Reference Guide

AudioCodes Multi-Service Business Router Series

CLI for MSBRs and MediaPack 5xx

Version 7.2

audiocodes

Notice

Date Published: April-18-2024

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.

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

Related Documentation

Document Name
Release Notes
MSBR and MediaPack 500 Series Release Notes
User's Manual

Document Name
Mediant 500 MSBR User's Manual
Mediant 500Li MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 800 MSBR User's Manual
Configuration Notes
M5G-EA Cellular Module Hardware Installation and Configuration Guide
Mediant 500Li MSBR Simplifying Network CLI Configuration Guide
Mediant MSBR IP Networking CLI Configuration Guide
Mediant MSBR Layer-2 Bridging CLI Configuration Guide
Mediant MSBR LAN-WAN Access CLI Configuration Guide
Mediant MSBR Security Setup CLI Configuration Guide
Mediant MSBR Simplifying Network CLI Configuration Note
Mediant MSBR Basic System Setup CLI Configuration Guide
Troubleshooting the MSBR Configuration Note
Upgrading MSBR Firmware from Ver. 6.8 to Ver. 7.2 Configuration Note
Configuring Mediant MSBR Wireless Access Configuration Guide
Hardware Installation Manuals
MediaPack 504-508 Hardware Installation Manual
MediaPack 524 & 532 Hardware Installation Manual
Mediant 500Li MSBR Hardware Installation Manual
Mediant 500L MSBR Hardware Installation Manual
Mediant 500 MSBR Hardware Installation Manual
Mediant 800 MSBR Hardware Installation Manual

Document Revision Record

LTRT	Description
17929	Initial document release for Ver. 7.2.
17937	■ Updated to Ver. 7.20A.200.019 ■ New: tail; show network http-proxy; clear voip ids blacklist; admin streaming; copy configuration-pkg; copy nginx-conf-files; automatic-update mt-firmware| vmt-firmware; sbc-performance-settings; http-proxy debug-level; http-proxy directive-sets; http-proxy dns-primary-server; http-proxy dns-secondary-server; http-proxy http-proxy-app; http-proxy upstream-host| upstream-group; public-key display; alternative-name-add; alternative-name-clear; sbc-enhanced-plc; max-streaming-calls; cac-profile; external-media-source; cac-profile; user-info ■ Updated: show voip proxy sets status; write; write factory keep-network-and-users-configuration; http-proxy
17939	■ Updated to Ver. 7.20A.202.112 ■ New commands: filter commands descending, first <x>, last <x>, range <x-y>; show activity-log; show admin state; admin state lock |unlock; copy mt-firmware| vmc-firmware; ystem-snapshot; automatic-update > aupd-graceful-shutdown| vmc-firmware; floating-license; time-zone-format; dhcp-server server > name; configure network > mtc; fxs-callid-cat-brazil ■ Updates: clear voip ids blacklist entry; "prefix" changed to "pattern"; parent-child tables structure update
17945	■ Updated to Ver. 7.20A.204.108 ■ New commands: isdn-ignore-18x-without-sdp; isdn-send-progress-for-te; force-generate-to-tag
17948	■ Updated to Ver. 7.20A.250.003 ■ Updated sections: Privileged User Mode (user levels, RADIUS-LDAP) ■ New commands: debug exception-syslog-history; debug reset-syslog-history; ping (tos|traffic-class); traceroute (proto); ids global-parameters (enable-ids on); automatic-update > credentials; rules-set-name; ssh-redundant-device-port; oauth-http-service; sbc-server-auth-type; p-preferred-id-list; account-name; re-register-on-invite-failure ■ Updated commands: trace-level (notes); copy ini-file (replaced voice-configuration); debug debug-recording; pstn-debug (replaced debug pstn-debug); logging-filters (description); alt-res-name; show system

LTRT	Description
	temperature; registrar-stickiness; charge-code; message (path); inbound-map-set (path); outbound-map-set (path)
17950	■ Updated to Ver. 7.20A.252.062 ■ New commands: snmp alarm-customization; qoe additional-parameters; call-end-cdr-sip-reasons-filter; call-end-cdr-zero-duration-filter; export-csv-to; import-csv-from; fxs-offhook-timeout-alarm; http-login-needed (http-services); verify-cert-subject-name (http-services); key-port-configure; obscure-password-mode; hostname (network-settings); keep-alive-time / secondary-server-name / tls / verify-certificate / verify-certificate-subject-name (qoe qoe-settings); operational-state-delay; history at-start show system utilization; debug-level-high-threshold; log-level; (test-call test-call-table) allowed-audio-coders-group-name / allowed-coders-mode / media-security-mode / offered-audio-coders-group-name / play-dtmf-method / play-tone-index; dedicated-connection-mode ■ Updated commands: verify-cert-subject-name (name change); message call-setup-rules ("none" added to action-type / request-key / request-target / request-type with http-post-notify and http-post-query; password-obscurity; crypto isakmp policy
17954	Updated commands (typo): graceful command added to reload without-saving command; keep-network-and-users-configuration (removed)
	■ Updated to Ver. 7.20A.254. ■ New commands: topology-hiding-header-list; call-failure-internal-reasons; call-failure-sip-reasons; call-success-internal-reasons; call-success-sip-reasons; call-transferred-after-connect; call-transferred-before-connect; no-user-response-after-connect; no-user-response-before-connect; video-rec-sync-timeout; mfr1-detector-enable; dtmf-detector-enable; alt-route-reasons-set; alt-route-reasons-rules; short-call-seconds; mf-transport-type; sbc-msrp-empty-message-format; sbc-msrp-offer-setup-role; sbc-msrp-re-invite-update-supp; data-diffserv; web-password-change-interval: heartbeat-interval; initial-rto; minimum-rto; maximum-rto; max-path-retransmit; max-association-retransmit; max-data-tx-burst; max-data-chunks-before-sack
17957	■ Updated to Ver. 7.20A.254.375 ■ New commands: web-password-change-interval ■ Updated commands: hotline-dia-ltone-duration (typo); energy-detector-cmd (removed); format-dst-phone-number (removed); qsig-tunneling-mode (description); nel open only fo Rx (removed)

LTRT	Description
17958	■ Updated sections: Accessing the CLI (miscellaneous) ■ Updated commands: Answer Detector commands removed (answer-detector-activativity-delay, answer-detector-enable, answer-detector-redirection, answer-detector-sensitivity, answer-detector-silence-time); (radius)# source data; ■ New commands: format-dst-phone-number; snmp-transport-type
17960	■ Updated to Ver. 7.20A.254.733 ■ Updated commands: show running config (Local Users table); (config-isakmp) ike ■ New commands: tls-renegotiation; min-web-password-len; internal-media-realm-name; teams-media-optimization-handling
17965	■ Updated to Ver. 7.2.256.107 ■ Updated commands: interface gigabitEthernet (typo); interface gpon (removed); proxy-enable-keep-alive (using-options-on-active-server); tls-version (TLS 1.3); floating-license (flex); external-media-source (typo); ntp (example typo); optional values added for ISDN commands; topology-hiding-headerlist (removed) ■ New commands: show data interfaces <Interface> history bandwidth; send-screen-to-isdn-1; send-screen-to-isdn-2; layer_2_only; port-monitor-save-after-reset; dns-rebinding-protection-enabled; ciphers-client-tls13; ciphers-server-tls13; key-exchange-groups; middlebox-compat-mode; forking-handling; : user-defined-failure-pm; ovoc-tunnel-settings (address, path, username, password, secured, verify-server); rest-message-type (new value); push-notification-servers; pns-reminderperiod; pns-registertimeout; remote-monitoring; remote-monitor-reporting-period; remote-monitor-status; remote-monitor-alarms; remote-monitor-kpi; remote-monitor-registration; sipsource-host-name; sip-topology-hiding-mode; reserve-dsp-onsdp- offer; teams-mo-initial-behavior
17968	■ Updated to Ver. 7.20M1.256.029 ■ New commands: period-inform-enable; crypto isakmp identity ip; accept-dhcp-proxy-list; register-by-served-tg-status; configure system > cwmp > source data; ip dhcp-client authentication; ipv6 dhcp-client authentication; show system floating-license; show system floating-license reports; floating-license; show data cellular status history; date-header-time-sync; date-header-time-sync-interval; isdn-ntt-noid-interworking-mode; ipv6 enable; cwmp > source data source-address interface loopback (replaces vrf-name) ■ Updated commands: crypto ipsec transform-set (new value esp-sha256-

LTRT	Description
	hmac)
17974	■ Updated to Ver. 7.24A.256.329 ■ New commands: graceful forever; where (table search); configure system > provision (auto commands); gw-digital-settings isdn-channel-id-format; isdn-channel-id-format-for-trunk; proxy-and-registration use-rand-user ■ Updated commands: interface vti (removed); crypto isakmp key address (FQDN added); https-cipher-string (removed); track (retries-up and max-rtt added); ipv6 route (2 tracks); ipv6 nd (no-import-to-dhcps added); ipv6 nd pd (no-import-to-ra added)
17981	■ Updated to Ver. 7.24A.356.069 ■ New commands: set tunnel start-action-mode; account-registrar-avoidance-time; handle-isdn-facility-on-disconnect; syslog-servers; sbc-terminate-options; where (table search); teams-direct-routing-mode; used-by-routing-server (Media Realm); preserve-multipart-content-type; dtls-time-between-transmissions; sbc-renumber-mid; use-conn-sdpses-or-media; cwmp > day-of-week|start|end ■ Updated commands: ping (Ctrl+C); fax-sig-method (value); snmp-transport-type (obsolete); auth-protocol (values); copy <File Type> from|to scp; track (description); show data track brief; welcome-msg (display); traceroute max-ttl|proto|resolve-to-name; session-exp-method (3); registrar-search-mode (new value)
17984	■ Updated to Ver. 7.24A.356.248 ■ New commands: syslog-protocol; syslog-tlscontext; ignore-auth-stale; sbc-no-alert-timeout ■ Updated commands: use-rand-user (new value); access-list (multiple per IPSec)
17989	■ Updated to Ver. 7.20A.356.468 (with Mediant 500Li merge) ■ New commands: show data qos tc; cli-alias; show aliases; lldp set-lan-as-client; port-redundancy; web-data-config; web-data-lan-if; web-data-wan-if; ipv6 dhcp-server dns-server auto; show data bridge info; show data access-lists resolved; isdn-send-progress-on-183-without-sdp; show data dot1x-supplicant-status ■ Updated commands: access-list (multiple rules per ACL and max.); ip nat translation tcp-timeout (default); ipv6 dhcp-server dns-server; ipv6 dhcp-client (opt-17-sub-1 enterprise / cable-labs-opt-17); dot1x supplicant (identity / mode / password / port-type / tls-ctx); config-crypto-map (peer

LTRT	Description
	as FQDN)
18005	■ Updated to Ver. 7.26A.356.070 (M9) ■ New commands: show system technical-information; show data cellular network-scan; show data cellular status servingcell; conf-cellular (profile, mcc, mnc, profile-selection fixed, profile-selection policy priority, sim roaming, desc); sim_lock_status; sim_pin_code_change; sim_pin_code_ unlock; sim_puk_code_unlock; show run (flow control); show data track brief failures; show data track <track ID> history failures; dedicated-connection-mode; pi-location-to-isdn; fxs-ntt-polarity-reversal; fxs-ntt-noid-interworking-mode; reload-timeout-for-emergency-call; emerg-alert-info-uri; attempted-call-count-on-start; ovoc-tunnel-settings; wfq_mode; enable-authentication-trap; flowcontrol; startup-dark-mode ■ Updated commands: show data cellular status (IMEI); show data ip interface brief (secondary); traceroute (syntax); interface osn; show network interface osn; crypto ipsec transform-set (ah-sha256-hmac); ip domain localhost (MAC / serial placeholders); dot1x supplicant (identity, mode, password, port-type, tls-ctx); crypto ipsec transform-set (esp-gcm)
18009	■ Updated to Ver. 7.26A.356.174 (M9.1) ■ New commands: dyn-dns-server; ipv6 enable; ipv6 address autoconfig extnd-prfx-lan; vrrp <id> ipv6; wan-copper-fiber-mode; ntp-dependency; gw-ignore-multiple-answers
18011	■ Updated to Ver. 7.26A.356.459 (M10) ■ New commands: fxs-emg-call-for-unreg-port; ipv6 dhcp-server vrrp_id; router clat; sim disable-nr5g-mode; apn (cell-profile-config); ip sla responder udp-echo; show data ip sla responder; configuration-pkg (auto-update); default-configuration-package-password (auto-update); show running-config data static-routes; show running-config data tracks; password-history-visible; clear history ■ Updated commands: mode ppp (removed); ip dhcp-client request (160); copy configuration-pkg (encrypted / certificates); classification-fail-response-type (typo)
18016	■ Updated to Ver. 7.26A.356.630 (M11) ■ New commands: debug dsl; debug cellular; direct-exec; nslookup indet.me; debug get-global-ip; ipv6 nd ra propagate-mtu; dynamic-dns service custom; mode scan-priority ■ Updated commands: debug usb-3g cellular (removed); qos match-map

LTRT	Description
	(typo); hostname (CLI path); password (Accounts table re question mark); sim_lock_status (renamed sim-lock-status); sim_pin_code_change (renamed sim-pin-code-change); sim_pin_code_unlock (renamed sim-pin-code-unlock); sim_puk_code_unlock (renamed sim-puk-code-unlock); audc_sw_ver (renamed audc-sw-ver); firmware_rev_id (renamed firmware-rev-id); firmware_version (renamed firmware-version); sim_iccid (renamed sim-iccid); write factory keep-network-and-users-configuration (removed)
18019	■ Updated to Ver. 7.26A.356.763 (M12) ■ New commands: clat-enable; ip dhcp-source-address interface; generate ecdsa; generate rsa; usb-power; port-restriction; display-allowed-acs-ips; gw-suppl-serv flash-key-toggle-to-secondary; gw-suppl-serv flash-key-toggle-to-primary; gw-suppl-serv flash-key-call-transfer; gw-suppl-serv flash-key-conference; gw-suppl-serv flash-key-bye-and-toggle; gw-suppl-serv flash-key-bye-2-secondary; gw-dtmf-and-dial secondary-digitmapping; digitmapping (Tel Profile); fake-retry-after ■ Updated commands: ip dhcp-client request (160); show data cellular status (firmware ver); authentication (additional values); dns-rebinding-protection-enabled (removed)

Table of Contents

1 Introduction

This document describes the Command- Line Interface (CLI) commands for configuring, monitoring and diagnosing AudioCodes Multi-Service Business Routers (MSBR) and MediaPack 5xx series.

