate signing request and a new self-signed certificate.
`display`	Displays the X.509 fields configuration for CSR and new self signed certificates.
`self-signed`	Creates a self-signed certificate (by the device) with the current key.
`set-`	Defines or deletes the extended key usage X.509 field for CSR and new

Command	Description
`extended-key-usage {add|clear}`	self-signed certificates. The `add` option provides the following sub-commands to define the key (string) and optionally, to define the key as critical: `set-extended-key-usage add <String> [critical]`
`set-key-usage {add|clear}`	Defines or deletes the key usage X.509 field for CSR and new self-signed certificates. The `add` option provides the following sub-commands to define the key (string) and optionally, to define the key as critical: `set-extended-key-usage add <String> [critical]`
`set-authority-information-access-ocsp {add|clear}`	Defines or deletes the Authority Information Access (AIA) extension field for CSR and new self-signed certificates with the URL of the server where the client can check the validity of the device's certificate during the TLS handshake.
`set-signature-algorithm {sha-256|sha-512}`	Defines the signature algorithm for CSR and new self-signed certificates.
`set-subject {add|clear|copy}`	Defines, deletes or copies the certificate subject name for CSR and new self-signed certificates. The `add` option provides the following sub-commands to define the subject: `certificate create set-subject add {common-name|country|locality|org-unit|organization|state}`
`set-subject-alternative-name {add|clear}`	Defines or deletes the Subject Alternative Name (SAN) fields, which can be a DNS, e-mail, IP address or URI. The `add` option provides the following sub-commands to define the SAN fields: `certificate create set-subject-alternative-name add {dns|email|ip-addr|uri}`
`set-subject-key-identifier {add|clear}`	Defines or deletes the subject key identifier (SKI) X.509 field for CSR and new self-signed certificates. The `add` option provides the following sub-commands to define the SKI: `certificate create set-subject-key-identifier add {<HEX STRING>|hash-sha1|hash-sha1-60lsb}`

Command	Description
`signing-request`	Creates a certificate signing request with the current key, which needs to be sent to the CA. To view more of the output of the CSR text, press Enter (from "BEGIN CERTIFICATE REQUEST" to "END CERTIFICATE REQUEST"). To send the CSR to a remote server, type the URL with a CSR file name, and then press Enter (see **bold** text): (tls-1)# certificate create signing-request Certificate signing request: -----BEGIN CERTIFICATE REQUEST----- MIIDVjCCAb4CAQAwADCCAaIwDQYJKoZIhvcNAQEBBQ ADggGPADCCAYoCggGBAKyT 2ULFybbBtkT/zX+oiiMQO+86DLeFZ7eD+uZ35vrtrALaV0T2 V/m88NR9uULCsCVy 6L0ItCQ5pZ1DreGcKzdfgNmhNPCzUdoqkw/BeBBERMqIh KwnO2ucmeOu0qx/DUBm .... -----END CERTIFICATE REQUEST----- Send this request to your security administrator for signing, then upload the new signed certificate to the device. In order to copy the CSR to url, enter the url or press enter to quit: **tftp://10.11.2.2/my.csr** Sending file...
`current-installed`	Performs various actions on the currently installed TLS certificate.
`display`	Displays certificate information of currently installed certificate.
`export`	Exports the currently installed certificate in PEM format.
`import`	Imports a certificate in textual PEM format. **Note:** The imported certificate replaces the currently installed certificate.
`status`	Displays status of currently installed certificate (e.g., expiration day).

Command Mode

Privileged User

Example

This example displays the status of a currently installed TLS certificate (TLS Context 0):

```
(tls-0)# certificate current-installed statusSecurity context #0 - default
Certificate subject: /CN=ACL_5967925
Certificate issuer : /CN=ACL_5967925

Time to expiration : 5625 days

Key size: 2048 bits
Active sockets: 0
The currently-loaded private key matches this certificate..
```

private-key

This command lets you do various actions on private keys.

Syntax

```
(config-network)# tls <Index>
(tls-<Index>)# private-key
```

Command	Description
`delete`	Deletes the private key.
`generate ecdsa {256|384|521} password`	Generates an ECDSA private key based on private key size with an optional password (passphrase) to encrypt the private key file, and generates a self-signed certificate.
`generate rsa {2048|3072|4096} password`	Generates an RSA private key based on private key size with an optional password (passphrase) to encrypt the private key file, and generates a self-signed certificate.
`import {password|without-password}`	Imports a private key file, with an optional passphrase. Type the private key in the console.

Command Mode

Privileged User

Example

This example deletes a private key:

```
(config-network)# tls 0
(tls-0)# private-key delete
Private key deleted.
```

trusted-root

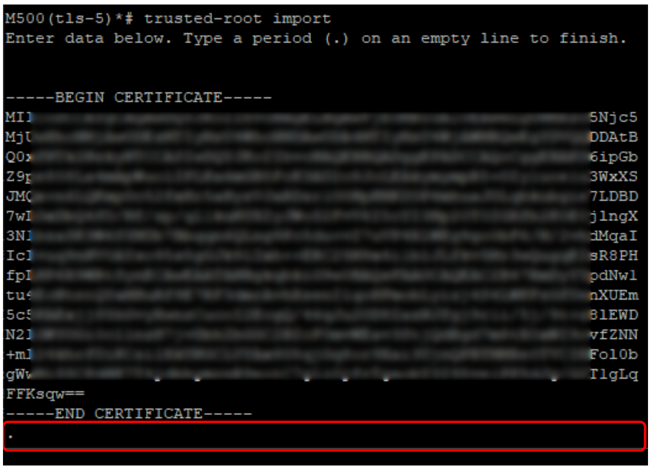
This subcommand lets you do various actions on the Trusted Root Certificate Store.

Syntax

```
(tls-<Index>)# trusted-root
```

Command	Description
clear-and-import	Deletes all trusted root certificates and imports new ones. Type the certificate directly in the console.
default-ca-bundle {disable|enable }	Enables the use of the default list of certificate authorities (CAs).
delete {<number>|all}	Deletes a specific trusted root certificates or all.
detail <number>	Displays the details of a specific trusted root certificate.
export	Displays the trusted root certificate in the console.
import	Imports a trusted root certificate. Type the certificate after the command. **Note:** When importing certificates into the trusted root CA store through CLI, make sure you add a blank line containing a period (.) after the 'END CERTIFICATE' line, as shown in the following example:

Command	Description

	
	`M500(tls-5)*# trusted-root import`
	`Enter data below. Type a period (.) on an empty line to finish.`
	`-----BEGIN CERTIFICATE-----`
	[redacted]
	`FFKsqw==`
	`-----END CERTIFICATE-----`
	`.`

`summary`	Displays a summary of the trusted root certificate.

Command Mode

Privileged User

Example

This example displays a summary of the root certificate:

```
(config-network)# tls 0
(tls-0)# trusted-root summary
1 trusted certificates.
Num Subject              Issuer          Expires
----------------------------------------------------------------
  1 ilync15-DC15-CA      ilync15-DC15-CA        11/01/2022
```

Part VI

VoIP-Level Commands

86 Introduction

This part describes the commands located on the voice-over-IP (VoIP) configuration level. The commands of this level are accessed by entering the following command at the root prompt:

```
# configure voip
(config-voip)#
```

This level includes the following commands:

Command	Description
`application`	See application on page 370
`coders-and-profiles`	See coders-and-profiles on page 439
`gateway`	See gateway on page 371
`ids`	See ids on page 467
`interface`	See interface on page 472
`ip-group`	See ip-group on page 482
`media`	See media on page 489
`message`	See message on page 505
`proxy-set`	See proxy-set on page 513
`qoe`	See qoe on page 517
`realm`	See realm on page 526
`remote-interface`	See remote-interface on page 531
`rtp-only sessions`	See rtp-only sessions on page 532
`sbc`	See sbc on page 535
`sip-definition`	See sip-definition on page 568
`sip-interface`	See sip-interface on page 598
`srd`	See srd on page 602

Command Mode

Privileged User

87 application

This command enables the SBC application.

Syntax

```
(config-voip)# application
(sip-application)#
```

Command	Description
`enable-sbc{off|on}`	Enables / disables the SBC application.

Command Mode

Privileged User

Example

This example shows how to enable the SBC application:

```
(config-voip)# application
(sip-application)# enable-sbc on
```

88 gateway

This command configures the gateway and includes the following subcommands:

- advanced (see advanced below)
- analog (see analog on the next page)
- digital (see digital on page 387)
- dtmf-supp-service (see dtmf-supp-service on page 398)
- manipulation (see manipulation on page 407)
- routing (see routing on page 424)
- trunk-group (see trunk-group on page 433)
- trunk-group-setting (see trunk-group-setting on page 434)
- voice-mail-setting (see voice-mail-setting on page 435)

advanced

This command configures advanced gateway parameters.

Syntax

```
(config-voip)# gateway advanced
(gw-settings)#
```

Command	Description
`enable-rai {off|on}`	Enables generation of an RAI (Resource Available Indication) alarm if the device's busy endpoints exceed a user-defined threshold.
`enforce-media-order {off|on}`	Enables the device to include all previously negotiated media lines ('m=') within the current session in the SDP offer-answer exchange (RFC 3264).
`forking-handling {parallel-handling|sequential-handling}`	Defines how the device handles the receipt of multiple SIP 18x forking responses for Tel-to-IP calls.
`forking-timeout`	Defines the timeout (in seconds) that is started after the first SIP 2xx response has

Command	Description
	been received for a User Agent when a Proxy server performs call forking (Proxy server forwards the INVITE to multiple SIP User Agents).
`reans-info-enbl {off|on}`	Enables the device to send a SIP INFO message with the On-Hook/Off-Hook parameter when the FXS phone goes on-hook during an ongoing call and then off-hook again, within the user-defined regret timeout.
`register-by-served-tg-status`	Defines if the device sends a registration request (SIP REGISTER) to a Serving IP Group (SIP registrar), based on the Trunk Group's status (in-service or out-of-service) for ISDN PRI and CAS.
`tel2ip-no-ans-timeout`	Defines the time (in seconds) that the device waits for a 200 OK response from the called party (IP side) after sending an INVITE message, for Tel-to-IP calls.
`time-b4-reordr-tn`	Defines the delay interval (in seconds) from when the device receives a SIP BYE message (i.e., remote party terminates call) until the device starts playing a reorder tone to the FXS phone.
`use-conn-sdpses-or-media {dont-care|session-only|media-only}`	Defines how the device displays the Connection ("c=") line in the SDP Offer/Answer model.

Command Mode

Privileged User

analog

This command configures analog parameters.

Syntax

```
(config-voip)# gateway analog
```

Command	Description
`authentication`	See authentication below
`automatic-dialing`	See automatic-dialing on the next page
`call-forward`	See call-forward on page 375
`call-waiting`	See call-waiting on page 376
`caller-display-info`	See caller-display-info on page 377
`enable-caller-id`	See enable-caller-id on page 378
`enable-did`	See enable-did on page 379
`fxo-setting`	See fxo-setting on page 380
`fxs-setting`	See fxs-setting on page 382
`keypad-features`	See keypad-features on page 383
`metering-tones`	See metering-tones on page 385
`reject-anonymous-calls`	See reject-anonymous-calls on page 385
`tone-index`	See tone-index on page 386

Command Mode

Privileged User

authentication

This command configures the Authentication table, which lets you define an authentication username and password per FXS and FXO port.

Syntax

```
(config-voip)# gateway analog authentication <Port>
(authentication-<Port>)#
```

Command	Description
port	Defines the port.

Command	Description
`password`	Defines the password for authenticating the port.
`user-name`	Defines the user name for authenticating the port.

Command Mode

Privileged User

Note

To view the port-module numbers and port type, enter the display command at the index prompt, for example:

```
(authentication-0)# display
```

Example

This example configures authentication credentials for a port:

```
(config-voip)# gateway analog authentication 0
(authentication-0)# password 1234
(authentication-0)# user-name JDoe
```

automatic-dialing

This command configures the Automatic Dialing table, which lets you define telephone numbers that are automatically dialed when FXS or FXO ports go off-hook.

Syntax

```
(config-voip)# gateway analog automatic-dialing <Index>
(automatic-dialing-<Index>)#
```

Command	Description
Index	Defines the table row index.
`auto-dial-status {disable|enable|hotline}`	Enables automatic dialing.
dst-number	Defines the destination telephone number to auto-

Command	Description
	matically dial.
hotline-dial-tone-duration	Defines the duration (in seconds) after which the destination phone number is automatically dialed.

Command Mode

Privileged User

Note

To view the port-module numbers and port type, enter the display command at the index prompt, for example:

```
(automatic-dialing-0)# display
```

Example

This example configures automatic dialing where the number dialed is 9764401:

```
(config-voip)# gateway analog automatic-dialing 0
(automatic-dialing-0)# auto-dial-status enable
(automatic-dialing-0)# dst-number 9764401
```

call-forward

This command configures the Call Forward table, which lets you define call forwarding per FXS or FXO port for IP-to-Tel calls.

Syntax

```
(config-voip)# gateway analog call-forward <Index>
(call-forward-<Index>)#
```

Command	Description
Index	Defines the table row index.
destination	Defines the telephone number or URI (<number>@<IP address>) to where the call is forwarded.

Command	Description
`no-reply-time`	If you have set type for this port to no-answer or on-busy-or-no-answer, then configure the number of seconds the device waits before forwarding the call to the specified phone number.
`type {deactivate|dont-disturb|no-answer|on-busy|on-busy-or-no-answer|unconditional}`	Defines the condition upon which the call is forwarded.

Command Mode

Privileged User

Note

To view the port-module numbers and port type, enter the display command at the index prompt, for example:

```
(call-forward-0)# display
```

Example

This example configures unconditional call forwarding to phone 9764410:

```
(config-voip)# gateway analog call-forward 0
(call-forward-0)# destination 9764410
(call-forward-0)# type unconditional
(call-forward-0)# activate
```

call-waiting

This command configures the Call Waiting table, which lets you enable call waiting per FXS port.

Syntax

```
(config-voip)# gateway analog call-waiting <Index>
(call-waiting-<Index>)#
```

Command	Description
Index	Defines the table row index.
`enable-call-waiting {disable|enable|not-configure}`	Enables call waiting for the port.

Command Mode

Privileged User

Note

To view the port-module numbers and port type, enter the display command at the index prompt, for example:

```
(call-waiting-0)# display
```

Example

This example enables call waiting:

```
(config-voip)# gateway call-waiting 0
(call-waiting-0)# enable-call-waiting enable
(call-waiting-0)# activate
```

caller-display-info

This command configures the Caller Display Information table, which lets you define caller identification strings (Caller ID) per FXS and FXO port.

Syntax

```
(config-voip)# gateway analog caller-display-info <Index>
(caller-display-info-<Index>)#
```

Command	Description
Index	Defines the table row index.
`display-string`	Defines the Caller ID string.

Command	Description
`presentation {allowed|restricted}`	Enables the sending of the caller ID string.

Command Mode

Privileged User

Note

To view the port-module numbers and port type, enter the display command at the index prompt, for example:

```
(caller-display-info-0)# display
```

Example

This example configures caller ID as "Joe Do":

```
(config-voip)# gateway caller-display-info 0
(caller-display-info-0)# display-string Joe Doe
(caller-display-info-0)# presentation allowed
(caller-display-info-0)# activate
```

enable-caller-id

This command configures the Caller ID Permissions table, which lets you enable Caller ID generation for FXS interfaces and detection for FXO interfaces, per port.

Syntax

```
(config-voip)# gateway analog enable-caller-id <Index>
(enable-caller-id-<Index>)#
```

Command	Description
Index	Defines the table row index.
`caller-id {disable|enable|not-configured}`	Enables Caller ID.

Command Mode

Privileged User

Note

To view the port-module numbers and port type, enter the display command at the index prompt, for example:

```
(enable-caller-id-0)# display
```

Example

This example enables caller ID:

```
(config-voip)# gateway enable-caller-id 0
(enable-caller-id-0)# caller-id enable
(enable-caller-id-0)# activate
```

enable-did

This command configures the Enable DID table, which lets you enable support for Japan NTT 'Modem' DID per FXS port.

Syntax

```
(config-voip)# gateway analog enable-did <Index>
(enable-did-<Index>)#
```

Command	Description
Index	Defines the FXS port.
`did {disable|enable|not-configured}`	Enables DID.

Command Mode

Privileged User

Note

- To view the port-module numbers and port type, enter the display command at the index prompt, for example: `(enable-did-0)# display`.
- To enable DID for all FXS ports, use the `enable-did` command as described in settings on page 578.

Example

This example enables Japan DID:

```
(config-voip)# gateway enable-did 0
(enable-did-0)# did enable
(enable-did-0)# activate
```

fxo-setting

This command configures various FXO parameters.

Syntax

```
(config-voip)# gateway analog fxo-setting
(gw-analog-fxo)#
```

Command	Description
`answer-supervision {disable|enable}`	Enables sending a SIP 200 OK when speech, fax or modem is detected.
`dialing-mode {one-stage|two-stages}`	Global parameter configuring the dialing mode for IP-to-Tel (FXO) calls.
`disc-on-bsy-tone-c {off|on}`	Global parameter enabling call disconnection when a busy tone is detected.
`disc-on-dial-tone {off|on}`	Enables the device to disconnect a call when it detects a dial tone from the PBX.
`fxo-autodial-play-bsytn {off|on}`	Defines if the device plays a busy / reorder tone to the PSTN side if a Tel-to-IP call is rejected by a SIP error response (4xx, 5xx or 6xx). If a SIP error response is received, the device seizes the line (off-hook), and then plays a busy / reorder tone to the PSTN side (for the duration defined by the parameter TimeForReorderTone).

Command	Description
`fxo-consult-call-transfer {off|on}`	Enables FXO consultative call transfers (initiated by the PSAP operator) for emergency (NG9-1-1) calls, based on the NENA i3 Standard for Next Generation 9-1-1 (NENA-STA-010.2-2016).
`fxo-dbl-ans {off|on}`	Enables FXO Duoble Answer.{@}all incoming TEL2IP call are refused.
`fxo-number-of-rings`	Defines the number of rings before the device's FXO interface answers a call by seizing the line.
`fxo-ring-timeout`	Defines the delay (in 100 msec) for generating INVITE after RING_START detection. The valid range is 0 to 50.
`fxo-seize-line {off|on}`	If not set, the FXO will not seize the line.
`fxo-voice-delay-on-200ok`	Defines the time (in msec) that the device waits before opening the RTP (voice) channel with the FXO endpoint, after receiving a 200 OK from the IP side.
`ground-start-use-ring {off|on}`	Ground start use regular ring.
`guard-time-btwn-calls`	Defines the time interval (in seconds) after a call has ended and a new call can be accepted for IP-to-Tel calls.
`psap-support {off|on}`	Enables the PSAP Call flow.
`reorder-tone-duration`	Global parameter configuring the duration (in seconds) that the device plays a busy or reorder tone before releasing the line.
`ring-detection-tout`	Defines the timeout (in seconds) for detecting the second ring after the first detected ring.
`rings-b4-det-callerid`	Number of rings after which the Caller ID is detected.
`snd-mtr-msg-2ip {disable|enable}`	Send metering messages to IP on detection of analog metering pulses.

Command	Description
time-wait-b4-dialing	Defines the delay before the device starts dialing on the FXO line.
waiting-4-dial-tone {disable|enable}	Determines whether or not the device waits for a dial tone before dialing the phone number for IP-to-Tel calls.

Command Mode

Privileged User

Example

This example configures two rings before Caller ID is sent:

```
(config-voip)# gateway fxo-setting
(gw-analog-fxo)# rings-b4-det-callerid 2
(gw-analog-fxo)# activate
```

fxs-setting

This command configures various FXS parameters.

Syntax

```
(config-voip)# gateway analog fxs-setting
(gw-analog-fxs)#
```

Command	Description
fxs-callid-cat-brazil	Enable Interworking of Calling Party Category (cpc) from INVITE to FXS Caller ID first digit for Brazil Telecom.
fxs-offhook-timeout-alarm	Defines the duration (in seconds) of an FXS phone in off-hook state after which the device sends the SNMP alarm, acAnalogLineLeftOffhookAlarm.
max-streaming-calls	Defines the maximum concurrent on-held sessions to which the device can play Music on Hold (MoH) originating from an external media (audio) source connected to an FXS port.

Command	Description
prefix-to-ext-line	Defines a prefix to dial for the external line.

Command Mode

Privileged User

Example

This example configures a maximum of 10 streaming sessions for MoH:

```
(config-voip)# gateway analog fxs-setting
(gw-analog-fxs)# max-streaming-calls 10
(gw-analog-fxs)# activate
```

keypad-features

This command configures phone keypad features.

Syntax

```
(config-voip)# gateway analog keypad-features
(gw-analog-keypad)#
```

Command	Description
blind-transfer	Defines the keypad sequence to activate blind transfer for established Tel-to-IP calls
caller-id-restriction-act	Defines the keypad sequence to activate the restricted Caller ID option
cw-act	Defines the keypad sequence to activate the Call Waiting option
cw-deact	Defines the keypad sequence to deactivate the Call Waiting option
fwd-busy-or-no-ans	Defines the keypad sequence to activate the forward on 'busy or no answer' option
fwd-deactivate	Defines the keypad sequence to deactivate any of the call forward

Command	Description
	options
`fwd-dnd`	Defines the keypad sequence to activate the Do Not Disturb option
`fwd-no-answer`	Defines the keypad sequence to activate the forward on no answer option
`fwd-on-busy`	Defines the keypad sequence to activate the forward on busy option
`fwd-unconditional`	Defines the keypad sequence to activate the immediate call forward option
`hotline-act`	Defines the keypad sequence to activate the delayed hotline option
`hotline-deact`	Defines the keypad sequence to deactivate the delayed hotline option
`id-restriction-deact`	Defines the keypad sequence to deactivate the restricted Caller ID option
`key-port-configure`	Defines the keypad sequence for configuring a telephone number for the FXS phone.
`reject-anony-call-activate`	Defines the keypad sequence to activate the reject anonymous call option, whereby the device rejects incoming anonymous calls.
`reject-anony-call-deactivate`	Defines the keypad sequence that de-activates the reject anonymous call option.

Command Mode

Privileged User

Example

This example configures the call forwarding on-busy or no answer keypad sequence:

```
(config-voip)# gateway keypad-features
(gw-analog-keypad)# fwd-busy-or-no-ans 567
(gw-analog-keypad)# activate
```

metering-tones

This command configures metering tones settings.

Syntax

```
(config-voip)# gateway analog metering-tones
(gw-analog-mtrtone)#
```

Command	Description
`gen-mtr-tones {aoc-sip-interworking|disable|internal-table|sip-interval-provided|sip-raw-data-incr-provided|sip-raw-data-provided}`	Defines the method for automatically generating payphone metering pulses.
`metering-type {12-kHz-sinusoidal-bursts|16-kHz-sinusoidal-bursts|polarity-reversal-pulses}`	Defines the metering method for generating pulses (sinusoidal metering burst frequency) by the FXS port.

Command Mode

Privileged User

Example

This example configures metering tone to be based the Charge Codes table:

```
(config-voip)# gateway analog metering-tones
(gw-analog-mtrtone)# gen-mtr-tones internal-table
(gw-analog-mtrtone)# activate
```

reject-anonymous-calls

This command configures the Reject Anonymous Call Per Port table, which lets the device reject incoming anonymous calls per FXS port.

Syntax

```
(config-voip)# gateway analog reject-anonymous-calls <Index>
(reject-anonymous-calls-<Index>)#
```

Command	Description
Index	Defines the table row index.
`reject-calls {disable|enable}`	Enables rejection of anonymous calls.

Command Mode

Privileged User

Note

To view the port-module numbers and port type, enter the display command at the index prompt, for example:

```
(reject-anonymous-calls-0)# display
```

Example

This example configures metering tone to be based the Charge Codes table:

```
(config-voip)# gateway analog reject-anonymous-calls 0
(reject-anonymous-calls-0)# reject-calls enable
(reject-anonymous-calls-0)# activate
```

tone-index

This command configures the Tone Index table, which lets you define distinctive ringing tones and call waiting tones per calling (source) and called (destination) number (or prefix) for IP-to-Tel calls.

Syntax

```
(config-voip)# gateway analog tone-index <Index>
(tone-index-<Index>)#
```

Command	Description
Index	Defines the table row index.
dst-pattern	Defines the prefix of the called number.
fxs-port-first	Defines the first port in the FXS port range.
fxs-port-last	Defines the last port in the FXS port range.
priority	Defines the index of the distinctive ringing and call waiting tones.
src-pattern	Defines the prefix of the calling number.

Command Mode

Privileged User

Example

This example configures distinctive tone Index 12 for FXS ports 1-4 for called prefix number "976":

```
(config-voip)# gateway analog tone-index 0
(tone-index-0)# fxs-port-first 1
(tone-index-0)# fxs-port-last 4
(tone-index-0)# dst-pattern 976
(tone-index-0)# priority 12
(tone-index-0)# activate
```

digital

This command configures the various digital parameters.

Syntax

```
(config-voip)# gateway digital
```

Command	Description
`rp-network-domains`	See rp-network-domains on the next page
`settings`	See settings on the next page

Command Mode

Privileged User

rp-network-domains

This command configures user-defined MLPP network domain names (namespaces)**, which is used in the AS-SIP Resource-Priority header of the outgoing SIP INVITE request**. The command also maps the Resource-Priority field value of the SIP Resource-Priority header to the ISDN Precedence Level IE.

Syntax

```
(config-voip)# gateway digital rp-network-domains <Index>
(rp-network-domains-<Index>)#
```

Command	Description
Index	Defines the table row index.
`ip-to-tel-interworking {disable|enable}`	Enables IP-to-Tel interworking.
`name`	Defines a name.

Command Mode

Privileged User

Example

This example configures supplementary service for port 2:

```
(config-voip)# gateway digital rp-network-domains 0
(rp-network-domains-0)# ip-to-tel-interworking enable
(rp-network-domains-0)# name dsn
(rp-network-domains-0)# activate
```

settings

This command configures various digital settings.

Syntax

```
(config-voip)# gateway digital settings
(gw-digital-settings>)#
```

Command	Description
`911-location-id-in-ni2 {off|on}`	Enables 911 Location Id in NI2 protocol.
`add-ie-in-setup`	Additional information element to send in ISDN Setup message.
`add-pref-to-redir-nb`	Prefix added to Redirect phone number.
`amd-timeout`	AMD Detection Timeout <msec>.
`b-ch-negotiation {any|exclusive| preferred}`	ISDN B-Channel negotiation mode for all trunks.
`binary-redirect {off|on}`	Search for Redirect number coded in binary 4 bit style.
`blind-xfer-add-prefix {off|on}`	Add keying sequence for performing blind transfer as transfer number prefix.
`blind-xfer-disc-tmo`	Maximum time (milliseconds) to wait for disconnect from Tel before performing blind transfer.
`as-sndhook-flsh`	Hookflash forwarding.
`cic-support {off|on}`	Enables CIC -> ISDN TNS IE interworking.
`cid-not-included-notification {off|on}`	Enables presentation in the outgoing SIP message when the incoming ISDN message doesn't include presentation.
`cid-notification {off|on}`	Enables presentation in the outgoing SIP message when the presentation indicator in the incoming ISDN message has the value "not available".
`cind-mode {none|r2-charge-info-int}`	Charge Indicator Mode.
`cisco-sce-mode {off|on}`	In use with G.729 - if enabled and SCE=2 then AnnexB=no.

Command	Description
`clir-reason-support {off|on}`	Enables sending of Reason for Non Notification of Caller Id.
`connect-on-progress-ind {off|on}`	FXS: generate Caller Id signals during ringing FXO: collect Caller Id and use it in Setup message.
`copy-dst-on-empty-src {off|on}`	In case there is an empty source number from PSTN the source number will be the same as the destination.
`cp-dst-nb-2-redir-nb {cp-after-ph-num-manipulation| cp-b4-ph-num-manipulation| dont-copy}`	Copy Destination Number to Redirect Number.
`cpc-mode { argentina-r2| brazil-r2| none}`	Calling Party Category Mode.
`cug-data-mode {disabled| send-as-xml}`	Enables interworking between the ISDN Closed User Group (CUG) supplementary service and SIP, for Tel-to-IP calls.
`cut-through-enable {off|on}`	Enable call connection without On-Hook/Off-Hook process 'Cut-Through'.
`cut-thru-reord-dur`	Duration of reorder tone played after release from IP side for CutThrogh application
`dflt-call-prio`	SIP Default Call Priority.
`dflt-cse-map-isdn2sip`	Common cause value to use for most ISDN release causes.
`dig-oos-behavior {alarm| block| d-channel| default| service| service-and-dchannel}`	Digital OOS Behavior.
`disc-call-pi8-alt-rte {off|on}`	If set to 1 and ISDN DISCONNECT with PI is received, 183 with SDP will be sent toward IP only if no IP-to-Tel alternative route exists.

Command	Description
`disc-on-bsy-tone-c {off|on}`	Disconnect Call on Busy Tone Detection – CAS.
`disc-on-bsy-tone-I {off|on}`	Disconnect Call on Busy Tone Detection – ISDN.
`dscp-4-mlpp-flsh`	RTP DSCP for MLPP Flash.
`dscp-4-mlpp-flsh-ov {dscp-4-mlpp-flsh-ov}`	RTP DSCP for MLPP Flash Override.
`dscp-4-mlpp-flsh-ov-ov`	RTP DSCP for MLPP Flash-Override-Override.
`dscp-4-mlpp-immed`	RTP DSCP for MLPP Immediate.
`dscp-for-mlpp-prio`	RTP DSCP for MLPP Priority.
`dscp-for-mlpp-rtn`	RTP DSCP for MLPP Routine.
`dst-number-plan {Private| e164-public| not-included| unknown}`	Enforce this Q.931 Destination Number Type.
`dst-number-type {abbreviated| international-level2-regional| national-level1-regional| network-pisn-specific| not-included| subscriber-level0-regional| unknown}`	Enforce this Q.931 Destination Number Type.
`dtmf-used {off|on}`	Send DTMFs on the Signaling path (not on the Media path).
`e911-mlpp-bhvr {routine| standard}`	Defines the MLPP E911 Preemption mode.
`early-amd {off|on}`	If set to 1, AMD detection is started on PSTN alerting otherwise on connect.
`early-answer-timeout`	Max time (in seconds) to wait from sending Setup message to PSTN to receiving Connect message from PSTN.
`epn-as-cpn-ip2tel {off|on}`	Use endpoint number as calling number for

Command	Description
	IP-to-Tel.
`epn-as-cpn-tel2ip {off|on}`	Use endpoint number as calling number for Tel-to-IP.
`etsi-diversion {off|on}`	Use supplementary service ETSI Diverting Leg Information 2 to send redirect number.
`fallback-transfer-to-tdm {off|on}`	Disable fallback from ISDN call transfer to TDM.
`fax-rerouting-delay`	Defines the time interval (in sec) to wait for CNG detection to re-route call to fax destinations.
`fax-rerouting-mode {connect-and-delay| disabled| progress-and-delay| without-delay}`	Enables the detection of the fax CNG tone in incoming calls, before sending the INVITE.
`first-call-waiting-tone-id`	Defines the index of the first Call Waiting tone in the Call Progress Tones file.
`format-dst-phone-number {remove-params| transparent}`	Defines if the destination phone number that the device sends to the Tel side (for IP-to-Tel calls) includes the user-part parameters (e.g., 'password' and 'phone-context') of the destination URI received in the incoming SIP INVITE message.
`gw-app-sw-wd {off|on}`	Uses the software watchdog for gateway tasks.
`gw-dest-src-id`	Defines gateway H.323-ID source field.
`ign-isdn-disc-w-pi {off|on}`	Enable ignoring of ISDN Disconnect messages with PI 1 or 8.
`isdn-channel-id-format`	Defines the channel number format (number or slotmap) in the Channel Identification IE when sending Q.931 ISDN messages.
`isdn-ignore-18x-without-sdp {off|on}`	Enables interworking SIP 18x without SDP and ISDN Q.931 Progress/Alerting

Command	Description
	messages.
`isdn-ntt-noid-interworking-mode {both|ip2tel|none|tel2ip}`	Defines SIP-ISDN interworking between NTT Japan's No-ID cause in the Facility information element (IE) of the ISDN Setup message, and the calling party number (display name) in the From header of the SIP INVITE message.
`isdn-send-progress-for-te {off|on}`	Defines whether the device sends Q.931 Progress messages to the ISDN trunk if the trunk is configured as User side (TE) and/or Network (NT) side, for IP-to-Tel calls.
`ignore-alert-after-early-media {off|on}`	Interwork of Alert from ISDN to SIP.
`ignore-bri-los-alarm {off|on}`	Ignore LOS alarms for BRI user side trunk.
`ip-to-cas-ani-dnis-del`	IP to CAS list of ANI and DNIS delimiters.
`isdn-facility-trace {off|on}`	Enable ISDN Facility Trace.
`isdn-subaddr-frmt {ascii| bcd| user-specified}`	ISDN SubAdress format.
`isdn-tnl-ip2tel {disable| using-body| using-header}`	Enable ISDN Tunneling IP to Tel.
`isdn-tnl-tel2ip {disable|using-body| using-header}`	Enable ISDN Tunneling Tel to IP.
`isdn-trsfr-on-conn {alert| connect}`	Send TBCT/ECT/RLT request only when second leg call is connected.
`isdn-xfer-complete-cause`	If such a cause received in ISDN DISCONNECT message of the first leg, NOTIFY 200 is sent toward IP.
`iso8859-charset {arabic| center-euro| cyrillic| hebrew| no-accented| north-euro| south-euro| turkish| west-euro}`	ISO 8859 Character Set Part.

Command	Description
`isub-number-of-digits`	Number of digits that will be taken from end of phone number as Subaddress.
`local-time-on-connect {always-send-local-time| dont-send-local-time| send-local-time-only-if-missing}`	0 - Don't Send Local Date and Time,1 - Send Local Date and Time Only If Missing,2 - Always Send Local Date and Time
`max-message-length`	Limit the maximum length in KB for SIP message.
`mfcr2-category`	MFC/R2 Calling Party's category.
`mfcr2-debug {off|on}`	Enable MFC-R2 protocol debug.
`mlpp-dflt-namespace {cuc| dod| drsn| dsn| interworking| uc| user-def}`	MLPP Default Namespace.
`mlpp-dflt-srv-domain`	MLPP Default Service Domain String (6 Hex Digits).
`mlpp-norm-ser-dmn`	MLPP Normalized Service Domain String (6 Hex Digits).
`mlpp-nwrk-id`	Sets the Network identifier value which is represented as the first 2 octets in the MLPP service domain field. values are [1-999].
`mrd-cas-support`	Enable/Disable MRD CAS behavior.
`mx-syslog-lgth`	Maximum length used for bundling syslog at debug level 7.
`ni2-cpc`	Enables NI2 calling party category translation to SIP.
`notification-ip-group-name`	IP Group for notification purposes.
`np-n-ton-2-redirnb`	Add NPI and TON as prefix to Redirect number.
`number-type-and-plan`	If selected, ISDN Type & Plan relayed from IP. Otherwise, ISDN Type & Plan are set to 'Unknown'.

Command	Description
`overlap-used`	Enables Overlap mode.
`pi-4-setup-msg`	Progress Indicator for ISDN Setup Message.
`play-l-rbt-isdn-trsfr`	Play local RBT on TBCT/ECT/RLT transfer.
`play-rb-tone-xfer-success`	Play RB tone on transfer success.
`preemp-tone-dur`	Preemption Tone Duration.
`q850-reason-code-2play-user-tone`	Q850 Reason Code which cause playing special PRT Tone.
`qsig-path-replacement-md`	Enables QSIG transfer for IP-to-Tel and Tel-to-IP calls.
`qsig-tunneling`	Enables QSIG Tunneling over SIP.
`qsig-tunneling-mode`	Defines the format of encapsulated QSIG message data in the SIP message MIME body.
`qsig-xfer-update`	Enable QSIG Transfer Update.
`r2-for-brazil-telecom`	Enable Interworking of Calling Party Category (cpc) from sip INVITE to MFCR2 category for Brazil Telecom.
`rekey-after-181`	Send re-INVITE after 181 with new SRTP keys.
`replace-tel-to-ip-calnum-to`	Maximum Time to wait between call setup and Facility with Redirecting Number for replacing calling number (msec).
`restarts-after-so`	Enable sending restarts to PSTN on channels experienced mismatch in CONNID usage.
`rls-ip-to-isdn-on-pro-cause`	Defines if to disconnect call while receiving ISDN PROGRESS with Cause.
`rmv-calling-name`	Removes calling name from IP > Tel calls.
`rmv-cli-when-restr`	Removes CLI from IP-to-Tel calls if received CLI is restricted.

Command	Description
`rtcp-act-mode`	RTCP activation policy.
`send-screen-to-ip`	Override screening indicator value in Setup messages to IP
`send-screen-to-isdn`	Override screening indicator value in Setup messages to ISDN
`send-screen-to-isdn-1`	Overrides the screening indicator for the first calling party number when the device includes two calling party numbers in the outgoing ISDN Setup message for IP-to-Tel ISDN calls.
`send-screen-to-isdn-2`	Overrides the screening indicator for the second calling party number when the device includes two calling party numbers in the outgoing ISDN Setup message for IP-to-Tel ISDN calls.
`setup-ack-used`	Enable SetupAck messages for overlap mode
`silence-supp-in-sdp`	SilenceSupp in SDP used for fax VBD
`src-number-plan`	if defined, enforce this Q.931 Source Number Plan
`src-number-type`	if defined, enforce this Q.931 Source Number Type
`swap-rdr-n-called-nb`	Swap Redirect and Called numbers
`tdm-over-ip-initiate-time`	Time between first INVITE issued within the same trunk (msec)
`tdm-over-ip-min-calls`	Minimum connected calls for trunk activation, if 0 - trunk is always active
`tdm-over-ip-retry-time`	Time between call release and new INVITE (msec)
`tdm-tunneling`	Enable gateway to maintain a permanent RTP connection
`third-party-transcoding`	Enables Third Party Call Control Transcoding

Command	Description
	functionality
`time-b4-reordr-tn`	Delay time before playing Reorder tone
`transparent-on-data-call`	In case the transfer capability of a call from ISDN is data open with transparent coder
`trk-alrm-disc-timeout`	Trunk alarm call disconnect timeout in seconds
`trkgrps-to-snd-ie`	Configure trunk groups on which to send additional IE
`trunk-restart-mode-on-powerup {no-restart|per-b-channel|per-trunk}`	Trunk Restart Mode on Power Up.
`trunk-status-reporting`	When TrunkGroup #1 is present and active response to options and/or send keep-alive to associated proxy(ies)
`use-to-header-as-called-num`	Use the user part of To header URL as called number (IP->TEL)
`user-info`	Provides a link to the user information file, to be downloaded using Automatic Update.
`user-info-file-name`	The file name to be loaded using TFTP
`uui-ie-for-ip2tel`	Enable User-User IE to pass in Setup from IP to ISDN
`uui-ie-for-tel2ip`	Enable User-User IE to pass in Setup from ISDN to IP
`wait-befor-pstn-rel-ack`	Defines the timeout (in milliseconds) to wait for the release ACK from the PSTN before releasing the channel.
`wait-for-busy-time`	Time to wait to detect busy and reorder tones. Currently used in semi supervised PBX transfer
`warning-tone-duration`	OfHook Warning Tone Duration [Sec]
`xfer-across-trunk-groups`	if set ECT RLT 2BCT call transfer is allowed

Command	Description
	across different trunks and trunkgroups
`xfer-cap-for-data-calls`	0: ISDN Transfer Capability for data calls will be 64k unrestricted (data), 1:ISDN Transfer Capabilityfor Data calls will be set according to ISDNTransferCapability parameter
`xfer-prefix-ip2tel`	Defines the prefix that is added to the destination number received in the SIP Refer-To header (for IP-to-Tel calls).

Command Mode

Privileged User

dtmf-supp-service

This command configures the DTMF supplementary services.

Syntax

```
(config-voip)# gateway dtmf-supp-service
```

Command	Description
`charge-code`	See charge-code below
`dtmf-and-dialing`	See dtmf-and-dialing on the next page
`isdn-supp-serv`	See isdn-supp-serv on page 401
`supp-service-settings`	See supp-service-settings on page 403

Command Mode

Privileged User

charge-code

This command configures the Charge Codes table, which lets you define metering tones.

Syntax

```
(config-voip)# gateway dtmf-supp-service charge-code <Index>
(charge-code-<Index>)#
```

Command	Description
Index	Defines the table row index.
`charge-code-name`	Defines a descriptive name.

`end-time-1, end-time-2, end-time-3,`
`end-time-4`
	Defines the end of the time period in a 24 hour format.

`pulse-interval-1, pulse-interval-2,`
`pulse-interval-3, pulse-interval-4`
	Defines the time interval between pulses (in tenths of a second).

`pulses-on-answer-1, pulses-on-answer-2,`
`pulses-on-answer-3, pulses-on-answer-4`
	Defines the number of pulses that the device generates upon call answer.

Command Mode

Privileged User

Example

This example configures a Charge Code:

```
(config-voip)# gateway dtmf-supp-service charge-code 0
(charge-code-0)# charge-code-name INT
(charge-code-0)# end-time-1 04
(charge-code-0)# pulse-interval-1 2
(charge-code-0)# activate
```

dtmf-and-dialing

This command configures DTMF and dialing parameters.

Syntax

```
(config-voip)# gateway dtmf-supp-service dtmf-and-dialing
(gw-dtmf-and-dial)#
```

Command	Description
`auto-dtmf-mute`	Enables automatic muting of DTMF digits when out-of-band DTMF transmission is used.
`char-conversion`	Configures Unicode-to-ASCII character conversion rules.
`dflt-dest-nb`	Defines the default destination phone number which is used if the received message doesn't contain a called party number and no phone number is configured in the Trunk Group table.
`dial-plan-index`	Defines the Dial Plan Index.
`digitmapping`	Defines the digit map pattern used to reduce the dialing period when ISDN overlap dialing for digital interfaces.
`dt-duration`	Defines the duration, in seconds, that the dial tone is played, for digital interfaces, to an ISDN terminal.
`dtmf-inter-digit-threshold`	Defines the threshold of the received DTMF InterDigitTime, in milliseconds.
`first-dtmf-option-type`	Defines the first preferred transmit DTMF negotiation method.
`hook-flash-option`	Defines the hook-flash transport type.
`hotline-dt-dur`	Defines the duration, in seconds, of the hotline dial tone.
`isdn-tx-overlap`	Enables ISDN overlap dialing for IP-to-Tel calls.
`min-dg-b4-routing`	Defines the minimum number of overlap digits to collect - for ISDN overlap dialing - before sending the first SIP message for routing Tel-to-IP calls.
`mxdig-b4-dialing`	Defines the maximum number of collected destination number digits that can be received.
`oob-dtmf-format`	Defines the DTMF Out-of-Band transport method.
`rfc-2833-in-sdp`	Global parameter that enables the device to declare the RFC 2833 'telephony-event' parameter in the SDP.

Command	Description
`second-dtmf-option-type`	Defines the second preferred transmit DTMF negotiation method.
`special-digit-rep`	Defines the representation for ‘special’ digits‘*’ and ‘#’. that are used for out-of-band DTMF signaling using SIP INFO/NOTIFY.
`special-digits`	Determines whether the asterisk*. and pound#. digits can be used in DTMF.
`strict-dial-plan`	Enables Strict Dial Plan.
`telephony-events-payload-type-tx`	Defines the Tx RFC 2833 DTMF relay dynamic payload type for outbound calls. **Note:** The location of this command in the CLI is for backward compatibility. The correct location is `configure voip > media rtp-rtcp`.
`time-btwn-dial-digs`	Analog: Defines the time, in seconds, that the device waits between digits that are dialed by the user. ISDN overlap dialing: Defines the time, in seconds, that the device waits between digits that are received from the PSTN or IP during overlap dialing.

Command Mode

Privileged User

isdn-supp-serv

This command configures the Supplementary Services table, which lets you define supplementary services for endpoints (FXS and ISDN BRI) connected to the device.

Syntax

```
(config-voip)# gateway dtmf-supp-service isdn-supp-serv <Index>
(isdn-supp-serv-<Index>)#
```

Command	Description
Index	Defines the table row index.

Command	Description
`caller-id-enable {allowed|not-configured|restricted}`	Enables the receipt of Caller ID.
`caller-id-number`	Defines the caller ID name of the endpoint (sent to the IP side).
`cfu-to_phone-number`	Defines the phone number for BRI Call Forward Unconditional (CFU) services.
`cfb-to_phone-number`	Defines the phone number for BRI Call Forward Busy (CFB) services.
`cfnr-to_phone-number`	Defines the phone number for BRI Call Forward No Reply (CFNR) services.
`local-phone-number`	Configures a local telephone extension number for the endpoint.
`module`	Defines the device's module number to which the endpoint is connected.
`no-reply-time`	Defines the timeout, in seconds.
`phone-number`	Configures a global telephone extension number for the endpoint.
`port`	Defines the port number on the module to which the endpoint is connected.
`presentation-restricted {allowed|not-configured|restricted}`	Determines whether the endpoint sends its Caller ID information to the IP when a call is made.
`user-id`	Defines the User ID for registering the endpoint to a third-party softswitch for authentication and/or billing.
`user-password`	Defines the user password for registering the endpoint to a third-party softswitch for authentication and/or billing.

Command Mode

Privileged User

Example

This example configures supplementary service for port 2:

```
(config-voip)# gateway dtmf-supp-service isdn-supp-serv 0
(isdn-supp-serv-0)# phone-number +15032638005
(isdn-supp-serv-0)# local-phone-number 402
(isdn-supp-serv-0)# module 1
(isdn-supp-serv-0)# port 2
(isdn-supp-serv-0)# user-id JoeD
(isdn-supp-serv-0)# user-password 1234
(isdn-supp-serv-0)# caller-id-enable allowed
(isdn-supp-serv-0)# activate
```

supp-service-settings

This command configures supplementary services.

Syntax

```
(config-voip)# gateway dtmf-supp-service supp-service-settings
(gw-suppl-serv)#
```

Command	Description
`3w-conf-mode`	Defines the mode of operation for three-way conferencing.
`3w-conf-nonalloc-prts`	Define the ports that are not affected by three-way conferencing.
`aoc-support`	Enables AoC-D and AoC-E from ISDN to SIP.
`as-subs-ipgroupname`	Defines the IP Group (by name) for AS subscribe purposes.
`blind-transfer`	Keying sequence for performing blind transfer.
`call-forward`	Enable Call Forward service.
`call-hold-remnd-rng`	Call-hold reminder ring maximum ringing time, in seconds.
`call-prio-mode`	Priority mode.

Command	Description
`call-waiting`	Enables Call Waiting service.
`caller-id-type`	Defines the Caller ID standard.
`cfb-code`	Supplementary Service code for activating Call Forward Busy.
`cfb-deactivation-code`	Supplementary Service code for deactivating Call Forward Busy.
`cfe-ring-tone-id`	Ringtone type for Call forward notification.
`cfnr-code`	Supplementary Service code for activating Call Forward No Reply.
`cfnr-deactivation-code`	Supplementary Service code for deactivating Call Forward No Reply.
`cfu-code`	Supplementary Service code for activating Call Forward Unconditional.
`cfu-deactivation-code`	Supplementary Service code for deactivating Call Forward Unconditional.
`conf-id`	Identification of conference call used by SIP INVITE.
`connected-number-plan`	Enforces Q.931 Connected Number Type.
`connected-number-type`	Enforces Q.931 Connected Number Type.
`dtmf-during-hold`	Enables playing DTMF to Tel during hold.
`enable-3w-conf`	Enables 3-way conferencing feature.
`enable-caller-id`	FXS: Generate Caller ID; FXO: Collect Caller ID information.
`enable-mwi`	Enables MWI.
`enable-transfer`	Enables Call Transfer service.

Command	Description
`estb-conf-code`	Control Key activation for 3-way conference.
`flash-key-seq-style`	Flash key sequence.
`flash-key-seq-tmout`	Flash key sequence timeout.
`held-timeout`	Maximum time allowed for call to be retrieved from IP, in seconds.
`hold`	Enables Call Hold service.
`hold-format`	Call hold format.
`hold-to-isdn`	Enables Hold/Retrieve from and to ISDN.
`hook-flash-code`	If Rx during session, act as if hook flash Rx from Tel side.
`ignore-isdn-subaddress`	Ignores ISDN Subaddress.
`isdn-xfer-complete-timeout`	Max time, in seconds, to wait for transfer response from PSTN.
`mlpp-diffserv`	DiffServ value for MLPP calls.
`music-on-hold`	Enables playing Music On Hold.
`mute-dtmf-in-overlap`	In overlap mode if set mute in-band DTMF till destination number is received.
`mwi-analog-lamp`	Enables MWI using an analog lamp 110 Volt.
`mwi-display`	Enables MWI using Caller ID interface.
`mwi-ntf-timeout`	Defines the maximum duration (timeout) that a message waiting indication (MWI) is displayed on endpoint equipment (phones' LED, screen notification or voice tone).
`mwi-qsig-party-num`	Party Number from msgCentreId in MWIactivate and MWIdeactivate.
`mwi-srvr-ip-addr`	MWI server IP address.

Command	Description
`mwi-srvr-transp-type`	MWI server transport type.
`mwi-subs-expr-time`	MWI service subscription expiration time, in seconds.
`mwi-subs-ipgrpid`	IP Group ID for MWI subscribe purposes.
`mwi-subs-rtry-time`	MWI service subscriptions retry time after last subscription failure, in seconds.
`mx-3w-conf-onboard`	Max on-board conference calls.
`nb-of-cw-ind`	Number of call waiting indications to be played to the user.
`nrt-sub-retry-time`	NRT subscribe retry time.
`nrt-subscription`	Enable subscription for Call forward ringtone indicator services.
`precedence-ringing`	Index of the first Call RB tone in the call-progress tones file.
`qsig-calltransfer-reverse-enddesignation`	QSIG Call Transfer Reverse End Designation.
`reminder-ring {disable|enable}`	Enables the reminder ring.
`send-all-cdrs-on-rtrv`	Send only chosen coder or all supported coders.
`should-subscribe`	Related to Subscribe/UnSubscribe buttons.
`snd-isdn-ser-aftr-restart`	ISDN SERVICE message is sent after restart.
`sttr-tone-duration`	Time for playing confirmation tone before normal dial tone is played (msec).

Command	Description
`subscribe-to-mwi`	Enable subscription for MWI service.
`time-b4-cw-ind`	Time before call waiting indication is sent to a busy line, in seconds.
`time-between-cw`	Time between one call waiting indication to the next, in seconds.
`transfer-prefix`	Prefix added to the called number of a transferred call.
`waiting-beep-dur`	Call Waiting tone beep length (msec).

Command Mode

Privileged User

Example

This example enables the reminder ring feature:

```
(config-voip)# gateway dtmf-supp-service supp-service-settings
(gw-suppl-serv)# reminder-ring enable
(gw-suppl-serv)# reminder-ring enable
```

manipulation

This subcommand configures the gateway's advanced parameters.

Syntax

```
(config-voip)# gateway manipulation
```

Command	Description
`calling-name-map-ip2tel`	See calling-name-map-ip2tel on the next page
`calling-name-map-tel2ip`	See calling-name-map-tel2ip on page 409
`cause-map-isdn2isdn`	See cause-map-isdn2isdn on page 410
`cause-map-isdn2sip`	See cause-map-isdn2sip on page 411

Command	Description
`cause-map-sip2isdn`	See cause-map-sip2isdn on page 412
`dst-number-map-ip2tel`	See dst-number-map-ip2tel on page 413
`dst-number-map-tel2ip`	See dst-number-map-tel2ip on page 414
`phone-context-table`	See phone-context-table on page 415
`redirect-number-map-ip2tel`	See redirect-number-map-ip2tel on page 416
`redirect-number-map-tel2ip`	See redirect-number-map-tel2ip on page 418
`settings`	See settings on page 419
`src-number-map-ip2tel`	See src-number-map-ip2tel on page 421
`src-number-map-tel2ip`	See src-number-map-tel2ip on page 423

Command Mode

Privileged User

calling-name-map-ip2tel

This command configures the Calling Name Manipulation for IP-to-Tel Calls table, which lets you define manipulation rules for manipulating the calling name (i.e., caller ID) in SIP messages for IP-to-Tel calls.

Syntax

```
(config-voip)# gateway manipulation calling-name-map-ip2tel <Index>
(calling-name-map-ip2tel-<Index>)#
```

Command	Description
Index	Defines the table row index.
`calling-name-pattern`	Defines the caller name (i.e., caller ID) prefix.
`dst-host-pattern`	Defines the Request-URI host name prefix of the incoming SIP INVITE message.

Command	Description
`dst-pattern`	Defines the destination (called) telephone number prefix and/or suffix.
`manipulation-name`	Defines a descriptive name, which is used when associating the row in other tables.
`num-of-digits-to-leave`	Defines the number of characters that you want to keep from the right of the calling name.
`prefix-to-add`	Defines the number or string to add at the front of the calling name.
`remove-from-left`	Defines the number of characters to remove from the left of the calling name.
`remove-from-right`	Defines the number of characters to remove from the right of the calling name.
`src-host-pattern`	Defines the URI host name prefix of the incoming SIP INVITE message in the From header.
`src-ip-address`	Defines the source IP address of the caller for IP-to-Tel calls.
`src-pattern`	Defines the source (calling) telephone number prefix and/or suffix.
`suffix-to-add`	Defines the number or string to add at the end of the calling name.

Command Mode

Privileged User

calling-name-map-tel2ip

This command configures the Calling Name Manipulation for Tel-to-IP Calls table, which lets you define manipulation rules for manipulating the calling name (i.e., caller ID) in SIP messages for Tel-to-IP calls.

Syntax

```
(config-voip)# gateway manipulation calling-name-map-tel2ip <Index>
(calling-name-map-tel2ip-<Index>)#
```

Command	Description
Index	Defines the table row index.
`calling-name-pattern`	Defines the caller name (i.e., caller ID) prefix.
`dst-pattern`	Defines the destination (called) telephone number prefix and/or suffix.
`manipulation-name`	Defines a descriptive name, which is used when associating the row in other tables.
`num-of-digits-to-leave`	Defines the number of characters that you want to keep from the right of the calling name.
`prefix-to-add`	Defines the number or string to add at the front of the calling name.
`remove-from-left`	Defines the number of characters to remove from the left of the calling name.
`remove-from-right`	Defines the number of characters to remove from the right of the calling name.
`src-pattern`	Defines the source (calling) telephone number prefix and/or suffix.
`src-trunk-group-id`	Defines the source Trunk Group ID from where the Tel-to-IP call was received.
`suffix-to-add`	Defines the number or string to add at the end of the calling name.

Command Mode

Privileged User

cause-map-isdn2isdn

This command configures the Release Cause ISDN to ISDN table, which lets you define ISDN ITU-T Q.850 release cause code (call failure) to ISDN ITU-T Q.850 release cause code mapping rules.

Syntax

```
(config-voip)# gateway manipulation cause-map-isdn2isdn <Index>
(cause-map-isdn2isdn-<Index>)#
```

Command	Description
Index	Defines the table row index.
`map-q850-cause`	Defines the ISDN Q.850 cause code to which you want to change the originally received cause code.
`orig-q850-cause`	Defines the originally received ISDN Q.850 cause code.

Command Mode

Privileged User

Example

This example maps ISDN cause code 127 to 16:

```
(config-voip)# gateway manipulation cause-map-isdn2isdn 0
(cause-map-isdn2isdn-0)# orig-q850-cause 127
(cause-map-isdn2isdn-0)# map-q850-cause 16
(cause-map-isdn2isdn-0)# activate
```

cause-map-isdn2sip

This command configures the Release Cause Mapping from ISDN to SIP table, which lets you define ISDN ITU-T Q.850 release cause code (call failure) to SIP response code mapping rules.

Syntax

```
(config-voip)# gateway manipulation cause-map-isdn2sip <Index>
(cause-map-isdn2sip-<Index>)#
```

Command	Description
Index	Defines the table row index.
`q850-causes`	Defines the ISDN Q.850 cause code.
`sip-response`	Defines the SIP response code.

Command Mode

Privileged User

Example

This example maps ISDN cause code 6 to SIP code 406:

```
(config-voip)# gateway manipulation cause-map-isdn2sip 0
(cause-map-isdn2sip-0)# q850-causes 6
(cause-map-isdn2sip-0)# sip-response 406
(cause-map-isdn2sip-0)# activate
```

cause-map-sip2isdn

This command configures the Release Cause Mapping from SIP to ISDN table, which lets you define SIP response code to ISDN ITU-T Q.850 release cause code (call failure) mapping rules.

Syntax

```
(config-voip)# gateway manipulation cause-map-sip2isdn <Index>
(cause-map-sip2isdn-<Index>)#
```

Command	Description
Index	Defines the table row index.
`q850-causes`	Defines the ISDN Q.850 cause code.
`sip-response`	Defines the SIP response code.

Command Mode

Privileged User

Example

This example maps SIP code 406 to ISDN cause code 6:

```
(config-voip)# gateway manipulation cause-map-sip2isdn 0
(cause-map-sip2isdn-0)# q850-causes 6
```

```
(cause-map-sip2isdn-0)# sip-response 406
(cause-map-sip2isdn-0)# activate
```

dst-number-map-ip2tel

This command configures the Destination Phone Number Manipulation for IP-to-Tel Calls table, which lets you define manipulation rules for manipulating the destination number for IP-to-Tel calls.

Syntax

```
(config-voip)# gateway manipulation dst-number-map-ip2tel <Index>
(dst-number-map-ip2tel-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dst-host-pattern`	Defines the Request-URI host name prefix of the incoming SIP INVITE message.
`dst-pattern`	Defines the destination (called) telephone number prefix and/or suffix.
`is-presentation-restricted`	Enables caller ID.
`manipulation-name`	Defines a descriptive name, which is used when associating the row in other tables.
`npi`	Defines the Numbering Plan Indicator (NPI).
`num-of-digits-to-leave`	Defines the number of digits that you want to keep from the right of the phone number.
`prefix-to-add`	Defines the number or string that you want added to the front of the telephone number.
`remove-from-left`	Defines the number of digits to remove from the left of the telephone number prefix.
`remove-from-right`	Defines the number of digits to remove from the right of the telephone number prefix.
`src-host-pattern`	Defines the URI host name prefix of the incoming SIP INVITE message in the From header.

Command	Description
`src-ip-address`	Defines the source IP address of the caller.
`src-ip-group-name`	Defines the IP Group to where the call is sent.
`src-pattern`	Defines the source (calling) telephone number prefix and/or suffix.
`suffix-to-add`	Defines the number or string that you want added to the end of the telephone number.
`ton`	Defines the Type of Number (TON).

Command Mode

Privileged User

dst-number-map-tel2ip

This command configures the Destination Phone Number Manipulation for IP-to-Tel Calls table, which lets you define manipulation rules for manipulating the destination number for Tel-to-IP calls.

Syntax

```
(config-voip)# gateway manipulation dst-number-map-tel2ip <Index>
(dst-number-map-tel2ip-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dest-ip-group-name`	Defines the IP Group to where the call is sent.
`dst-pattern`	Defines the destination (called) telephone number prefix and/or suffix.
`is-presentation-restricted`	Enables caller ID.
`manipulation-name`	Defines a descriptive name, which is used when associating the row in other tables.

Command	Description
npi	Defines the Numbering Plan Indicator (NPI).
num-of-digits-to-leave	Defines the number of digits that you want to keep from the right of the phone number.
prefix-to-add	Defines the number or string that you want added to the front of the telephone number.
remove-from-left	Defines the number of digits to remove from the left of the telephone number prefix.
remove-from-right	Defines the number of digits to remove from the right of the telephone number prefix.
src-pattern	Defines the source (calling) telephone number prefix and/or suffix.
src-trunk-group-id	Defines the source Trunk Group for Tel-to-IP calls.
suffix-to-add	Defines the number or string that you want added to the end of the telephone number.
ton	Defines the Type of Number (TON).

Command Mode

Privileged User

phone-context-table

This command configures the Phone Contexts table, which lets you define rules for mapping the Numbering Plan Indication (NPI) and Type of Number (TON) to the SIP 'phone- context' parameter, and vice versa.

Syntax

```
(config-voip)# gateway manipulation phone-context-table <Index>
(phone-context-table-<Index>)#
```

Command	Description
Index	Defines the table row index.

Command	Description
`context`	Defines the SIP 'phone-context' URI parameter.
`npi {e164-public|not-included|private|unknown}`	Defines the NPI.
`ton`	Defines the TON.

Command Mode

Privileged User

Example

This example maps NPI E.164 to "context= na.e.164.nt.com":

```
(config-voip)# gateway manipulation phone-context-table 0
(phone-context-table-0)# npi e164-public
(phone-context-table-0)# context na.e.164.nt.com
(phone-context-table-0)# activate
```

redirect-number-map-ip2tel

This command configures the Redirect Number IP-to-Tel table, which lets you define manipulation rules for manipulating the redirect number received in SIP messages for IP-to-Tel calls.

Syntax

```
(config-voip)# gateway manipulation redirect-number-map-ip2tel <Index>
(redirect-number-map-ip2tel-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dst-host-pattern`	Defines the Request-URI host name prefix, which appears in the incoming SIP INVITE message.
`dst-pattern`	Defines the destination

Command	Description
	(called) telephone number prefix.
`is-presentation-restricted {allowed|not-configured|restricted}`	Enables caller ID.
`manipulation-name`	Defines a descriptive name, which is used when associating the row in other tables.
`npi {e164-public|not-included|private|unknown}`	Defines the Numbering Plan Indicator (NPI).
`num-of-digits-to-leave`	Defines the number of digits that you want to retain from the right of the redirect number.
`prefix-to-add`	Defines the number or string that you want added to the front of the redirect number.
`redirect-pattern`	Defines the redirect telephone number prefix.
`remove-from-left`	Defines the number of digits to remove from the left of the redirect number prefix.
`remove-from-right`	Defines the number of digits to remove from the right of the redirect number prefix.
`src-host-pattern`	Defines the URI host name prefix of the caller.
`src-ip-address`	Defines the IP address of the caller.
`suffix-to-add`	Defines the number or string that you want added to the end of the redirect number.
`ton {abbreviated|international-level2-`	Defines the Type of Number

Command	Description
`regional|national-level1-regional|network-pstn-specific|not-included|subscriber-level0-regional|unknown}`	(TON).

Command Mode

Privileged User

redirect-number-map-tel2ip

This command configures the Redirect Number IP-to-Tel table, which lets you define manipulation rules for manipulating the redirect number received in SIP messages for IP-to-Tel calls.

Syntax

```
(config-voip)# gateway manipulation redirect-number-map-tel2ip <Index>
(redirect-number-map-tel2ip-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dst-pattern`	Defines the destination (called) telephone number prefix.
`is-presentation-restricted {allowed|not-configured|restricted}`	Enables caller ID.
`manipulation-name`	Defines a descriptive name, which is used when associating the row in other tables.
`npi {e164-public|not-included|private|unknown}`	Defines the Numbering Plan Indicator (NPI).
`num-of-digits-to-leave`	Defines the number of digits that you want to retain from the right of the redirect number.

Command	Description
`prefix-to-add`	Defines the number or string that you want added to the front of the redirect number.
`redirect-pattern`	Defines the redirect telephone number prefix.
`remove-from-left`	Defines the number of digits to remove from the left of the redirect number prefix.
`remove-from-right`	Defines the number of digits to remove from the right of the redirect number prefix.
`src-trunk-group-id`	Defines the Trunk Group from where the Tel call is received.
`suffix-to-add`	Defines the number or string that you want added to the end of the redirect number.
`ton {abbreviated|international-level2-regional|national-level1-regional|network-pstn-specific|not-included|subscriber-level0-regional|unknown}`	Defines the Type of Number (TON).

Command Mode

Privileged User

settings

This command configures the Redirect Number IP-to-Tel table, which lets you define manipulation rules for manipulating the redirect number received in SIP messages for IP-to-Tel calls.

Syntax

```
(config-voip)# gateway manipulation settings
(gw-manip-settings)#
```

Command	Description
`add-cic`	If add carrier identification code as prefix.
`add-ph-cntxt-as-pref`	Adds the phone context to src/dest phone number as prefix.
`add-prefix-for-isdn-hlc-fax`	If set and incoming ISDN SETUP contains High Layer Compatability IE with Facsimile, prefix FAX will be added to received Calling number.
`alt-map-tel-to-ip`	Enables different number manipulation rules for redundant calls.
`ip2tel-redir-reason`	Set the IP-to-TEL Redirect Reason.
`map-ip-to-pstn-refer-to`	if set to 1, manipulate destination number from REFER-TO in TDM blind transfer.
`prefix-2-ext-line`	FXS: If enabled (1) and Prefix2ExtLine is detected, it is added to the dial number as prefix
`prfm-ip-to-tel-dst-map`	Perform Additional IP2TEL Destination Manipulation
`prfm-ip-to-tel-src-map`	Perform Additional IP2TEL Source Manipulation
`swap-tel-to-ip-phone-num`	Swaps calling and called numbers received from Tel side.
`tel-to-ip-dflt-redir-rsn`	Tel-to-IP Default Redirect Reason.
`tel2ip-dst-nb-map-dial-index`	Tel to IP Destination Number Mapping Dial Plan Index.
`tel2ip-redir-reason`	Tel-to-IP Redirect Reason.
`tel2ip-src-nb-map-dial-index`	Tel to IP Source Number Mapping Dial Plan Index.
`tel2ip-src-`	Tel to IP Source Number Mapping Dial Plan Mode.

Command	Description
`nb-map-dial-mode`	
`use-refer-by-for-calling-num`	If set to 1, use a number from Referred-By URI, as a calling number in outgoing Q.931 SETUP.

Command Mode

Privileged User

src-number-map-ip2tel

This command configures the Source Phone Number Manipulation for IP-to-Tel Calls table, which lets you define manipulation rules for manipulating the source number for IP-to-Tel calls.