- 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 Version 7.2. Therefore, ignore commands that are applicable only to these specific products. For a list of the products supported in Version 7.2, refer to the *Release Notes* of the MSBR and MediaPack 5xx series, which can be downloaded from AudioCodes website.

Part I

Getting Started

2 Accessing the CLI

You can access the device's CLI through the following:

- **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).
- 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.

3 CLI Structure

This section describes the CLI structure.

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 ">".

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.
- If you're a user with Security Administrator user levels, you can skip the `enable` command stage and start directly in Privileged User mode upon regular CLI login, by configuring the `direct-exec` command to `on`.

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

Configuration Command Sets	Description

Data	Contains data-router related commands.
	To access this command set:
	`# configure data`
	`(config-data)#`

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)#`

Configuration Command Sets	Description

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 between 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
>
```

CLI Configuration Wizard

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

- Login passwords of 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.

To access the CLI Wizard, enter the following command at the root-prompt level:

```
# configure-wizard
```

For more information on how to use this utility, refer to the CLI Wizard User's Guide.

CLI Shortcut Keys

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

Table 3-1: CLI Shortcut Keys

Shortcut Key	Description
↑	(Up arrow key) Retypes the previously entered command. 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.

Common CLI Commands

The table below describes common CLI commands.

Table 3-2: 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 the filter expression:

Command	Description
	<command>|<filter string or expression> The filter expression can be: ■ **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. ■ **grep <options> <expression>:** Filters the output according to common options ("-v" and "-w") of the global regular expression print ("grep") UNIX utility. ✓ "-v": Excludes all output lines that match the regular expression. If the "-v" option is not specified, all output lines matching the regular expression are displayed. ✓ "-w": Filters the output lines to display only lines matching whole words form of the regular expression. For example: **show system version|grep Number** ;Serial Number: 2239835;Slot Number: 1 ■ **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

Command	Description
	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 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

Command	Description
`activate`	Applies (activates) the command setting. **Note:** ■ Offline configuration changes require a reset of the device. A reset can be performed at the end of your configuration changes. A required reset is indicated by an asterisk (*) before the command prompt. To reset the device, use the `reload now` command (resetting the device by powering off-on the device or by pressing the reset pinhole button will not preserve your 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:

Command	Description
	(clock)# do show running-config
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 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 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.
no	Undoes an issued command, disables a feature or deletes a table row. Enter the **no** before the command, for example:

Command	Description

	■ 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 a range of entries from x to y. For example, the following displays only the entries from 1 to 4: `# show voip calls active range 1-4` **Note:** Currently, this filter is supported only by certain 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 table for a row index whose table column 'name' contains the value "ITSP":
	`(config-voip)# ip-group where name ITSP`
	`(ip-group-1)#`

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:

- SBC:
  - IP-to-IP Routing
  - Classification
  - Message Condition
  - IP-to-IP Inbound Manipulation
  - IP-to-IP Outbound Manipulation

- SBC and Gateway:
  - Message Manipulations
- Gateway:
  - Destination Phone Number Manipulation Tables for IP-to-Tel / Tel-to-IP Calls
  - Calling Name Manipulation Tables for IP-to-Tel / Tel-to-IP Calls
  - Source Phone Number Manipulation Tables IP-to-Tel / Tel-to-IP Calls
  - Redirect Number Tel-to-IP

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
```

CLI Error Messages

The table below lists common error messages displayed in the CLI.

Table 3-3: CLI Error Messages

Message	Description
"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 CLI commands whose value can be any integer within a specific range of numbers, if you enter a number that is outside of the range, the error message also displays the valid range, as shown in the following example: `(cli-settings)# window-height 70000`

Message	Description
	`Invalid argument "70000". Value must be in range [0-65535]`

Typographical Conventions

This document uses the following typographical conventions:

Table 3-4: 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}

Part II

Root-Level Commands

4 Introduction

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

Command	Description
`debug`	See Debug Commands on page 20
`show`	See Show Commands on page 77
`clear`	See Clear Commands on page 183
Maintenance commands	See General Root Commands on page 199

5 Debug Commands

This section describes the debug commands.

Syntax

```
# debug
```

This command includes the following commands:

Command	Description
adsl-connection	See debug adsl-connection on page 22
adsl-firmware	See debug adsl-firmware on page 23
auxilary-files	See debug auxilary-files on page 23
bfd	See debug bfd on page 25
bgp	See debug bgp on page 26
capture	See debug capture on page 27
cellular	See debug cellular on page 42
cli	See debug cli delayed-command on page 43
cwmp	See debug cwmp send-connection-request on page 44
data-syslog	See debug data-syslog on page 45
debug-recording	See debug debug-recording on page 45
dhcpv6_client	See debug dhcpv6_client on page 47
dhcpv6_server	See debug dhcpv6_server on page 47
dial-plan	See debug dial plan on page 48
dsl	See debug dsl on page 50
dot11radio	See debug dot11radio on page 48
dynamic-routing	See debug dynamic-routing on page 50
ethernet	See debug ethernet on page 51

Command	Description
exception-info	See debug exception-info on page 52
exception-syslog-history	See debug exception-syslog-history on page 53
fax	See debug fax on page 55
get-global-ip	See debug get-global-ip on page 54
ipv6-ra	See debug ipv6-ra on page 56
log	See debug log on page 56
ospf	See debug ospf on page 57
ospf6	See debug ospf6 on page 59
persistent-log show	See debug persistent-log show on page 61
phy-err-injection	See debug phy-err-injection on page 62
pstn	See pstn-debug on page 318
reset-history	See debug reset-history on page 64
reset-syslog-history	See debug reset-syslog-history on page 65
rip	See debug rip on page 65
ripng	See debug ripng on page 66
rmx-serial	See debug rmx-serial on page 67
serial-port	See debug serial-port on page 68
sip	See debug sip on page 69
speedtest	See debug speedtest on page 69
syslog	See debug syslog on page 70
syslog-server	See debug syslog-server on page 71
test-call	See debug test-call on page 72
usb	See debug usb on page 74
voip	See debug voip on page 74

Command	Description
vrf	See debug vrf on page 75
zebra	See debug zebra on page 75

debug adsl-connection

This command displays the ADSL line synchronization status (Physical Interface). The output can be displayed in the CLI as well as in the Syslog viewer after Syslog is enabled.

Syntax

```
# debug adsl-connection
```

Command Mode

Privileged User

Example

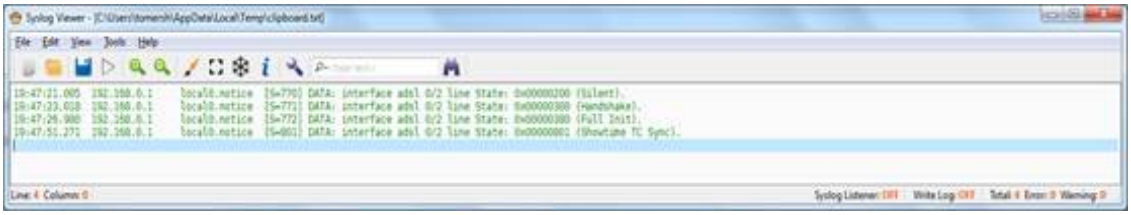
This example displays the ADSL line synchronization status. Note that the debug log command, run first, displays logs. If you run the debug adsl-connection command without running the debug log command, the log messages of the debug adsl-connection command will be sent to a log that can be displayed by running the show log command. If Syslog messaging is configured, the message will be sent to the Syslog server.

```
# debug log
# debug adsl-connection

May 16 20:01:01  DATA: interface adsl 0/2 line State: 0x00000200 (Silent).
May 16 20:01:03  DATA: interface adsl 0/2 line State: 0x00000300 (Handshake).
May 16 20:01:07  DATA: interface adsl 0/2 line State: 0x00000380 (Full Init).
May 16 20:01:32  DATA: interface adsl 0/2 line State: 0x00000801 (Showtime TC
Sync).
```

This example displays the ADSL line synchronization status in the Syslog server:

```
# enable syslog
# debug adsl-connection
```



debug adsl-firmware

This command configures the method for copying the ADSL firmware file.

Syntax

```
# debug adsl-firmware <tftp | usb>
```

Command	Description
tftp	■ [A.B.C.D] = Configures the TFTP server address ■ old-image = Configures using the old-image for copying the firmware file
usb	■ [VRX File Name] = Configures the Visual ReportX Data file name ■ old-image = Configures using the old-image for copying the firmware file

Command Mode

Privileged User

Example

This example configures the USB method of copying the firmware file:

```
# debug adsl-firmware usb usb
```

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>}
```

Command	Description	
info	Displays the loaded Dial Plan file and lists the names of its configured Dial Plans.	
match-number	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.	
	Dial Plan Number	Defines the Dial Plan in which to search for the 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 bfd

The Bidirectional Forwarding Detection (BFD) debug command configures the logging of debugging information for critical BFD events, normal BFD events, and BFD packets. The command configures BFD event traces and BFD event logs. The command helps administrators identify and analyze issues with BFD sessions.

Syntax

```
# debug bfd
```

Command	Description
`fsm`	Associates the Finite State Machine with **Virtual Routing and Forwarding** (VRF**) technology which allows multiple instances of a routing table to co-exist within the same router. Routing instances are independent so the same or overlapping IP addresses can be used without conflicts.** Enter the name of the VRF table with which to associate the Finite State Machine.
`net`	Associates the BFD network messages with a VRF. Enter the name of the VRF table with which to associate the BFD network messages.
`zebra`	Associates the BFD Zebra messages with a VRF. Enter the name of the VRF table with which to associate the BFD Zebra messages. Zebra routing software provides TCP/IP based routing services with support from routing protocols RIP, OSPF and BGP. Zebra also supports IPv4 and IPv6 routing protocols.

Command Mode

Privileged User

Example

This example associates BFD network messages with a VRF:

```
# debug bfd net vrf
  VRF-table-1
```

debug bgp

This command debugs Border Gateway Protocol (BGP) processing.

Syntax

```
# debug dbg
```

Command	Description
`events`	Debugs BGP events.
`filters`	Debugs BGP filters.

Command	Description
`fsm`	Debugs BGP Finite State Machine.
`keepalives`	Debugs BGP keepalives.
`updates {in|out}`	Debugs BGP updates.
`zebra`	Debugs BGP Zebra messages. Zebra routing software provides TCP/IP based routing services with support from routing protocols RIP, OSPF and BGP. Zebra also supports IPv4 and IPv6 routing protocols.

Command Mode

Privileged User

Example

This example shows how to configure debugging outbound updates:

```
# debug bgp updates
 BGP updates debugging is on
# debug bgp updates out
 BGP updates debugging is on (outbound)
```

debug capture

This command captures network traffic.

Syntax

```
# debug capture {data|trim|voip}
```

Command	Description
data	See debug capture data on the next page
`trim`	See debug capture trim on page 37
`voip`	See debug capture voip on page 38

Command Mode

Privileged User

debug capture data

This command debugs data-routing functionality.

The captured files are saved to a pcap file. You can also send the file to an FTP or a TFTP server or save the file to a USB device connected to the MSBR. You can also save the file locally on the MSBR, but in this case, the file size is limited to 20 MB.

debug capture data interface

This command captures network traffic on one of the data sub-system network interfaces.

Syntax

The syntax of this command includes the following variations:

```
debug capture data interface <interface type> <interface ID> [ipsec]  proto
<protocol filter> host <host filter>
debug capture data interface <interface type> <interface ID> [ipsec] proto
<protocol> host <host filter> port <port filter>
debug capture data interface <interface type> <interface ID> [ipsec] proto
<protocol> host <host filter> port <port filter> tftp-server <tftp server ip address>
debug capture data interface <interface type> <interface ID> [ipsec] proto  udp
<host filter> any port <port filter> ftp-server <ftp server ip address>
```

The command's syntax format is described below:

Arguments	Description
interface type interface ID	Defines the Interface Type and ID of the network interface on which to start the debug capture process. Each interface type has its own interface ID options: ■ vlan <vlan number> ■ GigabitEthernet <slot/port> ■ GigabitEthernet <slot/port.vlan number>
protocol filter	Captures specific protocol, or all protocols. Available options are: ■ all ■ ip ■ ipv6 ■ tcp

Arguments	Description
	■ udp ■ arp ■ icmp
host filter	Captures traffic from/to a specific host (IP address), or any.
port filter	Captures traffic from/to a specific port. Valid ports are 1-65535, or the keyword any. When using arp or icmp as protocol filter, port filter cannot be used, and the only valid value is any. This argument is optional.
tftp server ip address	When this argument is omitted, captured traffic is printed to the CLI console. When using this argument, the captured traffic is saved to a file in pcap format, and when the capture is stopped (using ctrl-c), the capture file is uploaded, via TFTP, to the TFTP server specified in this argument. The TFTP server IP address specified in this argument must be accessible from one of the data sub-system network interfaces, so that the capture file will be uploaded to the server successfully. Use ping test to make sure this TFTP server is accessible. This argument is optional.
ftp server ip address	This command provides support for sending debug captures to an FTP server. Note: This is only applicable to MSBR devices.

Default

NA

Command Mode

Enable

Related Commands

debug capture voip

Examples

The following example starts a debug capture on the network interface vlan 77, with a protocol filter (tcp), a host filter (192.168.0.15), and a port filter (80). The captured traffic will be printed to the CLI session:

```
# debug capture data interface vlan 77 proto tcp host 192.168.0.15 port 80
```

The following example starts a debug capture on the network interface GigabitEthernet 0/0, with a protocol filter (udp), no host filter, and no port filter. The captured traffic will be saved to a temporary file, and will be sent, when ctrl-c is used, to the TFTP server at address 192.168.1.12. This server is accessible via network interface vlan 1:

```
# debug capture data interface GigabitEthernet 0/0 proto udp host any port any tftp-server 192.168.0.15
```

debug capture data physical clear

The command deletes debug captured files from the device's RAM..

Syntax

```
debug capture data physical clear
```

Command Mode

Enable

Related Commands

NA

Examples

The following example deletes debug captured files from the device's RAM.