Syntax

```
(config-voip)# gateway manipulation src-number-map-ip2tel <Index>
(src-number-map-ip2tel-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dst-host-pattern`	Defines the Request-URI host name prefix of the incoming SIP INVITE message.
`dst-pattern`	Defines the destination (called) telephone number prefix and/or suffix.
`is-presentation-restricted {allowed|not-configured|restricted}`	Enables caller ID.
`manipulation-name`	Defines a descriptive name, which is used when associating the row in other tables.
`npi {e164-public|not-included|private|unknown}`	Defines the Numbering Plan Indicator (NPI).

Command	Description
`num-of-digits-to-leave`	Defines the number of digits that you want to keep from the right of the phone number.
`prefix-to-add`	Defines the number or string that you want added to the front of the telephone number.
`remove-from-left`	Defines the number of digits to remove from the left of the telephone number prefix.
`remove-from-right`	Defines the number of digits to remove from the right of the telephone number prefix.
`src-host-pattern`	Defines the URI host name prefix of the incoming SIP INVITE message in the From header.
`src-ip-address`	Defines the source IP address of the caller.
`src-ip-group-name`	Defines the IP Group to where the call is sent.
`src-pattern`	Defines the source (calling) telephone number prefix and/or suffix.
`suffix-to-add`	Defines the number or string that you want added to the end of the telephone number.
`ton {abbreviated|international-level2-regional|national-level1-regional|network-pstn-specific|not-included|subscriber-level0-regional|unknown}`	Defines the Type of Number (TON).

Command Mode

Privileged User

src-number-map-tel2ip

This command configures the Source Phone Number Manipulation for Tel-to-IP Calls table, which lets you define manipulation rules for manipulating the source number for Tel-to-IP calls.

Syntax

```
(config-voip)# gateway manipulation src-number-map-tel2ip <Index>
(src-number-map-tel2ip-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dst-pattern`	Defines the destination (called) telephone number prefix and/or suffix.
`is-presentation-restricted {allowed|not-configured|restricted}`	Enables caller ID.
`manipulation-name`	Defines a descriptive name, which is used when associating the row in other tables.
`npi {e164-public|not-included|private|unknown}`	Defines the Numbering Plan Indicator (NPI).
`num-of-digits-to-leave`	Defines the number of digits that you want to keep from the right of the phone number.
`prefix-to-add`	Defines the number or string that you want added to the front of the telephone number.
`remove-from-left`	Defines the number of digits to remove from the left of the telephone number prefix.
`remove-from-right`	Defines the number of digits to remove from the right of the telephone number prefix.
`src-pattern`	Defines the source (calling) telephone number prefix

Command	Description
	and/or suffix.
`src-trunk-group-id`	Defines the source Trunk Group for Tel-to-IP calls.
`suffix-to-add`	Defines the number or string that you want added to the end of the telephone number.
`ton {abbreviated|international-level2-regional|national-level1-regional|network-pstn-specific|not-included|subscriber-level0-regional|unknown}`	Defines the Type of Number (TON).

Command Mode

Privileged User

routing

This subcommand configures gateway routing.

Syntax

```
(config-voip)# gateway routing
```

Command	Description
`alt-route-cause-ip2tel`	See alt-route-cause-ip2tel on the next page
`alt-route-cause-tel2ip`	See alt-route-cause-tel2ip on the next page
`fwd-on-bsy-trk-dst`	See fwd-on-bsy-trk-dst on page 426
`gw-routing-policy`	See gw-routing-policy on page 427
`ip2tel-routing`	See ip2tel-routing on page 428
`settings`	See settings on page 429
`tel2ip-routing`	See tel2ip-routing on page 431

Command Mode

Privileged User

alt-route-cause-ip2tel

This command configures the Reasons for IP-to-Tel Alternative Routing table, which lets you define ISDN Q.931 release cause codes that if received from the Tel side, the device reroutes the IP-to-Tel call to an alternative Trunk Group.

Syntax

```
(config-voip)# gateway routing alt-route-cause-ip2tel <Index>
(alt-route-cause-ip2tel-<Index>)#
```

Command	Description
Index	Defines the table row index.
`rel-cause`	**Defines a Q.931 release code.**

Command Mode

Privileged User

Example

This example configures an ISDN release code 17 for alternative routing:

```
(config-voip)# gateway routing alt-route-cause-ip2tel 0
(alt-route-cause-ip2tel-0)# rel-cause 17
(alt-route-cause-ip2tel-0)# activate
```

alt-route-cause-tel2ip

This command configures the Reasons for Tel-to-IP Alternative Routing table, which lets you define SIP response codes that if received from the IP side, the device reroutes the call to an alternative destination.

Syntax

```
(config-voip)# gateway routing alt-route-cause-tel2ip <Index>
(alt-route-cause-tel2ip-<Index>)#
```

Command	Description
Index	Defines the table row index.
`rel-cause`	Defines a SIP response code.

Command Mode

Privileged User

Example

This example configures a SIP response code 406 for alternative routing:

```
(config-voip)# gateway routing alt-route-cause-ip2tel 0
(alt-route-cause-tel2ip-0)# rel-cause 406
(alt-route-cause-tel2ip-0)# activate
```

fwd-on-bsy-trk-dst

This command configures the Forward on Busy Trunk Destination table, which lets you define alternative routing rules for forwarding (i.e., call redirection) IP-to-Tel calls to an alternative IP destination using SIP 3xx responses.

Syntax

```
(config-voip)# gateway routing fwd-on-bsy-trk-dst <Index>
(fwd-on-bsy-trk-dst-<Index>)#
```

Command	Description
Index	Defines the table row index.
`forward-dst`	Defines the alternative IP destination for the call used if the Trunk Group is busy or unavailable.
`trunk-group-id`	Defines the Trunk Group ID to where the IP call is destined.

Command Mode

Privileged User

Example

This example configures 10.15.7.96 as the alternative destination for calls destined for Trunk Group 1:

```
(config-voip)# gateway routing fwd-on-bsy-trk-dst 0
(fwd-on-bsy-trk-dst-0)# forward-dst 10.15.7.96
(fwd-on-bsy-trk-dst-0)# trunk-group-id 1
(fwd-on-bsy-trk-dst-0)# activate
```

gw-routing-policy

This command configures the Routing Policies table, which lets you edit the default Routing Policy rule.

Syntax

```
(config-voip)# gateway routing gw-routing-policy <Index>
(gw-routing-policy-<Index>)#
```

Command	Description
Index	Defines the table row index.
`lcr-call-length`	Defines the average call duration (in minutes) and is used to calculate the variable portion of the call cost.
`lcr-default-cost`	Defines whether routing rules in the Tel-to-IP Routing table that are not assigned a Cost Group are considered a higher cost or lower cost route compared to other matched routing rules that are assigned Cost Groups.
`lcr-enable {disabled|enabled}`	Enables the Least Cost Routing (LCR) feature for the Routing Policy.
`ldap-srv-group-name`	Assigns an LDAP Server Group to the Routing Policy.
`name`	Defines a descriptive name, which is used when associating the row in other tables.

Command Mode

Privileged User

Example

This example configures a Routing Policy "ITSP", which uses LDAP Servers Group "ITSP-LDAP":

```
(config-voip)# gateway routing gw-routing-policy 0
(gw-routing-policy-0)# name ITSP
(gw-routing-policy-0)# ldap-srv-group-name ITSP-LDAP
(gw-routing-policy-0)# activate
```

ip2tel-routing

This command configures the IP-to-Tel Routing table, which lets you define IP-to-Tel routing rules.

Syntax

```
(config-voip)# gateway routing ip2tel-routing <Index>
(ip2tel-routing-<Index>)#
```

Command	Description
Index	Defines the table row index.
`call-setup-rules-set-id`	Assigns a Call Setup Rule Set ID to the routing rule.
`dst-host-pattern`	Defines the prefix or suffix of the called (destined) telephone number.
`dst-phone-pattern`	Defines the Request-URI host name prefix of the incoming INVITE message.
`dst-type {trunk|trunk-group}`	Defines the type of Tel destination.
`ip-profile-name`	Assigns an IP Profile to the call.
`route-name`	Defines a descriptive name, which is used when associating the row in other tables.
`src-host-pattern`	Defines the prefix of the URI host name in the From header of the incoming INVITE message.

Command	Description
`src-ip-address`	Defines the source IP address of the incoming IP call.
`src-ip-group-name`	Assigns an IP Group from where the SIP message (INVITE) is received.
`dst-phone-pattern`	Defines the prefix or suffix of the calling (source) telephone number.
`src-sip-interface-name`	Defines the SIP Interface on which the incoming IP call is received.
`trunk-group-id`	Defines the Trunk Group ID to where the incoming SIP call is sent.
`trunk-id`	Defines the Trunk to where the incoming SIP call is sent.

Command Mode

Privileged User

Example

This example configures a routing rule that routes calls from IP Group "ITSP" to Trunk Group 1:

```
(config-voip)# gateway routing ip2tel-routing 0
(ip2tel-routing-0)# name PSTN-to-ITSP
(ip2tel-routing-0)# src-ip-group-name ITSP
(ip2tel-routing-0)# trunk-group-id 1
(ip2tel-routing-0)# activate
```

settings

This command configures gateway routing parameter.

Syntax

```
(config-voip)# gateway routing settings
(gw-routing-settings)#
```

Command	Description
`alt-routing-tel2ip`	Enables Alternative Routing Tel to IP.

Command	Description
alt-rte-tel2ip-keep-alive	Time interval between OPTIONS Keep-Alive messages for IP connectivity (seconds).
alt-rte-tel2ip-mode	Methods used for Alternative Routing operation.
alt-rte-tone-duration	Alternative Routing Tone Duration (milliseconds).
empty-dst-w-bch-nb	Replace empty destination number (received from Tel side) with port number.
gw-routing-server	Enables Gateway Routing Server.
ip-dial-plan-name	Assigns a Dial Plan (by name) for tag-based IP-to-Tel routing rules.
ip-to-tel-tagging-dst	IP-to-Tel Tagging Destination Dial Plan Index.
ip-to-tel-tagging-src	IP-to-Tel Tagging Source Dial Plan Index.
ip2tel-rmv-rte-tbl	Remove prefix defined in IP to Trunk Group table (IP-to-Tel calls).
ip2tel-rte-mode	Defines order between routing incoming calls from IP side and performing manipulations.
mx-all-dly-4-alt-rte	The maximum delay that will not prevent normal routing (msec).
mx-pkt-loss-4-alt-rte	The maximum percentage of packet loss that will not prevent normal routing.
npi-n-ton-to-cld-nb	Add NPI and TON as prefix to called number.
npi-n-ton-to-cng-nb	Add NPI and TON as prefix to calling number.
probability-on-qos-problem	If QoS problem, a call has this probability (in percentage) to continue in order to reevaluate the QoS.
redir-nb-si-to-tel	Override screening indicator value of the redirect number in Setup messages to PSTN interface..
redundant-routing-m	Defines the mode of redundant routing.

Command	Description
`src-ip-addr-input`	Source IP address input.
`src-manipulation`	Describes the hdrs containing source nb after manipulation.
`tel-dial-plan-name`	Assigns a Dial Plan (by name) for tag-based IP-to-Tel routing rules.
`tel2ip-rte-mode`	Defines order between routing incoming calls from Tel side and performing manipulations.
`tgrp-routing-prec`	TGRP Routing Precedence.
`trk-id-as-prefix`	Add Trunk/Port as nb prefix.
`trkgrpid-prefix`	Add Trunk Group ID as prefix.

Command Mode

Privileged User

tel2ip-routing

This command configures the Tel-to-IP Routing table, which lets you define Tel-to-IP routing rules.

Syntax

```
(config-voip)# gateway routing tel2ip-routing <Index>
(tel2ip-routing-<Index>)#
```

Command	Description
Index	Defines the table row index.
`call-setup-rules-set-id`	Assigns a Call Setup Rule Set ID to the routing rule.
`charge-code-name`	Assigns a Charge Code to the routing rule for generating metering pulses (Advice of Charge).
`cost-group-id`	Assigns a Cost Group to the routing rule for determining the cost of the call (i.e., Least Cost Routing or LCR).

Command	Description
`dest-ip-group-name`	Assigns an IP Group to where you want to route the call.
`dest-sip-interface-name`	Assigns a SIP Interface to the routing rule.
`dst-ip-address`	Defines the IP address (in dotted-decimal notation or FQDN) to where the call is sent.
`dst-phone-pattern`	Defines the prefix and/or suffix of the called (destination) telephone number.
`dst-port`	Defines the destination port to where you want to route the call.
`forking-group`	Defines a Forking Group number for the routing rule.
`ip-profile-name`	Assigns an IP Profile to the routing rule in the outgoing direction.
`route-name`	Defines a descriptive name, which is used when associating the row in other tables.
`dst-phone-pattern`	Defines the prefix and/or suffix of the calling (source) telephone number.
`src-trunk-group-id`	Defines the Trunk Group from where the call is received.
`transport-type {not-configured|tcp|tls|udp}`	Defines the transport layer type used for routing the call.

Command Mode

Privileged User

Example

This example configures a routing rule that routes calls from Trunk Group 1 to IP Group "ITSP":

```
(config-voip)# gateway routing tel2ip-routing 0
(tel2ip-routing-0)# name ITSP-to-PSTN
(tel2ip-routing-0)# src-trunk-group-id 1
```

```
(tel2ip-routing-0)# dest-ip-group-name ITSP
(tel2ip-routing-0)# activate
```

trunk-group

This command configures the Trunk Group table, which lets you define Trunk Groups.

Syntax

```
(config-voip)# gateway trunk-group <Index>
(trunk-group-<Index>)#
```

Command	Description
Index	Defines the table row index.
`first-b-channel`	Defines the first channel/port (analog module) or Trunk B-channel (digital module).
`first-phone-number`	Defines the telephone number(s) of the channels.
`first-trunk-id`	Defines the starting physical Trunk number in the Trunk Group.
`last-b-channel`	Defines the last channel/port (analog module) or Trunk B-channel (digital module).
`last-trunk-id`	Defines the ending physical Trunk number in the Trunk Group.
`module`	Defines the telephony interface module / FXS blade for which you want to define the Trunk Group.
`tel-profile-name`	Assigns a Tel Profile to the Trunk Group.
`trunk-group-id`	Defines the Trunk Group ID for the specified channels.

Command Mode

Privileged User

Example

This example configures Trunk Group 1 for Trunk 1, channels 1-30:

```
(config-voip)# gateway trunk-group 0
(trunk-group-0)# first-b-channel 1
(trunk-group-0)# last-b-channel 30
(trunk-group-0)# first-trunk-id 1
(trunk-group-0)# trunk-group-id 1
(trunk-group-0)# activate
```

trunk-group-setting

This command configures the Trunk Group Settings table, which lets you define various settings per Trunk Group.

Syntax

```
(config-voip)# gateway trunk-group-setting <Index>
(trunk-group-setting-<Index>)#
```

Command	Description
Index	Defines the table row index.
`channel-select-mode {always-ascending|always-descending|channel-cyclic-ascending|cyclic-descending|dst-number-ascending|dst-number-cyclic-ascending|dst-phone-number|not-configured|ring-to-hunt-group|select-trunk-by-supp-serv-table|src-phone-number|trunk-channel-cyclic-ascending|trunk-cyclic-ascending}`	Defines the method by which IP-to-Tel calls are assigned to the channels of the Trunk Group.
`contact-user`	Defines the user part for the SIP Contact URI in INVITE messages, and the From, To, and Contact headers in REGISTER requests.
`dedicated-connection-mode {connection-per-endpoint|reuse-connection}`	Enables the use of a dedicated TCP socket for SIP traffic (REGISTER, re-REGISTER, SUBSCRIBE, and INVITE messages) per FXS analog channel (endpoint).

Command	Description
`gateway-name`	Defines the host name for the SIP From header in INVITE messages, and the From and To headers in REGISTER requests.
`mwi-interrogation-type {none|not-configured|result-not-used|use-activate-only|use-result}`	Defines message waiting indication (MWI) QSIG-to-IP interworking for interrogating MWI supplementary services.
`registration-mode {dont-register|not-configured|per-account|per-endpoint|per-gateway}`	Defines the registration method of the Trunk Group.
`serving-ip-group-name`	Assigns an IP Group to where the device sends INVITE messages for calls received from the Trunk Group.
`trunk-group-id`	Defines the Trunk Group ID that you want to configure.
`trunk-group-name`	Defines a descriptive name, which is used when associating the row in other tables.
`used-by-routing-server {not-used|used}`	Enables the use of the Trunk Group by a routing server for routing decisions.

Command Mode

Privileged User

Example

This example configures channel select method to ascending for Trunk Group 1:

```
(config-voip)# gateway gateway trunk-group-setting 0
(trunk-group-setting-0)# trunk-group-name PSTN
(trunk-group-0)# trunk-group-id 1
(trunk-group-0)# channel-select-mode always-ascending
(trunk-group-0)# activate
```

voice-mail-setting

This command configures the voice mail parameters.

Syntax

```
(config-voip)# gateway voice-mail-setting
(gw-voice-mail)#
```

Command	Description
`dig-to-ignore-dig-pattern`	A digit (0-9,A-D,* or #) that if received as Src (S) or Redirect (R), the digit is ignored and not added to that number. Used in DTMF VoiceMail.
`disc-call-dig-ptrn`	Disconnect call if digit string is received from the Tel side during session.
`enable-smdi {SMDI_PROTOCOL_BELCORE|SMDI_PROTOCOL_ERICSSON|SMDI_PROTOCOL_NEC_ICS|SMDI_PROTOCOL_NONE}`	Enables the Simplified Message Desk Interface (SMDI).
`ext-call-dig-ptrn`	Digit pattern to indicate external call (PBX to voice mail)
`fwd-bsy-dig-ptrn-ext`	Digit pattern to indicate Call Forward on busy (PBX to voice mail)
`fwd-bsy-dig-ptrn-int`	Digit pattern to indicate Call Forward on busy (PBX to voice mail)
`fwd-dnd-dig-ptrn-ext`	Digit pattern to indicate Call Forward on Do Not Disturb (PBX to voice mail)
`fwd-dnd-dig-ptrn-int`	Digit pattern to indicate Call Forward on Do Not Disturb (PBX to voice mail)
`fwd-no-ans-dig-ptrn-ext`	Digit pattern to indicate Call Forward on no answer (PBX to voice mail)
`fwd-no-ans-dig-ptrn-int`	Digit pattern to indicate Call Forward on no answer (PBX to

Command	Description
	voice mail)
`fwd-no-rsn-dig-ptrn-ext`	Digit pattern to indicate Call Forward with no reason (PBX to voice mail)
`fwd-no-rsn-dig-ptrn-int`	Digit pattern to indicate Call Forward with no reason (PBX to voice mail)
`int-call-dig-ptrn`	Digit pattern to indicate internal call (PBX to voice mail)
`line-transfer-mode`	Line transfer mode.
`mwi-off-dig-ptrn`	Digit pattern to notify PBX about no messages waiting for extension (added as prefix)
`mwi-on-dig-ptrn`	Digit pattern to notify PBX about messages waiting for extension (added as prefix)
`mwi-source-number`	Phone number sent as source number toward PSTN for MWI setup.
`mwi-suffix-pattern`	MWI suffix code to notify PBX about messages waiting for extension (added as suffix to the extension number)
`smdi-timeout`	SMDI timeout.
`vm-interface {dtmf|etsi|ip2ip|ni2|none|qsig|qsig-matra| qsig-siemens|setup-only|smdi}`	Method of communication between PBX and the device that is used instead of legacy voicemail.

Command Mode

Privileged User

Example

```
(config-voip)# gateway voice-mail-setting
(gw-voice-mail)# vm-interface dtmf
(gw-voice-mail)# activate
```

89 coders-and-profiles

This command configures coders and profiles.

Syntax

```
(config-voip)# coders-and-profiles
```

Command	Description
`allowed-audio-coders-groups`	See allowed-audio-coders-groups below
`allowed-video-coders-groups`	See allowed-video-coders-groups on page 441
`audio-coders-groups`	See audio-coders-groups on page 442
`ip-profile`	See ip-profile on page 444
`tel-profile`	See tel-profile on page 463

allowed-audio-coders-groups

This command configures the Allowed Audio Coders Groups table, which lets you define Allowed Audio Coders Groups **for SBC calls**. The table is a "parent" of the Allowed Audio Coders table.

Syntax

```
(config-voip)# coders-and-profiles allowed-audio-coders-groups <Index>
(allowed-audio-coders-groups-<Index>)#
```

Command	Description
Index	Defines the table row index.
`allowed-audio-coders`	Defines the Allowed Audio Coders table. For more information, see allowed-audio-coders on the next page.
`coders-group-name`	Defines a name for the Allowed Audio Coders Group.

Command Mode

Privileged User

Example

This example configures the name "ITSP" for the Allowed Audio Coders Group:

```
(config-voip)# coders-and-profiles allowed-audio-coders-groups 0
(allowed-audio-coders-groups-0)# coders-group-name ITSP
(allowed-audio-coders-groups-0)# activate
```

allowed-audio-coders

This command configures the Allowed Audio Coders table, which lets you define Allowed Audio Coders **for SBC calls**. The table is a "child" of the Allowed Audio Coders Groups table.

Syntax

```
(config-voip)# coders-and-profiles allowed-audio-coders-groups <Index>
(allowed-audio-coders-groups-<Index>)# allowed-audio-coders <Index>
(allowed-audio-coders-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`coder`	Defines a coder from a list.
`user-defined-coder`	Defines a user-defined coder.

Command Mode

Privileged User

Example

This example configures the Allowed Audio Coders table with G.711:

```
(config-voip)# coders-and-profiles allowed-audio-coders-groups 0
(allowed-audio-coders-groups-0)# allowed-audio-coders 1
(allowed-audio-coders-0/1)# coder g711-alaw
(allowed-audio-coders-0/1)# activate
```

allowed-video-coders-groups

This command configures the Allowed Video Coders Groups table, which lets you define Allowed Video Coders Groups **for SBC calls**. The table is a "parent" of the Allowed Video Coders table.

Syntax

```
(config-voip)# coders-and-profiles allowed-video-coders-groups <Index>
(allowed-video-coders-groups-<Index>)#
```

Command	Description
Index	Defines the table row index.
`allowed-video-coders`	
`coders-group-name`	Defines a name for the Allowed Video Coders Group.

Command Mode

Privileged User

Example

This example configures the name "ITSP" for the Allowed Video Coders Group:

```
(config-voip)# coders-and-profiles allowed-video-coders-groups 0
(allowed-video-coders-groups-0)# coders-group-name ITSP
(allowed-video-coders-groups-0)# activate
```

allowed-video-coders

This command configures the Allowed Video Coders table, which lets you define Allowed video coders **for SBC calls**. The table is a "child" of the Allowed Video Coders Groups table.

Syntax

```
(config-voip)# coders-and-profiles allowed-video-coders-groups <Index>
(allowed-video-coders-groups-<Index>)# allowed-video-coders <Index>
(allowed-video-coders-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`user-defined-coder`	Defines a user-defined video coder.

Command Mode

Privileged User

Example

This example configures the Allowed Video Coders table with G.711:

```
(config-voip)# coders-and-profiles allowed-video-coders-groups 0
(allowed-video-coders-groups-0)# allowed-video-coders 1
(allowed-video-coders-0/1)# user-defined-coder mpeg2
(allowed-video-coders-0/1)# activate
```

audio-coders-groups

This command configures the Coders Groups table, which lets you define Coder Groups. The table is the parent of the Coders table.

Syntax

```
(config-voip)# coders-and-profiles audio-coders-groups <Index>
(audio-coders-groups-<Index>)#
```

Command	Description
Index	Defines the table row index.
`audio-coders`	Defines coders in the Coders table for the Coder Group. For more information, see audio-coders on the next page.
`coders-group-name`	Defines a name for the Coder Group.

Command Mode

Privileged User

Example

This example configures the name "ITSP" for the Coders Groups table:

```
(config-voip)# coders-and-profiles audio-coders-groups 0
(audio-coders-groups-0)# coders-group-name ITSP
(audio-coders-groups-0)# activate
```

audio-coders

This command configures the Coder table, which lets you define coders per Coder Group. The table is a child of the Coders Groups table.

Syntax

```
(config-voip)# coders-and-profiles audio-coders-groups <Index>
(audio-coders-groups-<Index>)# audio-coders <Index>
(audio-coders-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`coder-specific`	Defines additional settings specific to the coder.
`name`	Defines the coder type.
`p-time`	Defines the packetization time (in msec) of the coder.
`payload-type`	Defines the payload type if the payload type (i.e., format of the RTP payload) of the coder is dynamic.
`rate`	Defines the bit rate (in kbps) of the coder.
`silence-suppression {disable|enable|enable-no-adaptation|not-configured}`	Enables silence suppression for the coder.

Command Mode

Privileged User

Example

This example configures the Coders table with G.711 for Coder Group 0:

```
(config-voip)# coders-and-profiles audio-coders-groups 0
(audio-coders-groups-0)# audio-coders 1
(audio-coders-0/1)# name g711-alaw
(audio-coders-0/1)# rate 64
(audio-coders-0/1)# p-time 20
(audio-coders-0/1)# silence-suppression enable
(audio-coders-0/1)# activate
```

ip-profile

This command configures the IP Profiles table, which lets you define IP Profiles.

Syntax

```
(config-voip)# coders-and-profiles ip-profile <Index
(ip-profile-<Index>)#
```

Command	Description
Index	Defines the table row index.
`add-ie-in-setup`	Configures an additional information element to send in ISDN Setup message.
`allowed-audio-coders-group-name`	Defines the SBC Allowed Audio Coders Group Name (this references a table that contains a list of allowed audio coders).
`allowed-video-coders-group-name`	Defines the SBC Allowed Video Coders Group

Command	Description
	Name (this references a table that contains a list of allowed video coders).
`amd-max-greeting-time`	Defines the AMD Max Greeting Time.
`amd-max-post-silence-greeting-time`	Defines the AMD Max Post Silence Greeting Time.
`amd-mode {dont-disconnect|disconnect-on-amd}`	Defines the AMD (Answering Machine Detector) mode.
`amd-sensitivity-level`	Defines the AMD level of detection sensitivity.
`amd-sensitivity-parameter-suite`	Defines the serial number of the AMD sensitivity suite.
`bfcp-ip-from-audio {according-to-global-parameter|disable|enable}`	Enables the handling of calls with voice and Binary Floor Control Protocol (BFCP) media streams that are received from behind a NAT.
`call-limit`	Defines the maximum number of concurrent calls per IP Profile.

Command	Description
`cng-mode {disable|t38-relay|events-only}`	Defines the CNG Detector Mode.
`coders-group`	Defines the Coders Group Name.
`copy-dst-to-redirect-number {after-manipulation|before-manipulation|disable}`	Enables the device to copy the called number, received in the SIP INVITE message, to the redirect number in the outgoing Q.931 Setup message, for IP-to-Tel calls.
`crypto-suites-group`	Assigns an SBC Crypto Suite Group to the IP Profile, which defines the supported SRTP crypto suites.
`data-diffserv`	Defines the DiffServ value of MSRP traffic in the IP header's DSCP field.
`disconnect-on-broken-connection {ignore|disable|disconnect|yes|reroute|reroute-with-original-sip-headers}`	Defines the behavior when receiving an RTP or MSRP broken notification.
`disconnect-on-broken-signaling-connection {ignore|disconnect|reroute|reroute-with-original-sip-headers}`	Defines the handling of established calls when the device detects a

Command	Description
	disconnection in the associated SIP signaling path (socket).
`disconnect-in-dialog-subscribe-failure {enable|disable}`	Defines if the device ends the call if a subscription request (SIP SUBSCRIBE) sent during the call (in-dialog) fails.
`early-answer-timeout`	Defines the maximum time (in seconds) to wait from sending a setup message to the PSTN to receiving a connect message from the PSTN.
`early-media {enable|disable}`	Enables Early Media.
`echo-canceller {disable|line|acoustic}`	Enables echo cancellation (i.e., echo from voice calls is removed).
`enable-early-183 {enable|disable}`	Enables Early 183.
`enable-hold {enable|disable}`	Enables Call Hold service.
`enable-qsig-tunneling`	Enables QSIG Tunneling over SIP.
`enable-symmetric-mki`	Enables

Command	Description
	symmetric MKI negotiation.
`fax-sig-method {no-fax|t.38-relay|g.711-transport| fax-fallback|g.711-reject-t.38}`	Defines the SIP signaling method for establishing and transmitting a fax session when the device detects a fax.
`first-tx-dtmf-option`	Defines the first priority DTMF methods, offered during the SIP negotiation.
`generate-srtp-keys {only-if-required|always|keep-original}`	Enables the device to generate (or not) a new SRTP key upon receipt of a re-INVITE from the SIP UA associated with the IP Profile.
`header-for-transfer {none|remote-party-id}`	Enables the device to add a SIP Remote-Party-ID header to outgoing SIP messages (e.g., INVITE, UPDATE, or 200 OK) when handling call transfers.
`ice-mode {disable|lite|full}`	Enables ICE.
`input-gain`	Defines the voice TDM Input Gain.
`ip-preference`	Configures Profile

Command	Description
	Preference - the priority of the IP Profile.
`is-dtmf-used {enable|disable}`	Enables sending DTMFs on the Signaling path (not on the Media path).
`jitter-buffer-max-delay`	Defines the maximum delay (in msec) for the Dynamic Jitter Buffer.
`jitter-buffer-minimum-delay`	Defines the minimum delay (in msec) for the Dynamic Jitter Buffer.
`jitter-buffer-optimization-factor`	Defines the Dynamic Jitter Buffer frame error-delay optimization factor.
`local-held-tone-index`	Defines the user-defined Held tone by index number as it appears in the PRT file.
`local-ringback-tone-index`	Defines the user-defined ringback tone by index number as it appears in the PRT file.
`media-ip-version-preference {only-ipv4|only-`	Defines the

Command	Description
`ipv6|prefer-ipv4|prefer-ipv6}`	preference of the Media IP version.
`media-security-behaviour {as-is|secured|srtp|not-secured|rtp| both|offer-both-answer-prefer-secured}`	Defines the gateway behavior when receiving offer/response for media encryption.
`mki-size`	Defines the size (in bytes) of the Master Key Identifier (MKI) in transmitted SRTP packets. The
`nse-mode {enable|disable}`	Enables Cisco compatible fax and modem bypass mode.
`play-held-tone`	Defines the SBC Play Held Tone.
`play-rbt-to-ip {dont-play|play}`	Enables a ringback tone playing towards IP.
`profile-name`	Configures a Profile Name (string).
`prog-ind-to-ip {not-configured|no-pi|pi-is-1|pi-is-8}`	Determines whether to send the Progress Indicator to IP.
`reliable-heldtone-source {enable|disable}`	Defines the SBC Reliable Held Tone Source.
`remote-hold-Format {transparent|sendonly|sendonlyzeroip|inactive|`	Defines the SBC Remote Hold

Command	Description
`inactivezeroip|notsupported|holdandretrievenotsupported}`	Format.
`reset-srtp-upon-re-key {enable|disable}`	Resets SRTP State Upon Re-key.
`rtcp-encryption {as-is|active|inactive}`	Defines the encryption of RTCP packets (i.e., SRTCP).
`rtp-ip-diffserv`	Defines the DiffServ for RTP audio (and media if `rtp-video-diffserv` not defined).
`rtp-redundancy-depth {enable|disable}`	Defines the RTP Redundancy Depth - enables the device to generate RFC 2198 redundant packets.
`rtp-video-diffserv`	Defines the DiffServ for RTP video.
`rx-dtmf-option {supported|not-supported}`	Defines the supported receive DTMF negotiation method.
`sbc-2833dtmf-payload`	Defines the SBC RFC2833 DTMF Payload Type Value.
`sbc-adapt-rfc2833-bw-voice-bw {enable|disable}`	Adapts RFC 2833 BW to Voice coder BW.

Command	Description
`sbc-allow-only-negotiated-pt {disable|enable}`	Enables the device to allow only media (RTP) packets, from the UA associated with this IP Profile, using the single coder (payload type) that was negotiated during the SDP offer/answer exchange.
`sbc-allowed-coders-mode {restriction|preference|restriction-and-preference}`	Defines the SBC Allowed Coders Mode.
`sbc-allowed-media-types`	Defines the SBC allowed media types (comma separated string).
`sbc-alternative-dtmf-method {as-is|http|in-band|info-cisco| info-nortel|info-lucent|http}`	Defines the SBC Alternative DTMF Method. For legs where RFC 2833 is not negotiated successfully, the device uses this parameter to determine the Alternative DTMF Method.
`sbc-assert-identity {as-is|add|remove}`	Defines the device's privacy handling of the P-asserted-Identity header. This indicates how the outgoing SIP message asserts

Command	Description
	identity.
`sbc-diversion-mode {as-is|add|remove}`	Defines the device's handling of the Diversion header.
`sbc-dm-tag`	Defines the tag to work without media anchoring.
`sbc-enforce-mki-size`	Defines SBC Enforce MKI Size.
`sbc-enhanced-plc {disable|enable}`	Enables PLC.
`sbc-ext-coders-group-name`	Defines the SBC Extension Coders Group Name.
`sbc-fax-answer-mode {all-coders|single-coder}`	Defines the coders included in the outgoing SDP answer (sent to the calling fax).
`sbc-fax-behavior {as-is|handle-always|handle-on-re-invite}`	Defines the offer negotiation method.
`sbc-fax-coders-group-name`	Defines the supported fax coders.
`sbc-fax-offer-mode {all-coders|single-coder}`	Defines if the fax coders sent in the outgoing SDP offer.
`sbc-fax-rerouting-mode {disable|rerouting-without_delay}`	Enables the re-routing of incoming SBC calls that are identified as fax calls.

Command	Description
`sbc-generate-noop {disable|enable}`	Enables the device to send RTP or T.38 No-Op packets during RTP or T.38 silence periods (SBC calls only).
`sbc-generate-rtp {none|until-rtp-detected}`	Generates silence RTP packets.
`sbc-handle-xdetect {not-supported|handle}`	Defines the support of X-Detect handling.
`sbc-history-info-mode {not-configured|as-is|add|remove}`	Defines the device's handling of the History-Info header.
`sbc-isup-body-handling {transparent|remove|create|create-if-not-exists}`	Defines the ISUP Body Handling.
`sbc-isup-variant {itu92|spirou}`	Defines the ISUP Variant.
`sbc-jitter-compensation {disable|enable}`	Defines the SBC Jitter Compensation.
`sbc-keep-routing-headers {according-to-mode|disable|enable}`	Keeps the Record-Route and in-dialog Route headers from incoming request in the outgoing request.
`sbc-keep-user-agent {according-to-mode|disable|enable}`	Keeps the User-Agent header from the incoming request

Command	Description
	in the outgoing request.
`sbc-keep-via-headers {according-to-mode|disable|enable}`	Keeps the VIA headers from incoming request in the outgoing request.
`sbc-max-call-duration`	Limits the call time duration (minutes).
`sbc-max-opus-bandwidth`	Defines the maximum bandwidth for OPUS [bps].
`sbc-media-security-behaviour {as-is|secured|srtp| not-secured|rtp|both|offer-both-answer-prefer-secured}`	Defines the transcoding method between SRTP and RTP.
`sbc-media-security-method {sdes|dtls|both}`	Defines the SRTP method SDES/DTLS.
`sbc-msrp-empty-message-format {default|with-content-type}`	On an active MSRP leg, enables the device to add the Content-Type header to the first empty (i.e., no body) MSRP message that is used to initiate the MSRP connection.
`sbc-msrp-offer-setup-role {active|passive|actpass}`	Defines the device's MSRP role in SDP offer-answer

Command	Description
	negotiations ('a=setup' line) for MSRP sessions.
`sbc-msrp-re-invite-update-supp {not-supported|supported}`	Defines if the SIP UA (MSRP endpoint) associated with this IP Profile supports the receipt of re-INVITE and UPDATE SIP messages.
`sbc-multi-answers {disable|enable}`	Enables the SBC to respond with multiple answers within the same dialog (non-standard).
`sbc-multi-early-diag {according-to-mode|disable|enable}`	Enables the SBC to respond with multiple SIP dialogs (forking).
`sbc-play-rbt-to-transferee {disable|enable}`	Plays Ring Back Tone to transferred side on call transfer.
`sbc-prack-mode {disabled|optional|mandatory|transparent|optional-with-adaptations}`	Defines the LEG's related PRACK behavior.
`sbc-precondition {not-supported|supported}`	Defines if the UA associated with this IP Profile supports SIP session preconditions according to RFC

Command	Description
	3312.
`sbc-preferred-ptime`	Defines the SBC Preferred Ptime.
`sbc-receive-multiple-dtmf-methods {disable|enable}`	Enables the device to receive DTMF digits out-of-band (not with audio stream) using both the SIP INFO and RFC 2833 methods.
`sbc-rfc2833-behavior {as-is|extend|disallow}`	Affects the RFC 2833 SDP offer/answer negotiation.
`sbc-remove-csrc {disable|enable}`	Enables the device to remove the contributing source (CSRC) identifiers (CC field) from the RTP header in RTP packets.
`sbc-remove-extmap {disable|enable}`	Enables the device to remove the 'a=extmap' SDP line in outgoing SIP-initiating INVITE requests.
`sbc-renumber-mid {disable|enable}`	Enables the device to change the value of the 'a=mid:n' attribute (where *n* is a unique value) to 0 (or next consecutive

Command	Description
	number), if it is present in the outgoing SDP offer.
`sbc-rmt-3xx-behavior {transparent|db-url|handle-locally| ip-group-name|local-host}`	Defines the SBC Remote 3xx Behavior.
`sbc-rmt-can-play-ringback {disable|enable}`	Configures remote endpoint capability to play a local ringback tone.
`sbc-rmt-delayed-offer {not-supported|supported}`	Configures SBC remote delayed offer support.
`sbc-rmt-early-media-resp {transparent|180|183}`	Defines the SBC remote early media response type.
`sbc-rmt-early-media-rtp {by-signaling|immediate| by-media|delayed}`	Defines the SBC remote early media RTP mode.
`sbc-rmt-early-media-supp {not-supported|supported}`	Defines SBC remote early media support.
`sbc-rmt-mltple-18x-supp {not-supported|supported}`	Defines SBC remote multiple 18x support.
`sbc-msrp-re-invite-update-supp {not-supported|supported}`	Defines if the remote MSRP endpoint supports the receipt of re-INVITE and UPDATE SIP messages.

Command	Description
`sbc-rmt-re-invite-supp {not-supported|supported-only-with-sdp|supported}`	Defines SBC remote re-INVITE support.
`sbc-rmt-refer-behavior {regular|db-url|handle-locally|ip-group-name| local-host|keep-uri|keep-host}`	Defines SBC remote refer behavior.
`sbc-rmt-renegotiate-on-fax-detect {transparent| only-in-answer-side|no}`	Defines if remote renegotiate when fax is detected.
`sbc-rmt-replaces-behavior {standard|handle-locally|keep-as-is}`	Defines how the SBC manages REFER/INVITE with Replaces.
`sbc-rmt-rfc3960-supp {not-supported|supported}`	Defines the SBC remote RFC 3960 gateway model support.
`sbc-rmt-rprsntation {according-to-mode| replace-contact|add-routing-headers|transparent}`	Defines how to represent the SBC's contact information to the remote side.
`sbc-rmt-update-supp {not-supported| supported-only-after-connect|supported|acc-remote-allow}`	Defines SBC remote UPDATE support.
`sbc-rtcp-feedback {feedback-off|feedback-on|as-is}`	Defines RTCP feedback support.
`sbc-rtcp-mode {transparent|generate-always|generate-only-if-rtp-active}`	Defines the SBC RTCP mode.
`sbc-rtcp-mux {not-supported|supported}`	Defines support of RTP-RTCP multiplexing.
`sbc-rtp-red-behav {as-is|enable|extend| disable|disallow}`	Defines SBC RTP redundancy

Command	Description
	behavior.
`sbc-sdp-handle-rtcp {dont-care|add|remove}`	Defines SBC SDP Handle RTCP.
`sbc-sdp-ptime-ans {remote-ans|orig-offer|pref-val}`	Defines SBC SDP Ptime answer.
`sbc-sdp-remove-crypto-lifetime {not-remove|remove}`	Defines SBC SDP Remove Crypto Lifetime.
`sbc-send-multiple-dtmf-methods {disable|enable}`	Enables the device to send DTMF digits out-of-band (not with audio stream) using both the SIP INFO and RFC 2833 methods for the same call on the leg to which this IP Profile is associated.
`sbc-session-expires-mode {transparent|observer|supported|not-supported}`	Defines SBC behavior with 'Session-Expires' header.
`sbc-use-silence-supp {transparent|add|remove}`	Defines SBC to use Silence Suppression.
`sbc-usr-reg-time`	Defines the duration (in seconds) of the periodic registrations between the user and the device (the device responds with this value to the

Command	Description
	user).
`sbc-usr-tcp-nat-reg-time`	Defines the duration (in seconds) of the periodic registrations between the user and the device when the user registers over TCP and is behind NAT.
`sbc-usr-udp-nat-reg-time`	Defines the duration (in seconds) of the periodic registrations between the user and the device when the user registers over UDP and is behind NAT.
`sbc-voice-quality-enhancement {disable|enable}`	Activates Voice Quality Enhancement.
`sdp-origin-same-session-ver {handle-all|handle-only-first}`	Defines which SDPs in incoming SIP responses to SIP dialog-initiating INVITE requests are processed by the device.
`second-tx-dtmf-option {not-set|not-supported|info-nortel|info-notify|info-cisco|rfc2833|info-korea}`	Defines the second priority DTMF methods, offered during the SIP

Command	Description
	negotiation.
`signaling-diffserv`	Defines the SIP Signaling DiffServ.
`switch-coder-upon-voice-quality {disable|enable}`	Enables the device to detect poor voice quality during a call for an unregistered user, and then change IP Profiles to switch between the G.711 and Opus coders.
`transcoding-mode {only-if-required|rtp-mediation|force-transcoding|rtp-forwarding}`	Defines the voice transcoding mode between the two SBC legs for the SBC application.
`used-by-routing-server {not-used| used}`	Enables the IP Profile to be used by a third-party routing server for call routing decisions.
`voice-volume`	Defines the voice TDM output gain.
`vxx-transport-type {not-configured|disable|enable-bypass|events-only}`	Defines the Vxx modem transport type.

Command Mode

Privileged User

Example

This example shows how to configure an IP Profile:

```
(config-voip)# coders-and-profiles ip-profile 0
(ip-profile-0)# group-name ITSP
(ip-profile-0)# activate
```

tel-profile

This command configures the Tel Profiles table, which lets you define Tel Profiles.

Syntax

```
(config-voip)# coders-and-profiles tel-profile <Index>
(tel-profile-<Index>)#
```

Command	Description
Index	Defines the table row index.
`call-priority-mode`	Defines the call priority mode.
`coders-group`	Defines the coders group name.
`current-disconnect`	Enables current disconnect.
`dial-plan-index`	Defines the dial plan index.
`digit-delivery`	Enables automatic digit delivery to the Tel side after the line is off-hooked or seized.
`digital-cut-through`	Enables a call connection without the On-Hook/Off-Hook process 'Cut-Through'.
`disconnect-on-busy-tone`	Releases the call if the gateway receives a busy or fast busy tone before the call is answered.
`dtmf-volume`	Defines the DTMF generation volume.
`early-media`	Enables early media.
`echo-canceller`	Enables echo cancellation (i.e., echo from voice calls is removed).

Command	Description
`echo-canceller-nlp-mode`	Configures EC NLP mode.
`enable-911-psap`	Enables 911 PSAP.
`enable-agc`	Activates AGC (Automatic Gain Control).
`enable-did-wink`	Enables support for DID lines using Wink.
`enable-voice-mail-delay`	Enables voice mail delay.
`fax-sig-method {no-fax|t.38-relay|g.711-transport| fax-fallback|g.711-reject-t.38}`	Defines the SIP signaling method for establishing and transmitting a fax session when the device detects a fax.
`flash-hook-period`	Defines the flashhook detection and generation period (in msec).
`fxo-consult-call-transfer {disable|enable}`	Enables support for FXO consultative call transfers (initiated by PSAP operators) for emergency (NG9-1-1) calls, based on the NENA i3 Standard for Next Generation 9-1-1 (NENA-STA-010.2-2016).
`fxo-double-answer`	Enables FXO double answer. All incoming TEL2IP call are refused.
`fxo-ring-timeout`	Defines the delay (in 100 msec) for generating an INVITE after RING_START is detected.
`input-gain`	Defines the TDM input gain.
`ip2tel-cutthrough_call_behavior`	Enables a call connection without an On-Hook/Off-Hook process.
`is-two-stage-dial`	Configures Dialing Mode - One-Stage (PBX Pass-thru) or Two-Stage.
`jitter-buffer-maximum-delay`	Defines the maximum delay (in msec) for the Dynamic Jitter Buffer.
`jitter-buffer-minimum-delay`	Defines the minimum delay (in msec) for the Dynamic Jitter Buffer.

Command	Description
`jitter-buffer-optimization-factor`	Defines the Dynamic Jitter Buffer frame error-delay optimization factor.
`mwi-analog-lamp`	Enables MWI support using an analog lamp (110 Volt).
`mwi-display`	Enables MWI support using Caller ID interface.
`mwi-ntf-timeout`	Defines the maximum duration (timeout) that a message waiting indication (MWI) is displayed on endpoint equipment (phones' LED, screen notification or voice tone).
`play-bsy-tone-2tel`	Configures Don't play, Play Busy or Reorder tone when disconnecting ISDN call and Send PI=8, Play before disconnect.
`polarity-rvrsl`	Enables Polarity Reversal.
`profile-name`	Defines the Profile Name (string).
`prog-ind-to-ip`	Determines whether to send the Progress Indicator to IP.
`rtp-ip-diffserv`	Defines the RTP IP DiffServ.
`signaling-diffserv`	Defines the SIP Signaling DiffServ.
`swap-teltoip-phone-numbers`	Swaps Tel to IP phone numbers.
`tel-preference`	Defines the Profile Preference - the priority of the Tel Profile.
`time-for-reorder-tone`	Defines the duration of the reorder tone that plays before the FXO releases the line [seconds].
`voice-volume`	Defines the voice TDM output gain.

Command Mode

Privileged User

Example

This example configures a Tel Profile:

```
(config-voip)# coders-and-profiles tel-profile 0
(tel-profile-0)# profile-name PSTN
(tel-profile-0)# activate
```

90 ids

This command configures the Intrusion Detection System (IDS) feature, which detects malicious attacks on the device and reacts accordingly.

Syntax

```
(config-voip)# ids
```

Command	Description
`global-parameters`	See global-parameters below
`match`	See match on the next page
`policy`	See policy on page 469

Command Mode

Privileged User

global-parameters

This command configures various IDS parameters.

Syntax

```
(config-voip)# ids global-parameters
(sip-security-ids-settings)#
```

Command	Description
`alarm-clear-period`	Defines the interval (in seconds) after which an IDS alarm is cleared from the Active Alarms table if no thresholds are crossed during this time.
`enable-ids {off|on}`	Enables the IDS feature.
`excluded-responses`	Defines the SIP response codes that are excluded form the IDS count for SIP dialog establishment failures.

Command Mode

Privileged User

Example

This example enables IDS:

```
(config-voip)# ids global-parameters
(sip-security-ids-settings)# enable-ids on
```

match

This command configures the IDS Matches table, which lets you implement your configured IDS Policies.

Syntax

```
(config-voip)# ids match <Index>
(match-<Index>)#
```

Command	Description
Index	Defines the table row index.
`policy`	Assigns an IDS Policy.
`proxy-set`	Assigns a Proxy Set(s) to the IDS Policy.
`sip-interface`	Assigns a SIP Interface(s) to the IDS Policy.
`subnet`	Defines the subnet to which the IDS Policy is assigned.

Command Mode

Privileged User

Example

This example configures an IDS Match that applies IDS Policy "DOS" to SIP Interfaces 1 through 2:

```
(config-voip)# ids match 0
(match-0)# policy DOS
(match-0)# sip-interface 1-2
(match-0)# activate
```

policy

This command configures the IDS Policies table, which lets you define IDS Policies. The table is a parent of the IDS Rule table.

Syntax

```
(config-voip)# ids policy <Index>
(policy-<Index>)#
```

Command	Description
Index	Defines the table row index.
`description`	Defines a brief description for the IDS Policy.
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`rule`	Defines the IDS Rule table, which lets you define IDS rules per IDS Policy. The table is a child of the IDS Policies table. For more information, see rule below.

Command Mode

Privileged User

Example

This example configures Trunk Group 1 for Trunk 1, channels 1-30:

```
(config-voip)# ids policy 0
(policy-0)# name DOS
(policy-0)# activate
```

rule

This command configures the IDS Rule table, which lets you define IDS rules. The table is a child of the IDS Policies table.

Syntax

```
(config-voip)# ids policy <Index>
(policy-<Index>)# ids rule <Index>
(rule-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`critical-alrm-thr`	Defines the threshold that if crossed a critical severity alarm is sent.
`deny-period`	Defines the duration (in sec) to keep the attacker on the blacklist, if configured using deny-thr.
`deny-thr`	Defines the threshold that if crossed, the device blocks (blacklists) the remote host (attacker).
`major-alrm-thr`	Defines the threshold that if crossed a major severity alarm is sent.
`minor-alrm-thr`	Defines the threshold that if crossed a minor severity alarm is sent.
`reason {abnormal-flow|any|auth-failure|connection-abuse|establish-fail|malformed-msg}`	Defines the type of intrusion attack.
`threshold-scope {global |ip|ip-port}`	Defines the source of the attacker to consider in the device's detection count.
`threshold-window`	Defines the threshold interval (in seconds) during which the device counts the attacks to check if a threshold is crossed.

Command Mode

Privileged User

Example

This example configures this IDS policy rule: If 15 malformed SIP messages are received within a period of 30 seconds, a minor alarm is sent. Every 30 seconds, the rule’s counters are cleared. If more than 25 malformed SIP messages are received within this period, the device blacklists for 60 seconds the remote IP host from where the messages were received:

```
(config-voip)# ids policy 0
(policy-0)# ids rule 1
(rule-0/1)# reason malformed-msg
(rule-0/1)# threshold-scope ip
(rule-0/1)# threshold-window 30
(rule-0/1)# deny-thr 25
(rule-0/1)# deny-period 60
(rule-0/1)# minor-alrm-thr 15
(rule-0/1)# major-alrm-thr 20
(rule-0/1)# critical-alrm-thr 25
(rule-0/1)# activate
```

91 interface

This command configures the PSTN interfaces.

Syntax

```
(config-voip)# interface
```

Command	Description
bri	See bri below
e1-t1	See e1-t1 on page 475
fxs-fxo	See fxs-fxo on page 479

Command Mode

Privileged User

bri

This command configures BRI interfaces.

Syntax

```
(config-voip)# interface bri <Slot (Module)/Port>
(bri <Slot/Port>)#
```

Command	Description
b-channel-nego-for-trunk {any| exclusive| not-set | preferred}	ISDN B-Channel negotiation mode for the trunk.
call-re-rte-mode	Call Rerouting Mode for Trunk.
clock-priority	Sets the trunk priority for auto-clock fallback.
dig-oos-behavior	Setting Digital OOS Behavior

Command	Description
`isdn-bits-cc-behavior`	Sets the ISDN Call Control Layer (Layer 4) behavior options.
`isdn-bits-incoming-calls-behavior`	Sets the ISDN incoming calls behavior options.
`isdn-bits-ns-behavior`	Sets the ISDN Network Layer (Layer 3) behavior options.
`isdn-bits-ns-extension-behavior`	Sets additional ISDN Network Layer (Layer 3) behavior options.
`isdn-bits-outgoing-calls-behavior`	Sets the ISDN outgoing calls behavior options.
`isdn-layer2-mode`	Sets the ISDN layer2 mode.
`isdn-termination-side`	Sets the ISDN termination side.
`isdn-xfer-cab`	Send transfer capability to ISDN side on setup message.
`local-isdn-rbt-src`	If the ringback tone source is not IP, who should supply the Ringback tone.
`ovrlp-rcving-type`	Select reception type of overlap dialing from ISDN side
`pi-in-rx-disc-msg`	Configure PIForDisconnectMsg to overwrite PI value received in ISDN Disconnect message
`pi-to-isdn`	Override the value of progress indicator to ISDN side in ALERT, PROGRESS,

Command	Description
	and PROCEEDING messages
`play-rbt-to-trk`	Enable ringback tone playing towards trunk side.
`port-info`	Defines a descriptive name for the port.
`protocol`	Sets the PSTN protocol to be used for this trunk.
`pstn-alrt-timeout`	Max time (in seconds) to wait for connect from PSTN
`rmv-calling-name`	Remove Calling Name For Trunk.
`tei-assign-trigger`	Bit-field defines when TEI assignment procedure is invoked
`tei-config-p2mp`	TEI value for P2MP BRI trunk.
`tei-config-p2p`	TEI value for P2P BRI trunk.
`tei-remove-trigger`	Bit-field defines when TEI should be removed.
`trace-level {full-isdn| full-isdn-with-duplications| layer3| layer3-no-duplications| no-trace| q921-raw-data| q931| q931-q921-raw-data| q931-raw-data}`	Defines the BRI trunk trace level. **Note:** ■ To configure and start a PSTN trace per trunk, use the following command: `configure troubleshoot > logging logging-filters`

Command	Description
	■ To start a PSTN trace for all trunks configured with the **trace-level** command option, use the following command: `debug debug-recording <IP Address> pstn-trace` ■ To send PSTN traces to a Syslog server (instead of Wireshark), use the following command: `configure troubleshoot > pstn-debug`
`trk-xfer-mode-type`	Type of transfer the PSTN/PBX supports.

Command Mode

Privileged User

Example

This example configures BRI to NI2 ISDN protocol type (51):

```
(config-voip)# interface bri 2/1
(bri 2/1)# protocol 51
(bri 2/1)# activate
```

e1-t1

This command configures E1/T1 interfaces.

Syntax

```
(config-voip)# interface e1-t1 <Trunk ID|Slot (Module)/Port>
(e1-t1 <Trunk ID | Slot/Port>)#
```

Command	Description
`b-channel-nego-for-trunk {any|exclusive| not-set|preferred}`	ISDN B-Channel negotiation mode for the trunk.
`call-re-rte-mode`	Call Rerouting Mode for Trunk.
`cas-channel-index`	Defines the CAS Protocol Table index per channel.
`cas-delimiters-types`	Defines the digits string delimiter padding usage for the specific trunk.
`cas-dial-plan-name`	Defines the Dial Plan name that will be used on the specific trunk.
`cas-table-index`	Indicates the CAS Protocol file to be used on the specific Trunk.
`clock-master`	Defines the trunk clock source.
`clock-priority`	Defines the trunk priority for auto-clock fallback.
`dig-oos-behavior`	Defines Digital OOS Behavior
`framing`	Defines the physical framing method to be used for this trunk.
`isdn-bits-cc-behavior`	Defines the ISDN Call Control Layer (Layer 4) behavior options.
`isdn-bits-incoming-calls-behavior`	Defines the ISDN incoming calls behavior options.
`isdn-bits-ns-behavior`	Defines the ISDN Network Layer (Layer 3) behavior options.
`isdn-bits-ns-extension-behavior`	Sets additional ISDN Network Layer (Layer 3) behavior options.
`isdn-bits-outgoing-calls-behavior`	Sets the ISDN outgoing calls behavior options.

Command	Description
isdn-channel-id-format-for-trunk	Defines the channel number format (number or slotmap) in the Channel Identification IE when sending Q.931 ISDN messages, per trunk.
isdn-japan-ntt-timer-t305	Defines a timeout (in seconds) that the device waits before sending an ISDN Release message after it has sent a Disconnect message, if no SIP message (e.g., 4xx response) is received within the timeout.
isdn-nfas-dchannel-type	Defines the ISDN NFAS D-channel type.
isdn-nfas-group-number	Defines the group number of the ISDN NFAS group.
isdn-nfas-interface-id	Defines the ISDN NFAS Interface ID. Applicable only if the NS_EXPLICIT_INTERFACE_ID behavior bit is set.
isdn-termination-side	Defines the ISDN termination side.
isdn-xfer-cab	Send transfer capability to ISDN side on setup message.
line-build-out-loss	Defines the line build out loss to be used for this trunk.
line-build-out-overwrite	Overwrites the Framer's XPM register values which control the line pulse shape.
line-build-out-xpm0	Controls the Framer's XPM0 register value (line pulse shape control).
line-build-out-xpm1	Defines the Framer's XPM1 register value (line pulse shape control).
line-build-out-xpm2	Defines the Framer's XPM2 register value (line pulse shape control).
line-code	Defines the line code type to be used for this trunk.
local-isdn-rbt-src	If the ringback tone source is not IP, who should supply the Ringback tone.
ovrlp-rcving-type	Defines reception type of overlap dialing from ISDN side
pi-in-rx-disc-msg	Configure PIForDisconnectMsg in order to overwrite PI value received in ISDN Disconnect message

Command	Description
`pi-to-isdn`	Override the value of progress indicator to ISDN side in ALERT, PROGRESS, and PROCEEDING messages
`play-rbt-to-trk`	Enable ringback tone playing towards trunk side. Refer to User's Manual for details
`port-info`	Defines a descriptive name for the port.
`protocol`	Defines the PSTN protocol to be used for this trunk.
`pstn-alrt-timeout`	Defines max. time (in seconds) to wait for connect from PSTN
`rmv-calling-name`	Removes Calling Name For Trunk.
`trace-level {full-isdn| full-isdn-with-duplications| layer3| layer3-no-duplications| no-trace| q921-raw-data| q931| q931-q921-raw-data| q931-raw-data}`	Defines the PSTN trace level. **Note:** ■ To configure and start a PSTN trace per trunk, use the following command: configure troubleshoot > logging logging-filters. ■ To start a PSTN trace for all trunks that have been configured with the **trace-level** command option, use the following command: debug debug-recording <IP Address> pstn-trace. ■ To send PSTN traces to a Syslog server (instead of Wireshark), use the following command: configure troubleshoot > pstn-debug.
`trk-xfer-mode-type`	Defines the type of transfer the PSTN/PBX supports

Command Mode

Privileged User

Note

`interface e1-t1 <`**`Trunk ID`**`>` is applicable only to Mediant 3100; `interface e1-t1 <`**`Slot/Port`**`> is applicable to the rest.`

Example

This example configures E1/T1 to E1 EURO ISDN protocol type (1):

```
(config-voip)# interface e1-t1 1/1
(e1-t1 1/1)# protocol 1
(e1-t1 1/1)# activate
```

fxs-fxo

This command configures FXS and FXO interfaces.

Syntax

```
(config-voip)# interface fxs-fxo
(fxs-fxo)#
```

Command	Description
`analog-port-enable`	Enables the analog port.
`bellcore-callerid-type-one-sub-standard`	Selects the sub-standard of the Bellcore Caller ID type.
`bellcore-vmwi-type-one-standard`	Defines the Bellcore VMWI standard.
`caller-id-timing-mode`	Defines the Analog Caller ID Timing Mode.
`caller-id-type`	Defines the Caller ID standard.
`current-disconnect-duration`	Defines the current-disconnect duration (in msec).
`default-linepolarity-state`	Sets the default line polarity state.
`disable-analog-auto-calibration`	Determines whether to enable the analog Autocalibration in the DAA.
`enable-analog-dc-remover`	Determines whether to enable the analog DC remover in the DAA.
`enable-fxo-current-limit`	Enables loop current limit to a maximum of 60mA (TBR21) or disables the FXO line current limit.
`etsi-callerid-type-one-sub-standard`	Selects the number denoting the ETSI CallerID Type 1 sub-standard.

Command	Description
`etsi-vmwi-type-one-standard`	Selects the number denoting the ETSI VMWI Type 1 Standard.
`far-end-disconnect-type`	Sets the source for the acEV_FAR_END_DISCONNECTED event.
`flash-hook-period`	Defines the flashhook detection and generation period (in msec).
`fxo-country-coefficients`	Line characteristic (AC and DC) according to country.
`fxo-dc-termination`	Defines the FXO line DC termination.
`fxs-country-coefficients`	Defines the line characteristic (AC and DC) according to country.
`fxs-line-testing <Module/Port> {66|70}`	Performs an FXS line test for a specified FXS port and coefficient type (66 for TBR21 and 70 for USA).
`fxs-rx-gain-control`	Defines gain\attenuation of the FXS Rx path between -17db and 18db.
`fxs-tx-gain-control`	Defines gain\attenuation of the FXS Tx path between -22db and 10db.
`metering-on-time`	Defines the metering signal duration to be detected
`metering-type`	Defines the metering method for charging pulses.
`min-flash-hook-time`	Defines the minimal time (in msec) for detection of a flash hook event (for FXS only).
`mwi-indication-type`	Defines the type of (MWI) Message Waiting Indicator (for FXS only).
`polarity-reversal-type`	Defines type of polarity reversal signal used for network far-end answer and disconnect indications.
`port-info`	Defines a descriptive name for the port.
`rx-gain-control`	Defines gain attenuation of the FXO Rx path between -15db and 12db.
`time-to-sample-analog-line-voltage`	Defines the time to sample the analog line voltage after offhook, for the current disconnect threshold.

Command	Description
`tx-gain-control`	Defines gain attenuation of the FXO Tx path between -15db and 12db.
`wink-time`	Defines time elapsed between two consecutive polarity reversals.

Command Mode

Privileged User

Example

This example enables FXS port 1 in Module 2:

```
(config-voip)# interface fxs-fxo
(fxs-fxo)# analog-port-enable 1/2
(fxs-fxo)# activate
```

92 ip-group

This command configures the IP Groups table, which lets you define IP Groups.

Syntax

```
(config-voip)# ip-group <Index>
(ip-group-<Index>)#
```

Command	Description
Index	Defines the table row index.
`always-use-route-table {disable|enable}`	Defines the Request-URI host name in outgoing INVITE messages.
`always-use-source-addr {disable|enable}`	Enables the device to always send SIP requests and responses, within a SIP dialog, to the source IP address received in the previous SIP message packet.
`authentication-method-list`	Defines SIP methods received from the IP Group that must be challenged by the device when the device acts as an Authentication server.
`authentication-mode {sbc-as-client|sbc-as-server|user-authenticates}`	Defines the authentication mode.
`bandwidth-profile`	Assigns a Bandwidth Profile rule.
`cac-profile`	Assigns a Call Admission Control Profile.
`call-setup-rules-set-id`	Assigns a Call Setup Rule Set ID.
`classify-by-proxy-set {disable|enable|enable-for-options}`	Enables the classification of incoming SIP dialog messages to a **Server**-type IP Group based on Proxy Set.
`contact-user`	Defines the user part of the From, To, and Contact headers of SIP REGISTER messages, and the user part of the

Command	Description
	Contact header of INVITE messages received from this IP Group and forwarded by the device to another IP Group.
`dedicated-connection-mode {disable|per-sbc-user-info}`	Enables the device to establish and use a dedicated TCP (or TLS) connection with the SIP registrar server per user that is listed in the SBC User Information table.
`dst-uri-input`	Defines the SIP header in the incoming INVITE to use as a call matching characteristic based on destination URIs.
`dtls-context`	Assigns a TLS Context (certificate) to the IP Group, which is used for DTLS sessions (handshakes) with the IP Group.
`inbound-mesg-manipulation-set`	Assigns a Message Manipulation Set (rule) to the IP Group for SIP message manipulation on the inbound leg.
`internal-media-realm-name`	Assigns an "internal" Media Realm to the IP Group. This is applicable when the device is deployed in a Microsoft Teams environment. The device selects this Media Realm (instead of the Media Realm assigned by the `media-realm-name` command) if the value of the X-MS-UserLocation header in the incoming SIP message is "Internal" and the`teams-local-media-optimization-handling` command is configured to any value other than none.
`ip-profile-name`	Assigns an IP Profile to the IP Group.
`local-host-name`	Defines the host name (string) that the device uses in the SIP message's Via and Contact headers.

Command	Description
`max-num-of-reg-users`	Defines the maximum number of users in this IP Group that can register with the device.
`media-realm-name`	Assigns a Media Realm to the IP Group.
`metering-remote-type {regular|vaic}`	Defines if the IP Group represents AudioCodes VoiceAI Connect entity. **Note:** Leave the parameter at its default setting (i.e., **Regular**). The parameter is used only by AudioCodes support.
`msg-man-user-defined-string1`	Defines a value for the SIP user part that can be used in Message Manipulation rules configured in the Message Manipulations table.
`msg-man-user-defined-string2`	Defines a value for the SIP user part that can be used in Message Manipulation rules configured in the Message Manipulations table.
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`oauth-http-service`	Assigns a Remote Web Service to the IP Group for OAuth-based authentication of incoming SIP requests.
`outbound-mesg-manipulation-set`	Assigns a Message Manipulation Set (rule) to the IP Group for SIP message manipulation on the outbound leg.
`password-as-client`	Defines the shared password that is used when the device is challenged by an authentication server (SIP 401/407) to authenticate outgoing SIP requests received from this IP Group.
`password-as-server`	Defines the shared password that is

Command	Description
	used when the device challenges (authenticates) incoming SIP requests from users belonging to this IP Group (for User-type IP Groups), or challenges SIP servers (for Server-type IP Groups).
`proxy-keepalive-use-ipg {disable|enable}`	Enables the device to apply certain IP Group settings to keep-alive SIP OPTIONS messages that are sent by the device to the proxy server.
`proxy-set-name`	Assigns a Proxy Set to the IP Group. All INVITE messages destined to the IP Group are sent to the IP address configured for the Proxy Set.
`qoe-profile`	Assigns a Quality of Experience Profile rule.
`re-routing-mode {not-configured|proxy|routing-table|standard}`	Defines the routing mode after a call redirection (i.e., a 3xx SIP response is received) or transfer (i.e., a SIP REFER request is received).
`registration-mode {no-registrations|sbs-initiates|user-initiates}`	Defines the registration mode for the IP Group.
`sbc-alt-route-reasons-set`	Assigns an Alternative Reasons Set to the IP Group.
`sbc-client-forking-mode {parallel|sequential|sequential-available-only}`	Defines call forking of INVITE messages to up to five separate SIP outgoing legs for User-type IP Groups.
`sbc-dial-plan-name`	Assigns a Dial Plan to the IP Group.
`sbc-keep-call-id`	Enables the device to use the same call identification (SIP Call-ID header value) received in incoming messages for the call identification in outgoing messages.
`sbc-operation-mode {b2bua|call-`	Defines the device's operational

Command	Description
`stateful-proxy|microsoft-server|not-configured}`	mode for the IP Group.
`sbc-psap-mode {disable|enable}`	Enables E9-1-1 emergency call routing in a Microsoft Skype for Business environment.
`sbc-server-auth-type {according-to-global-parameter|arm|locally|remotely-according-draft-sterman|remotely-by-oauth}`	Defines the authentication method when the device, as an Authentication server, authenticates SIP requests from the IP Group.
`sbc-user-stickiness {disable|enable}`	Enables SBC user registration "stickiness" to a registrar.
`sip-connect`	Defines the IP Group as a registered server that represents multiple users.
`sip-group-name`	Defines the SIP Request-URI host name in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group.
`sip-source-host-name`	Defines the hostname of the URI in certain SIP headers, overwriting the original host part of the URI.
`src-uri-input`	Defines the SIP header in the incoming INVITE that is used for call matching characteristics based on source URIs.
`srd-name`	Assigns an SRD to the IP Group.
`tags`	Assigns Dial Plan tags for routing and manipulation.
`teams-direct-routing-mode {disable|enable}`	Enables the device to include Microsoft's proprietary X-MS-SBC header in outgoing SIP INVITE and OPTIONS messages in a Microsoft Teams Direct Routing environment.

Command	Description
`teams-local-media-optimization-handling {none| sbc-decides| teams-decides}`	Enables and defines media optimization handling when the device is deployed in a Microsoft Teams environment. The handling is based on Microsoft proprietary SIP headers, X-MS-UserLocation and X-MS-MediaPath.
`teams-local-mo-initial-behavior {direct-media| external| internal}`	Defines how the central SBC device (proxy SBC scenario) initially sends the received INVITE message with the SDP Offer to Teams when the device is deployed in a Microsoft Teams environment for Local Media Optimization.
`teams-local-mo-site`	Defines the name of the Teams site (e.g., "Singapore") within which the Teams client is located.
`topology-location {down|up}`	Defines the display location of the IP Group in the Topology view of the Web interface.
`type {gateway|server|user}`	Defines the type of IP Group
`use-requri-port {disable|enable}`	Enables the device to use the port indicated in the Request-URI of the incoming message as the destination port when routing the message to the IP Group.
`used-by-routing-server {not-used|used}`	Enables the IP Group to be used by a third-party routing server for call routing decisions.
`user-voice-quality-report {disable|enable}`	Enables MOS calculation and reporting of calls belonging to users that are registered with the device.
`username-as-client`	Defines the shared username that is used when the device is challenged by an authentication server (SIP 401/407) to authenticate outgoing SIP

Command	Description
	requests received from this IP Group.
`username-as-server`	Defines the shared username that is used when the device challenges (authenticates) incoming SIP requests from users belonging to this IP Group (for User-type IP Groups), or challenges SIP servers (for Server-type IP Groups).
`uui-format {disable|enable}`	Enables the generation of the Avaya UCID value, adding it to the outgoing INVITE sent to this IP Group.
`validate-source-ip {disable|enable}`	Enables the device to validate the source IP address of incoming SIP dialog-initiating requests (e.g., INVITE messages) by checking that it matches an IP address (or DNS-resolved IP address) in the Proxy Set that is associated with the IP Group.

Command Mode

Privileged User

Example

This example configures a Server-type IP Group called "ITSP":

```
(config-voip)# ip-group 0
(ip-group-0)# name ITSP
(ip-group-0)# type server
(ip-group-0)# media-realm-name ITSP
(ip-group-0)# activate
```

93 media

This command configures media.

Syntax

```
(config-voip)# media
```

Command	Description
`crypto-suites-groups`	See crypto-suites-groups below
`fax-modem`	See fax-modem on the next page
`ip-media-settings`	See ip-media-settings on page 494
`ipmedia`	See ipmedia on page 493
`rtp-rtcp`	See rtp-rtcp on page 495
`security`	See security on page 498
`settings`	See settings on page 499
`tdm`	See tdm on page 502
`voice`	See voice on page 503

Command Mode

Privileged User

crypto-suites-groups

This command configures the SBC Crypto Suite Groups table, which defines SRTP crypto suites that can be assigned to IP Profiles. The table is a parent of the Crypto Suites table table.

Syntax

```
(config-voip)# media crypto-suites-groups <Index>
(crypto-suites-groups-<Index>)#
```

Command	Description
Index	Defines the table row index.
`crypto-suites <Index> crypto-suite {aes-256-cm-hmac-sha1-32| aes-256-cm-hmac-sha1-80| aes-cm-128-hmac-sha1-32| aes-cm-128-hmac-sha1-80| all}`	Defines up to four crypto suites for the SBC Crypto Suite Group.
`crypto-suites-group-name`	Defines a descriptive name, which is used when associating the row in other tables.

Command Mode

Privileged User

Example

This example configures an SBC Crypto Suite Group with crypto suite aes-256-cm-hmac-sha1-32:

```
(config-voip)# media crypto-suites-groups 2
(crypto-suites-groups-2)# crypto-suites-group-name ITSP
(crypto-suites-groups-2)# crypto-suites 0
(crypto-suites-2/0)# crypto-suite aes-256-cm-hmac-sha1-32
(crypto-suites-3/0)# activate
```

fax-modem

This command configures fax parameters.

Syntax

```
(config-voip)# media fax-modem
(media-fax-modem)#
```

Command	Description
`FaxRelayTimeoutSec`	A channel during fax relay session cannot relatch on another RTP/RTCP/T38 stream until no T38 packets arrived from or sent to current stream during the timeout (sec).
`V1501AllocationProfile`	Defines the V.150.1 profile.
`caller-id-transport-type`	Defines the Caller ID Transport type.
`ced-transfer-mode`	Defines the CED transfer mode.
`cng-detector-mode`	Defines the fax CNG tone detector mode.
`coder`	Defines the Fax/Modem bypass coder.
`ecm-mode`	Enables ECM (Error Correction Mode) during T.38 Fax Relay.
`enhanced-redundancy-depth`	Defines the number of repetitions to be applied to control packets when using T.38 standard.
`fax-cng-mode`	0-Does not send a SIP re-INVITE, 1-Sends T.38 re-INVITE upon detection of fax CNG tone, 2-Sends T.38 re-INVITE upon detection of fax CNG tone or v8-cn signal
`fax-transport-mode {bypass|disable|events-only|t.38-relay}`	Defines the Fax over IP transport method.
`max-rate`	Limits the maximum transfer rate of the fax during T.38 Fax Relay session.
`modem-bypass-output-gain`	Defines the modem bypass output gain [dB].
`packing-factor`	Defines the number of 20 msec payloads to be generated in a single RTP fax/modem bypass packet.
`redundancy-depth`	Defines the depth of redundancy for non-V.21 T.38 fax packets.

Command	Description
`rx-t38-over-rtp-payload-type`	Defines the received T.38 over RTP payload type.
`sprt-transport-channel0-max-payload-size`	Defines the V.150.1 SPRT transport channel 0 max payload size.
`sprt-transport-channel2-max-payload-size`	Defines the V.150.1 SPRT transport channel 2 max payload size.
`sprt-transport-channel2-max-window-size`	Defines the V.150.1 SPRT transport channel 2 max window size.
`sprt-transport-channel3-max-payload-size`	Defines the V.150.1 SPRT transport channel 3 max payload size.
`sse-redundancy-depth`	Defines the V.150.1 SSE redundancy depth.
`v1501-sprt-payload-type-rx`	Defines the received V.150.1 SPRT payload type.
`v1501-sse-payload-type-rx`	Defines the received V.1501.1 SSE RTP payload type.
`v21-modem-transport-type`	Defines the V.21 modem transport method.
`v22-modem-transport-type`	Defines the V.22 modem transport method.
`v23-modem-transport-type`	Defines the V.23 modem transport method.
`v32-modem-transport-type`	Defines the V.32 modem transport method.
`v34-modem-transport-type`	Defines the V.34 modem transport method.
`version`	Defines the T.38 fax relay version.

Command Mode

Privileged User

Example

This example configures the fax transport type to T.38:

```
(config-voip)# media fax-modem
(media-fax-modem)# fax-transport-mode t.38-relay
(media-fax-modem)# activate
```

ipmedia

This command configures various IP-media parameters.

Syntax

```
(config-voip)# media ipmedia
(media-ipmedia)#
```

Command	Description
`agc-disable-fast-adaptation`	Disables the AGC (Automatic Gain Control) Fast Adaptation mode.
`agc-enable`	Activates the AGC (Automatic Gain Control).
`agc-gain-slope`	Defines the AGC convergence rate.
`agc-max-gain`	Defines the maximum signal gain of the AGC [dB].
`agc-min-gain`	Defines the minimum signal gain of the AGC [dB].
`agc-redirection`	Redirects the AGC output towards the TDM instead of towards the network.
`agc-target-energy`	Defines the target signal energy level of the AGC [-dBm]
`answer-detector-activity-delay`	Defines the time (in 100-msec resolution) between when the device activates the Answer Detector and when it actually starts to detect.
`answer-detector-enable {off|on}`	Enables the device's Answer Detector feature.
`answer-detector-low-energy-sensitivity {0|1}`	Enables low-energy sensitivity for the Answer Detector.
`answer-detector-`	Enables the Answer Detector to apply to the IP network side (1)

Command	Description
`redirection {0|1}`	instead of the PSTN side (0).
`answer-detector-sensitivity`	Defines the Answer Detector sensitivity.
`answer-detector-silence-time`	Defines the duration of silence (in 100-msec resolution) from when no speech input is detected by the Answer Detector until the device sends an End Of Speech event
`energy-detector-enable`	Activates the Energy Detector.
`energy-detector-redirection`	Redirect the Energy Detector towards the network instead of TDM.
`energy-detector-sensitivity`	Defines the Energy Detector's sensitivity.
`energy-detector-threshold`	Defines the ED's (Energy Detector's) threshold according to the formula: -44 + (EDThreshold * 6) [- dBm].
`ipm-detectors-enable`	Enables DSP IP Media Detectors.

Command Mode

Privileged User

Example

This example enables AD:

```
(config-voip)# media ipmedia
(media-ipmedia)# answer-detector-enable on
(media-ipmedia)# activate
```

ip-media-settings

This command configures various IP-media parameters.

Syntax

```
(config-voip)# media ip-media-settings
(media-settings)#
```

Command	Description
http-streaming-playback-requests-timeout	Defines a timeout for no packets received (e.g., due to playback underruns) from the text-to-speech (TTS) service provider can now be configured. **Note:** The parameter is for AudioCodes **internal use only** and is applicable only when the device operates with AudioCodes VoiceAI Connect Enterprise.

Command Mode

Privileged User

Example

This example enables AD:

```
(config-voip)# media ip-media-settings
(media-ipmedia-settings)# http-streaming-playback-requests-timeout 1,1000-ms
(media-ipmedia-settings)# activate
```

rtp-rtcp

This command configures various RTP-RTCP parameters.

Syntax

```
(config-voip)# media rtp-rtcp
(media-rtp-rtcp)#
```

Command	Description
`AnalogSignalTransportType`	Defines the analog signal transport type.
`enable-standard-sid-payload-type`	Defines the Silence Indicator (SID) packets that are sent and received are according to RFC 3389.
`L1L1ComplexTxUDPPort`	Defines the Source UDP port for the outgoing UDP Multiplexed RTP packets, for

Command	Description
	Complex-Multiplex RTP mode
`RTPFWInvalidPacketHandling`	Defines the way an invalid packet should be handled.
`RTPPackingFactor`	Defines the number of DSP payloads for generating one RTP packet.
`RtpFWNonConfiguredPTHandling`	Defines the the way a packet with non-configured payload type should be handled.
`VQMONBURSTHR`	Defines the voice quality monitoring - excessive burst alert threshold
`VQMONDELAYTHR`	Defines the voice quality monitoring - excessive delay alert threshold
`VQMONEOCRVALTHR`	Defines the voice quality monitoring - end of call low quality alert threshold
`VQMONGMIN`	Defines the voice quality monitoring - minimum gap size (number of frames)
`base-udp-port`	Defines the lower boundary of UDP ports to be used by the board.
`com-noise-gen-nego`	CN payload type is used and being negotiate
`disable-rtcp-randomization`	Defines the RTCP report intervals.
`fax-bypass-payload-type`	Defines the Fax Bypass (VBD) Mode payload type.
`jitter-buffer-minimum-delay`	Defines the Dynamic Jitter Buffer Minimum Delay [msec]
`jitter-buffer-optimization-factor`	Defines the Dynamic Jitter Buffer attack/decay performance.
`modem-bypass-payload-type`	Defines the Modem Bypass (VBD) Payload type.
`publication-ip-group-id`	Defines the IP Group to where the device sends RTCP XR reports.

Command	Description
`remote-rtp-b-udp-prt`	Defines the Remote Base UDP Port For Aggregation
`rtcp-interval`	Defines the time interval between the adjacent RTCP report (in msec).
`rtcp-xr-coll-srvr`	Defines the RTCP-XR server IP address
`rtcp-xr-rep-mode`	0:rtcpxr is not sent over SIP at all {@}1:rtcpxr is sent over sip when call ended {@}2:rtcpxr is sent over sip when on periodic interval and when call ended {@}3:rtcpxr is sent over sip when media segment ended and when call ended
`rtcpxr-collect-serv-transport`	Defines the RtcpXrEsc transport type
`rtp-redundancy-depth`	Defines the redundancy depth of RTP redundancy packets.
`rtp-redundancy-payload-type`	Defines the RTP Redundancy packet's Payload Type field.
`sbc-rtcpxr-report-mode`	0:rtcpxr is not sent over SIP at all,1:rtcpxr is sent over sip when call ended
`telephony-events-payload-type-rx`	Defines the Rx RFC 2833 DTMF relay dynamic payload type for inbound calls.
`telephony-events-payload-type-tx`	Defines the Tx RFC 2833 DTMF relay dynamic payload type for outbound calls.
`udp-port-spacing {2|4|5|10}`	Defines the UDP port spacing.
`voice-quality-monitoring-enable`	Defines the voice quality monitoring (RTCP-XR) mode.

Command Mode

Privileged User

Example

This example configures UDP port spacing:

```
(config-voip)# media rtp-rtcp
(media-rtp-rtcp)# udp-port-spacing 5
(media-rtp-rtcp)# activate
```

security

This command configures various security parameters.

Syntax

```
(config-voip)# media security
(media-security)#
```

Command	Description
`aria-protocol-support {off|on}`	Enables ARIA media encryption algorithm.
`media-sec-bhvior {mandatory|preferable|preferable-single-media}`	Defines the device behavior when receiving offer/response for media encryption.
`media-security-enable {off|on}`	Enables the media security protocol (SRTP).
`offer-srtp-cipher {aes-256-cm-hmac-sha1-32|aes-256-cm-hmac-sha1-80|aes-cm-128-hmac-sha1-32|aes-cm-128-hmac-sha1-80|all|aria-cm-128-hmac-sha1-80|aria-cm-192-hmac-sha1-80|not-configured}`	Defines the offered SRTP cipher suite.
`reset-srtp-upon-re-key`	Resets SRTP State Upon Re-key.
`rtcp-encryption-disable-tx {disable|enable}`	On a secured RTP session, disables encryption on transmitted RTCP packets.
`rtp-authentication-disable-tx {disable|enable}`	On a secured RTP session, disables authentication on transmitted RTP packets.
`rtp-encryption-disable-tx {disable|enable}`	On a secured RTP session, disables encryption on transmitted RTP packets.

Command	Description
`srtp-reset-tx-rx-separately {off|on}`	Enables the device to reset only the SRTP stream (roll-over counter / ROC index and other SRTP fields) with the call party that changes the SRTP key (‘a=crypto’ line in SDP body) during a call.
`srtp-tnl-vld-rtcp-auth {off|on}`	Validates SRTP Tunneling Authentication for RTCP.
`srtp-tnl-vld-rtp-auth {srtp-tnl-vld-rtcp-auth|srtp-tnl-vld-rtp-auth}`	Validates SRTP Tunneling Authentication for RTP.
`srtp-tx-packet-mKi-size`	Defines the size of the Master Key Identifier (MKI) in transmitted SRTP packets.
`rsymmetric-mki`	Enables symmetric MKI negotiation.

Command Mode

Privileged User

Example

This example enables SRTP:

```
(config-voip)# media security
(media-security)# media-security-enable on
(media-security)# activate
```

settings

This command configures various media settings.

Syntax

```
(config-voip)# media settings
(media-settings)#
```

Command	Description
`AmrOctetAlignedEnable`	Defines the AMR payload format.
`arp-manager-timeout`	Defines the maximum duration or timeout (in seconds) that the device waits for an Address Resolution Protocol (ARP) reply.
`G729EVLocalMBS`	Defines the maximum generation bitrate of the G729EV coder for a specific channel.
`G729EVMaxBitRate`	Defines the maximum generation bitrate for all participants in a session using G729EV coder.
`G729EVReceiveMBS`	Defines the maximum generation bitrate of the G729EV coder to be requested from the other party.
`media-ip-ver-pref {ipv4-only| ipv6-only| prefer-ipv4| prefer-ipv6}`	Defines the preference of the Media IP version.
`NewRtcpStreamPackets`	Defines the minimal number of continuous RTCP packets, allowing latching an incoming RTCP stream.
`NewRtpStreamPackets`	Defines the minimal number of continuous RTP packets, allowing latching an incoming RTP stream.
`NewSRTPStreamPackets`	Defines the minimal number of continuous RTP packets, allowing latching an incoming RTP stream during SRTP session.
`NewSRtcpStreamPackets`	Defines the minimal number of continuous RTCP packets, allowing latching an incoming RTCP stream during SRTP session.
`TimeoutToRelatchRTCPMsec`	If a channel latched on an incoming RTCP stream, it cannot relatch onto another one until no packets of the old stream arrive during the timeout (msec).
`TimeoutToRelatchRTPMsec`	A channel during RTP session cannot relatch onto another RTP/RTCP/T38 stream until no RTP packets arrived from current stream

Command	Description
	during the timeout (msec).
`TimeoutToRelatchSRTPMsec`	A channel during SRTP session cannot relatch on another RTP/RTCP/T38 stream until no RTP packets arrived from current stream during the timeout (msec).
`TimeoutToRelatchSilenceMsec`	A channel in silence mode during RTP/SRTP session cannot relatch on another RTP/RTCP/T38 stream until no packets arrived from current stream during the timeout (msec).
`cot-detector-enable {off|on}`	Enables COT (Continuity Tones) detection and generation.
`disable-nat-traversal {0|1|2|3|4}`	Defines the NAT mode.
`inbound-media-latch-mode {strict|dynamic|dynamic-strict| strict-on-first}`	Defines the handling of incoming media packets from non-expected address/port.
`silk-max-average-bitrate`	Defines the SILK coder maximal average bit rate.
`silk-tx-inband-fec {off|on}`	Enables the SILK FEC (Forward Error Correction).

Command Mode

Privileged User

Example

This example defines the NAT mode so that NAT traversal is performed only if the UA is located behind NAT:

```
(config-voip)# media settings
(media-settings)# disable-nat-traversal 0
(media-settings)# activate
```

tdm

This command configures various TDM clock synchronization and bus.

Syntax

```
(config-voip)# media tdm
(media-tdm)#
```

Command	Description
`tdm-bus-clock-source {internal|network}`	Defines the clock source on which the device synchronizes.
`idle-abcd-pattern`	Defines ABCD (CAS) pattern applied on signaling bus before it is changed.
`idle-pcm-pattern`	Defines the PCM pattern applied to the E1/T1 timeslot (B-channel) when the channel is closed and during silence periods when Silence Compression is used.
`pcm-law-select {alaw|automatic|mulaw}`	Defines the type of PCM companding law in the input/output TDM bus.
`pstn-bus-auto-clock {off|on}`	Enables the PSTN Trunk Auto-Fallback feature.
`pstn-bus-auto-clock-reverting {off|on}`	Enables the PSTN Trunk Auto-Fallback Reverting feature.
`tdm-bus-auto-fallback {holdover| internal}`	Defines the fallback clock (when auto clock on).
`tdm-bus-local-reference <Trunk ID>`	Defines the Trunk ID for the clock synchronization source of the device.

Command Mode

Privileged User

Example

This example defines the clock source as internal and uses Trunk Group ID 1:

```
(config-voip)# media tdm
(media-tdm)# tdm-bus-clock-source internal
(media-tdm)# tdm-bus-local-reference 1
(media-tdm)# activate
```

voice

This command configures various voice settings.

Syntax

```
(config-voip)# media voice
(media-voice)#
```

Command	Description
`acoustic-echo-suppressor-attenuation-intensity`	Defines acoustic echo suppressor signals identified as echo attenuation intensity.
`acoustic-echo-suppressor-enable {off|on}`	Enables network acoustic echo suppressor.
`acoustic-echo-suppressor-max-erl`	Defines acoustic echo suppressor max ratio between signal level and returned echo from phone [dB].
`acoustic-echo-suppressor-max-reference-delay`	Defines acoustic echo suppressor max reference delay [10 ms].
`acoustic-echo-suppressor-min-reference-delay`	Defines acoustic echo suppressor min reference delay [10 ms].
`caller-id-transport-type`	Defines the Caller ID Transport type.
`default-dtmf-signal-duration`	Defines the time to play DTMF (in msec).
`dtmf-detector-enable`	Enables the detection of DTMF signaling.
`dtmf-generation-twist`	Defines a delta between the high and low frequency components in the DTMF signal [db].

Command	Description
`dtmf-transport-type`	Defines the transport method of DTMFs over the network.
`dtmf-volume`	Defines the DTMF generation volume [-dbm].
`echo-canceller-enable`	Enables the Echo Canceller.
`echo-canceller-type`	Defines the Echo Canceller type.
`input-gain`	Defines the TDM input gain [dB].
`inter-digit-interval`	Defines the time between DTMFs played (in msec).
`mf-transport-type`	Defines the method for transport MFs over the network.
`mfr1-detector-enable`	Enables the detection of MF-R1 signaling.
`voice-volume`	Defines the voice TDM output gain [dB]

Command Mode

Privileged User

Example

This example enables the Acoustic Echo Suppressor:

```
(config-voip)# media voice
(media-voice)# acoustic-echo-suppressor-enable on
(media-voice)# activate
```

94 message

This command configures SIP message manipulation tables.

Syntax

```
(config-voip)# message
```

Command	Description
`call-setup-rules`	See call-setup-rules below
`message-manipulations`	See message-manipulations on page 507
`message-policy`	See message-policy on page 508
`pre-parsing-manip-sets`	See pre-parsing-manip-sets on page 510
`settings`	See settings on page 511

Command Mode

Privileged User

call-setup-rules

This command configures the Call Setup Rules table, which lets you define Call Setup rules. Call Setup rules define various sequences that are run upon the receipt of an incoming call (dialog) at call setup, before the device routes the call to its destination.

Syntax

```
(config-voip)# message call-setup-rules <Index>
(call-setup-rules-<Index>)#
```

Command	Description
Index	Defines the table row index.
`action-subject`	Defines the element (e.g., SIP header, SIP parameter, SIP body, or Dial Plan tag) upon which you want to perform the action if the condition,

Command	Description
	configured in the 'Condition' parameter (see above) is met.
`action-type {add|add-prefix|add-suffix|exit|modify|none|remove|remove-prefix|remove-suffix|run-rules-set}`	Defines the type of action to perform.
`action-value`	Defines a value that you want to use in the action.
`attr-to-get`	Defines the Attributes of the queried LDAP record that the device must handle (e.g., retrieve value).
`request-key`	Defines the key to query.
`condition`	Defines the condition that must exist for the device to perform the action.
`request-target`	Defines the request target.
`request-type {dial-plan|enum|http-get|http-post-notify| http-post-query|ldap|none}`	Defines the type of request.
`row-role {use-current-condition|use-previous-condition}`	Determines which condition must be met for this rule to be performed.
`rules-set-id`	Defines a Set ID for the rule.
`rules-set-name`	Defines an arbitrary name to easily identify the row.

Command Mode

Privileged User

Example

This example replaces (manipulates) the incoming call's source number with a number retrieved from the AD by an LDAP query. The device queries the AD server for the attribute record, "telephoneNumber" whose value is the same as the received source number (e.g., "telephoneNumber =4064"). If such an Attribute exists, the device retrieves the number of the Attribute record, "alternateNumber" and uses this number as the source number:

```
(config-voip)# message call-setup-rules 0
(call-setup-rules-0)# query-type ldap
(call-setup-rules-0)# query-target LDAP-DC-CORP
(call-setup-rules-0)# attr-to-query ‘telephoneNumber=’ + param.call.src.user
(call-setup-rules-0)# attr-to-get alternateNumber
(call-setup-rules-0)# row-role use-current-condition
(call-setup-rules-0)# condition ldap.attr. alternateNumber exists
(call-setup-rules-0)# action-subject param.call.src.user
(call-setup-rules-0)# action-type modify
(call-setup-rules-0)# action-value ldap.attr. alternateNumber
(call-setup-rules-0)# activate
```

message-manipulations

This command configures the Message Manipulations table, which lets you define SIP Message Manipulation rules.

Syntax

```
(config-voip)# message message-manipulations <Index>
(message-manipulations-<Index>)#
```

Command	Description
Index	Defines the table row index.
`action-subject`	Defines the SIP header upon which the manipulation is performed.
`action-type {add|add-prefix|add-suffix|modify|normalize|remove|remove-prefix|remove-suffix}`	Defines the type of manipulation.
`action-value`	Defines a value that you want to use in the manipulation.
`condition`	Defines the condition that must exist for the rule to be

Command	Description
	applied.
`manipulation-name`	Defines a descriptive name, which is used when associating the row in other tables.
`manipulation-set-id`	Defines a Manipulation Set ID for the rule.
`message-type`	Defines the SIP message type that you want to manipulate.
`row-role`	Determines which message manipulation condition (configured by the 'Condition' parameter) to use for the rule.

Command Mode

Privileged User

Example

This example adds ";urgent=1" to the To header if the URL of the Request-URI in the INVITE message equals "120":

```
(config-voip)# message message-manipulations 0
(message-manipulations-0)# message-type invite.request
(message-manipulations-0)# condition header.request.uri.url=='120'
(message-manipulations-0)# action-subject header.to
(message-manipulations-0)# action-type modify
(message-manipulations-0)# action-value header.to +';urgent=1'
(message-manipulations-0)# activate
```

message-policy

This command configures the Message Policies table, which lets you define SIP Message Policy rules.

Syntax

```
(config-voip)# message message-policy <Index>
(message-policy-<Index>)#
```

Command	Description
Index	Defines the table row index.
`body-list`	Defines the SIP body type (i.e., value of the Content-Type header) to blacklist or whitelist.
`body-list-type {policy-blacklist|policy-whitelist}`	Defines the policy (blacklist or whitelist) for the SIP body specified in the 'Body List' parameter (above).
`max-body-length`	Defines the maximum SIP message body length.
`max-header-length`	Defines the maximum SIP header length.
`max-message-length`	Defines the maximum SIP message length.
`max-num-bodies`	Defines the maximum number of bodies (e.g., SDP) in the SIP message.
`max-num-headers`	Defines the maximum number of SIP headers.
`method-list`	Defines SIP methods (e.g., INVITE\BYE) to blacklist or whitelist.
`method-list-type {policy-blacklist|policy-whitelist}`	Defines the policy (blacklist or whitelist) for the SIP methods specified in the 'Method List' parameter (above).
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`send-rejection {policy-drop|policy-reject}`	Defines whether the device sends a SIP response if it rejects a message request due to the Message Policy.
`signature-db-enable {disabled|enabled}`	Enables the use of the Malicious Signature database (signature-based detection).

Command Mode

Privileged User

Example

This example configures the maximum number of bodies in SIP messages to two:

```
(config-voip)# message message-policy 0
(message-policy-0)# name ITSP-Message
(message-policy-0)# max-num-bodies 2
(message-policy-0)# activate
```

pre-parsing-manip-sets

This command configures the Pre-Parsing Manipulation Set table, which lets you define Pre-Parsing Manipulation Sets. The table is a parent of the Pre-Parsing Manipulation Rules table.

Syntax

```
(config-voip)# message pre-parsing-manip-sets <Index>
(pre-parsing-manip-sets-<Index>)#
```

Command	Description
Index	Defines the table row index.
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`pre-parsing-manip-rules`	Defines the Pre-Parsing Manipulation Rules table, which lets you define Pre-Parsing Manipulation rules. The table is a child of the Pre-Parsing Manipulation Set table. For more information, see pre-parsing-manip-rules on the next page.

Command Mode

Privileged User

Example

This example configures the maximum number of bodies in SIP messages to two:

```
(config-voip)# message pre-parsing-manip-sets 0
(pre-parsing-manip-sets-0)# name ITSP-PreManip
(pre-parsing-manip-sets-0)# activate
```

pre-parsing-manip-rules

This command configures the Pre-Parsing Manipulation Rules table, which lets you define Pre-Parsing Manipulation rules. The table is a child of the Pre-Parsing Manipulation Set table.

Syntax

```
(config-voip)# message pre-parsing-manip-sets <Index>
(pre-parsing-manip-sets-<Index>)# pre-parsing-manip-rules <Index>
(pre-parsing-manip-rules-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`message-type`	Defines the SIP message type to which you want to apply the rule.
`pattern`	Defines a pattern, based on regex, to search for (match) in the incoming message.
`replace-with`	Defines a pattern, based on regex, to replace the matched pattern.

Command Mode

Privileged User

Example

This example replaces the user part (if exists) in the From header URL with "1000", for INVITE messages:

```
(config-voip)# message pre-parsing-manip-sets 0
(pre-parsing-manip-sets-0)# pre-parsing-manip-rules 1
(pre-parsing-manip-rules-0/1)# message-type invite.request
(pre-parsing-manip-rules-0/1)# pattern From: *<sip:([^@]+)(@\S*)
(pre-parsing-manip-rules-0/1)# replace-with ‘From: <sip:’ + ‘1000’ + $2
(pre-parsing-manip-rules-0/1)# activate
```

settings

This command configures various manipulation options.

Syntax

```
(config-voip)# message settings
(sip-message-settings)#
```

Command	Description
inbound-map-set	Assigns a Manipulation Set ID for manipulating for manipulating all inbound INVITE messages (Gateway only) or incoming responses of requests that the device initiates.
`outbound-map-set`	Assigns a Manipulation Set ID for manipulating for manipulating all outbound INVITE messages (Gateway only) or outgoing responses of requests that the device initiates.

Command Mode

Privileged User

Example

This example assigns Manipulation Set ID 2 for manipulating incoming responses of requests that the device initiates:

```
(config-voip)# message settings
(sip-message-settings)# inbound-map-set 2
```

95 proxy-set

This command configures the Proxy Sets table, which lets you define Proxy Sets. The table is a parent of the Proxy Address table.

Syntax

```
(config-voip)# proxy-set <Index>
(proxy-set-<Index>)#
```

Command	Description
Index	Defines the table row index.
`accept-dhcp-proxy-list {disable|enable}`	Enables the device to obtain the Proxy Set's address(es) from a DHCP server using DHCP Option 120.
`classification-input {ip-only|ip-port-transport}`	Defines how the device classifies incoming IP calls to the Proxy Set.
`connection-reuse {enable|disable|use-global-setting}`	nables the reuse of the initially established TCP or TLS connection between the device and the proxy server for all subsequent SIP requests sent to the proxy server.
`dns-resolve-method {a-record|ms-lync|naptr|not-configured|srv}`	Defines the DNS query record type for resolving the proxy server's host name (FQDN) into an IP address.
`fail-detect-rtx`	Defines the maximum number of UDP retransmissions that the device sends to an offline proxy, before the device considers the proxy as being offline.
`gwipv4-sip-int-name`	Assigns an IPv4-based SIP Interface for Gateway calls to the Proxy Set.
`gwipv6-sip-int-name`	Assigns an IPv6-based SIP Interface for Gateway calls to the Proxy Set.
`in-call-route-mode {disable|enable}`	Enables the device to send in-call SIP messages (e.g., re-INVITE and BYE) to the currently active proxy if the proxy to which the dialog-initiating INVITE message was sent is currently

Command	Description
	offline.
`is-proxy-hot-swap {disable| enable| enable-only-before-alternative-routing}`	Enables the Proxy Hot-Swap feature, whereby the device switches to a redundant proxy upon a failure in the primary proxy (no response is received).
`keepalive-fail-resp`	Defines SIP response codes that if any is received in response to a keep-alive message using SIP OPTIONS, the device considers the proxy as down.
`priority <0-65535>`	Defines the priority of the proxy server.
`min-active-serv-lb`	Defines the minimum number of proxies in the Proxy Set that must be online for the device to consider the Proxy Set as online, when proxy load balancing is used.
`peer-host-name-verification-mode {disable|server-&-client|server-only|use-global-setting}`	Enables the device to verify the Subject Name of the TLS certificate received from the remote side for authentication and establishing a TLS connection.
`proxy-enable-keep-alive {disable|using-fake-register|using-options|using-options-on-active-server|using-register}`	Enables the device's Proxy Keep-Alive feature, which checks communication with the proxy server.
`proxy-ip`	Defines the Proxy Address table, which defines addresses for the Proxy Set. The table is a child of the Proxy Sets table. For more information, see proxy-ip on page 516.
`proxy-keep-alive-time`	Defines the interval (in seconds) between keep-alive messages sent by the device when the Proxy Keep-Alive feature is enabled (see the 'Proxy Keep-Alive' parameter in this table).
`proxy-load-balancing-method {disable|random-weights|round-robin}`	Enables load balancing between proxy servers of the Proxy Set.

Command	Description
`proxy-name`	Defines a descriptive name, which is used when associating the row in other tables.
`proxy-redundancy-mode {homing|not-configured|parking}`	Determines whether the device switches from a redundant proxy to the primary proxy when the primary proxy becomes available again.
`sbcipv4-sip-int-name`	Assigns an IPv4-based SIP Interface for SBC calls to the Proxy Set.
`sbcipv6-sip-int-name`	Assigns an IPv6-based SIP Interface for SBC calls to the Proxy Set.
`srd-name`	Assigns an SRD to the Proxy Set.
`success-detect-int`	Defines the interval (in seconds) between each keep-alive retries (as configured by the 'Success Detection Retries' parameter) that the device performs for offline proxies.
`success-detect-retries`	Defines the minimum number of consecutive, successful keep-alive messages that the device sends to an offline proxy, before the device considers the proxy as being online.
`tls-context-name`	Assigns a TLS Context (SSL/TLS certificate) to the Proxy Set.
`weight <0-65535>`	Defines the weight of the proxy server.

Command Mode

Privileged User

Example

This example configures proxy keep-alive and redundancy:

```
(config-voip)# proxy-set 0
(proxy-set-0)# proxy-enable-keep-alive using-options
(proxy-set-0)# is-proxy-hot-swap enable
(proxy-set-0)# proxy-redundancy-mode homing
(proxy-set-0)# activate
```

proxy-ip

This command configures the Proxy Address table, which defines addresses for the Proxy Set. The table is a child of the Proxy Sets table.

Syntax

```
(config-voip)# proxy-set <Index>
(proxy-set-<Index>)# proxy-ip <Index>
(proxy-ip-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`priority`	Defines the priority of the proxy.
`proxy-address`	Defines the address of the proxy.
`transport-type {not-configured|tcp|tls|udp}`	Defines the transport type for communicating with the proxy.
`weight`	Defines the weight of the proxy.