```
# debug capture data physical clear
```

debug capture data physical start

The command starts capturing files.

Syntax

```
debug capture data physical start
```

Default

By default, capture is inactive.

Note:

- Once this command is issued, recording is performed to an in-memory buffer.
- If the buffer becomes full, recording stops.

Command Mode

Enable

Related Commands

NA

Examples

The following example performs a network capture of both LAN and ADSL.

```
# debug capture data physical start
Note: Debug capture data will be collected locally, and later
sent to a PC via TFTP/FTP. Please make sure that
VLAN 1 is defined and the PC is accessible through it.
```

debug capture data physical stop

This command stops capturing files.

Syntax

```
debug capture data physical stop <Server IP> vrf <VRF name>
```

Arguments	Description
<Server IP>	Defines the IP address of the TFTP/FTP server.
`vrf <name>`	Defines the VRF name.

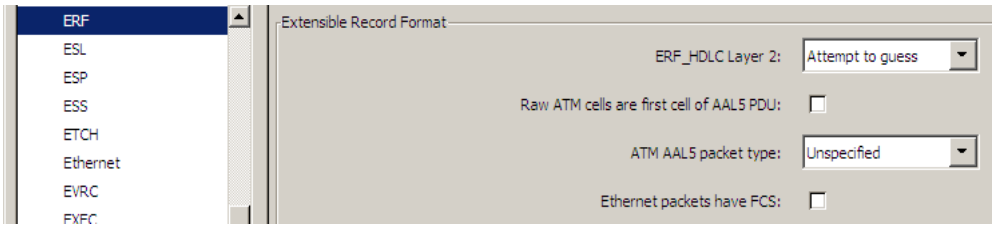
Default

By default, capture is inactive.

Note:

- The captured data is collected locally, and only then sent to the PC later on.
- The usb option is only applicable when a USB stick is connected to the device.

- Once the start command is issued, recording is performed to an in-memory buffer. If the buffer becomes full, recording stops.
- The stop command creates a file named debug-capture-data-<timestamp>.pcap and sends it to the TFTP server. The TFTP server must be configured to allow file uploads.
- The generated PCAP file is in the Extensible Record Format (ERF); recent versions of Wireshark (1.5.0 or newer) are recommended for proper dissection.
- Wireshark's ERF settings must be configured as follows:



Command Mode

Enable

Related Commands

NA

Examples

The debug capture is de-activated using the following existing commands:

```
# debug capture data physical stop 192.168.0.3 vrf vrf1
Trying to send capture to TFTP/FTP server , filename debug-capture-data-
16032014-154400
Finished
```

debug capture data physical insert-pad

This command makes a manual mark in the captured file.

Syntax

```
debug capture data physical insert-pad
```

Default

By default, capture is inactive.

Command Mode

Enable

Related Commands

NA

Examples

The following example inserts a manual mark in the captured file.

```
# debug capture data physical insert-pad
```

debug capture data physical target

This command defines the destination server for the captured packet file.

Syntax

```
debug capture data physical target ftp user <ftp username> password <ftp password>
debug capture data physical target tftp
debug capture data physical target usb
```

Arguments	Description
ftp	Defines using an FTP server.
tftp	Sends the capture to a TFTP server.
usb	Saves the capture to USB storage.

Default

By default, capture is inactive.

Note:

The usb option is only applicable when a USB stick is connected to the device. This applies only to Mediant 5xx and Mediant 8xx devices.

Command Mode

Enable

Related Commands

NA

Examples

The following example sets the destination for the captured packet file as a TFTP server.

```
# debug capture data physical target tftp
```

debug capture data physical autostop

This command provides support for starting a debug-traffic capture on the device's physical network interfaces and allowing it to run until a user-defined event. This event can be a Syslog message or an interface state-change.

All physical targets (TFTP, FTP, and USB), and SSH retrieval are supported, as well as regular and cyclic-buffer modes. When combined with cyclic-buffer mode, this command makes diagnosis of network problems easier.

Syntax

```
debug capture data physical auto-stop {event|keep|send} syslog <message>
debug capture data physical auto-stop event state-change <interface>
debug capture data physical auto-stop event state-change any
debug capture data physical auto-stop {send <IP address>|keep}
no debug capture data physical auto-stop
```

Arguments	Description
auto-stop	Enables auto-stop capture on predefined events. ■ event – Selects events ■ keep – Keeps capture for SSH retrieval ■ send - Sends capture to the TFTP/FTP server
<interface>	Use one of the following: ■ eth-lan ■ eth-wan ■ cellular-wan ■ shdsl-wan ■ t1-wan

Arguments	Description
	■ dsl-wan depending on the hardware capabilities of the device. This command may be issued multiple times to capture data from several interfaces at once.

Default

By default, capture is inactive.

Command Mode

Enable

Related Commands

NA

Examples:

The following are examples of how this command can be used.

■ Defines the Syslog message event, upon which the device stops the debug capture:

```
# debug capture data physical auto-stop event syslog "<message>"
```

■ Defines the state change on a specific interface, upon which the device stops the debug capture:

```
# debug capture data physical auto-stop event state-change <interface, e.g., GigabitEthernet 0/0>
```

■ Defines a state change on any interface, upon which the device stops the debug capture:

```
# debug capture data physical auto-stop event state-change any
```

■ Defines what to do with the debug capture when it is automatically stopped:

```
# debug capture data physical auto-stop {send <IP address>|keep}
```

Where:

- send: sends the capture to the defined IP address

- keep: saves the capture on the device for later retrieval

- Disables the automatic stopping feature for debug captures:

```
# no debug capture data physical auto-stop
```

debug capture data physical <interface>

This command records all traffic on the device's interfaces, saving the result in a PCAP-format file (suitable for Wireshark) on a TFTP server. This command provides support for debug capturing of Asynchronous Transfer Mode (ATM) packets over ADSL through the ADSL/VDSL PHY (physical layer) chipset. It also supports ATM AAL5 (ATM Adaptation Layer 5) and ATM OAMP cells.

Syntax

```
debug capture data physical <interface>
```

<interface>	Description
cellular-wan	Defines the cellular WAN interface.
eth-lan	Defines LAN Ethernet interfaces.
eth-wan	Defines WAN Ethernet interfaces.
fiber-wan	Defines the WAN fiber interface.
xdsl-wan	Defines any DSL interface (ADSL, VDSL) that is installed on the MSBR.
t1-e1-wan	Defines E1/T1 packet capture. **Note:** This is not applicable to Mediant 500Li MSBR.
shdsl-wan	Defines WAN SHDSL interfaces. **Note:** This is not applicable to Mediant 500Li MSBR.
eth-lan vlan4001	Defines internal link between Data and Voice-CPU, and LAN Ethernet interfaces. **Note:** This is not applicable to Mediant 500Li MSBR.
eth-lan vlan4001 only	Defines internal link between Data and Voice-CPUs only. **Note:** This is not applicable to Mediant 500Li MSBR.
eth-lan all-int-	Defines all internals links between Data and Voice-CPUs, and LAN Ethernet interfaces.

<interface>	Description
voip	**Note:** This is applicable only to Mediant 500/500L/800 MSBR operating in Single Networking mode, and applicable to Mediant 500L MSBR.
eth-lan all-int-voip only	Defines all internals links between Data and Voice-CPUs only. **Note:** This is applicable only to Mediant 500/500L/800 MSBR operating in Single Networking mode, and applicable to Mediant 500L MSBR.
wifi-lan	Defines the Wi-Fi interface.

Default

By default, capture is inactive.

Command Mode

Enable

Related Commands

NA

Examples:

The following example performs a network capture of both LAN and DSL.

```
# debug capture data physical eth-lan
# debug capture data physical dsl-wan
```

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.

Command	Description
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.

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 40

debug capture voip interface

This command captures network traffic on a VoIP network interface (VLAN).

Syntax

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

➢ **To start and stop the capture:**

1. After typing the above command, press Enter.

2. To stop the capture, press Ctrl+C.

Command	Description
vlan	Defines the VLAN ID of the network interface on which to start the debug capture.
proto	Configures a protocol filter: ■ **all** (all protocols) ■ arp (ARP packets) ■ icmp (ICMP packets) ■ ip (IP packets) ■ ipv6 (IPv6 packets) ■ tcp (TCP packets) ■ udp (UDP packets)
host	Configures a host (IP address) from/to which the packets are captured. To specify all hosts, enter **any**.
port	(Optional) Configures a port filter: 1-65535 or **any** (all ports). When using **arp** or **icmp** as the protocol filter, port filter cannot 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 (in .pcap file format) 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 of the VoIP network interfaces for the capture file to be successfully uploaded 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 (in .pcap file format) 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 uploaded 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.

Command	Description	
eth-lan	Captures LAN frames.	
get_last_capture	Retrieves the last captured PCAP file sent to a specified TFTP/FTP server IP address. Note: The file is saved to the device's memory (not flash) and is erased after a device reset.	
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. The capture file is named: "debug-capture-voip-<timestamp>.pcap"	
target	Defines the capture storage target: ■ ftp ■ tftp ■ usb	
	`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 cellular

This command debugs the cellular interfaces.

Syntax

```
# debug cellular {<Interface Index>|qmi_proxy|remote|usb_devices} [syslog]
```

Command	Description
Interface Index [0/0 or 0/0/sub_if_ID]	Defines the cellular interface to debug: - `0/0`: Main cellular interface. - `0/0/<Sub Interface ID>`: Debugs a specific APN when dual APNs are configured.
`qmi_proxy`	Enables QMI proxy debug log messages for the cellular interface.
`remote {dmesg|logcat|watchdog)`	Enables debug logging on the M5G-EA cellular module: - `dmesg`: Collects kernel logs from remote M5G-EA cellular module. - `logcat`: Runs logging operations on remote

Command	Description
	M5G-EA cellular module. ■ `watchdog`: Stops watchdog service on remote M5G-EA cellular module for debugging
`usb_devices`	Displays connected cellular USB devices.
`syslog`	Enables sending debug of the cellular interface to Syslog.

Command Mode

Privileged User

Example

This example displays connected USB devices:

```
# debug cellular usb_devices

T:  Bus=01 Lev=00 Prnt=00 Port=00 Cnt=00 Dev#=  1 Spd=480 MxCh= 1
B:  Alloc=  0/800 us ( 0%), #Int=  0, #Iso=  0
D:  Ver= 2.00 Cls=09(hub  ) Sub=00 Prot=01 MxPS=64 #Cfgs=  1
P:  Vendor=0000 ProdID=0000 Rev= 2.06
S:  Manufacturer=Linux 2.6.21.7-Cavium-Octeon dwc_otg_hcd
S:  Product=DWC OTG Controller
S:  SerialNumber=dwc_otg
C:* #Ifs= 1 Cfg#= 1 Atr=e0 MxPwr=  0mA
I:* If#= 0 Alt= 0 #EPs= 1 Cls=09(hub  ) Sub=00 Prot=00 Driver=hub
E:  Ad=81(I) Atr=03(Int.) MxPS=   4 Ivl=256ms
```

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>`	Configures how much time (in minutes or seconds) to wait

Command	Description
{minutes|seconds} '<Command Name>'	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 cwmp send-connection-request

This command sends a connection request to the ACS to start a TR-069 (CWMP) session with the device.

Syntax

```
debug cwmp send-connection-request
```

Default

NA

Command Mode

All

Related Commands

```
(config-system)# cwmp
(cwmp-tr069)# send-connection-request
```

debug data-syslog

This command configures sending data networking debugging messages to Syslog.

Syntax