Command Mode

Privileged User

Example

This example configures address 201.10.5.1 for the Proxy Set:

```
(config-voip)# proxy-set 0
(proxy-set-0)# proxy-ip 1
(proxy-ip-0/1)# proxy-address 201.10.5.1
(proxy-ip-0/1)# transport-type udp
(proxy-ip-0/1)# activate
```

96 qoe

This command configures Quality of Experience (QoE).

Syntax

```
(config-voip)# qoe
```

Command	Description
`additional-parameters`	See additional-parameters call-flow-report on page 519
`bw-profile`	See bw-profile below
`qoe-profile`	See qoe-profile on page 519
`qoe-settings`	See qoe-settings on page 523
`quality-of-service-rules`	See quality-of-service-rules on page 522
`reg-user-voice-quality`	See qoe-reg-user-voice-quality on page 524

Command Mode

Privileged User

bw-profile

This command configures the Bandwidth Profile table, which lets you define Bandwidth Profiles.

Syntax

```
(config-voip)# qoe bw-profile <Index>
(bw-profile-<Index>)#
```

Command	Description
Index	Defines the table row index.
`egress-audio-bandwidth`	Defines the major (total) threshold for outgoing audio traffic (in Kbps).

Command	Description
egress-video-bandwidth	Defines the major (total) threshold for outgoing video traffic (in Kbps).
generate-alarms {disable|enable}	Enables the device to send an SNMP alarm if a bandwidth threshold is crossed.
hysteresis	Defines the amount of fluctuation (hysteresis) from the configured bandwidth threshold in order for the threshold to be considered as crossed (i.e., avoids false reports of threshold crossings).
ingress-audio-bandwidth	Defines the major (total) threshold for incoming audio traffic (in Kbps).
ingress-video-bandwidth	Defines the major (total) threshold for incoming video traffic (in Kbps).
minor-threshold	Defines the Minor threshold value, which is the lower threshold located between the Yellow and Green states.
name	Defines a descriptive name, which is used when associating the row in other tables.
total-egress-bandwidth	Defines the major (total) threshold for video and audio outgoing bandwidth (in Kbps).
total-ingress-bandwidth	Defines the major (total) threshold for video and audio incoming bandwidth (in Kbps).

Command Mode

Privileged User

Example

This example configures a Bandwidth profile where the Major (total) bandwidth threshold is configured to 64,000 Kbps, the Minor threshold to 50% (of the total) and the hysteresis to 10% (of the total):

```
(config-voip)# qoe bw-profile 0
(bw-profile-0)# egress-audio-bandwidth 64000
(bw-profile-0)# minor-threshold 50
(bw-profile-0)# hysteresis 10
(bw-profile-0)# activate
```

additional-parameters call-flow-report

This command enables the device to send SIP messages (in XML fomat) to OVOC for displaying SIP call dialog sessions as call flow diagrams.

Syntax

```
(config-voip)# qoe additional-parameters
(qoe)# call-flow-report {off|on}
```

Command Mode

Privileged User

Default

```
off
```

Example

This example enables the sending of SIP messages to OVOC for call flow diagrams:

```
(config-voip)# qoe additional-parameters
(qoe)# call-flow-report on
```

qoe-profile

This command configures the Quality of Experience Profile table, which defines a name for the Quality of Experience Profile. The table is a parent of the Quality of Experience Color Rules table.

Syntax

```
(config-voip)# qoe qoe-profile <Index>
(qoe-profile-<Index>)#
```

Command	Description
Index	Defines the table row index.
`name`	Defines a descriptive name, which is used when

Command	Description
	associating the row in other tables.
`qoe-color-rules`	Defines the Quality of Experience Color Rules table, which defines a name for the Quality of Experience Profile. The table is a child of the Quality of Experience Profile table. For more information, see qoe-color-rules below.
`sensitivity-level {high|low|medium|user-defined}`	Defines the pre-configured threshold profile to use.

Command Mode

Privileged User

Example

This example configures a Quality of Experience Profile named "QOE-ITSP" and with a pre-defined high sensitivity level:

```
(config-voip)# qoe qoe-profile 0
(qoe-profile-0)# name QOE-ITSP
(qoe-profile-0)# sensitivity-level high
(qoe-profile-0)# activate
```

qoe-color-rules

This command configures the Quality of Experience Color Rules table, which defines a name for the Quality of Experience Profile. The table is a child of the Quality of Experience Profile table.

Syntax

```
(config-voip)# qoe qoe-profile <Index>
(qoe-profile-<Index>)# qoe-color-rules <Index>
(qoe-color-rules-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`direction {device-`	Defines the monitoring direction.

Command	Description
`side|remote-side}`	
`major-hysteresis-red`	Defines the amount of fluctuation (hysteresis) from the Major threshold, configured by the 'Major Threshold (Red)' parameter for the threshold to be considered as crossed.
`major-threshold-red`	Defines the Major threshold value, which is the upper threshold located between the Yellow and Red states. To consider a threshold crossing:
`minor-hysteresis-yellow`	Defines the amount of fluctuation (hysteresis) from the Minor threshold, configured by the 'Minor Threshold (Yellow)' parameter for the threshold to be considered as crossed.
`minor-threshold-yellow`	Defines the Minor threshold value, which is the lower threshold located between the Yellow and Green states.
`monitored-parameter {delay|jitter|mos|packet-loss|rerl}`	Defines the parameter to monitor and report.
`sensitivity-level {high-sensitivity|low-sensitivity|med-sensitivity|user-defined}`	Defines the sensitivity level of the thresholds.

Command Mode

Privileged User

Example

This example configures a Quality of Experience Color Rule for MOS, where a Major alarm is considered if MOS is less than 2:

```
(config-voip)# qoe qoe-profile 0
(qoe-profile-0)# qoe-color-rules 1
(qoe-color-rules-0/1)# monitored-parameter mos
(qoe-color-rules-0/1)# major-threshold-red 20
```

```
(qoe-color-rules-0/1)# major-hysteresis-red 0.1
(qoe-color-rules-0/1)# activate
```

quality-of-service-rules

This command configures the Quality of Service Rules table, which lets you define Quality of Service rules.

Syntax

```
(config-voip)# qoe quality-of-service-rules <Index>
(quality-of-service-rules-<Index>)#
```

Command	Description
Index	Defines the table row index.
`alt-ip-profile-name`	Assigns a different IP Profile to the IP Group or call (depending on the 'Rule Metric' parameter) if the rule is matched.
`calls-reject-duration`	Defines the duration (in minutes) for which the device rejects calls to the IP Group if the rule is matched.
`ip-group-name`	Assigns an IP Group.
`rule-action {alternative-ip-profile|reject-calls]`	Defines the action to be done if the rule is matched.
`rule-metric {acd|asr|bandwidth|ner|poor-invoice-quality|registered-user-voice-quality|voice-quality}`	Defines the performance monitoring call metric to which the rule applies if the metric's threshold is crossed.
`severity {major|minor}`	Defines the alarm severity level.

Command Mode

Privileged User

Example

This example configures a Quality of Service rule that rejects calls to IP Group "ITSP" if bandwidth severity is Major:

```
(config-voip)# qoe quality-of-service-rules 0
(quality-of-service-rules-0)# ip-group-name ITSP
(quality-of-service-rules-0)# rule-action reject-calls
(quality-of-service-rules-0)# rule-metric bandwidth
(quality-of-service-rules-0)# severity major
(quality-of-service-rules-0)# activate
```

qoe-settings

This command configures the OVOC server to where the devicesends QoE data.

Syntax

```
(config-voip)# qoe qoe-settings 0
(qoe-settings-0)#
```

Command	Description
`filter-reports {disable|enable}`	Enables the filtering (e.g., by IP Group #2) of the QoE reports that the device sends to OVOC.
`interface`	Defines the IP network interface on which the quality experience reports are sent.
`keep-alive-time <0-64>`	Defines the interval (in seconds) between every consecutive keep-alive message that the device sends to the OVOC server.
`report-mode {during-call|end-call}`	Defines at what stage of the call the device sends the QoE data of the call to the OVOC server.
`secondary-server-name`	Defines the IP address or FQDN (hostname) of the secondary OVOC server to where the quality experience reports are sent.
`tls{off|on}`	Enables a TLS connection with the OVOC server.
`server-name`	Defines the IP address or FQDN (hostname) of the primary OVOC server to where the quality experience reports are sent.

Command	Description
`tls-context-name`	Assigns a TLS Context or certificate (configured in the TLS Contexts table) for the TLS connection with the OVOC server.
`verify-certificate {off|on}`	Enables TLS verification of the certificate provided by OVOC.
`verify-certificate-subject-name {off|on}`	Enables subject name (CN/SAN) verification of the certificate provided by OVOC.

Command Mode

Privileged User

Note

Only one table row (index) can be configured.

Example

This example configures the IP address of OVOC as 10.15.7.89 and uses IP network interface OAMP for communication:

```
(config-voip)# qoe qoe-settings 0
(qoe-settings-0)# server-name 10.15.7.89
(qoe-settings-0qoe)# interface OAMP
(qoe-settings-0qoe)# activate
```

qoe-reg-user-voice-quality

This command configures the Voice Quality (MOS) feature for users registered to the device.

Syntax

```
(config-voip)# qoe reg-user-voice-quality
(reg-user-voice-quality)#
```

Command	Description
`mos-observ-`	Defines the length of each interval (in hours) in the observation

Command	Description
`win {1|2}`	window (12 intervals) for calculating average MOS of calls belonging to users registered with the device.
`mos-stored-timeout-for-no-calls`	Defines the duration (in minutes) of no calls after which the MOS measurement is reset (0 and gray color).

Command Mode

Privileged User

Note

This command is applicable only to the SBC application.

Example

This example configures the interval of each observation window to one hour:

```
(config-voip)# qoe reg-user-voice-quality
(reg-user-voice-quality)# mos-observ-win 1
(reg-user-voice-quality)# activate
```

97 realm

This command configures the Media Realms table, which lets you define a pool of SIP media interfaces, termed Media Realms.

Syntax

```
(config-voip)# realm <Index>
(realm-<Index>#
```

Command	Description
Index	Defines the table row index.
`bw-profile`	Assigns a Bandwidth Profile to the Media Realm.
`ipv4if`	Assigns an IPv4 interface to the Media Realm.
`ipv6if`	Assigns an IPv6 interface to the Media Realm.
`is-default {disable|enable}`	Defines the Media Realm as the default Media Realm.
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`port-range-start`	Defines the starting port for the range of media interface UDP ports.
`qoe-profile`	Assigns a QoE Profile to the Media Realm.
`realm-extension`	Defines the Media Realm Extension table, which lets you define Media Realm Extensions per Media Realm. The table is a child of the Media Realm table. For more information, see realm-extension on page 528.
`remote-ipv4if`	Assigns an IPv4 interface for media of a Media Component(s) operating under this Cluster Manager (Signaling Component) to the Media Realm. **Note:** This command is applicable only to Mediant CE SBC.

Command	Description
`remote-ipv6if`	Assigns an IPv6 interface for media of a Media Component(s) operating under this Cluster Manager (Signaling Component) to the Media Realm. **Note:** This command is applicable only to Mediant CE SBC.
`remote-media-subnet`	Defines the Remote Media Subnets table, which lets you define destination subnets for media (RTP/SRTP) traffic on a specific Media Realm. The table is a child of the Media Realm table. For more information, see remote-media-subnet on page 529.
`session-leg`	Defines the number of media sessions for the configured port range.
`tcp-port-range-end`	Defines the ending port of the range of media interface TCP ports for media (RTP, RTCP and T.38) and MSRP traffic.
`topology-location {down|up]`	Defines the display location of the Media Realm in the Topology view of the Web interface.
`used-by-routing-server {not-used| used}`	Enables the Media Realm to be used by a third-party routing server or ARM for call routing decisions.

Command Mode

Privileged User

Example

This example configures a Media Realm for IPv4 network interface "Voice", with port start from 5061 and with 10 sessions:

```
(config-voip)# realm 0
(realm-0)# name ITSP
(realm-0)# ipv4if Voice
(realm-0)# port-range-start 5061
```

```
(realm-0)# session-leg 10
 (realm-0)# activate
```

realm-extension

This command configures the Media Realm Extension table, which lets you define Media Realm Extensions. A Media Realm Extension defines a port range with the number of sessions for a specific Media-type network interface (configured in the IP Interfaces table). The table is a child of the Media Realm table.

Syntax

```
(config-voip)# realm <Index>
(realm-<Index># realm-extension <Index>
(realm-extension-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`ipv4if`	Assigns an IPv4 network interface (configured in the IP Interfaces table) to the Media Realm Extension.
`ipv6if`	Assigns an IPv6 network interface (configured in the IP Interfaces table) to the Media Realm Extension.
`port-range-start`	Defines the first (lower) port in the range of media UDP ports for the Media Realm Extension.
`session-leg`	Defines the number of media sessions for the port range.

Command Mode

Privileged User

Example

This example configures a Media Realm Extension where two sessions are for interface "Voice":

```
(config-voip)# realm 0
(realm-0)# realm-extension 1
(realm-extension-0/1)# ipv4if Voice
```

```
(realm-extension-0/1)# session-leg 2
(realm-extension-0/1)# activate
```

remote-media-subnet

This command configures the Remote Media Subnets table, which lets you define destination subnets for media (RTP/SRTP) traffic on a specific Media Realm. The table is a child of the Media Realm table.

Syntax

```
(config-voip)# realm <Index>
(realm-<Index># remote-media-subnet <Index>
(remote-media-subnet-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`address-family {ipv4|ipv6}`	Defines the IP address protocol.
`bw-profile`	Assigns a Bandwidth Profile to the Remote Media Subnet.
`dst-ip-address`	Defines the IP address of the destination.
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`prefix-length`	Defines the subnet mask in Classless Inter-Domain Routing (CIDR) notation.
`qoe-profile`	Assigns a Quality of Experience Profile to the Remote Media Subnet.

Command Mode

Privileged User

Example

This example configures a Remote Media Subnet for international calls to 201.10.5.1 assigned Bandwidth Profile "INT":

```
(config-voip)# realm 0
(realm-0)# remote-media-subnet 1
(remote-media-subnet-0/1)# name INT-Calls
(remote-media-subnet-0/1)# dst-ip-address 201.10.5.1
(remote-media-subnet-0/1)# bw-profile INT
(remote-media-subnet-0/1)# activate
```

98 remote-interface

This command configures the Remote Media Interface table, which lets you define media IP interfaces of the Media Components operating under the Cluster Manager (Signaling Component).

Syntax

```
(config-voip)# remote-interface <Index>
(remote-interface-<Index>)#
```

Command	Description
Index	Defines the table row index.
`name`	Defines the name of the IP Interface for media that is configured on the Media Component(s) in the IP Interfaces table.
`no-of-mcs`	Displays the number of Media Components that have the same media IP Interface name.

Command Mode

Privileged User

Note

- This table is configured automatically by the Stack Manager and therefore, it should be used only for viewing.
- This command is applicable only to Mediant CE SBC.

99 rtp-only sessions

This command configures the RTP-Only table, which lets you define RTP-only sessions, whereby RTP-to-RTP sessions are established based on pre-defined configuration (without SIP configuration). These sessions are established upon device startup and remain established (even if no voice) until configuration is deleted or the device is powered down.

Syntax

```
(config-voip)# rtp-only sessions <Index>
(sessions-<Index>)#
```

Command	Description
Index	Defines the table row index.
`group-name`	Defines a name for the group.
`incoming-rtp-payload-type-side-a`	Defines the payload type (0-127; -1 is any) of the incoming RTP for leg A.
`incoming-rtp-payload-type-side-b`	Defines the payload type (0-127; -1 is any) of the incoming RTP for leg B.
`local-interface-side-a`	Defines the IP Interface (IP Interfaces table) for leg A. **Note:** The IP Interface must have at least media for its 'Application Type'.
`local-interface-side-b`	Defines the IP Interface (IP Interfaces table) for leg B. **Note:** The IP Interface must have at least media for its 'Application Type'.
`local-udp-port-side-a`	Defines the local UDP port for side A. Local UDP spacing is configured by the [UdpPortSpacing] parameter. It is shared for all session groups and requires a device restart. The port is calculated as follows: `local-udp-port-side-a` + `session-count` * [UdpPortSpacing]
`local-udp-port-side-b`	Defines the local UDP port for side B. Local UDP spacing is configured by the [UdpPortSpacing] parameter. It is shared for all session groups and requires a device restart.

Command	Description
	The port is calculated as follows: `local-udp-port-side-b` + `session-count` * [UdpPortSpacing]
`remote-ip-side-a`	Defines the remote IP address (IPv4 or IPv6) of side A.
`remote-ip-side-b`	Defines the remote IP address (IPv4 or IPv6) of side B.
`remote-port-spacing-a`	Defines the remote UDP port spacing between sessions for side A. **Note:** Minimum port spacing is 2 (one for RTP and one for RTCP).
`remote-port-spacing-b`	Defines the remote UDP port spacing between sessions for side B. **Note:** Minimum port spacing is 2 (one for RTP and one for RTCP).
`remote-udp-port-side-a`	Defines the remote UDP port for side A. The port is calculated as follows: `remote-udp-port-side-a` + `session-count` * `remote-port-spacing-a`
`remote-udp-port-side-b`	Defines the remote UDP port for side B. The port is calculated as follows: `remote-udp-port-side-b` + `session-count` * `remote-port-spacing-b`
`sbc-connection-type {full-duplex|half-duplex}`	Defines the connection type - half duplex (A to B); full duplex (A-to-B and B-to-A).
`session-count`	Defines the number of sessions.

Command Mode

Privileged User

Note

- The feature can only be enabled and configured by the Security Administrator user.
- This command is applicable only to Mediant VE/CE SBC.
- For each session in the group, the local interfaces and remote IPs are shared.

Example

```
# configure voip
(config-voip)# rtp-only sessions 0
(sessions-0)# group-name media_rtp_1
(sessions-0)# session-count 3
(sessions-0)# local-interface-side-a media1
(sessions-0)# local-interface-side-b media2
(sessions-0)# local-udp-port-side-a 6000
(sessions-0)# local-udp-port-side-b 8000
(sessions-0)# remote-ip-side-a 10.4.2.138
(sessions-0)# remote-ip-side-b 10.4.4.138
(sessions-0)# remote-udp-port-side-a 6000
(sessions-0)# remote-udp-port-side-b 8000
(sessions-0)# remote-port-spacing-a 2
(sessions-0)# remote-port-spacing-b 2
(sessions-0)# sbc-connection-type full-duplex
(sessions-0)# incoming-rtp-payload-type-side-a -1
(sessions-0)# incoming-rtp-payload-type-side-b -1
(sessions-0)# activate
```

100 sbc

This command configures SBC tables.

Syntax

```
(config-voip)# sbc
```

Command	Description
classification	See classification below
dial-plan	See dial-plan <Index> on page 538
external-media-source	See external-media-source on page 541
malicious-signature-database	See malicious-signature-database on page 542
manipulation	See manipulation on page 543
routing	See routing on page 548
cac-profile	See cac-profile on page 558
settings	See settings on page 560

Command Mode

Privileged User

classification

This command configures the Classification table, which lets you define Classification rules.

Syntax

```
(config-voip)# sbc classification <Index>
(classification-<Index>)#
```

Command	Description
Index	Defines the table row index.

Command	Description
`action-type {allow|deny }`	Defines a whitelist or blacklist for the matched incoming SIP dialog.
`classification-name`	Defines a descriptive name, which is used when associating the row in other tables.
`dest-routing-policy`	Assigns a Routing Policy to the matched incoming SIP dialog.
`dst-host`	Defines the prefix of the destination Request-URI host name as a matching characteristic for the incoming SIP dialog.
`dst-user-name-pattern`	Defines the prefix of the destination Request-URI user part as a matching characteristic for the incoming SIP dialog.
`ip-group-selection {src-ip-group|tagged-ip-group}`	Defines how the incoming SIP dialog is classified to an IP Group.
`ip-group-tag-name`	Defines the source tag of the incoming SIP dialog.
`ip-profile-id`	Assigns an IP Profile to the matched incoming SIP dialog.
`message-condition-name`	Assigns a Message Condition rule to the Classification rule as a matching characteristic for the incoming SIP dialog.
`src-host`	Defines the prefix of the source URI host name as a matching characteristic for the incoming SIP dialog.
`src-ip-address`	Defines a source IP address as a matching characteristic for the incoming SIP dialog.
`src-ip-group-name`	Assigns an IP Group to the matched incoming SIP dialog.
`src-port`	Defines the source port number as a matching characteristic for the incoming SIP dialog.
`src-sip-interface-name`	Assigns a SIP Interface to the rule as a matching characteristic for the incoming SIP dialog.
`src-transport-type {any|tcp|tls|udp}`	Defines the source transport type as a matching characteristic for the incoming SIP dialog.
`src-user-name-pattern`	Defines the prefix of the source URI user part as a matching characteristic for the incoming SIP dialog.

Command	Description
`srd-name`	Assigns an SRD to the rule as a matching characteristic for the incoming SIP dialog.
`tls-remote-subject-name`	Defines the subject name (Common Name / CN or Subject Alternative Name / SAN) of the certificate used for the TLS connection upon which the SIP dialog message is received, as a matching characteristic for the incoming SIP dialog.

Command Mode

Privileged User

Example

This example configures a Classification rule whereby calls received from IP address 201.2.2.10 are classified as received from IP Group "ITSP":

```
(config-voip)# sbc classification 0
(classification-0)# classification-name ITSP
(classification-0)# src-ip-group-name ITSP
(classification-0)# src-ip-address 201.2.2.10
(classification-0)# activate
```

dial-plan

This command configures Dial Plans.

Syntax

```
(config-voip)# sbc dial-plan
```

Command	Description
<Index>	Defines the Dial Plan table row index (see dial-plan <Index> on the next page).
`dial-plan-rule`	Defines the Dial Plan Rule table, which defines the dial plans (rules) per Dial Plan. The table is a child of the Dial Plan table. For more information, see dial-plan-rule <Index> on page 539.
`export-csv-to <URL>`	Exports all Dial Plans (without their Dial Plan Rules) as a .csv file from the device to a remote server.

Command	Description
`import-csv-from <URL>`	Imports Dial Plans (without their Dial Plan Rules) to the device from a .csv file on a remote server. It deletes all existing Dial Plan Rules.

Command Mode

Privileged User

Example

This example exports all Dial Plans to a remote server:

```
(config-voip)# sbc dial-plan export-csv-to tftp://172.17.137.52/11.csv
```

dial-plan <Index>

This command configures the Dial Plan table, which defines the name of the Dial Plan. The table is a parent of the Dial Plan Rule table.

Syntax

```
(config-voip)# sbc dial-plan <Index>
(dial-plan-<Index>)#
```

Command	Description
<Index>	Defines the Dial Plan table row index.
`name`	Defines a name for the Dial Plan.
`prefix-case-sensitivity {disable|enable}`	Enables the matching process for the Dial Plan's prefix patterns, configured for its Dial Plan rules, to take into consideration the case (upper or lower) of alphabetical letters.

Command Mode

Privileged User

Example

This example configures a Dial Plan with the name "ITSP":

```
(config-voip)# sbc dial-plan 0
(dial-plan-0)# name ITSP
(dial-plan-0)# activate
```

dial-plan-rule

This command provides various commands for Dial Plan Rules.

Syntax

```
(config-voip)# sbc dial-plan <Dial Plan Index>
(dial-plan-<Dial Plan Index>)# dial-plan-rule {<Dial Plan Rule Index>|export-csv-to|import-csv-from}
```

Command	Description
<Dial Plans Rule Index>	Defines the Dial Plan Rules table (see dial-plan-rule <Index> below) for the specified Dial Plan.
`export-csv-to <URL>`	Exports all the Dial Plan Rules of the Dial Plan as a .csv file to a remote server.
`import-csv-from <URL>`	Imports all the Dial Plan Rules into the Dial Plan from a .csv file on a remote server. All the previously configured Dial Plan Rules of the Dial Plan are deleted.

Command Mode

Privileged User

Example

This example exports the Dial Plan Rules of Dial Plan #0 to a remote TFTP server:

```
(config-voip)# sbc dial-plan 0
(dial-plan-0)# dial-plan-rule export-csv-to tftp://172.17.137.52/My-Dial-Plan.csv
```

dial-plan-rule <Index>

This command configures the Dial Plan Rule table, which defines the dial plans (rules) per Dial Plan. The table is a child of the Dial Plan table.

Syntax

```
(config-voip)# sbc dial-plan <Dial Plan Index>
(dial-plan-<Dial Plan Index>)# dial-plan-rule <Dial Plan Rule Index>
(dial-plan-rule-<Index>/<Index>)#
```

Command	Description
<Dial Plan Rule Index>	Defines the Dial Plan Rule table row index.
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`prefix`	Defines the prefix number of the source or destination number.
`tag`	Defines a tag. **Note:** The entire tag's value (name and name=value) must be enclosed in double quotation marks ("..."). For example: `(dial-plan-rule-0/0)# tag "Tenant=10.1.1.1;ATT=10.2.3.4;BT=10.2.4.5"`

Command Mode

Privileged User

Example

This example configures a Dial Plan rule for Dial Plan #0, for calls received with prefix "1" with the name "ITSP":

```
(config-voip)# sbc dial-plan 0
(dial-plan-0)# name dial-plan-rule 1
(dial-plan-rule-0/1)# name INT
(dial-plan-rule-0/1)# prefix 1
(dial-plan-rule-0/1)# activate
```

dial-plan dial-plan-rule

This command exports and imports Dial Plan Rules of a specified Dial Plan.

Syntax

```
(config-voip)# sbc dial-plan dial-plan-rule
```

Command	Description
`export-csv-to <Dial Plan Index> <URL>`	Exports all the Dial Plan Rules of the specified Dial Plan as a .csv file to a remote server.
`import-csv-from <Dial Plan Index> <URL>`	Imports all the Dial Plan Rules into the specified Dial Plan, from a .csv file on a remote server. All the previously configured Dial Plan Rules of the specified Dial Plan are deleted.

Command Mode

Privileged User

Example

This example exports the Dial Plan Rules of Dial Plan #0 to a remote TFTP server:

```
(config-voip)# sbc dial-plan dial-plan-rule export-csv-to 0 tftp://172.17.137.52/My-Dial-Plan.csv
```

external-media-source

This command configures the External Media Source table, which defines an external media source for playing Music on Hold (MoH) to call parties that have been placed on-hold.

Syntax

```
(config-voip)# sbc external-media-source <Index>
(external-media-source-<Index>)#
```

Command	Description
Index	Defines the table row index. Only Index 0 is supported.
`dst-uri`	Defines the destination URI (user@host) of the SIP To header contained in the INVITE message that the device sends to the external media source.
`ip-group-name`	Assigns an IP Group from the IP Groups table.
`src-uri`	Defines the source URI (user@host) of the SIP From header

Command	Description
	contained in the INVITE message that the device sends to the external media source.

Command Mode

Privileged User

Example

This example configures an external media source for MoH:

```
(config-voip)# sbc sbc external-media-source 0
(external-media-source-0)# ip-group-name MoH-Player
(external-media-source-0)# activate
```

malicious-signature-database

This command configures the Malicious Signature table, which lets you define Malicious Signature patterns.

Syntax

```
(config-voip)# sbc malicious-signature-database <Index>
(malicious-signature-database-<Index>)#
```

Command	Description
Index	Defines the table row index.
name	Defines a descriptive name, which is used when associating the row in other tables.
pattern	Defines the signature pattern.

Command Mode

Privileged User

Example

This example configures a Malicious Signature for the SIP scan attack:

```
(config-voip)# sbc malicious-signature-database 0
(malicious-signature-database-0)# name SCAN
(malicious-signature-database-0)# pattern header.user-agent.content prefix 'sip-
scan'
(malicious-signature-database-0)# activate
```

manipulation

This command configures SBC manipulation tables.

Syntax

```
(config-voip)# sbc manipulation
```

Command	Description
`ip-inbound-manipulation`	See ip-inbound-manipulation below
`ip-outbound-manipulation`	See ip-outbound-manipulation on page 545

Command Mode

Privileged User

ip-inbound-manipulation

This command configures the Inbound Manipulations table, which lets you define IP-to-IP Inbound Manipulation rules. An Inbound Manipulation rule defines a manipulation sequence for the source or destination SIP URI user part of inbound SIP dialog requests.

Syntax

```
(config-voip)# sbc manipulation ip-inbound-manipulation <Index>
(ip-inbound-manipulation-<Index>)#
```

Command	Description
Index	Defines the table row index.
`dst-host`	Defines the destination SIP URI host name - full name, typically located in the Request URI and To headers.

Command	Description
`dst-user-name-pattern`	Defines the prefix of the destination SIP URI user name, typically located in the Request-URI and To headers.
`is-additional-manipulation {disable|enable}`	Determines whether additional SIP URI user part manipulation is done for the table entry rule listed directly above it.
`leave-from-right`	Defines the number of characters that you want retained from the right of the user name.
`manipulated-uri {destination|source}`	Determines whether the source or destination SIP URI user part is manipulated.
`manipulation-name`	Defines an arbitrary name to easily identify the manipulation rule.
`prefix-to-add`	Defines the number or string that you want added to the front of the user name.
`purpose {normal|routing-input-only|shared-line}`	Defines the purpose of the manipulation:
`remove-from-left`	Defines the number of digits to remove from the left of the user name prefix.
`remove-from-right`	Defines the number of digits to remove from the right of the user name prefix.
`request-type {all|invite|invite-and-register|invite-and-subscribe|register|subscribe}`	Defines the SIP request type to which the manipulation rule is applied.
`routing-policy-name`	Assigns a Routing Policy to the rule.
`src-host`	Defines the source SIP URI host

Command	Description
	name - full name (usually in the From header).
`src-ip-group-name`	Defines the IP Group from where the incoming INVITE is received.
`src-user-name-pattern`	Defines the prefix of the source SIP URI user name (usually in the From header).
`suffix-to-add`	Defines the number or string that you want added to the end of the user name.

Command Mode

Privileged User

Example

This example configures an Inbound Manipulation rule that adds prefix "40" to the URI if the destination hostname is "abc.com":

```
(config-voip)# sbc manipulation ip-inbound-manipulation 0
(ip-inbound-manipulation-0)# manipulation-name ITSP-MAN
(ip-inbound-manipulation-0)# dst-host abc.com
(ip-inbound-manipulation-0)# prefix-to-add 40
(ip-inbound-manipulation-0)# manipulated-uri destination
(ip-inbound-manipulation-0)# activate
```

ip-outbound-manipulation

This command configures the Outbound Manipulations table, which lets you define IP-to-IP Outbound Manipulation rules. An Outbound Manipulation rule defines a manipulation action for the SIP Request-URI user part (source or destination) or calling name of outbound SIP dialog requests.

Syntax

```
(config-voip)# sbc manipulation ip-outbound-manipulation <Index>
(ip-outbound-manipulation-<Index>)#
```

Command	Description
Index	Defines the table row index.
`calling-name-pattern`	Defines the prefix of the calling name (caller ID). The calling name appears in the SIP From header.
`dest-tags`	Assigns a prefix tag to denote destination URI user names corresponding to the tag configured in the associated Dial Plan.
`dst-host`	Defines the destination SIP URI host name - full name, typically located in the Request-URI and To headers.
`dst-ip-group-name`	Defines the IP Group to where the INVITE is to be sent.
`dst-user-name-pattern`	Defines the prefix of the destination SIP URI user name, typically located in the Request-URI and To headers.
`is-additional-manipulation {disable|yes}`	Determines whether additional manipulation is done for the table entry rule listed directly above it.
`leave-from-right`	Defines the number of digits to keep from the right of the manipulated item.
`manipulated-uri {destination|source}`	Defines the element in the SIP message that you want manipulated.
`manipulation-name`	Defines a descriptive name, which is used when associating the row in other tables.
`message-condition-name`	Assigns a Message Condition rule as a matching characteristic. Message Condition rules define required SIP message formats.
`prefix-to-add`	Defines the number or string to add in the front of the manipulated item.

Command	Description
`privacy-restriction-mode {dont-change-privacy|remove-restriction|restrict|transparent}`	Defines user privacy handling (i.e., restricting source user identity in outgoing SIP dialogs).
`re-route-ip-group-name`	Defines the IP Group that initiated (sent) the SIP redirect response (e.g., 3xx) or REFER message.
`remove-from-left`	Defines the number of digits to remove from the left of the manipulated item prefix.
`remove-from-right`	Defines the number of digits to remove from the right of the manipulated item prefix.
`request-type {all|invite|invite-and-register|invite-and-subscribe|register|subscribe}`	Defines the SIP request type to which the manipulation rule is applied.
`routing-policy-name`	Assigns a Routing Policy to the rule.
`src-host`	Defines the source SIP URI host name - full name, typically in the From header.
`src-ip-group-name`	Defines the IP Group from where the INVITE is received.
`src-tags`	Assigns a prefix tag to denote source URI user names corresponding to the tag configured in the associated Dial Plan.
`src-user-name-pattern`	Defines the prefix of the source SIP URI user name, typically used in the SIP From header.
`suffix-to-add`	Defines the number or string to add at the end of the manipulated item.
`trigger {3xx|3xx-or-refer|any|initial-only|refer}`	Defines the reason (i.e., trigger) for the re-routing of the SIP request.

Command Mode

Privileged User

Example

This example configures an Outbound Manipulation rule that removes two digits from the right of the destination URI if the calling name prefix is "WEI":

```
(config-voip)# sbc manipulation ip-outbound-manipulation 0
(ip-outbound-manipulation-0)# manipulation-name ITSP-OOUTMAN
(ip-outbound-manipulation-0)# calling-name-pattern WEI
(ip-outbound-manipulation-0)# manipulated-uri destination
(ip-outbound-manipulation-0)# remove-from-right 2
(ip-outbound-manipulation-0)# activate
```

routing

This command configures SBC routing.

Syntax

```
(config-voip)# sbc routing
```

Command	Description
`condition-table`	See condition-table below
`ip-group-set`	See ip-group-set on the next page
`ip2ip-routing`	See ip2ip-routing on page 551
`sbc-alt-routing-reasons`	See alt-routing-reasons on page 555
`sbc-routing-policy`	See sbc-routing-policy on page 557

Command Mode

Privileged User

condition-table

This command configures the Message Conditions table, which lets you define Message Condition rules. A Message Condition defines special conditions (requisites) for incoming SIP messages.

Syntax

```
(config-voip)# sbc routing condition-table <Index>
(condition-table-<Index>)#
```

Command	Description
Index	Defines the table row index.
`condition`	Defines the condition of the SIP message.
`name`	Defines a descriptive name, which is used when associating the row in other tables.

Command Mode

Privileged User

Example

This example configures a Message Condition rule whose condition is that a SIP Via header exists in the message:

```
(config-voip)# sbc routing condition-table 0
(condition-table-0)# name ITSP
(condition-table-0)# condition header.via.exists
(condition-table-0)# activate
```

ip-group-set

This command configures the IP Group Set table, which lets you define IP Group Sets. An IP Group Set is a group of IP Groups used for load balancing of calls, belonging to the same source, to a call destination (i.e., IP Group). The table is a parent of the IP Group Set Member table.

Syntax

```
(config-voip)# sbc routing ip-group-set <Index>
(ip-group-set-<Index>)#
```

Command	Description
Index	Defines the table row index.
ip-group-set-member	conf Defines igures the IP Group Set Member table, which lets you assign IP Groups to IP Group Sets. The table is a child of

Command	Description
	the IP Group Set table. For more information, see ip-group-set-member below.
`name`	Defines a descriptive name, which is used when associating the row in other tables.
`policy {homing|random-weight|round-robin}`	Defines the load-balancing policy.
`tags`	Defines tags.

Command Mode

Privileged User

Example

This example configures an IP Group Set where the IP Group load-balancing is of homing type:

```
(config-voip)# sbc routing ip-group-set 0
(ip-group-set-0)# name ITSP
(ip-group-set-0)# policy homing
(ip-group-set-0)# activate
```

ip-group-set-member

This command configures the IP Group Set Member Table, which lets you assign IP Groups to IP Group Sets. The table is a child of the IP Group Set table.

Syntax

```
(config-voip)# sbc routing ip-group-set <Index>
(ip-group-set-<Index>)# ip-group-set-member <Index>
(ip-group-set-member-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`ip-group-name`	Assigns an IP Group to the IP Group Set.