```
# debug data syslog
```

Command Mode

Privileged User

Example

This example configures sending data networking debugging messages to Syslog:

```
# debug data-syslog
```

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).

Command	Description
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 dhcpv6_client

This command configures debugging the functioning of the Dynamic Host Configuration Protocol (DHCP) version 6 client.

Syntax

```
# debug dhcpv6_client
```

Command Mode

Privileged User

Example

This example configures debugging DHCP v6 client functioning:

```
# debug dhcpv6_client
```

debug dhcpv6_server

This command configures debugging Dynamic Host Configuration Protocol (DHCP) version 6 server processing.

Syntax

```
# debug dhcpv6_server
```

Command Mode

Privileged User

Example

This example configures debugging DHCP v6 server processing:

```
# debug dhcpv6_server
```

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 dot11radio

This command configures debugging the functioning of the router's wireless module.

Syntax

```
# debug dot11radio
```

Command	Description
`ath-debug`	Configures debugging Atheros Communications Inc. wireless module. ■ aggr-mem (Aggregated packets memory handling) ■ beacon (Beacon handling) ■ bt-coex (BT coexistence) ■ calibrate (Periodic calibration) ■ cwm (Channel width management) ■ dcsDynamic (channel switch) ■ fatal-error (Fatal errors) ■ greenap (Green AP) ■ htc-wmi (HTC/WMI) ■ keycache (Key cache management) ■ matMAT (for ProxySTA) ■ node (Node management) ■ power-save (PS Poll and PS save) ■ ppm (PPM management) ■ rateRate (control) ■ recv (Basic RX operation) ■ reset (Reset processing) ■ scan (Scan) ■ state (802.11 state transitions) ■ swr (SwRetry mechanism) ■ uapsd (UAPSD) ■ watchdog (Watchdog timeout) ■ xmit (Basic TX operation)
`ieee80211-debug`	VAP and protocol-related messages.

Command Mode

Privileged User

Example

This example configures debugging the power save function of the router's Atheros Communications Wi-Fi driver:

```
# debug dot11radio ath-debug power-save
```

debug dsl

This command enables and defines the debug level for DSL interfaces.

Syntax

```
# debug dsl {1-8}
```

Command Mode

Privileged User

Example

This example sets the DSL interface debug level to 4:

```
# debug dsl 4
```

debug dynamic-routing

This command configures debugging the MSBR device's memory storage capabilities.

Syntax

```
# debug dynamic-routing
```

Command	Description
all	Debugs using all the commandss listed below.
bgp	Debugs Border Gateway Protocol memory.
lib	Debugs Library memory.
ospf	Debugs Open Shortest Path First (OSPF) memory.

Command	Description
ospf6	Debugs Open Shortest Path First for Internet Protocol version 6 (OSPF6) memory.
rip	Debugs Routing Information Protocol (RIP) memory.
ripng	Debugs RIPng (RIP next generation), defined in RFC 2080, extends RIPv2 to support next generation Internet Protocol, IPv6.
vrf	Associates memory debug messages with a VRF. Enter the name of the VRF table with which to associate the debug messages.
zebra	Debugs Zebra routing software which provides TCP/IP based routing services with support from routing protocols RIP, OSPF and BGP (see above). Zebra also supports IPv4 and IPv6 routing protocols.

Command Mode

Privileged User

Example

This example shows how to configure debugging OSPF memory:

```
# debug dynamic-routing memory ospf
 OSPF if info            :      12
 OSPF if params          :      12
```

debug ethernet

This command configures loopback testing on specific WAN interfaces, for monitoring and troubleshooting (debugging).

Loopback debugging can be activated on any WAN interface (name or type) and allows the remote side to loop traffic back through the device's WAN interface (typically used to check traffic flow). This is to comply with the IEEE 802.3ah standard for Operation, Administration, and Management (OAM) for link-fault management by remote loopback (on the Ethernet WAN interface).

The no debug command is used to disable the feature.

Syntax

```
# debug ethernet loopback interface
```

Command	Description
`fiber [slot/port]`	Configures the fiber interface in Loopback mode.
`gigabitethernet [slot/port]`	Configures the Gigabit Ethernet interface in Loopback mode.

Command Mode

Privileged User

Note

- The command is applicable only to Mediant 500 MSBR and Mediant 800/B MSBR.
- All communication through the loopback WAN interface stops when the command is enabled.

Example

This example shows how to use debug ethernet:

```
# debug ethernet loopback interface gigabitethernet 0/0
    Interface is in LOOPBACK mode.
    You will be unable to pass traffic across that interface.
```

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 get-global-ip

This command configures the device's interface through which it sends the global IP address to the public (e.g., when an ident.me request is received).

Syntax

- **MSBR:**

```
debug get-global-ip source data [source-address] interface
<Interface><Number>
```

- **Mediant 500Li, Mediant 800Ci, MP-5xx:**

```
debug get-global-ip network-source <Interface Name>
```

Command	Description
`source data [source-address] interface`	Source interface, for example, gigabitethernet 0/0.
`network-source <Interface Name>`	Source interface, for example, gigabitethernet 0/0.

Note

When configuring the global IP address for a specific interface, you also need to configure a DNS server (see `ip name-server`).

Command Mode

Basic and Privileged User

Related Commands

`nslookup indent.me` - displays the device's global IP address sent in response to an indent.me request.

Example

The following example configures the interface through which the device sends its global IP address to the public:

- **MSBR:**

```
debug get-global-ip source data interface <Interface><Number>
```

- **Mediant 500Li, Mediant 800Ci, MP-5xx:**

```
debug get-global-ip network-source <Interface Name>
```

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 ipv6-ra

This command debugs Internet Protocol Version 6 (IPv6) Router Advertisement (RA), which enables the MSBR device to advertise its presence.

Syntax

```
# debug ipv6-ra <Debug Level>
```

Command	Description
`Debug Level`	Configures the IP Version 6 RA debug level. ■ 1 = Low ■ 5 = High

Command Mode

Privileged User

Example

This example configures the IP version 6 RA debug level to 5:

```
# debug ipv6-ra 5
```

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 ospf

This command debugs Open Shortest Path First (OSPF) routing protocol for Internet Protocol (IP) networks.

Syntax

```
# debug ospf
```

Command	Description
`event`	Displays OSPF event information.
`ism {events|status|timers}`	Debugs the OSPF Interface State Machine (ISM Event Information, ISM Status Information and ISM TImer Information).
`lsa {flooding|generate|install|refresh}`	Debugs the OSPF Link State Advertisement (LSA Flooding, LSA Generation, LSA Install/Delete and LSA Refresh).
`nsm {events|status|timers}`	Debugs the OSPF Neighbor State Machine (NSM Event Information, NSM Status Information and NSM Timer Information).
`nssa`	Debugs the OSPF NSSA (Not-So-Stubby Area), a non-proprietary extension of the existing stub area feature that allows external routes to be injected in a limited fashion into the stub area. See http://www.ietf.org/rfc/rfc1587.txt for more information.
`packet {all|dd|hello|ls-ack|ls-request|ls-update} {detail|recv|send}`	Debugs the OSPF packets (detailed information, packets received or packets sent). Packets can be all, database (dd), hello, link state acknowledgement, link state request or link state update).
`zebra {interface|redistribute}`	Debugs the OSPF Zebra routing software which provides TCP/IP based routing services with support from routing protocol OSPF.

Command Mode

Privileged User

Example

This example displays OSPF event information:

```
# debug ospf event
```

debug ospf6

This command debugs the Open Shortest Path First (OSPF) routing protocol for Internet Protocol (IP) Version 6 networks.

Syntax

```
# debug ospf6
```

Command	Description
`abr`	Debugs the OSPF Version 6 Area Border Router (ABR) function. ABRs connect one or more areas to the main backbone network.
`asbr`	Debugs the OSPF Version 6 ASBR (Autonomous System Boundary Router) function.
`border-routers {area-id|router-id}`	Debugs the border router (debugs a specific area according to area ID in A.B.C.D. notation, or debugs a specific border router according to that border router's ID in A.B.C.D. notation).
`flooding`	Debugs the OSPF Version 6 flooding function.
`interface`	Debugs the OSPF Version 6 interface.
`lsa [XXXX/0xXXXX] {as-external|inter-prefix|inter-router|intra-prefix|link|network|router|unknown}`	Debugs the OSPF Link State Advertisement. Debugs according to LS type specified as hexadecimal, or debugs AS-External, Inter-Prefix, Inter-Router, Intra-Prefix, Link, Network, Router or Unknown). Possible value for each of these: ■ examin (debugs Examining) ■ flooding (debugs Flooding) -or- ■ originate (debugs Originating)
`message {all|dbdesc|hello|lsack|lsreq|lsupdate|unknown} (recv|send}`	Debugs the OSPF Version 6 messages. Debugs: ■ all (All messages) ■ dbdesc (Database Description messages) ■ hello (Hello messages) ■ lsack (Link State Acknowledgement messages)

Command	Description
	■ lsreq (Link State Request messages) ■ lsupdate (Link State Update messages) ■ unknown (Unknown messages) Possible value for each of these: ■ All ■ Received only -or- ■ Sent only
`neighbor {event|state}`	Debugs the OSPF Version 6 Neighbor. After two routers become OSPF neighbors, they can become adjacent and exchange routing information. ■ event (Debugs OSPF Version 6 neighbor event) ■ state (Debugs OSPF Version 6 neighbor state change)
`route {inter-area|intra-area|memory|table}`	Debugs the calculation of the route table: ■ inter-area (Debugs the calculation of the inter-area route) ■ intra-area (Debugs the calculation of the intra-area route) ■ memory (Debugs route memory use) ■ table (Debugs detail)
`spf {database|process|time}`	Debugs the calculation of the SPF algorithm which computes the best path to all known destinations based on the data in their link state database. ■ database (Log number of Link State Advertisements at the time the SPF is calculated) ■ process (Debugs the detailed SPF process) ■ time (Measures how long it takes to calculate the SPF)
`zebra {recv|send}`	Debugs Zebra routing software. Zebra provides TCP/IP based routing services with support from routing protocols RIP, OSPF and BGP. Zebra also supports IPv4 and IPv6 routing protocols.

Command	Description
	■ Possible values: ■ recv (Debugs only messages received) ■ send (Debugs only messages sent)

Command Mode

Privileged User

Example

This example debugs how long it takes the SPF algorithm to make its calculation:

```
# debug ospf6 spf time
```

debug persistent-log show

This command displays logged messages that are stored on the device's Persistent Logging storage.

Syntax

```
# debug persistent-log show
```

Command	Description
`category-list {conf|err|ha|init|other}`	Filters display by category of logged messages. You can filter by more than one category; make sure that you have spaces between the category subcommands (e.g., category-list conf ha).
`count <Number of Logs>`	Filters display by number of most recently logged messages.
`offset <Logged Message Index>`	When the count command is used, it filters display by displaying from this logged message index onward.
`start-date <Date> end-date <Date>`	Filters display by date range of logged event. The date is in the format YYYY-MM-DD, where YYYY is the year (e.g., 2017), MM the month (e.g., 01), and DD the day (e.g., 20).

Command	Description
`stats`	Displays statistics of the persistent logging: ■ "Number of received logs": Number of logs that were sent to the Persistent Logging storage. ■ "Number of logs sent to DB": Number of logs that were successfully saved to the Persistent Logging storage. ■ "Number of dropped logs": Difference between "Number of received logs" and "Number of logs sent to DB". Dropped logs (typically, due to a high load) indicates that the information in the Persistent Logging storage may be inconsequential or missing.

Note

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

Command Mode

Privileged User

Example

This example filters persistent logging by displaying two logged messages, starting from logged message at index 120:

```
# debug persistent-log show count 2 offset 120
120|2017-04-26 16:10:26|TPApp: [S=11008][BID=da4aec:20]  SNMP
Authentication Failure - source: IP = 172.17.118.45, Port = 1161, failed community
string = public. [File:dosnmpv3.c Line:187]
121|2017-04-26 16:10:46|TPApp: [S=11009][BID=da4aec:20]  SNMP
Authentication Failure - source: IP = 172.17.118.45, Port = 1161, failed community
string = public. [File:dosnmpv3.c Line:187]
```

debug phy-err-injection

This command debugs the Rx physical error injection.

Syntax

```
# debug phy-err-injection
```

Command	Description
`set delay-depth <Value>`	Configures the delay depth, in packets
`set delay-rate <Value>`	Configures the delay rate
`set drop-rate <Value>`	Configures the drop rate
`set interface {atm|efm|fiber|gigabitethernet}`	Configures the interface to run the Rx error on: ■ atm <Group/Subinterface> ■ efm <Slot/Port.vlanID> ■ fiber <Slot/Port> ■ gigabitethernet <Slot/Port.vlanID> Example: 0/0.150 where slot=0, port=0 and vlanID=150
`show`	Shows the configuration of the Rx physical error injection.
`start`	Starts the Rx physical error injection.
`stop`	Stops the Rx physical error injection.

Command Mode

Privileged User

Example

This example starts debugging the RX physical error injection on the Gigabit Ethernet interface, slot 0, port 0 and VLAN ID 150:

```
# debug phy-err-injection set interface gigabitethernet 0/0.150
```

debug reset-history

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

Syntax

```
# debug reset-history
```

Command Mode

Privileged User

Example

This example resets 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 resets.

Syntax

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

Where 0 is the latest syslog.

Command Mode

Privileged User

Example

This example debugs the latest syslog reset history:

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

debug rip

This command configures Routing Information Protocol (RIP) which enables routing information to be exchanged between routers.

Syntax

```
# debug rip
```

Command	Description
`events`	Debugs RIP events
`packet {recv [detail]|send [detail]}`	Debugs RIP packets: ■ recv (Debugs only RIP packets received) ■ send (Debugs only RIP packets sent)
`zebra`	Debugs Zebra routing software. Zebra provides TCP/IP based routing services.

Command Mode

Privileged User

Example

This example debugs RIP packets sent:

```
# debug rip packet send detail
```

debug ripng

This command RIPng (RIP next generation), defined in RFC 2080, is an extension of RIPv2 for support of IPv6 - next generation Internet Protocol.

Syntax

```
# debug ripng
```

Command	Description
`events`	Debugs RIPng events
`packet {recv [detail]|send [detail]}`	Debugs RIPng packets: ■ recv (Debugs only RIPng packets received) ■ send (Debugs only RIPng packets sent)
`zebra`	Debugs Zebra routing software which provides TCP/IP based routing services.

Command Mode

Privileged User

Example

This example shows how to debug RIPng packets that are sent:

```
# debug ripng packet send detail
```

debug rmx-serial

This command configures serial debugging of the RMX (Real-Time Multitasking Executive) real-time operating system, used with the Intel 8080 and 8086 family of processors.

Syntax

```
# debug rmx-serial
```

Command	Description
`clear-logs`	Clears all logs.
`copy-logs-usb`	Copies all saved RMX logs to USB storage.
`list-logs`	Lists the saved RMX serial debug logs.
`profile {current| list-logs|read-log <Number>}`	CPU profiling logs: ■ Current (Prints the currently run RMX CPU profiling log) ■ list-logs (Lists the saved RMX CPU profiling logs) ■ read-log (Read the saved RMX CPU profiling log according to the log's run number)
`read-log <Number>`	Reads the saved RMX serial debug log according to the log's run number.
`tap`	Starts debugging the RMX serial Test Access Port (TAP).

Command Mode

Privileged User

Note

This command is applicable only to Mediant 500/500L/800 MSBR. For Mediant 500Li MSBR, use the command show system logr.

Example

This example debugs the RMX's serial TAP:

```
# debug rmx-serial tap
 [Start RMX serial tap]
```

```
Password: [1129554.457] cn3xxx_check_adsl:1394: @@@ interface adsl 0/2 Line State: 0x000000FF (Idle Request).
[1129556.463] cn3xxx_check_adsl:1394: @@@ interface adsl 0/2 Line State: 0x00000200 (Silent).
[1129618.440] cn3xxx_check_adsl:1394: @@@ interface adsl 0/2 Line State: 0x000000FF (Idle Request).
```

This example lists the saved RMX serial debug logs:

```
# debug rmx-serial list-logs
FILE                        SIZE
--------------------------- --------
log_160.txt                 50024
```

debug serial-port

This command debugs the serial port.

Syntax

```
# debug serial-port
```

Command	Description
`configuration {show}`	Displays the configuration of the second serial port: RMX (default), DSL1 or DSL2.
`dsl {burn-to-flash}`	Configures the second serial port to DSL.
`dsl2 {burn-to-flash}`	Configures the second serial port to DSL2.
`rmx {burn-to-flash}`	Configures the second serial port to RMX (default).

Command Mode

Privileged User

Example

This example shows how to display the second serial port's configuration:

```
# debug serial-port configuration show
The Yellow connector serial port is configured to the RMX
```

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 connectivity, media, etc., are correct. 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) ✓ **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.

Command	Description
`open-channel {analog|digital|virtual} <Channel ID>`	Opens a channel .
`wait-for-detection`	Waits for a digit detection event

Command Mode

Privileged User

debug vrf

This command debugs the MSBR's VRF (Virtual Routing and Forwarding) table which determines what routes to import/export.

Syntax

```
# debug vrf <VRF table name>
```

Command Mode

Privileged User

Example

This example debugs the VRF table:

```
# debug vrf table1
```

debug zebra

This command debugs Zebra routing software. Zebra provides TCP/IP based routing services with support from routing protocols RIP, OSPF and BGP. Zebra also supports IPv4 and IPv6 routing protocols.

Syntax

```
# debug zebra
```

Command	Description
`events`	Debug option set for Zebra events
`kernel`	Debug option set for Zebra between kernel interface
`packet {recv|send} {detail}`	Debugs Zebra routing packets: ■ recv detail (Debugs received Zebra packets) ■ send detail (Debugs sent Zebra packets)
`rib {queue}`	Debugs RIB (Routing Information Base) events. Each routing protocol has its own RIB. The main RIB associates all routing protocols with one another. ■ queue (Debugs RIB queueing)

Command Mode

Privileged User

Example

This example debugs sent Zebra routing packets:

```
# debug zebra packet send detail
```

6 Show Commands

This section describes the show commands.

Syntax

```
show
```

This command includes the following commands:

Command	Description
activity-log	See show activity-log below
admin state	See show admin state on the next page
alias	See show alias on page 79
data	See show data on page 79
debug-file	See show debug-file on page 130
global-mac-table	See show global-mac-table on page 134
ini-file	See show ini-file on page 134
last-cli-script-log	See show last-cli-script-log on page 136
network	See show network on page 136
running-config	See show running-config on page 141
startup-script	See show startup-script on page 145
storage-history	See show storage-history on page 146
system	See show system on page 146
users	See show users on page 160
voip	See show voip on page 161

show activity-log

This command displays the device's logged CLI activities.

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 Command

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

Example

This example displays the logged messages:

```
show activity log
Jan  4 00:44:39 local0.notice [S=4666] [BID=5b1035:208]  HTTPTaskHCTL - Run
selfCheck
Jan  4 00:45:40 local0.notice [S=4667] [BID=5b1035:208]  HTTPTaskHCTL - Run
selfCheck
```

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

Example

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

show data

These commands display data-router functionality.

Syntax

```
show data
```

Command	Description
access-lists	See show data access-lists on page 82
arp	See show data arp on page 83
backup-group	See show data backup-group on page 83
bfd	See show data bfd neighbors on page 84
bgp	See show data bgp on page 85
bridge configuration	See show data bridge configuration on page 86
bridge info	See show data bridge info on page 86
cellular	See show data cellular on page 87
crypto	See show data crypto on page 90
ddns	See show data ddns on page 92
debugging	See show data debugging on page 93
dns-views	See show data dns-views on page 94
dot11radio	See show data dot11radio on page 95
dot1x-status	See show data dot1x-status on page 96
dot1x-supplicant-status	See show data dot1x-supplicant-status on page 97
dsl	See show data dsl on page 98
ethernet	See show data ethernet on

Command	Description
	page 98
f-path rate	See show data f-path rate on page 100
hosts	See show data hosts on page 101
interfaces	See show data interfaces on page 102
ip	See show data ip on page 107
ipv6	See show data ipv6 on page 117
l2tp-server	See show data l2tp-server on page 120
lldp	See show data lldp on page 120
mac-address-table	See show data mac-address-table on page 120
port-monitor	See show data port-monitor on page 122
port-security	See show data port-security on page 122
pptp-server	See show data pptp-server on page 123
qos	See show data qos on page 123
route-map	See show data route-map on page 125
spanning-tree	See show data spanning-tree on page 125
tacacs	See show data tacacs on page 126
track	See show data track on

Command	Description
	page 127
vrrp	See show data vrrp on page 130

Command Mode

Basic User and Privileged User

show data access-lists

This command displays configured access lists (ACL).

Syntax

```
show data access-lists [resolved]
```

Command	Description
resolved	Displays the DNS-resolved IP addresses of hostnames that are configured in the ACL.

Command Mode

Basic User and Privileged User

Example

- Viewing ACLs:

```
show data access-lists
total access list rules [1]
Extended IP access list 100
 100  10 permit ip host example.com host google.com   (0 matches)
```

- To view DNS-resolved IP addresses:

```
show data access-lists resolved
access-list 100 permit ip host example.com [13.226.6.71 13.226.6.16
13.226.6.124 13.226.6.20] host google.com [172.217.16.142]
```

show data arp

This command displays all Address Resolution Protocol (ARP) entries in the cache.

Syntax

```
show data arp
```

Command Mode

Basic User and Privileged User

Example

This example displays all ARP entries in the cache:

```
show data arp

IP Address    MAC Address          Interface        Type
172.17.141.1  64:64:9b:3b:6a:81    VLAN 1           DYNAMIC

End of arp table, 1 entries displayed.
```

show data backup-group

This command displays the configuration of a set of interfaces in a backup group.

Syntax

```
show data backup-group
```

Command Mode

Basic User and Privileged User

Related Commands

```
(config-data)backup-group
```

Example

This example displays the configuration of a set of interfaces in a backup group:

```
show data backup-group
Group Name:  WAN_BACKUP_GROUP
Priority 1   GigabitEthernet 0/0
Priority 2   Fiber 0/1
Priority 3
Currently active interface:  GigabitEthernet 0/0
```

show data bfd neighbors

This command displays details about Bidirectional Forwarding Detection (BFD) neighbors.

Syntax

```
show data bfd neighbors
```

Command	Description
`details [vrf <VRF Table Name>]`	Displays detailed status of all configured BFD neighbors or, optionally, of a specified VRF table.
`vrf <VRF Table Name>`	Displays the status of configured BFD neighbors for a specified VRF table.

Command Mode

Basic User and Privileged User

Example

This example displays the status of all configured BFD neighbors:

```
show data neighbors details
VRF main-vrf
Protocol Codes: S - Static, O - OSPF
  Proto NeighAddr                Holdown(mult) RH/RS State       Int
  1 S   192.168.110.10             600(3)       Up Up       VLAN 2


 OutAddr: 192.168.100.254
 Local Diag: 1, Demand mode: 0, Poll bit: 0
 MinTxInt: 200000, MinRxInt: 200000, Multiplier: 3
 Received MinRxInt: 200000, Received Multiplier: 3
 Holdown (hits): 600(1), Hello (hits): 200(4575)
```

```
Rx Count: 4575
Tx Count: 4578
Last packet: Version: 1            - Diagnostic: 3
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr: 1           - Your Discr: 51
             Min tx interval: 200000  - Min rx interval: 200000
             Min Echo interval: 0
```

show data bgp

This command displays information about Border Gateway Protocol (BGP) processing.

Syntax

```
show data bgp
```

Command	Description
`memory`	Displays statistics on global BGP memory.
`view <BGP View Name>`	Displays information about BGP. ■ rsclient (BGP view name)
`vrf <VRF Table Name>`	Displays BGP status for a specified VRF table.

Command Mode

Basic User and Privileged User

Example

This example displays statistics on global BGP memory:

```
show data bgp memory
 4 RIB nodes, using 384 bytes of memory
 0 BGP routes, using 0 bytes of memory
 0 BGP attributes, using 0 bytes of memory
 0 BGP AS-PATH entries, using 0 bytes of memory
 0 BGP AS-PATH segments, using 0 bytes of memory
 0 peers, using 0 bytes of memory
```

```
7 hash tables, using 280 bytes of memory
8 hash buckets, using 192 bytes of memory
```

show data bridge configuration

This command displays the Ethernet bridging configuration.

Syntax

```
show data bridge configuration
```

Command Mode

Basic User and Privileged User

Example

This example displays the Ethernet bridging configuration:

```
show data bridge configuration
```

show data bridge info

This command displays Ethernet bridging status.

Syntax

```
show data bridge info
```

Command Mode

Basic User and Privileged User

Example

This example displays bridging information when traffic exists:

```
# sh d bridge info
Bridges info:
Bridge: BVI 2              MAC: 00:90:8f:b8:76:cc
VLAN 100
MAC: 00:00:19:82:be:5f
(73781104) eth1.4010.500->eth0.100     bridge_item = 65326500  GigabitEthernet
```

```
0/0.500
MAC: 00:00:19:82:be:5e
(7353f404) eth0.100->eth1.4010.500     bridge_item = 65326540
```

show data cellular

This command displays Internet connections via a cellular 3G/4G modem connected to the USB port, or the integrated LTE/4G cellular modem (QMI).

Syntax

```
show data cellular {config|network-scan|status}
```

Command	Description
`config`	Displays the running configuration.
`network-scan {3g-4g|4g}`	Scans for cellular networks (3G and 4G, or only 4G) in the surrounding area. This feature is useful, for example, for searching the best provider (i.e., strongest signal) to connect the device's SIM to. **Note:** ■ Before running this command, make sure the device is installed with a SIM card. ■ In the command's output, ignore the "QCOPS" lines; this is raw data from the LTE module for display purposes only.
`status`	Displays the current status of the cellular interface (e.g., signal strength per antenna, International Mobile Equipment Identity / IMEI, and firmware version compatible with Mediant 5G-EA).
`status history [1-60]`	Displays a history (in intervals by minutes) of the cellular status. This includes interface technology (e.g., LTE), signal strength (RSRP - Reference Signal Received Power), and IP address assigned by cellular provider to the interface.
`status servingcell`	Displays the cellular network provider (and status) to which the device (SIM) is currently connected. The status can be one of the following: ■ "Registration status code: Searching "

Command	Description
	"Registration description: UE is searching but could not yet find a suitable 2G/3G/4G cell." ■ "Registration status code: Limited service" "Registration description: UE is camping on a cell but has not registered to the network." ■ "Registration status code: Data mode connected" "Registration description: UE is camping on a cell and has registered to the network in data mode." ■ "Registration status code: Data mode connected while call in progress" "Registration description: UE is camping on a cell and has registered to the network with a call in progress." **Note:** ■ It's recommended to run the `no shutdown` command for the cellular interface (i.e., make sure cellular interface is up). ■ In the command's output, ignore the "QENG" lines; this is raw data for display purposes only.

Command Mode

Basic User and Privileged User

Example

■ To scan cellular networks:

```
show data cellular network-scan 3g-4g
Scanning network, please wait a few minutes to
complete..AT+QCOPS=6,1,0,5
.....
..
+QCOPS: "3G","Partner IL","42501","WCDMA
2100",10687,27B1,10CA1E,499,-77,-2
+QCOPS: "4G","Cellcom IL","42502","LTE BAND 3",1400,3a4,4F,-71,-109,-
15

OK
```

```
Technology:  3G
Operator:  Partner IL
Operator numeric format:  42501
Band:  WCDMA 2100
Channel: 10687
Location area code: 27B1
Cell ID: 10CA1E
Primary scrambling code: 499
RSCP: -77
ECIO: -2

Technology:  4G
Operator:  Cellcom IL
Operator numeric format:  42502
Band:  LTE BAND 3
Channel: 1400
Tracking area code: 3a4
Physical cell ID: 4F
RSSI: -71
RSRP: -109
RSRQ: -15
```

- To display the cellular network provider (and status) to which the device is currently connected:

```
show data cellular status servingcell
AT+QENG="servingcell"
+QENG:
"servingcell","NOCONN","LTE","FDD",425,01,CA1C02,157,1600,3,5,5,3EE
F,-82,-5,-57,23,39

OK
Registration status code: Data mode connected
Registration decription: UE is camping on a cell and has registered to the
network in data mode.
Technology:  LTE
TDD/FDD:  FDD
MCC: 425
MNC: 01
Cell ID: 0xCA1C02
Physical cell ID: 157
E-UTRA-ARFCN: 1600
E-UTRA frequency band: 3
UL bandwidth: 20 MHz
```

```
DL bandwidth: 20 MHz
Tracking area code: 3EEF
RSRP: -82
RSRQ: -5
RSSI: -57
SINR: 23
srxlev: 39
```

- To display the current status of the cellular interface:

```
show data cellular status
Cellular 0/0/ interface status:

    Modem status:      UP
    Interface status:       UP
    Cellular operator:  US OR
    Signal strength:    -102 dBm
        Antenna 0 (main): -103 dBm
        Antenna 1 (div): -104 dBm
    Technology: LTE
    Roam status:       HOME
    KB sent:          0
    KB received:       0
    Packets sent:      6
    Packets received:   6

IMEI: 860736041042845
```

- To display status history of cellular LTE:

```
board0-GRX(internal-dev)# do show data cellular status history
-------------------------------------------------------------------------------
|   Time   |    Date    | Radio If. Technology | Signal Strength | IP Assigned |
-------------------------------------------------------------------------------
  15:13:07   06/02/2020          LTE          2dBm        LTE
  15:14:04   06/02/2020          LTE          -62dBm      10.52.21.181
  15:15:00   06/02/2020          LTE          -62dBm      10.52.21.181
  15:16:00   06/02/2020          LTE          -62dBm      10.52.21.181
  15:17:00   06/02/2020          LTE          -62dBm      10.52.21.181
  15:18:00   06/02/2020          LTE          -62dBm      10.52.21.181
  15:19:01   06/02/2020          LTE          -62dBm      10.52.21.181
  15:20:01   06/02/2020          LTE          -62dBm      10.52.21.181
  15:21:01   06/02/2020          LTE          -63dBm      10.52.21.181
  15:22:01   06/02/2020          LTE          -64dBm      10.52.21.181
  15:23:01   06/02/2020          LTE          -63dBm      10.52.21.181
  15:24:01   06/02/2020          LTE          -63dBm      10.52.21.181
```

show data crypto

This command displays information about the encryption module.

Syntax

```
show data crypto
```

Command	Description
conf	Displays the configuration of the IPSec VPN.
debug	Displays diagnostic information about the IPSec VPN.
server	Displays information about the active VPN server.
status	Displays the status of the IPSec VPN.

Command Mode

Basic User and Privileged User

Example

This example displays diagnostic information about the IPSec VPN:

```
show data crypto debug
Kernel routing table:
169.254.254.252/30 dev eth0.4001  scope link  src 169.254.254.253  metric 4
169.254.254.252/30 dev ipsec1  scope link  src 169.254.254.253  metric 5
172.17.141.0/24 dev eth0.1  scope link  src 172.17.141.163  metric 4
172.17.141.0/24 dev ipsec0  scope link  src 172.17.141.163  metric 5
10.25.116.0/24 dev eth0.5  proto static  scope link  metric 1
default via 172.17.141.1 dev eth0.1  proto static  metric 1
---
Data Interfaces:
---
eth0     Link encap:Ethernet  HWaddr 00:90:8F:8C:D3:27
         inet6 addr: fe80::290:8fff:fe8c:d327/64 Scope:Link
         UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500
Metric:1
         RX packets:2792505 errors:0 dropped:0 overruns:0 frame:0
         TX packets:5753622 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:100
         RX bytes:267485784 (255.0 MiB)  TX bytes:911843542 (869.6 MiB)

eth0.1    Link encap:Ethernet  HWaddr 00:90:8F:8C:D3:27
         inet6 addr: fe80::290:8fff:fe8c:d327/64 Scope:Link
```

```
        inet6 addr: 2010:3::116:209/64 Scope:Global
        UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500
Metric:1
        RX packets:2064977 errors:0 dropped:0 overruns:0 frame:0
        TX packets:11246 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:199628814 (190.3 MiB)  TX bytes:846682 (826.8 KiB)

eth0.5    Link encap:Ethernet  HWaddr 00:90:8F:8C:D3:27
        inet6 addr: fe80::290:8fff:fe8c:d327/64 Scope:Link
        inet6 addr: 2010:25::116:209/64 Scope:Global
        UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500
Metric:1
        RX packets:33 errors:0 dropped:0 overruns:0 frame:0
        TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:2440 (2.3 KiB)  TX bytes:1036 (1.0 KiB)

eth0.6    Link encap:Ethernet  HWaddr 00:90:8F:8C:D3:27
        inet6 addr: fe80::290:8fff:fe8c:d327/64 Scope:Link
        inet6 addr: 2010:26::116:209/64 Scope:Global
        UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500
Metric:1
        RX packets:31 errors:0 dropped:0 overruns:0 frame:0
 --MORE--
```

show data ddns

This command displays the configuration of the Dynamic Domain Name System (DNS).

Syntax

```
show data ddns
```

Command Mode

Basic User and Privileged User

Example

This example displays the configuration of the DDNS:

```
show data ddns
```

show data debugging

This command displays debugging information.

Syntax

```
show data debugging
```

Command	Description
bgp	Displays debugging information about BGP.
ospf	Displays debugging information about OSPF.
ospf6	Displays debugging information about OSPF6.
rip	Displays debugging information about Routing Information Protocol (RIP) which enables routing information to be exchanged between routers.
ripng	Displays debugging information about Next Generation Routing Information Protocol (RIP), defined in RFC 2080.
vrf <VRF Table Name>	Displays debugging information for a specified Virtual Routing and Forwarding (VRF) table.
zebra	Displays debugging information about Zebra routing software which provides TCP/IP based routing services with support from routing protocols RIP, OSPF and BGP (see above). Zebra also supports IPv4 and IPv6 routing protocols.

Command Mode

Basic User and Privileged User

Example

This example displays debugging information about BGP:

```
show data debugging bgp
 BGP debugging status:
   BGP events debugging is on
   BGP keepalives debugging is on
   BGP updates debugging is on (outbound)
   BGP fsm debugging is on
```

```
BGP filter debugging is on
BGP zebra debugging is on
```

This example displays debugging information about Zebra:

```
show data debugging zebra
 Zebra debugging status:
  Zebra event debugging is on
  Zebra packet debugging is on
  Zebra kernel debugging is on
  Zebra RIB debugging is on
  Zebra RIB queue debugging is on
```

show data dns-views

This command displays the configuration of the DNS (Domain Name System) server's view feature which allows binding DNS queries source to a specified DNS server destination.

Syntax

```
show data dns-views
```

Command Mode

Basic User and Privileged User

Example

This example displays the configuration of the DNS server's view feature:

```
show data dns-views
dns-view dnsv1:
num of dns queries sent via this view: 3
source address 10.25.2.92/32
source address 10.17.2.92/16

dns-view dnsv2:
num of dns queries sent via this view: 1
source address 10.26.2.92/24
source address 10.17.2.92/16
server address 10.26.2.95
```

show data dot11radio

This command displays status information about the MSBR router's wireless module.

Syntax

```
show data dot11radio
```

Command	Description
`associations {all|interface|stats interface}`	Displays the stations associated with this WiFi access point: ■ all (Displays all stations associated with this access point) ■ interface n (Displays the dot11radio interface, where n is the dot11radio interface number in the range of 1-4) ■ stats interface n (Displays statistics about the associations connecting through the dot11radio interface, where n is the dot11radio interface number in the range of 1-4)
`channel`	Displays information about the current WiFi channel.
`country-code`	Displays the WiFi country code.
`hardware-stats`	Displays statistics about the WiFi hardware.
`interface`	Displays information according to Wi-Fi interface ID.
`other-ap`	Displays other Wi-Fi access points (APs) in the range.

Command Mode

Basic User and Privileged User

Example

This example displays information about the current WiFi channel:

```
show data dot11radio channel
Channel configured auto.  Current channel is 1 Width 20
```

This example displays information about Wi-Fi interface ID 1:

```
show data dot11radio interface 1
dot11radio 1 is Disabled.
 Description: LAN Wireless 802.11n Access Point
 bridge-group 1
 State Time:  91:02:49
 Time since creation:  91:02:49
 mtu auto (current value 1500)
 network lan
 ssid MSBR
 broadcast
 security mode NONE
 no security mac mode
 mode ngb
 channel width 40/20
 channel auto
 power 100
 beacon dtim-period 1
 beacon period 100
 fragment threshold 2346
 cts mode  none
 cts type  cts
 burst num 3
 burst time  2
 rts threshold 2346
 wmm
 country code 0x178 (376)
 DNS is configured dynamic
 IPv6 is disabled
 rx_packets 0              rx_bytes 0
 tx_packets 0              tx_bytes 0
 Device debug: state
 Connected clients: -1
 Global TX power limit: 24dBm
 15-seconds input rate:   0 bits/sec, 0 packets/sec
 15-seconds output rate:  0 bits/sec, 0 packets/sec
 5-minutes input rate:  0 bits/sec, 0 packets/sec
 5-minutes output rate: 0 bits/sec, 0 packets/sec
```

show data dot1x-status

This command displays the status of the 802.1x port.

Syntax

```
show data dot1x-status
```

Command Mode

Basic User and Privileged User

Note

The RADIUS server must be configured for EAP.

Example

This example displays the stations associated with this access point:

```
show data dot1x-status

Port   Auth     State       Timeout Username
----   ----     -----       ------- --------
 1    Disabled  Idle            0
 2    Enabled   Forwarding      75 John
 3    Disabled  Idle            0
 4    Disabled  Idle            0
```

show data dot1x-supplicant-status

This command displays the status of the 802.1x port when configured as a client (supplicant).

Syntax

```
show data dot1x-supplicant-status
```

Command Mode

Basic User and Privileged User

Related Commands

`dot1x supplicant`

Example

This example displays the status when the supplicant mode is disabled:

```
show data dot1x-supplicant-status
802.1x supplicant is disabled
```

show data dsl

This command displays information about digital subscriber line (DSL) connectivity. DSL includes both ADSL (asymmetric digital subscriber line) and VDSL (very-high-bit-rate digital subscriber line).

Syntax

```
show data dsl
```

Command	Description
`status`	Displays status information about the ADSL/VDSL connection.

Command Mode

Basic User and Privileged User

Example

This example displays status information about DSL connectivity:

```
show data dsl status
DSL interface 0/2:
Configuration:        no shutdown
Status: Connected
Line State:           0x801 (Showtime TC Sync)

ATM alarm status:
interface atm 0/2
  vc alarm status: No Alarm
  vp alarm status: No Alarm
```

show data ethernet

This command displays status information about CFM (Connectivity Fault Management).

Syntax

```
show data ethernet
```

Command	Description
`cfm {legend}`	Displays the status of the CFM (IEEE 802.1ag) standard defined by IEEE for local and metropolitan area networks virtual bridged local area networks. ■ legend (Displays descriptions of errors)
`oam {brief|configuration| counters|interface <fiber slot/port> <gigabitethernet slot/port>| status}`	Displays status information about OAM (Operations, Administration, and Maintenance) protocols and practices defined by IEEE 802.3ah for paths through 802.1 bridges and LANs. ■ brief (Displays information about the Ethernet OAM brief) ■ configuration (Displays information about the Ethernet OAM configuration) ■ counters (Displays information about the Ethernet OAM counters) ■ interface ✓ fiber slot/port (Displays information about the fiber interface) ✓ gigabitethernet slot/port (Displays information about the Gigabit Ethernet interface) ■ status (Displays status information about the Ethernet OAM)
`y1731`	Displays the status of ITU-T's Recommendation Y.1731 which addresses performance monitoring.

Command Mode

Basic User and Privileged User

Example

This example displays CFM status including descriptions of errors:

```
show ethernet
show data ethernet cfm legend
```

```
Local MEPs:
MPID  VLAN   RmtRDI MAC    Remote XCON   RmtAIS   RmtLCK
-------------------------------------------------------

Error legend:
VLAN  : The local logical interface is down.
RmtRDI: One of the remote MEPs is not receiving all CCMs.
MAC   : One of the remote MEPs has a blocked port status.
Remote: There are no known remote MEPs.
XCON  : The MEP is receiving CCMs from different domains or services.
RmtAIS: Alarm Indication Signal from MEP
RmtLCK: One of the remote MIP set administrative lock condition .