Command	Description
`weight {1-9}`	Defines the weight of the IP Group.

Command Mode

Privileged User

Example

This example configures an IP Group Set Member with IP Group "SIP-Trunk":

```
(config-voip)# sbc routing ip-group-set 0
(ip-group-set-0)# ip-group-set-member 1
(ip-group-set-member-0/1)# ip-group-name SIP-Trunk
(ip-group-set-member-0/1)# weight 9
(ip-group-set-member-0/1)# activate
```

ip2ip-routing

This command configures the IP-to-IP Routing table, which lets you define SBC IP-to-IP routing rules.

Syntax

```
(config-voip)# sbc routing ip2ip-routing <Index>
(ip2ip-routing-<Index>)#
```

Command	Description
Index	Defines the table row index.
`alt-route-options {alt-route-consider-inputs|alt-route-ignore-inputs|group-member-consider-inputs|group-member-ignore-inputs|route-row}`	Determines whether this routing rule is the main routing rule or an alternative routing rule (to the rule defined directly above it in the table).
`call-setup-rules-set-id`	Assigns a Call Setup Rule Set ID to the IP-to-IP Routing rule.
`cost-group`	Assigns a Cost Group to the routing rule for determining

Command	Description
	the cost of the call.
`dest-sip-interface-name`	Defines the destination SIP Interface to where the call is sent.
`dest-tags`	Assigns a prefix tag to denote destination URI user names corresponding to the tag configured in the associated Dial Plan.
`dst-address`	Defines the destination address to where the call is sent.
`dst-host`	Defines the host part of the incoming SIP dialog's destination URI (usually the Request-URI).
`dst-ip-group-name`	Defines the IP Group to where you want to route the call.
`dst-port`	Defines the destination port to where the call is sent.
`dst-transport-type {tcp|tls|udp}`	Defines the transport layer type for sending the call.
`dst-type {all-users|destination-tag|dial-plan|dst-address|enum|gateway|hunt-group|internal|ip-group|ip-group-set|ldap|request-uri|routing-server}`	Determines the destination type to which the outgoing SIP dialog is sent.
`dst-user-name-pattern`	Defines the prefix of the incoming SIP dialog's destination URI (usually the Request URI) user part. You can use special notations for denoting the prefix. T
`group-policy {forking|sequential}`	Defines whether the routing rule includes call forking.

Command	Description
`internal-action`	Defines a SIP response code (e.g., 200 OK) or a redirection response (with an optional Contact field indicating to where the sender must re-send the message) that the device sends to the sender of the incoming SIP dialog (instead of sending the call to another destination). The parameter is applicable only when the 'Destination Type' parameter in this table is configured to Internal.
`ipgroupset-name`	Assigns an IP Group Set to the routing rule.
`message-condition-name`	Assigns a SIP Message Condition rule to the IP-to-IP Routing rule.
`modified-dest-user-name`	Defines the user part of the Request-URI in the outgoing SIP dialog message.
`pre-route-call-setup-rules-set-id`	Assigns a Call Setup Rule Set ID to the IP-to-IP Routing rule.
`re-route-ip-group-name`	Defines the IP Group that initiated (sent) the SIP redirect response (e.g., 3xx) or REFER message.
`request-type {all|invite|invite-and-register|invite-and-subscribe|options|register|subscribe}`	Defines the SIP dialog request type (SIP Method) of the incoming SIP dialog.
`route-name`	Defines a descriptive name, which is used when associating the row in other tables.
`routing-tag-name`	Defines a routing tag name.

Command	Description
`sbc-routing-policy-name`	Assigns a Routing Policy to the rule.
`src-host`	Defines the host part of the incoming SIP dialog's source URI (usually the From URI).
`src-ip-group-name`	Defines the IP Group from where the IP call is received (i.e., the IP Group that sent the SIP dialog).
`src-tags`	Assigns a tag to denote source URI user names corresponding to the tag configured in the associated Dial Plan.
`src-user-name-pattern`	Defines the prefix of the user part of the incoming SIP dialog's source URI (usually the From URI).
`trigger {3xx|3xx-or-refer|any|broken-connection|fax-rerouting|initial-only|refer}`	Defines the reason (i.e., trigger) for re-routing (i.e., alternative routing) the SIP request.

Command Mode

Privileged User

Example

This example configures a routing rule for calls from IP Group "IPBX" to IP Group "ITSP":

```
(config-voip)# sbc routing ip2ip-routing 0
(ip2ip-routing-0)# route-name IPPBX-TO-SIPTRUNK
(ip2ip-routing-0)# src-ip-group-name IPBX
(ip2ip-routing-0)# dst-type ip-group
(ip2ip-routing-0)# dst-ip-group-name ITSP
(ip2ip-routing-0)# activate
```

alt-routing-reasons

This command configures the Alternative Reasons Set table, which lets you define a name for a group of SIP response codes for call release (termination) reasons that initiate alternative routing. The table is a parent of the Alternative Reasons Rules table, which defines the response codes.

Syntax

```
(config-voip)# sbc routing alt-route-reasons-set <Index>
(alt-route-reasons-set-<Index>)#
```

Command	Description
Index	Defines the table row index.
`alt-route-reasons-rules`	Defines the Alternative Reasons Rules table, which defines SIP response codes for the Alternative Reasons Set. The table is a child of the Alternative Reasons Set table. For more information, see alt-route-reasons-rules below.
`description`	Defines a description for the Alternative Reasons Set.
`name`	Defines a name for the Alternative Reasons Set, which is used when associating the row in other tables.

Command Mode

Privileged User

Example

This example configures an Alternative Reasons Set called "MyCodes":

```
(config-voip)# sbc routing alt-route-reasons-set 0
(alt-route-reasons-set-0)# name MyCodes
(alt-route-reasons-set-0)# activate
```

alt-route-reasons-rules

This command configures the Alternative Reasons Rules table, which lets you define SIP response codes per Alternative Reasons Set. The table is a child of the Alternative Reasons Set table.

Syntax

```
(config-voip)# sbc routing alt-route-reasons-set <Index>
(alt-route-reasons-set-<Index>)#  alt-route-reasons-rules <Index>
(alt-route-reasons-rules-<Index/Index>)
```

Command	Description
Index	Defines the table row index.
`rel-cause-code {400-bad-req|402-payment-req|403-forbidden|404-not-found|405-method-not-allowed|406-not-acceptable|408-req-timeout|409-conflict|410-gone|413-req-too-large|414-req-uri-too-long|415-unsup-media|420-bad-ext|421-ext-req|423-session-interval-too-small|480-unavail|481-transaction-not-exist|482-loop-detected|483-too-many-hops|484-address-incomplete|485-ambiguous|486-busy|487-req-terminated|488-not-acceptable-here|491-req-pending|493-undecipherable|4xx|500-internal-err|501-not-implemented|502-bad-gateway|503-service-unavail|504-server-timeout|505-version-not-supported|513-message-too-large|5xx|600-busy-everywhere|603-decline|604-does-not-exist-anywhere|606-not-acceptable|6xx|805-admission-failure|806-media-limits-exceeded|850-signalling-limits-exceeded}`	Defines a SIP response code for triggering the device's alternative routing mechanism.

Command Mode

Privileged User

Example

This example configures alternative routing when SIP response code 606 (Not Acceptable) is received:

```
(config-voip)# sbc routing alt-route-reasons-set 0
(alt-route-reasons-set-0)# alt-route-reasons-rules 0
(alt-route-reasons-rules-0/0)#  rel-cause-code 606-not-acceptable
(alt-route-reasons-rules-0/0)# activate
```

sbc-routing-policy

This command configures the Routing Policies table, which lets you define Routing Policy rules.

Syntax

```
(config-voip)# sbc routing sbc-routing-policy <Index>
(sbc-routing-policy-<Index>)#
```

Command	Description
Index	Defines the table row index.
`lcr-call-length`	Defines the average call duration (in minutes) and is used to calculate the variable portion of the call cost.
`lcr-default-cost {highest-cost|lowest-cost}`	Defines whether routing rules in the IP-to-IP Routing table that are not assigned a Cost Group are considered a higher cost or lower cost route compared to other matched routing rules that are assigned Cost Groups.
`lcr-enable {disabled|enabled}`	Enables the Least Cost Routing (LCR) feature for the Routing Policy.

Command	Description
`ldap-srv-group-name`	Assigns an LDAP Server Group to the Routing Policy.
`name`	Defines a descriptive name, which is used when associating the row in other tables.

Command Mode

Privileged User

Example

This example configures a Routing Policy for "ITSP" that is assigned LDAP Server Group "AD":

```
(config-voip)# sbc routing sbc-routing-policy 0
(sbc-routing-policy-0)# name ITSP
(sbc-routing-policy-0)# ldap-srv-group-name AD
(sbc-routing-policy-0)# activate
```

cac-profile

This command configures the Call Admission Control Profile table, which lets you define CAC profiles for call admission control (CAC) rules.

Syntax

```
(config-voip)# sbc cac-profile <Index>
(cac-profile-<Index>)#
```

Command	Description
Index	Defines the table row index.
cac-rule	Defines the Call Admission Control Rule table, which lets you define CAC rules per Call Admission Control Profile. The table is a child of the Call Admission Control Profile table. For more information, see cac-rule on the next page.

Command	Description
`name`	Defines a descriptive name, which is used when associating the row in other tables.

Command Mode

Privileged User

Example

This example configures a Call Admission Control Profile called "ITSP-CAC":

```
(config-voip)# sbc cac-profile 0
(cac-profile-0)# name ITSP-CAC
(cac-profile-0)# activate
```

cac-rule

This command configures the Call Admission Control Rule table, which lets you define Call Admission Control (CAC) rules per Call Admission Control Profile.

Syntax

```
(config-voip)# sbc cac-profile <Index>
(cac-profile-<Index>)# cac-rule <Index>
(cac-rule-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`limit`	Defines the maximum number of concurrent SIP dialogs.
`limit-per-user`	Defines the maximum number of concurrent SIP dialogs per user.
`max-burst`	Defines the maximum number of tokens (SIP dialogs) that the "bucket" can hold.
`max-burst-per-user`	Defines the maximum number of tokens (SIP dialogs) that the "bucket" can hold per user.

Command	Description
`rate`	Defines the maximum number of SIP dialogs per second for the token bucket.
`rate-per-user`	Defines the maximum number of SIP dialogs per second per user for the token bucket.
`request-direction {both|inbound|outbound}`	Defines the call direction of the SIP request to which the rule applies.
`request-type {all|invite|other|subscribe}`	Defines the SIP dialog-initiating request type to which you want to apply the rule (not the subsequent requests that can be of different type and direction).
`reservation`	Defines the guaranteed (minimum) call capacity.

Command Mode

Privileged User

Example

This example configures an Admission Rule that limits concurrent dialogs to 50:

```
(config-voip)# sbc cac-profile 0
(cac-profile-0)# cac-rule 1
(cac-rule-0/1)# limit 50
(cac-rule-0/1)# activate
```

settings

This command configures various SBC settings.

Syntax

```
(config-voip)# sbc settings
(sbc-settings)#
```

Command	Description
`abort-retries-on-icmp-`	If the device receives an ICMP error response as

Command	Description
`error {off|on}`	opposed to a timeout from a proxy, it may be desirable to abandon additional retries (configured by `fail-detect-rtx`) in favor of trying the next IP address (proxy) in the Proxy Set.
`auth-chlng-mthd {0|1}`	Set to 0 to use a www-authenticate header or 1 to send a proxy-authenticate header in the message
`auth-qop {0|1|3}`	Set to 0 to offer auth, 1 to offer auth-int or 2 to offer auth, auth-int, or 3 to not offer any QOP.
`backup-subscriptions {all|none|udp}`	Defines which SIP SUBSCRIBE dialogs for registered users the device backs up, based on transport protocol. The parameter is applicable only when the device operates in HA mode.
`bfcp-ip-from-audio {off|on}`	Enables the handling of calls with voice and Binary Floor Control Protocol (BFCP) media streams that are received from behind a NAT.
`disconnect-subscriptions`	Enables the device to disconnect (delete from storage) SUBSCRIBE dialogs associated with registered users, upon an unregister, upon register expiration, or upon a refresh register done from a different source IP address / port (like when the transport protocol is TCP or TLS).
`dtls-time-between-transmissions`	Defines the minimum interval (in msec) that the device waits between transmission of DTLS packets in the same DTLS handshake.
`early-media-broken-connection-timeout`	Defines the timeout for RTP broken connection on early media (msec).
`enable-msrp {off|on}`	Enables Message Session Relay Protocol (MSRP).
`end-point-call-priority`	Defines the ports call priority.
`enforce-media-order {off|on}`	Arrange media lines according to the previous offer-answer (required by RFC 3264).
`gw-direct-route-prefix`	Defines the prefix for call redirection from SBC to Gateway.
`gruu {off|on}`	Obtain and use GRUU (Global Routable

Command	Description
	UserAgentURIs).
`keep-contact-user-in-reg {keep-user|off|on|unique-param|unique-user}`	Keeps original Contact User in REGISTER requests.
`lifetime-of-nonce`	Defines the lifetime of the nonce in seconds.
`long-call-minutes`	Defines the minimum duration (in minutes) of an SBC call for it to be considered a long call and included in the performance monitoring count for long calls.
`media-channels`	Defines the number of channels associated with media services (announcements, conferencing).
`min-session-expires`	Defines the minimum amount of time that can occur between session refresh requests in a dialog before the session is considered timed out.
`msrp-connection-establish-timeout`	Defines the timeout (msec) for establishing MSRP connections.
`no-rtp-detection-timeout`	Defines the timeout (msec) for RTP packet detection after call connect, or during early media or upon call connect.
`no-rtp-mode {disconnect|reroute|reroute-with-original-sip-headers}`	Defines the device's handling of calls if RTP packets are not received (detected) during early media or upon call connect (i.e., never was RTP) within a user-defined timeout (no-rtp-detection-timeout).
`num-of-subscribes`	Defines the active SUBSCRIBE sessions limit.
`p-assert-id {0|1|2}`	0 - As Is,1- Add P-Asserted-Identity Header, 2 - Remove P-Asserted-Identity Header
`play-tone-on-connect-failure-behavior {Disconnect|Ignore}`	Defines if the device connects or disconnects the call if it can't play the specified tone to the call party.
`pns-register-timeout`	Defines the maximum time (in seconds) that the device waits for a SIP REGISTER refresh message from the user, before it forwards an incoming SIP

Command	Description
	dialog-initiating request (e.g., INVITE) to the user.
`pns-reminder-period`	Defines the time (in seconds) before the user's registration with the device expires, at which the device sends an HTTP message to the Push Notification Server to trigger it into sending a push notification to the user to remind the user to send a REGISTER refresh message to the device.
`regions-connectivity-dial-plan`	Defines the Dial Plan that the device must search in the Dial Plans table to check if the source and destination Teams sites share a common group number.
`reserve-dsp-on-sdp-offer {off|on}`	Enables the device to reserve (guarantee) DSP resources for a call on the SDP Offer.
`sas-notice {off|on}`	If enabled - when SBC needs to terminates a REGISTER request, it adds a body (survivability notice) to the 200OK response.
`sbc-100trying-upon-reinvite {off|on}`	Defines if the device sends a SIP 100 Trying response upon receipt of a re-INVITE request.
`sbc-3xx-bhvt {transparent|using-db}`	Defines how the device passes Contact in 3xx responses.
`sbc-broadworks-survivability {off|on}`	Indicates how the registration database is provisioned.
`sbc-bye-auth {off|on}`	Allows the media to remain active upon receipt of a 401/407 response by sending a releaseNackEvent, rather than releaseEvent.
`sbc-db-route-mode {all-permutations|uri-dependant}`	Defines the database binding mode for routing search.
`sbc-dialog-info-interwork`	Changes the WAN call identifiers in the dialog-info body of NOTIFY messages to LAN call identifiers.
`sbc-dialog-subsc-route-mode {0|1}`	Determines where in-dialog refresh subscribes are sent.
`sbc-direct-media`	Enables direct media.

Command	Description
`{off|on}`	
`sbc-diversion-uri-type {sip|tel|transparent}`	Defines which URI to use for Diversion header.
`sbc-dtls-mtu`	Defines the DTLS max transmission unit.
`sbc-emerg-condition`	Defines the Emergency Message Condition.
`sbc-emerg-rtp-diffserv`	Defines the RTP DiffServ value for Emergency calls.
`sbc-emerg-sig-diffserv`	Defines the Signaling DiffServ value for Emergency calls.
`sbc-fax-detection-timeout`	Defines the maximum time for fax detection (seconds).
`sbc-forking-handling-mode {latch-on-first|sequential}`	Defines the handling method for 18X response to forking.
`sbc-gruu-mode {as-proxy|both|none|public-only|temporary-only}`	Defines the GRUU behavior.
`sbc-keep-call-id {off|on}`	Keeps original call Id for outgoing messages.
`sbc-max-fwd-limit`	Defines the limit of the Max-Forwards header.
`sbc-media-sync {avoid|enable|never}`	Enables media sync process.
`sbc-mx-call-duration`	Defines the call duration limit.
`sbc-no-alert-timeout`	Defines the maximum time to wait for connect (seconds).
`sbc-preemption-mode {disabled|enabled}`	Defines the SBC Preemption mode.
`sbc-preferences`	Defines the coders combination in the outgoing message.
`sbc-prxy-rgstr-time`	Defines the duration (in seconds) in which the user is registered in the proxy DB, after the REGISTER

Command	Description
	was forwarded by the device.
`sbc-rand-expire`	Defines the upper limit for the number of seconds the SBC detracts from the Expires value in Register and Subscribe responses.
`sbc-refer-bhvr {regular|regular-using-db|set-host-part-to-ipgroup-name}`	Defines handling of Refer-To in REFER requests.
`sbc-remove-sips-non-sec-transp {off|on}`	Defines the SIP headers for which the device replaces “sips:” with “sip:” in the outgoing SIP-initiating dialog request (e.g., INVITE) when the destination transport type is unsecured (e.g., UDP).
`sbc-rgstr-time`	Defines the Expires value.
`sbc-routing-timeout`	Defines the maximum duration (in seconds) that the device is prepared to wait for a response from external servers when a routing rule is configured to query an external server (e.g., LDAP server) on whose response the device uses to determine the routing destination.
`sbc-rtcp-mode {generate-always|generate-only-if-rtp-active|transparent}`	Defines the RTCP mode.
`sbc-server-auth-mode {local_mode|remote_server| sterman}`	Defines the authentication mode.
`sbc-sess-exp-time`	Defines the session refresh timer for requests in a dialog.
`sbc-session-refresh-policy {remote-refresh|sbc-refresh}`	Defines whether Remote or SBC should be refresher when SBC terminates the Session Expire refreshing.
`sbc-shareline-reg-mode {as-configured|terminate-secondary-lines }`	Defines the registration handling mode in case of shared line manipulation.

Command	Description
`sbc-subs-try {off|on}`	If enabled, 100 Trying response will be sent for SUBSCRIBE and NOTIFY.
`sbc-surv-rgstr-time`	Defines the duration of the periodic registrations between the user and the SBC, when the SBC is in survivability state.
`sbc-terminate-options {off|on}`	Defines the handling of in-dialog SIP OPTIONS messages.
`sbc-usr-reg-grace-time`	Defines the additional grace time (in seconds) added to the user's timer in the database.
`sbc-usr-rgstr-time`	Defines the Expires value SBC responds to user with.
`sbc-xfer-prefix`	Defines the prefix for routing and manipulations when URL database is used.
`send-invite-to-all {disable|enable}`	Disable - SBC sends INVITE according to the Request-URI. Enabled-if the Request-URI is of specific contact, SBC sends the INVITE to all contacts under the parent AOR.
`session-expires-observer-mode [grace|strict]`	Defines the observer method when the IP Profile parameter, 'Session Expires Mode' is configured to **Observer**.
`short-call-seconds`	Defines the duration (in seconds) of an SBC call for it to be considered a short call and included in the count of the performance monitoring for short calls.
`sip-server-digest-algorithm {md5|sha256}`	Defines the cryptographic hash algorithm used in the outgoing authentication challenge (SIP 401 or 407) response when the device authenticates incoming SIP requests as an authentication server.
`sip-topology-hiding-mode {by-host-name-params-only| fallback-to-ip-addresses}`	Enables the device to overwrite the host part in SIP headers concerned with the source of the message with the IP address of the device's IP Interface, and SIP headers concerned with the destination of the message with the destination IP address, unless the relevant host name parameters of the IP Group ('SIP Group Name' and 'SIP Source Host Name') are

Command	Description
	configured.
`sliding-window-for-cac {off|on}`	Enables the rate-limiting Sliding Window Counter algorithm for Call Admission Control (CAC).
`transcoding-mode {force-transcoding|only-if-required|rtp-forwarding}`	Defines the transcoding mode.
`unclassified-calls {allow|reject}`	Allows unclassified incoming calls.
`uri-comparison-excluded-params`	Defines which URI parameters are excluded when the device compares the URIs of two incoming dialog-initiating SIP requests (e.g., INVITEs) to determine if they were sent from a user that is registered in the device's registration database (registered AOR and corresponding Contact URI), during Classification.
`xfer-success-time-out`	Defines the maximum time (in msec) to wait for release an original call on transfer.

Command Mode

Privileged User

Example

This example enables Direct Media:

```
(config-voip)# sbc settings
(sbc-settings)# sbc-direct-media on
(sbc-settings)# activate
```

101 sip-definition

This command configures various SIP settings.

Syntax

```
(config-voip)# sip-definition
```

Command	Description
`account`	See account below
`least-cost-routing cost-group`	See least-cost-routing cost-group on page 570
`proxy-and-registration`	See proxy-and-registration on page 572
`settings`	See settings on page 578
`sip-recording`	See sip-recording on page 594

Command Mode

Privileged User

account

This command configures the Accounts table, which lets you define user registration accounts.

Syntax

```
(config-voip)# sip-definition account <Index>
(account-<Index>)#
```

Command	Description
Index	Defines the table row index.
`account-name`	Defines an arbitrary name to easily identify the row.
`application-type {gw|sbc}`	Defines the application type.

Command	Description
`contact-user`	Defines the AOR username.
`host-name`	Defines the Address of Record (AOR) host name.
`password`	Defines the digest MD5 Authentication password. **Note:** If the password contains a question mark (?) and you're configuring the parameter through CLI, you must enclose the entire password in double quotation marks (e.g., "43LSyk+?").
`re-register-on-invite-failure`	Enables the device to re-register an Account upon the receipt of specific SIP response codes (e.g., 403, 408, and 480) for a failed INVITE message which the device routed from the Account to a remote user agent (UA).
`reg-by-served-ipg-status {reg-always| reg-if-online}`	Defines the device's handling of Account registration based on the connectivity status of the Served IP Group.
`reg-event-package-subscription {disable|enable}`	Enables the device to subscribe to Reg Event Package service with the registrar, which provides notifications of registration state changes, for the Registrar Stickiness feature.
`register {disable|gin|reg}`	Enables registration.
`registrar-search-mode {by-ims-spec|current-server|avoid-prev-until-expiry}`	Defines the method for choosing an IP address (registrar) in the Proxy Set (associated with the Serving IP Group) to which the Account initially registers and performs registration refreshes, when the Register Stickiness feature is enabled.
`registrar-stickiness {disable|enable|enable-for-non-register-requests}`	Enables the "Registrar Stickiness" feature, whereby the device always routes SIP requests of a registered Account to the same registrar server to where the last successful REGISTER request was routed.
`served-ip-group-name`	Defines the IP Group (e.g., IP-PBX) that you want to register and/or authenticate upon its behalf.
`served-trunk-group`	Defines the Trunk Group that you want to register and/or authenticate.

Command	Description
`serving-ip-group-name`	Defines the IP Group (Serving IP Group) to where the device sends the SIP REGISTER requests (if enabled) for registration and authentication (of the Served IP Group).
`udp-port-assignment {disable|enable}`	Enables the device to dynamically allocate local SIP UDP ports to Accounts using the same Serving IP Group, where each Account is assigned a unique port on the device's leg interfacing with the Accounts' Serving IP Group.
`user-name`	Defines the digest MD5 Authentication username.

Command Mode

Privileged User

Example

This example configures an Account with a username and password that registers IP Group "IPBX" with IP Group "ITSP":

```
(config-voip)# sip-definition account 0
(account-0)# user-name JoeD
(account-0)# password 1234
(account-0)# register reg
(account-0)# served-ip-group-name IPPBX
(account-0)# serving-ip-group-name ITSP
(account-0)# activate
```

least-cost-routing cost-group

This command configures Least Cost Routing (LCR). This command configures the Cost Groups table, which lets you define Cost Groups. A Cost Group defines a fixed call connection cost and a call rate (charge per minute.

Syntax

```
(config-voip)# sip-definition least-cost-routing cost-group <Index>
(cost-group-<Index>)#
```

Command	Description
Index	Defines the table row index.
`cost-group-name`	Defines a descriptive name, which is used when associating the row in other tables.
`cost-group-time-bands`	Defines the Time Band table, which lets you define Time Bands per Cost Group. The table is a child of the Cost Groups table. For more information, see cost-group-time-bands below.
`default-connection-cost`	Defines the call connection cost (added as a fixed charge to the call) for a call outside the time bands.
`default-minute-cost`	Defines the call charge per minute for a call outside the time bands.

Command Mode

Privileged User

Example

This example configures LCR "INT" with default connection cost of 10 and minute cost of 1:

```
(config-voip)# sip-definition least-cost-routing cost-group 0
(cost-group-0)# cost-group-name INT
(cost-group-0)# default-connection-cost 10
(cost-group-0)# default-minute-cost 1
(cost-group-0)# activate
```

cost-group-time-bands

This command configures the Time Band table, which lets you define Time Bands per Cost Group. A Time Band defines a day and time range (e.g., from Saturday 05:00 to Sunday 24:00) and a fixed call connection charge and call rate per minute for this interval. The table is a "child" of the Cost Groups table.

Syntax

```
(config-voip)# sip-definition least-cost-routing cost-group <Index>
(cost-group-<Index>)# cost-group-time-bands <Index>
(cost-group-time-bands-<Index>/<Index>)#
```

Command	Description
Index	Defines the table row index.
`connection-cost`	Defines the call connection cost during the time band.
`end-time`	Defines the day and time of day until when this time band is applicable.
`minute-cost`	Defines the call cost per minute charge during the time band.
`start-time`	Defines the day and time of day from when this time band is applicable.

Command Mode

Privileged User

Example

This example configures an LCR time band between Saturday 1 am to Sunday midnight with connection cost of 1 and minute cost of 0.5:

```
(config-voip)# sip-definition least-cost-routing cost-group 0
(cost-group-0)# cost-group-time-bands 1
(cost-group-time-bands-0/1)# start-time SAT:01:00
(cost-group-time-bands-0/1)# end-time SUN:23:59
(cost-group-time-bands-0/1)# connection-cost 1
(cost-group-time-bands-0/1)# minute-cost 0.5
(cost-group-time-bands-0/1)# activate
```

proxy-and-registration

This command configures various SIP proxy and registration settings.

Syntax

```
(config-voip)# sip-definition proxy-and-registration
(sip-def-proxy-and-reg)#
```

Command	Description
`account-registrar-`	Defines a graceful time (in seconds) which is intended to prevent the device from sending REGISTER requests to a

Command	Description
avoidance-time	registrar server where the device previously registered, if the device also registered successfully to another server since the last successful registration to the registrar server.
add-init-rte-hdr	Defines if the initial Route header is added to REGISTER request.
always-use-proxy	Sends all messages to proxy servers
authentication-mode	Defines the Authentication mode.
auth-password	Defines the password for authentication.
challenge-caching	SIP Challenge caching mode
cnonce-4-auth	Defines the Cnonce parameter used for authentication.
dns-query	Defines the DNS query type.
enable-proxy	Defines if SIP proxy is used.
enable-registration	Enables Proxy registration.
expl-un-reg	Enables if explicit unregister needed.
failed-options-retry-time	Defines how long the device waits (in seconds) before re-sending a SIP OPTIONS keep-alive message to the proxy once the device considers the proxy as offline.
fallback-to-routing	Enables fallback to internal Tel-to-IP Routing table if Proxy is not responding.
gen-reg-int	Defines the time interval in seconds for generating registers.
gw-name	Defines the Gateway name.
gw-registration-name	Defines the Gateway registration name.
ip-addrr-rgstrr	Defines the SIP Registrar IP address.
max-gen-reg-rate	Defines the max. generated Register requests per interval.

Command	Description
max-registration-backoff-time	Defines the Backoff mechanism that is applied between failed registration attempts initiated by the device.
mutual-authentication	Defines the Mutual Authentication mode.
nb-of-rtx-b4-hot-swap	Defines the number of retransmissions before Hotswap is done.
options-user-part	Defines the OPTIONS user part string for all gateways.
ping-pong-keep-alive [off|on]	Enables Ping-Pong for Keep-Alive to proxy via reliable connection.
ping-pong-keep-alive-time	Defines the Ping Keep-Alive, which is sent (using CRLFCRLF) each time this timer expires (seconds).
prefer-routing-table	Enables preference of Routing table.
proxy-dns-query	Defines the DNS proxy query type.
proxy-ip-lst-rfrsh-time	Defines the interval between refresh of proxies list (seconds).
proxy-name	Defines the SIP proxy name.
re-registration-timing	Defines the percentage of RegistrationTime when new REGISTER requests are sent.
redirect-in-facility	Enables search for Redirect number in Facility IE.
redundancy-mode	Defines the Redundancy mode.
reg-on-conn-failure	Enables re-registration on TCP/TLS connection failure.
reg-on-invite-fail	Enable re-register upon INVITE transaction failure.
reg-sync-mode {off| on}	Enables registration synchronization of Accounts (Accounts table) and users (SBC User Information table) that use the same proxy server (Serving IP Group) when a response timeout

Command	Description
	or failure (e.g., SIP 403) for a sent SIP REGISTER request occurs.
`registrar-name`	Defines the SIP Registrar name.
`registrar-transport`	Defines the Registrar transport type.
`registration-retry-time`	Defines the time in which the device tries to register after last registration failure (seconds).
`registration-time`	Defines the time in which registration to Gatekeeper/Proxy is valid.
`registration-time-thres`	Defines the registration time threshold.
`rte-tbl-4-host-names`	Enables always use routing table even though proxy is available.
`set-oos-on-reg-failure`	Defines whether to deactivate endpoint service on registration failure.
`should-register`	Defines the Register/UnRegister entities.
`sip-rerouting-mode`	Defines the routing mode after receiving 3xx response or transfer.
`subscription-mode`	Defines the Subscription mode.
`trusted-proxy`	Defines whether the proxy is a trusted node.
`use-gw-name-for-opt`	Enables use of Gateway name (instead of IP address) in Keep-Alive OPTIONS messages.
`use-proxy-ip-as-host`	Enables use of the Proxy IP as Host in From and To headers.
`use-rand-user`	Enables the device to assign a random string value for the user part of the SIP Contact header in the REGISTER message (generated by the device) for new user Account registrations with the device.
`user-info`	Defines the User Info tables (see user-info on the next page).
`user-name-4-auth`	Defines the username for authentication.

Command Mode

Privileged User

Example

This example enables ping-pong keep-alive:

```
(config-voip)# sip-definition proxy-and-registration
(sip-def-proxy-and-reg)# ping-pong-keep-alive on
(sip-def-proxy-and-reg)# activate
```

user-info

This command configures the User Info tables.

Syntax

```
(config-voip)# sip-definition proxy-and-registration
(sip-def-proxy-and-reg)# user-info
```

Command	Description
`find`	Searches an entry in the User Info table.
`gw-user-info {0-499|export-csv-to <URL>|find-by <Column and Value>|import-csv-from URL>|new}`	Defines and performs various actions on the Gateway User Info table: - Accesses a specific table row index. - Exports the User Info table as a .csv file to a URL - Searches a row entry by column {display-name|global-phone-num|password|pbx-ext|username} - Imports a User Info file (.csv) from a URL - Defines a new entry in the table
`sbc-user-info {0-499|export-csv-to <URL>|find-by <Column and Value>|import-csv-from <URL>|new}`	Defines and performs various actions on the SBC User Info table: - Accesses a specific table row index. - Exports the User Info table as a .csv file to a URL - Searches a row entry by column {ip-group-

Command	Description
	name|local-user|password|username} ■ Imports a User Info file (.csv) from a URL ■ Defines a new entry in the table

Command Mode

Privileged User

Example

This example searches for the user "Joe":

```
(config-voip)# sip-definition proxy-and-registration
(sip-def-proxy-and-reg)# user-info sbc-user-info find-by local-user Joe
sbc-user-info 2
 local-user "Joe"
 username ""
 password ""
 ip-group-name "MoH Users"
```

push-notification-servers

This command configures the Push Notification Servers table, which defines Push Notification Services.

Syntax

```
(config-voip)# sip-definition push-notification-servers <Index>
(push-notification-servers-<Index>)#
```

Command	Description
`protocol {ac-proprietary}`	Defines the protocol for exchanging information between the device and the Push Notification Server.
`provider`	Defines the name of the Push Notification Service.
`remote-http-service`	Assigns a Remote Web Service, which defines the URL address (and other related parameters) of the HTTP-based Push Notification Server.

Command Mode

Privileged User

Example

This example configures a Push Notification Service provided by Android's Firebase Cloud Messaging (FCM) at Index #0:

```
(config-voip)# sip-definition push-notification-servers 0
(push-notification-servers-0)# provider fcm
(push-notification-servers-0)# protocol ac-proprietary
(push-notification-servers-0)# remote-http-service PNS-Android
```

settings

This command configures various SIP settings.

Syntax

```
(config-voip)# sip-definition settings
(sip-def-settings)#
```

Command	Description
`100-to-18x-timeout`	Defines the time between 100 response and 18x response.
`183-msg-behavior {progress|alert}`	Sends ALERT to ISDN upon 183 receive.
`1st-call-rbt-id`	Defines the index of the first call ringback tone in the Call-Progress Tones file.
`3xx-use-alt-route {dont-use|no-6XX|yes}`	Enables use of Alternative Route Reasons Table for 3xx.
`FarEndDisconnectSilenceMethod {none|packets-count| voice-energy-detectors|all}`	Defines the far disconnect silence detection method.
`FarEndDisconnectSilencePeriod`	Defines the silence period detection time.
`authenticated-message-`	Defines if a Message Manipulation Set is

Command	Description
`handling {no-changes-permitted| register-changes-permitted}`	run again on incoming authenticated SIP messages received after the device sends a SIP 401 response for challenging initial incoming SIP REGISTER requests.
`aaa-indications {none|accounting-only}`	Defines the Authentication, Authorization and Accounting indications to use.
`accounting-port`	Defines the RADIUS accounting port.
`accounting-server-ip`	Defines the RADIUS accounting server IP.
`add-empty-author-hdr {off|on}`	Enables empty Authorization header to be added to Register request.
`amd-beep-detection {disable|start-after-amd|start-immediately}`	Defines the AMD beep detection mode.
`amd-mode {dont-disconnect|disconnect-on-amd}`	Defines the AMD mode.
`anonymous-mode {anonymous-invalid|ip-address}`	Defines the "anonymous" mode.
`app-sip-transport-type`	Defines the SIP transport type.
`application-profile`	Defines the Application Profile.
`backward-pt-behavior {off|on}`	Enables backward compatibility for using parameters that configure Rx payload types for media features.
`broken-connection-event-timeout`	Defines the duration the RTP connection should be broken before the Broken Connection event is issued [100ms].
`busy-out {off|on}`	Enables trunks to be taken out of service in case of LAN down.
`call-info-list {multiple-headers|single-header}`	Defines how the device handles SIP Call-Info headers with multiple values in outgoing SIP messages.
`call-num-plybck-id`	Defines the Calling Number Play Back ID.

Command	Description
`call-pickup-key`	Defines the key sequence for call pickup.
`call-transfer-using-reinvites {off|on}`	Enables Call Transfer using re-INVITEs.
`calls-cut-through {off|on}`	Enables call connection without on-hook/off-hook process 'Cut-Through'.
`cdr-report-level {none|end-call|start-and-end-call|connect-and-end-call|start-and-end-and-connect-call}`	Defines the CDR report timing.
`cdr-srvr-ip-adrr`	Defines the Syslog server IP address for sending CDRs.
`classify-by-proxy-set-mode {both|contact-header|ip-address}`	Defines which IP address to use for classifying the incoming SIP dialog message to an IP Group, based on Proxy Set.
`coder-priority-nego {sdp-remote-pri|sdp-local-pri}`	Defines the coder priority in SDP negotiation.
`crypto-life-time-in-sdp {off|on}`	Disables Crypto life time in SDP.
`current-disc {off|on}`	Enables disconnect call upon detection of current disconnect signal.
`default-record-uri`	Defines the default record location URI used by Media Ctrl.
`delay-after-reset`	Defines the Gateway delay time after restart (seconds).
`delay-b4-did-wink`	Defines the delay between off-hook detection and Wink generation (FXS).
`delayed-offer {off|on}`	Enables sending INVITE message with/without SDP offer.
`dflt-release-cse`	Defines the release cause sent to IP or Tel when device initiates release.
`dfrnt-port-after-hold {off|on}`	Enables use of different RTP port after

Command	Description
	hold.
`did-wink-enbl {disabled|single|double-wink|double-polarity}`	Enables DID lines using Wink.
`digest-auth-uri-mode {full|without-param}`	Defines if the device includes or excludes URI parameters for the Digest URI in the SIP Proxy-Authorization or Authorization headers of the request that the device sends in reply to a received SIP 401 (Unauthorized) or 407 (Proxy Authentication Required) response.
`digit-delivery-2ip {off|on}`	Enables automatic digit delivery to IP after call is connected.
`digit-delivery-2tel {off|on}`	Enables automatic digit delivery to Tel after line is off-hooked or seized.
`digit-pttrn-on-conn`	Enables Play Code string to Tel when connect message received from IP.
`disc-broken-conn`	Defines the behavior when receiving RTP or MSRP broken notification.
`disc-on-silence-det {disable|enable}`	Enables disconnect calls on a configured silence timeout.
`disp-name-as-src-nb {disable|enable|prefered}`	Enables display name to be used as source number.
`display-default-sip-port {off|on}`	Enables default port 5060 shown in the headers.
`e911-callback-timeout`	Defines the maximum time for an E911 ELIN callback to be valid (minutes).
`e911-gateway`	Enables E911 to NG911 gateway and ELIN handling.
`emerg-alert-info-uri`	Defines the URI of the SIP Alert-Info header, for the device to consider (identify) the incoming SIP INVITE message as an emergency call (IP-to-Tel).

Command	Description
`emerg-calls-regrt-t-out`	Defines the regret time for Emergency calls.
`emerg-nbs`	Defines emergency numbers.
`emrg-spcl-rel-cse`	set configuration
`enable {off|on}`	Enables RADIUS.
`enable-did {off|on}`	Enables DID for all FXS ports (that are are not enabled for DID per FXS port - see enable-did on page 379).
`enable-ptime {off|on}`	Enables requirement of ptime parameter in SDP.
`enable-sips`	Enables SIP secured URI usage.
`enbl-non-inv-408 {off|on}`	Enables sending 408 responses for non-INVITE transactions.
`encrypt-key-aes256`	Defines the AES-256 encryption key for encrypting (and decrypting) the SIP header value.
`enum-service-domain`	Defines the ENUM domain for ENUM resolution.
`fake-retry-after`	Defines if the device, upon receiving a SIP 503 response without a Retry-After header, behaves as if the 503 response included a Retry-After header and with the period (in seconds) specified by the parameter.
`fake-tcp-alias`	Enables enforcement reuse of TCP/TLS connection.
`fax-re-routing`	Enables rerouting of fax calls to fax destination.
`fax-sig-method {no-fax|t.38-relay|g.711-transport| fax-fallback|g.711-reject-t.38}`	Defines fax signaling method.

Command	Description
`filter-calls-to-ip`	Enables filtering of calls to IP.
`force-generate-to-tag {disable|enable}`	Enables the device to generate the 'tag' parameter's value in the SIP To header for SBC calls.
`force-rport`	Enables responses sent to the UDP port from where the Request was sent, even if RPORT parameter was not received in the Via header.
`forking-delay-time-invite`	Defines the forking delay time (in seconds) to wait before sending INVITE of second forking call.
`graceful-bsy-out-t-out`	Defines the Graceful Busy Out timeout in seconds.
`gw-mx-call-duration`	Limits the device call time duration (minutes).
`handle-reason-header`	
`hist-info-hdr`	Enables History-Info header support.
`ignore-auth-stale`	Enables the device to retry registering even if the last SIP 401\407 response included "stale=false".
`ignore-remote-sdp-mki`	Ignores MKI if present in the remote SDP
`immediate-trying`	Enables immediate trying sent upon INVITE receive.
`ip-security`	Defines the mode to handle calls based on ip-addr defined in ip2tel-rte-tbl.
`ldap-display-nm-attr`	Defines the name of the attribute which represents the user display name in the Microsoft AD database.
`ldap-mobile-nm-attr`	Defines the name of the attribute which represents the user Mobile number in the Microsoft AD database.
`ldap-ocs-nm-attr`	Defines the name of the attribute which

Command	Description
	represents the user OCS number in the Microsoft AD database.
`ldap-pbx-nm-attr`	Defines the name of the attribute which represents the user PBX number in the Microsoft AD database.
`ldap-primary-key`	Defines the name of the query primary key in the Microsoft AD database.
`ldap-private-nm-attr`	Defines the name of the attribute which represents the user Private number in the Microsoft AD database.
`ldap-secondary-key`	Defines the name of the query secondary key in the Microsoft AD database.
`max-491-timer`	Defines the maximum timer for next request transmission after 491 response.
`max-nb-of-act-calls`	Defines the limit of number of concurrent calls.
`max-sdp-sess-ver-id`	Defines the maximum number of characters allowed in the SDP body's "o=" (originator and session identifier) field for the session ID and session version values.
`media-cdr-rprt-level`	Defines the Media CDR reports,
`message-policy-reject-response-type`	Defines the response type returned when a message is rejected according to the Message Policy.
`microsoft-ext`	Enables Microsoft proprietary Extension to modify called-nb.
`min-session-expires`	Defines the time (in seconds) in the SIP Min-SE header, which is the minimum time that the user agent refreshes the session for Gateway calls.
`mn-call-duration`	Defines the minimum call duration.
`ms-mx-rcrd-dur`	Defines the maximum record duration

Command	Description
	supported by Microsoft.
`mult-ptime-format`	Defines the format of multiple ptime (ptime per coder) in outgoing SDP.
`mx-call-duration`	Defines the call time duration limit (minutes).
`mx-pr-dur-ivr-dia`	Defines the maximum duration for an IVR dialog.
`net-node-id`	Defines the Network Node ID.
`network-isdn-xfer`	Rejects ISDN transfer requests.
`no-audio-payload-type`	Defines the NoAudio payload type.
`non-call-cdr-rprt`	Enables CDR message for all non-call dialogs.
`number-of-active-dialogs`	Defines the number of concurrent non-responded dialogs.
`oos-behavior`	Defines the Out-Of-Service Behavior for FXS.
`opus-max-avg-bitrate`	Defines the Opus Max Average Bitrate (bps).
`overload-sensitivity-level`	Defines when to enter overload state.
`p-assrtd-usr-name`	Defines the user part of the user url in the P-Asserted-Identity header.
`p-preferred-id-list`	Defines the number of P-Preferred-Identity SIP headers included in the outgoing SIP message when the header contains multiple values.
`pii-mask-digits {off|on}`	Enables the masking of DTMF and other digits in syslog messages generated by the device.
`pii-mask-host {off|on}`	Enables the PII masking (with asterisks) of URI host parts (including IP addresses) in CDRs that the device sends to Web, CLI,

Command	Description
	Syslog, REST, RADIUS, and Local Storage (depending on pii-mask-private-info-in-cdrs), or to OVOC if pii-mask-private-info-for-ovoc is enabled.
`pii-mask-private-info-for-ovoc {off|on}`	Enables the PII masking (with asterisks) of phone numbers, URI user parts, and display names in CDRs that the device sends to OVOC.
`pii-mask-private-info-in-cdrs {disable| mask-pii-in-detailed-records| mask-pii-in-web-cli}`	Enables the masking of personally identifiable information (PII) in CDRs and SDRs generated by the device.
`pii-number-of-unmasked-chars`	Defines the number of PII characters to mask.
`pii-unmasked-chars-location {first-characters|last-characters}`	Defines from where to apply the PII mask, when the [PIIMaskPrivateInfoInCDRs] parameter is enabled.
`play-bsy-tone-2tel`	Enables play Busy Tone to Tel.
`play-rbt2ip`	Enables ringback tone playing towards IP.
`play-rbt2tel`	Enables ringback tone playing towards Tel side.
`polarity-rvrsl`	Enables FXO Connect/Disconnect call upon detection of polarity reversal signal. FXS: generates the signal.
`prack-mode`	Defines the PRACK mode for 1XX reliable responses.
`presence-publish-ip-group-name`	Assigns the IP Group configured for the Skype for Business Server for presence service.
`preserve-multipart-content-type {off| on}`	When the SBC sends out a SIP message that has multiple bodies, it enables the device to preserve the value of the Content-Type header (type and boundary) in the outgoing message.

Command	Description
`prog-ind-2ip`	Defines the whether to send the Progress Indicator to IP.
`pstn-alert-timeout`	Defines the max time (in seconds) to wait for connect from PSTN.
`q850-cause-for-sit-ic`	Defines the release cause for SIT IC.
`q850-cause-for-sit-ro`	Defines the release cause for SIT RO.
`q850-cause-for-sit-vc`	Defines the release cause for SIT VC.
`qos-effective-period`	Defines the QoS period - if during this period [in seconds], no updated QOS info received, the old QOS info is discarded. if QOS poor, and no calls allowed, after this period, calls will be allowed again
`qos-samples-to-avarage`	Defines the number of samples to average.
`qos-statistics-in-release-msg`	Defines whether to add statistics to call release.
`radius-accounting`	Defines the when RADIUS Accounting messages are sent.
`rai-high-threshold`	Defines the percentage of active calls to send 'Almost out of resources' RAI.
`rai-loop-time`	Defines the time period to check call resources (seconds).
`rai-low-threshold`	Defines the percentage of active calls to send 'Resources OK' RAI.
`reanswer-time`	Defines the time to wait between phone hang up and call termination.
`reason-header`	Enables Reason header in outgoing messages.
`record-uri-type`	Defines the type of default record URI used by Media Ctrl.
`reinvite-after-ha {off|on}`	Enables the device to send a SIP re-INVITE

Command	Description
	message with the local IP address of the new active device after a High-Availability (HA) switchover for current calls. **Note:** The parameter is applicable only to Mediant VE in HA mode that is deployed on the Azure cloud platform.
`rej-cancel-after-conn`	Defines whether or not reject Cancel request after connect.
`reject-on-ovrld`	If set to false (0), a 503 response will not be sent on overload.
`rel-cause-map-fmt`	Defines the release cause mapping format.
`release-cause-for-sit-nc`	Defines the release cause for SIT NC.
`reliable-conn-persistent`	If set to 1 - AllTCP/TLS connections are set as persistent and will not be released.
`reload-timeout-for-emergency-call`	Enables the blocking of device restarts that are triggered through CLI (`reload` command) during emergency calls and for a period (configured by the command) after the call ends (whether successfully established or failed).
`remote-party-id`	Enables the Remote-Party-ID header.
`remove-to-tag-in-fail-resp`	Removes to-tag in final reject response for setup INVITE transaction.
`rep-calling-w-redir`	Replaces Calling Number with Redirect Number ISDN to IP.
`replace-nb-sign-w-esc`	Replaces the number sign (#) with the escape character %23 in outgoing SIP messages.
`resource-prio-req`	Indicates whether or not Require header is able to contain the resource-priority tag.
`retry-after-mode {transparent|handle-locally}`	Defines the device’s behavior when it receives a SIP 503 (Service Unavailable)

Command	Description
	containing a Retry-After header, in response to a SIP message (e.g., REGISTER) sent to a proxy server.
`retry-aftr-time`	Retry After time for the proxy to be in state Unavailable.
`rfc4117-trnsc-enbl`	Enables transcoding call.
`rport-support`	Enables Rport option in Via header.
`rtcp-attribute`	Enables RCTP attribute in the SDP.
`rtcp-xr-coll-srvr`	Defines the RTCP-XR server IP address.
`rtcp-xr-rep-mode`	0:rtcpxr is not sent over SIP at all {@}1:rtcpxr is sent over sip when call ended{@}2:rtcpxr is sent over sip when on periodic interval and when call ended {@}3:rtcpxr is sent over sip when media segment ended and when call ended
`rtcpxr-collect-serv-transport`	Defines the RtcpXrEsc transport type.
`rtp-only-mode`	On RTP only mode there is no signaling protocol (for media parameters negotiation with the remote side). The channel is open immediately. 0 - regular call establishment. 1 - The RTP channel open for Rx & Tx. 2- The RTP channel open only for Tx 3 -The RTP channel open only for Rx
`rtp-rdcy-nego-enbl`	Enables RTP Redundancy negotiation.
`sbc-rtcpxr-report-mode`	0:rtcpxr is not sent over SIP at all,1:rtcpxr is sent over sip when call ended
`sdp-ecan-frmt`	Defines echo canceller format for outgoing SDP.
`sdp-session-owner`	Defines the SDP owner string.
`sdp-ver-nego`	Handle SDP offer/answer if SDP version was increased, otherwise takes SDP

Command	Description
	offer/answer parameters from last agreement (derived from previous SDP negotiations).
`sec-call-src`	Defines from where the second calling number is taken from (in an incoming INVITE request).
`self-check-audit`	Defines if resources self-check audit is used.
`send-180-for-call-waiting`	Sends 180 for call waiting.
`send-acsessionid`	Enables the use of the Global Session ID in SIP messages (AC-Session-ID header), which is a unique identifier of the call session, even if it traverses multiple devices.
`session-expires-time`	Defines the SIP session - refreshed (using INVITE) each time this timer expires (seconds).
`sess-exp-disc-time`	Defines the minimum time factor before the session expires.
`session-exp-method {re-invite|update}`	Determines the Method to refresh the SIP session.
`sig-cpu-usage-threshold`	Defines the signaling cpu usage threshold alarm (percentage)
`silk-max-avg-bitrate`	Defines the Silk max average bitrate (bps).
`single-dsp-transcoding`	Enables single DSP for G.711 to LBR coder.
`sip-dst-port`	Defines the default SIP destination port (usually 5060).
`sip-hold-behavior`	if set to 1, handle re-INVITE with a=recvonly as a=inactive
`sip-max-rtx`	Defines the maximum number of retransmissions.

Command	Description
`sip-nat-detect`	If not set, the incoming request will be always processed as user NOT behind NAT
`sip-remote-reset`	Enables remote management of device by receiving NOTIFY request with specific event type.
`sip-t38-ver`	Defines the SIP T.38 Version.
`sip-uri-for-diversion-header`	Use Tel uri or Sip uri for Diversion header.
`sit-q850-cause`	Defines the release cause for SIT.
`skype-cap-hdr-enable`	0 (default): Disable, 1:Add special header with capabilities for Skype
`src-hdr-4-called-nb`	Select source header for called number (IP->TEL), either from the user part of To header or the P-Called-Party-ID header.
`src-nb-as-disp-name`	if set to 1 Use source number as display name if empty.if set to 2 always use source number as display name .{@}if set to 3 use the source number before manipulation, if empty.
`src-nb-preference`	Defines from where the source number is taken (in an incoming INVITE request).
`t1-re-tx-time`	Defines the SIP T1 timeout for retransmission.
`t2-re-tx-time`	Defines the SIP T2 timeout for retransmission.
`t38-fax-mx-buff`	Defines the fax max buffer size in T.38 SDP negotiation.
`t38-mx-datagram-sz`	Defines the T.38 coder max datagram size.
`t38-sess-imm-strt`	T.38 Fax Session Immediate Start (Fax behind NAT)
`t38-use-rtp-port`	Defines the T.38 packets received on RTP port.

Command	Description
`tcp-keepalive-interval`	Defines the interval between subsequent keep-alive probes, regardless of what the connection has exchanged in the meantime.
`tcp-keepalive-retry`	Defines the number of unacknowledged probes to send before considering the connection down and notifying the application layer.
`tcp-keepalive-time`	Defines the interval between the last data packet sent (simple ACKs are not considered data) and the first keepalive probe.
`tcp-timeout`	Defines the SIP TCP time out.
`tel-to-ip-call-forking-mode`	Defines the Tel-to-IP call forking mode.
`time-between-did-winks`	Defines the time between first and second Wink generation (FXS).
`tr104-voice-profile-name`	Defines the TR-104 Voice Profile Name.
`trans-coder-present`	Defines the Transparent code presentation.
`transparent-payload-type`	Defines the payload type of the Transparent coder for outgoing data calls (ISDN-to-IP).
`unreg-on-startup {no-unreg|unreg-acc}`	Enables the device to unregister all user Accounts that were registered with the device, upon a device restart.
`uri-for-assert-id {off|on}`	Enables use of Tel uri or Sip uri for P-Asserted or P-Preferred headers.
`use-aor-in-refer-to-header {off|on}`	If enabled, we will use URI from To/From headers in Refer-To header. If disabled, we will take the URI from Contact
`use-dst-as-connected-num {off|on}`	Enables use of destination as connected number.

Command	Description
`use-dtg {0|1}`	Enables use of DTG parameter.
`use-tgrp-inf {disable|hotline|hotline-extended| send-only|send-only-incl-register|send-receive|send-receive-incl-register}`	Enables use of Tgrp information.
`user-agent-info`	Defines the string that is displayed in the SIP Header 'User-Agent' or 'Server'.
`user-inf-usage {off|on}`	Enables User-Information usage.
`user-phone-in-from {disable|enable}`	Adds 'User=Phone' to From header.
`user-phone-in-url {disable|enable}`	Adds User=Phone parameter to SIP URL.
`usr-def-subject`	Defines the SIP subject.
`usr2usr-hdr-frmt {with-encoding-hex| with-protocol-discriminator| with-text-pres x-user-to-user}`	Defines the interworking between the SIP INVITE's User-to-User header.
`verify-rcvd-requri {not-verify|verify-all-req| verify-in-call-req|verify-initial-req}`	Defines whether to verify Request URI Header in requests.
`verify-rcvd-via {off|on}`	Defines whether to verify Source IP with IP in top-most Via.
`websocket-keepalive`	Defines the period at which web socket PING messages are sent.
`x-channel-header {off|on}`	Enables X-Channel header.
`zero-sdp-behavior {board-ip|zero-sdp}`	Zero connection information in SDP behavior

Command Mode

Privileged User

Example

This example configures unlimited call duration:

```
(config-voip)# sip-definition settings
(sip-def-settings)# mx-call-duration 0
(sip-def-settings)# activate
```

sip-recording

This command configures SIPRec.

Syntax

```
(config-voip)# sip-definition sip-recording
```

Command	Description
`settings`	See settings below
`sip-rec-routing`	See sip-rec-routing on the next page

Command Mode

Privileged User

settings

This command configures various SIPRec settings.

Syntax

```
(config-voip)# sip-definition sip-recording settings
(sip-rec-settings)#
```

Command	Description
`fwd-signaling-to-siprec {disable|dtmf-sip-info}`	Enables the device to send SIP INFO messages (sent or received on outgoing leg) that contain DTMF digits to the SRS.
`siprec-metadata-format`	Defines the format of the recording metadata that is included in SIP messages sent to the SRS.

Command	Description
`{legacy|rfc7865}`	
`siprec-server-dest-username`	Defines the username of the SIPRec server (SRS).
`siprec-time-stamp {local-time|utc}`	Defines the device's time format (local or UTC) in SIP messages that are sent to the SRS.
`video-rec-sync-timeout`	Defines the video synchronization timeout (in msec), which is applicable when the device also records the video stream of audio-video calls for SIPRec.

Command Mode

Privileged User

Example

This example configures the metadata format so that it's according to RFC 7865:

```
(config-voip)# sip-definition sip-recording settings
(sip-rec-settings)# siprec-metadata-format RFC7865
(sip-rec-settings)# activate
```

sip-rec-routing

This command configures the SIP Recording Rules table, which lets you define SIP-based media recording rules. A SIP Recording rule defines call routes that you want to record.

Syntax

```
(config-voip)# sip-definition sip-recording sip-rec-routing <Index>
(sip-rec-routing-<Index>)#
```

Command	Description
Index	Defines the table row index.
`caller {both|peer-party|recorded-party}`	Defines which calls to record according to which party is the caller.

Command	Description
`condition-name`	Assigns a Message Condition rule to the SIP Recording rule.
`peer-ip-group-name`	Assigns an IP Group Set from the IP Group Set table to represent the peer IP Group that is participating in the call.
`peer-trunk-group-id`	Defines the peer Trunk Group that is participating in the call (applicable only to Gateway calls).
`recorded-dst-pattern`	Defines calls to record based on destination number or URI.
`recorded-ip-group-name`	Assigns an IP Group Set from the IP Group Set table to represent the entity participating in the call and the recording is done on the leg interfacing with this IP Group.
`recorded-src-pattern`	Defines calls to record based on source number or URI.
`srs-ip-group-name`	Assigns an IP Group Set from the IP Group Set table to represent the recording server (SRS).
`srs-ip-group-set-name`	Assigns an IP Group Set from the IP Group Set table to represent a group of SRSs (IP Groups) for load balancing.
`srs-red-ip-group-name`	Assigns an IP Group Set from the IP Group Set table to represent the redundant SRS in the active-standby pair for SRS redundancy.
`srs-role`	Defines a condition (optional) based on role value for matching the rule when the recording is triggered by a REST request.
`trigger {call-connect|media-start|rest}`	Defines what triggers the device to record the call for this rule.

Command Mode

Privileged User

Example

This example records calls between IP Groups "ITSP" and "IPBX", sending them to IP Group "SIPREC" (SRS):

```
(config-voip)# sip-definition sip-recording sip-rec-routing 0
(sip-rec-routing-0)# recorded-ip-group-name ITSP
(sip-rec-routing-0)# peer-ip-group-name IPBX
(sip-rec-routing-0)# srs-ip-group-name SIREC
(sip-rec-routing-0)# caller both
(sip-rec-routing-0)# activate
```

102 sip-interface

This command configures the SIP Interfaces table, which lets you define SIP Interfaces. A SIP Interface represents a Layer-3 network in your deployment environment, by defining a local, listening port number and type (e.g., UDP), and assigning an IP network interface for SIP signaling traffic.

Syntax

```
(config-voip)# sip-interface <Index>
(sip-interface-<Index>)#
```

Command	Description
Index	Defines the table row index.
`additional-udp-ports`	Defines a port range for the device's local, listening and source ports for SIP signaling traffic over UDP and is used to assign a specific local port to each SIP entity (e.g., PBX) communicating with a common SIP entity (e.g., proxy server).
`additional-udp-ports-mode [always-open|open-when-used]`	Defines the mode of operation for the Additional UDP Port feature.
`application-type {gw|sbc}`	Defines the application for which the SIP Interface is used.
`block-un-reg-users {acpt-all|acpt-reg-users|acpt-reg-users-same-src|not-conf}`	Defines the blocking (reject) policy for incoming SIP dialog-initiating requests (e.g., INVITE messages) from registered and unregistered users belonging to the SIP Interface.
`cac-profile`	Assigns a Call Admission Control Profile.
`call-setup-rules-set-id`	Assigns a Call Setup Rule Set ID.
`classification-fail-response-type`	Defines the SIP response code that the device sends if a received SIP request (OPTIONS, REGISTER, or INVITE) fails the SBC Classification process.
`classify-by-reg-db {disable|enable}`	Enables classification of incoming SIP dialog-initiating requests (e.g., INVITE) to IP Groups by the

Command	Description
	device's users registration database.
`enable-un-auth-registrs {disable|enable|not-conf}`	Enables the device to accept REGISTER requests and register them in its registration database from new users that have not been authenticated by a proxy/registrar server (due to proxy down) and thus, re-routed to a User-type IP Group.
`encapsulating-protocol {none|websocket}`	Defines the type of incoming traffic (SIP messages) expected on the SIP Interface.
`interface-name`	Defines a descriptive name, which is used when associating the row in other tables.
`max-reg-users`	Defines the maximum number of users belonging to the SIP Interface that can register with the device.
`media-realm-name`	Assigns a Media Realm to the SIP Interface.
`message-policy-name`	Assigns a SIP message policy to the SIP interface.
`msrp-tcp-port`	Defines the listening TCP port for MSRP sessions.
`msrp-tls-port`	Defines the listening TLS port for secured MSRP sessions (MSRPS).
`network-interface`	Assigns a Control-type IP network interface to the SIP Interface.
`pre-classification-manset`	Assigns a Message Manipulation Set ID to the SIP Interface.
`pre-parsing-man-set`	Assigns a Pre-Parsing Manipulation Set to the SIP Interface. T
`sbc-direct-media {disable|enable|enable-same-nat}`	Enables direct media (RTP/SRTP) flow (i.e., no Media Anchoring) between endpoints associated with the SIP Interface.
`sctp-port`	Defines the local SCTP port on which the device listens for inbound SCTP connections (i.e., SIP signaling over SCTP). **Note:** The parameter is applicable only to Mediant 90xx and Mediant Software.

Command	Description
`sctp-second-network-interface`	Assigns an additional IP network interface (Control-type) to the SIP Interface, which serves as the secondary (alternative) local IP address for SCTP multi-homing. **Note:** The parameter is applicable only to Mediant 90xx and Mediant Software.
`srd-name`	Assigns an SRD to the SIP Interface.
`tcp-keepalive-enable {disable|enable}`	Enables the TCP Keep-Alive mechanism with the IP entity on this SIP Interface.
`tcp-port`	Defines the device's listening port for SIP signaling traffic over TCP.
`tls-context-name`	Assigns a TLS Context (SSL/TLS certificate) to the SIP Interface.
`tls-mutual-auth {disable|enable|not-configured}`	Enables TLS mutual authentication for the SIP Interface (when the device acts as a server).
`tls-port`	Defines the device's listening port for SIP signaling traffic over TLS.
`topology-location {down|up}`	Defines the display location of the SIP Interface in the Topology view.
`udp-port`	Defines the device's listening and source port for SIP signaling traffic over UDP.
`used-by-routing-server {not-used|used}`	Enables the SIP Interface to be used by a third-party routing server for call routing decisions.

Command Mode

Privileged User

Example

This example configures SBC SIP Interface "ITSP" that uses IP network interface "Voice" and Media Realm "ITSP":

```
(config-voip)# sip-interface 0
(sip-interface-0)# interface-name ITSP
(sip-interface-0)# network-interface Voice
(sip-interface-0)# application-type sbc
(sip-interface-0)# udp-port 5080
(sip-interface-0)# media-realm-name ITSP
(sip-interface-0)# activate
```

103 srd

This command configures the SRDs table, which lets you define signaling routing domains (SRD). The SRD is a logical representation of an entire SIP-based VoIP network (Layer 5) consisting of groups of SIP users and servers.

Syntax

```
(config-voip)# srd <Index>
(srd-<Index>)#
```

Command	Description
Index	Defines the table row index.
block-un-reg-users {acpt-all|acpt-reg-users|acpt-reg-users-same-src}	Defines the blocking (reject) policy for incoming SIP dialog-initiating requests (e.g., INVITE messages) from registered and unregistered users belonging to the SRD.
cac-profile	Assigns a Call Admission Control Profile.
enable-un-auth-registrs {disable|enable}	Enables the device to accept REGISTER requests and register them in its registration database from new users that have not been authenticated by a proxy/registrar server (due to proxy down) and thus, re-routed to a User-type IP Group.
max-reg-users	Defines the maximum number of users belonging to the SRD that can register with the device.
name	Defines a descriptive name, which is used when associating the row in other tables.
sbc-dial-plan-name	Assigns a Dial Plan.
sbc-operation-mode {b2bua|call-stateful-proxy|microsoft-server}	Defines the device's operational mode for the SRD.
sbc-routing-policy-name	Assigns a Routing Policy to the SRD.

Command	Description
`type {isolated|shared}`	Defines the sharing policy of the SRD, which determines whether the SRD shares its SIP resources (SIP Interfaces, Proxy Sets, and IP Groups) with all other SRDs (Shared and Isolated).
`used-by-routing-server {not-used|used}`	Enables the SRD to be used by a third-party routing server for call routing decisions.

Command Mode

Privileged User

Example

This example configures SRD "ITSP" with max. registered users at 20:

```
(config-voip)# srd 0
(srd-0)# name ITSP
(srd-0)# max-reg-users 20
(srd-0)# activate
```

This page is intentionally left blank.

International Headquarters

6 Ofra Haza Street

Naimi Park

Or Yehuda, 6032303, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-18039