Remote MEPs:
MPID  Stat DomainName         MAC             Age    Intf Port
-----------------------------------------------------------------

M500Lshow data ethernet cfm

Local MEPs:
MPID  VLAN   RmtRDI MAC    Remote XCON   RmtAIS   RmtLCK
-------------------------------------------------------

Remote MEPs:
MPID  Stat DomainName         MAC             Age    Intf Port
-----------------------------------------------------------------

M500Lshow data ethernet cfm

Local MEPs:
MPID  VLAN   RmtRDI MAC    Remote XCON   RmtAIS   RmtLCK
-------------------------------------------------------

Remote MEPs:
MPID  Stat DomainName         MAC             Age    Intf Port
-----------------------------------------------------------------
```

show data f-path rate

This command displays throughput counters of traffic using fast-path or full-path.

Syntax

```
show data f-path rate [refreshing]
```

Command	Description
`show data f-path rate`	Displays throughput counters of traffic using fast-path or full-path.
`show data f-path rate refreshing`	Displays throughput counters of traffic using fast-path or full-path, and refreshes the output every three seconds until the CTRL+C keys are pressed.

Command Mode

Basic User and Privileged User

Example

This example displays the output of the command:

```
# sh data f-path rate refreshing
 15-seconds Fastpath rate: 430 pps, 0 bps
 5-minutes Fastpath rate: 445 pps, 0 bps
 15-seconds fullpath rate: 475 pps, 1476 Kbps
 5-minutes fullpath rate: 460 pps, 1494 Kbps
```

show data hosts

This command displays the configured DNS server entries and current DNS entries in cache for all Layer 3 interfaces. This includes A/SRV/NAPTR records, and their parameters.

Syntax

```
show data hosts
```

Command Mode

Basic User and Privileged User

Example

This example displays the configured DNS server addresses and current name/address list in cache for all Layer 3 interfaces:

```
show data hosts
```

show data interfaces

This command displays information about each MSBR interface.

Syntax

```
show data interfaces [description|rates|status|<Interface>] {history bandwith}
```

Command	Description
`atm <Group/Subinterface>`	Displays information about the ATM on xDSL interfaces (per DSL line group and ATM sub-interface ID).
`bvi <Bridge Interface ID>`	Displays information about the bridge interface.
`cellular 0/0`	Displays information about the cellular 3G/4G interface.
`description`	Displays a description of the interfaces.
`dot11radio`	Displays status information about the MSBR router's wireless (WiFi) module.
`dsl <Slot/Port>| {brief|history}`	Displays information about the ADSL/VDSL interfaces. ■ <slot/port>: Defines the slot and port of the DSL interface and displays detailed information about the DSL interface ■ `brief`: Displays summarized information about the DSL interface ■ `history`: Displays historical statistics of the upstream and downstream transmission (speed, power, SNR margin and attenuation) of the DSL interface. ✓ <Range>: minutes|hours|days ✓ <Direction>: downstream|upstream ✓ <Type>: attainable-rate|line-attenuation|power|snr-margin|line-state Example:

Command	Description
	show data interfaces dsl 0/2 history minutes upstream power The `history` command can also be written with the `line-state` command to show the last <Number> line state changes of the DSL line. If <Number> is not specified, all entries are shown (100 max.): show data interfaces dsl 0/2 history line-state <Number>
`efm <Slot/Port.vlanID>`	Displays information about Ethernet in the First Mile (EFM) interface's slot, port and VLAN ID.
`fastethernet <Slot/Port>`	Displays information about the Fast Ethernet interface's slot and port. ■ slot/port (FastEthernet interface slot and port)
`fiber <Slot/Port.vlanID>`	Displays information about the Fiber interface. ■ Slot/Port.vlanID
`gigabitethernet <Slot/Port.VLAN ID>`	Displays information about the Gigabit Ethernet interface's slot and port. VLAN ID is optional.
`gre <ID>`	Displays information about the Generic Routing Encapsulation (GRE) tunnel interfaces, according to interface ID. GRE tunneling encapsulates packets so they can be tunneled.
`history bandwidth [hours|minutes]`	Displays bandwidth usage history per specified interface. ■ hours: displays the mean bandwidth usage every 10 minutes for the past 72 hours ■ minutes: displays bandwidth usage every 15 seconds for the past 120 minutes The output is displayed in descending order (i.e., most recent measurement is displayed on top of the list).
`ipip <ID>`	Displays information about the IP-IP tunnel interfaces, according to interface ID. IP-IP Tunnel protocol encapsulates IP packets in IP to create a tunnel

Command	Description
	between two routers. The protocol enables multiple network schemes.
`ipipv6 <ID>`	Displays information about the IP-IP version 6 tunnel interfaces, according to interface ID.
`ipv6ip <ID>`	Displays information about the IP version 6 - IP tunnel interfaces, according to interface ID.
`l2tp <ID>`	Displays information about the Layer 2 Tunneling Protocol (L2TP) interfaces, according to interface ID. L2TP is used to support VPNs and for ISP services delivery.
`loopback <ID>`	Displays information about the Loopback interfaces, according to interface ID. The MSBR's loopback interface is logical and virtual rather than physical like the Fast Ethernet interface or the Gigabit Ethernet interface.
`pppoe <ID>`	Displays information about Point-to-Point Protocol over Ethernet (PPPoE) tunnel interfaces, according to interface ID.
`pptp <ID>`	Displays information about Point-to-Point Tunneling Protocol (PPTP) interfaces, according to interface ID.
`rates {refreshing}`	Displays information about the interfaces rates. ■ To stop the refreshing (if you choose the refreshing option): Press Ctrl+C.
`status`	Displays the interface line statuses.
`switchport {rates <refreshing>}`	Displays information about the switchport interface. ■ rates (Displays interface switchport data rates) ■ To stop the refreshing (if you choose the refreshing option): Press Ctrl+C.
`shdsl`	SHDSL
`vlan <ID>`	Displays information about the VLAN interfaces, according to interface ID.
`vti <ID>`	Displays information about the Virtual Tunnel

Command	Description
	Interfaces (VTIs), according to interface ID.

Command Mode

Basic User and Privileged User

Example

- Displays interface line status:

```
show data interfaces status

                Port        Description  Status      Vlan    Duplex  Speed
                FastEthernet 1/1          disconnected   trunk   -       -
                FastEthernet 1/2          disconnected   trunk   -       -
                FastEthernet 1/3          disconnected   trunk   -       -
                FastEthernet 1/4          disconnected   trunk   -       -
                GigabitEthernet 0/0 WAN Copper connected     -      FULL    1Gbps
            Fiber 0/1 WAN Fiber         disconnected   -      -       -
```

- Displays descriptions of all the interfaces:

```
show data interfaces description

                Interface               Status          Protocol  Description
                GigabitEthernet 0/0         Connected         Up      WAN Copper
                Fiber 0/1               Enabled           Up      WAN Fiber
                EFM 0/2                 Disabled          Down    VDSL
                FastEthernet 1/1          Disconnected      Down
                FastEthernet 1/2          Disconnected      Down
                FastEthernet 1/3          Disconnected      Down
                FastEthernet 1/4          Disconnected      Down
                ATM 0/2                 Connected         Up      ATM 0/2
                VLAN 1                  Connected         Up      LAN switch VLAN 1
                VLAN 4001               Connected         Up      LAN switch VLAN 4001
                BVI 1                   Connected         Up      LAN Bridge
                dot11radio 1            Disabled          Down    LAN Wireless 802.11n Access
Point
            Cellular 0/0            Disabled          Down    3G Cellular PPP connection
```

- Displays statistics of DSL interface transmission:

```
sh data interfaces dsl 0/2 history
                Time: 03/01/2018 11:11:03
                Downstream: Actual speed 112636000, power 13.9, SNR margin 26.2,
Attenuation 0.1
                Upstream: Actual speed 83680000, power 8.1, SNR margin 5.3, Attenuation
1.6
                Time: 03/01/2018 11:09:53
                Downstream: Actual speed 112636000, power 13.9, SNR margin 25.9,
Attenuation 0.1
            Upstream: Actual speed 83680000, power 8.1, SNR margin 5.2, Attenuation
1.6
```

- Displays the bandwidth usage every 15 minutes of the PPPoE interface:

```
show data interfaces pppoe 0 history bandwidth minutes
Jan 19 20 07:24:35  -  Tx:2533 [bps], Rx:25933 [bps]
Jan 19 20 07:24:20  -  Tx:2666 [bps], Rx:2666 [bps]
Jan 19 20 07:24:05  -  Tx:0 [bps], Rx:29333 [bps]
Jan 19 20 07:23:50  -  Tx:0 [bps], Rx:0 [bps]
```

- Displays information about VLAN ID 1 interface:

```
show data interfaces vlan 1

                VLAN 1 is Connected.
                 Description: LAN switch VLAN 1
                 Hardware address is 00:90:8f:87:e7:e2
                 IP address is 192.169.0.1
                 netmask is 255.255.255.0
                 bridge-group 1
                 State Time:  94:39:32
                 Time since creation:  94:40:05
                 Time since last counters clear :  94:38:45
                 mtu auto (current value 1500)
                 DNS is configured static
                 DNS primary IP address is not configured
                 IPv6 is disabled
                 rx_packets 8              rx_bytes 512
                 tx_packets 0              tx_bytes 0
                 15-seconds input rate:   0 bits/sec, 0 packets/sec
                 15-seconds output rate:  0 bits/sec, 0 packets/sec
                 5-minutes input rate:  0 bits/sec, 0 packets/sec
                 5-minutes output rate: 0 bits/sec, 0 packets/sec
```

- Displays DSL history of upstream for SNR margin:

```
show data interfaces dsl 0/2 history hours upstream snr-margin
|        MIN       |        MAX       |        AVG     |
-------------------------------------------------------------------------------------------
1 Hour(s) Ago(dB)    |          194      |          194     |          194     |
|-----------------------------------------------------------------------------------------
2 Hour(s) Ago(dB)    |          193      |          195     |          194     |
```

- Displays DSL line state changes:

```
# show data interfaces dsl 0/2 history line-state
|     Timestamp      |     Line State
-----------------------------------------------------------------------
1  |     00:10:10      |     Full Init
-----------------------------------------------------------------------
2  |     00:10:04      |     Handshake
-----------------------------------------------------------------------
3  |     00:10:02      |     Silent
-----------------------------------------------------------------------
```

show data ip

This command displays configured IP elements.

Syntax

```
show data ip
```

Command	Description
`access-list`	Configures the name or number of the access-list to display.
`arp <vrf>`	Displays the Address Resolution Protocol (ARP) table entries. - vrf (Displays ARP entries for

Command	Description
	a specified VRF table)
`as-path-access-list <Name of AS Path>`	Displays the as-path access list.
`bgp {neighbors <IP address> |summary|vrf}`	Displays information about Border Gateway Protocol (BGP) processing. ■ neighbors <IP address> (Displays detailed information about the neighbor router) ■ summary (Displays a summary of BGP neighbor status) ■ vrf (Displays BGP status information for a specified VRF table)
`captive-portal`	Displays information about the Captive Portal server.
`community-list`	Displays information about the current community list. When number or name is specified, information about

Command	Description
	the specified community list is displayed.
`connections {all|brief|interface| port|queue|summary|top}`	Displays the data router IP network connections. ■ all (Displays All IP connections) ■ brief (Displays IP connection summary) ■ interface (Displays from a specific interface) ■ port (Displays IP connections on a specific port) ■ queue (Displays IP connections on a specific QOS queue) ■ summary (Displays a summary of IP connections by ports) ■ top (Displays the last IP connections)
`dhcp {binding|pool|zone}`	Displays the items in the DHCP database. ■ binding (Displays DHCP address

Command	Description
	bindings) ■ pool (Displays DHCP pools information) ■ zone (Displays DHCP server zones)
`dhcp-server all`	Displays information on all DHCP server interfaces.
`extcommunity-list`	Displays information about the Extended Community Lists.
`firewall {max-conn-statistics|states}`	Displays firewall statistics: firewall max-conn-statistics {last-72-hours|last-hour} Displays firewall states: firewall states [brief]
`fullpath-profiler {enable|show|zero}`	Displays all IP connections.
`igmp proxy {groups} {lan-interface <atm|bvi|cellular| dot11radio|efm|fiber| gigabitethernet|gre|ipip|`	Displays information about IGMP (Internet Group

Command	Description
`ipipv6|ipv6ip|l2tp|loopback| pppoe|pptp|vlan|vti>} {lan-interfaces}`	Management Protocol) which is used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships.
`interface {brief|atm|bvi|cellular|dot11radio| efm|fiber|gigabitethernet| gre|ipip|ipipv6|ipv6ip|l2tp|loopback |pppoe|pptp|vlan|vti|rates}`	Displays the status of each IPv4 interface. 'brief' displays a brief summary of all statuses.
`mroute {active|interfaces|summary| vrf <VRF Table Name>}`	Displays the multicast route table entries. ■ active (Displays active multicast sources) ■ interfaces (Displays information about the multicast route interface) ■ summary (Displays a summary of the multicast route table entries) ■ vrf (Displays information about the multicast route table entries per VRF

Command	Description
	(Virtual Routing and Forwarding) table, according to the name of the VRF table)
`nat {activity <rates|refreshing> |brief|pools|rules| translations}`	Displays the NAT (Network Address Translation) connections. ■ activity (Displays NAT activity - top connections) ✓ rates (Displays NAT activity and statistics - with rate details) ✓ refreshing (Displays NAT activity and statistics – with auto-refreshing). To stop the refreshing (if you choose the refreshing option): Press Ctrl+C.111

Command	Description
	■ brief (Displays IP NAT summary) ■ pools (Displays IP NAT pools) ■ rules (Displays IP NAT rules) ■ translations (Displays currently active translations)
`ospf {border-routers|database|interface|neighbor< [A.B.C.D]|all|atm|bvi|cellular|dot11radio|efm| fiber| gigabitethernet|gre|ipip|ipipv6|ipv6ip|l2tp|loopback |pppoe|pptp|vlan>|route|vrf}`	Displays Open Shortest Path First (OSPF).
`pim {bsr-router|groups|interfaces|rp|vrf}`	Displays information about PIM (Protocol Independent Multicast) used by the MSBR to dynamically create a multicast distribution tree.
`port-map`	Displays information about the MSBR's port-to-application mapping.
`port-triggering`	Displays information about TFTP and L2TP port-triggering.
`prefix-list {<Prefix List`	Displays

Command	Description
Name>|detail|summary|vrf}	information about the IPv4 prefix-based filtering mechanism.
rip {status|vrf <VRF Table Name>}	Displays information about Routing Information Protocol (RIP).
sla responder	Displays the status of the IP SLA Responder service (enabled or disabled, which VRFs, and if active connections) when the device is configured as a responder to Cisco's IP Service Level Agreements (SLAs) UDP jitter test monitor protocol (MOS and QoS). To configure this feature, use the `ip sla responder udp-echo` command.
route {<A.B.C.D>|bgp|connected|kernel|ospf|rip|static|summary|supernets-only|vrf<VRF Table Name>}	Displays information about the IP routing tables.
vrf <VRF Table Name>	Displays information about the IP data routing status for a

Command	Description
	specified VRF table.

Command Mode

Basic User and Privileged User

Example

This example displays information on all DHCP server interfaces:

```
show data ip dhcp-server all
DHCP relay server of interface BVI 1 :
Relay Server is disabled.
DHCP relay server of interface VLAN 1 :
Relay Server is disabled.
DHCP relay server of interface dot11radio 1 :
Relay Server is disabled.
DHCP relay server of interface GigabitEthernet 0/0 :
Relay Server is disabled.
DHCP relay server of interface EFM 0/2 :
Relay Server is disabled.
DHCP relay server of interface GigabitEthernet 0/2 :
Relay Server is disabled.
DHCP relay server of interface Fiber 0/1 :
Relay Server is disabled.
DHCP relay server of interface GigabitEthernet 0/4 :
Relay Server is disabled.
DHCP relay server of interface GigabitEthernet 0/6 :
Relay Server is disabled.
DHCP relay server of interface EFM 0/2 :
Relay Server is disabled.
DHCP relay server of interface ATM 0/2 :
Relay Server is disabled.
DHCP relay server of interface Cellular 0/0 :
Relay Server is disabled.
```

This example displays information about the firewall states:

```
show data ip firewall states
Active Connections 1, quota 50000.
New connections will be created above the quota if there are more than 4096000
```

```
bytes of free memory. Current free memory is 83214336 bytes.
memory. free ram 66179072.
Fastpath packets: 10249, Fullpath packets: 6177852
Totals: TCP 1 UDP 0 ICMP 0
NAT total: 0, of them TCP 0 UDP 0 ICMP 0
Route fp total: 0
fpe total: 0
conn allocation failure: 0 peak: 7 ratio:0
1:      TCP   10.31.2.62:23      <-->10.31.2.62:23       [10.13.2.19:54490]
ESTABLISHED/ESTABLISHED ttl 3599 bytes 16.7/26.6 pkts 419/514 sticky
 0/0 kbps 0/0 pps 0.0/0.0 nas0 Route Incoming  FW-FP-ENA FW-FP-CAP HW-FP-
CAP
```

This example displays a brief summary of the status of each IPv4 interface:

```
show data ip interface brief
Interface           IP Address      Status       Protocol
GigabitEthernet 0/0   1.1.1.1       Connected    Up
                                    1.1.2.1 (s)
                                    1.1.3.1 (s)
Fiber 0/1           unassigned      Enabled      Up
EFM 0/2             unassigned      Disabled     Down
ATM 0/2             10.31.2.62      Connected    Up
VLAN 1              192.169.0.1     Connected    Up
VLAN 4001           169.254.254.253  Connected    Up
BVI 1               192.168.0.1     Connected    Up
dot11radio 1        unassigned      Disabled     Down
Cellular 0/0        0.0.0.0         Disabled     Down
```

This example displays information about port-to-application mapping:

```
show data ip port-map
ip port-map ftp port[21] active[Y]
ip port-map dns port[53] active[Y]
ip port-map dhcp port[67] active[Y]
ip port-map ike port[500] active[Y]
ip port-map pptp port[1723] active[N]
ip port-map aim port[5190] active[Y]
ip port-map msn Messenger port[1863] active[Y]
ip port-map sip port[5060] active[N]
ip port-map h323 cs port[1720] active[Y]
ip port-map h323 ras port[1719] active[Y]
ip port-map mgcp port[2727] active[N]
ip port-map l2tp port[1701] active[Y]
```

```
ip port-map rtsp port[554] active[Y]
ip port-map dhcpv6 port[547] active[Y]
```

This example displays information about TFTP and L2TP port-triggering.

```
show data ip port-triggering
ip port-triggering tftp active[Y]
ip port-triggering l2tp active[Y]
```

show data ipv6

This command displays information related to Internet Protocol version 6.

Syntax

```
show data ipv6
```

Command	Description
`bgp {neighbors <IP address> |summary|vrf}`	Displays information about Border Gateway Protocol (BGP) processing. ■ neighbors <IP address> (Displays detailed information about the connections of the TCP and BGP neighbor router whose IP address is X:X::X:X)

Command	Description
	■ summary (Displays a summary of BGP neighbor status) ■ vrf (Displays BGP status information for a specified VRF table)
dhcp6 {binding|atm| bvi|cellular|dot11radio|efm|fiber| gigabitethernet|gre|ipip|ipipv6|ipv6ip|l2tp| loopback|pppoe|pptp|vlan|vti|pool}	Displays the items in the DHCP database.
interface {brief|atm<Group/Subinterface>|bvi| cellular<Cellular Interface ID>|dot11radio<WiFi Interface ID> |efm<Slot/Port.VLAN ID>|fiber<Slot/Port.VLAN ID>| gigabitethernet<Slot/Port.VLAN ID>|gre<Tunnel GRE ID>|ipip<Tunnel IPIP ID>| ipv6<Tunnel IP v6 ID>|ipv6ip<Tunnel IP v6 IP ID>|l2tp<L2TP Tunnel ID>|loopback<Loopback Interface Index>| pppoe<PPPOE Interface ID>|pptp|vlan<VLAN ID>|vti<VTI ID>}	Displays the status of the IPv6 interface.
neighbors {vrf}	Displays information about IP version 6 neighbors for a specified VRF table.
ospf6 {area<Area ID in A.B.C.D IP Version 4 Format>|border-routers<Router ID><detail>|database<*|adv-router|	Displays Open Shortest Path

Command	Description
as-external|detail|dump|group-membership|inter-prefix|inter-router| internal|intra-prefix|link|linkstate-id|network|router|self-originated type-7>|interface<atm|bvi|cellular| dot11radio|efm|fiber|gigabitethernet| gre|ipip|ipipv6|ipv6ip|l2tp|loopback| pppoe|pptp|vlan|prefix>|linkstate<detail |network router>|neighbor<detail| drchoice>|redistribute |route<IP Version 6 Address in X:X::X:X format|detail|external-1|external-2|inter-area |intra-area|summary>|simulate<SPF Tree>|spf<SPF Tree>|vrf<VRF Table Name>}	First (OSPF) for IP Version 6.
prefix-list {Prefix List Name|detail| summary|vrf}	Displays a prefix list.
ripng {status|vrf<VRF Table Name>}	Displays RIPng (RIP next generation) routes.
route {<IP Version 6 address / prefix in the routing table to display, in X:X::X:X/M format>|bgp|connected|kernel|ospf6|ripng|static|summary|vrf<VRF Table Name>}	Displays the IP Version 6 routing table.

Command Mode

Basic User and Privileged User

Example

This example displays the IP Version 6 routing table associated with BGP:

```
show data ipv6 route bgp
Codes: K - kernel route, C - connected, S - static,
       R - RIPng, O - OSPFv6, B - BGP
```

show data l2tp-server

This command displays the Layer 2 Tunneling Protocol (L2TP) server connections.

Syntax

```
show data l2tp
```

Command Mode

Basic User and Privileged User

Example

This example displays displays incoming L2TP connections:

```
show data l2tp-server
```

show data lldp

This command displays information about Link Layer- 2 Discovery Protocol (LLDP) which advertises/discovers neighbors on IEEE 802 LANs.

Syntax

```
show data lldp neighbors
```

Command Mode

Basic User and Privileged User

Example

This example displays information about LLDP neighbors:

```
show data lldp neighbors
LLDP totals: received 0 packets, sent 0 packets
```

show data mac-address-table

This command displays information about the Ethernet switch's MAC addresses table.

Syntax

```
show data mac-address-table
```

Command	Description
`address`	Finds an Ethernet switch's MAC address in the MAC address table. Use format XX:XX:XX:XX:XX:XX when searching.
`count {vlan <VLAN ID>}`	Displays the size of the Ethernet switch's MAC table, according to VLAN (ID).
`interface {bvi<Bridge Interface ID>}`	Displays the Ethernet switch's MAC table for a specific BVI (Bridge Virtual Interface), according to interface ID.
`vlan <VLAN Interface ID>`	Displays the Ethernet switch's MAC table per VLAN interface, according to VLAN interface ID.
`vrf <VRF Name>`	Displays the Ethernet switch's MAC table per VRF (Virtual Routing and Forwarding) table, according to the name of the VRF table.

Command Mode

Basic User and Privileged User

Example

This example displays the size of the Ethernet switch's MAC table for VLAN ID 1:

```
show data mac-address-table count vlan 1
GE switch: 0 occupied entries.
```

This example displays the Ethernet switch's MAC table for BVI ID 1:

```
show data mac-address-table interface bvi 1
Bridge 1 MAC table:
     MAC Address
-------------------------------------------------
Interface VLAN 1, 0 entries.
-------------------------------------------------
Bridge 1 total 0 entries.
```

show data port-monitor

This command displays the monitoring status for all ports.

Syntax

```
show data port-monitor wan
```

Command Mode

Basic User and Privileged User

Example

This example displays the monitoring status for all ports:

```
show data port-monitor wan
    There is no active Port Monitor session.
```

show data port-security

This command displays information about port security according to interface.

Syntax

```
show data port-security interface
```

Command	Description
`fastethernet <Slot/Port>`	Displays information about security for the Fast Ethernet interface.
`gigabitethernet <Slot/Port>`	Displays information about port security for the Gigabit Ethernet interface.

Command Mode

Basic User and Privileged User

Example

This example displays information about security for the Fast Ethernet interface, Slot 1, Port 1:

```
show data port-security interface fastethernet 1/1
 Port security       : Disabled
 Violation Mode      : Protect
 Aging Time          : 330sec
 Mac Addresses Limit  : 0
 Mac Addresses count  : 0
 Security Violation   : No
```

show data pptp-server

This command displays information about the Point-to-Point Tunneling Protocol (PPTP) VPN server.

Syntax

```
show data pptp-server
```

Command Mode

Basic User and Privileged User

Example

This example displays information about the Point-to-Point Tunneling Protocol (PPTP) VPN server:

```
show data pptp-server
ConnUsername                    IP              Rx/Tx   Uptime
----- ---------------------------------- ---------------- ----------- ------
Total 0 connections.
```

show data qos

This command displays quality of service (QoS) statistics according to specified criteria.

Syntax

```
show data qos
```

Command	Description
match-map	Displays QoS

Command	Description
{atm|cellular|efm|fiber|gigabitethernet|gre|input|ipip|ipipv6|ipv6ip|l2tp|loopback|output|pppoe|pptp|vlan} <Interface ID>	statistics for a group of match-maps or a specific match-map.
queue {atm|cellular|efm|fiber|gigabitethernet|lan} <Slot/Port>	Displays QoS statistics for a group of queues or a specific queue.
service-map {atm|cellular|efm|fiber|gigabitethernet|lan} <Slot/Port>	Displays QoS statistics for a group of service-maps or a specific service-map.
toc	Displays current traffic classification ID - "TC" assignment to queues and classifiers (QoS).

Command Mode

Basic User and Privileged User

Example

This example displays QoS statistics for LAN/WAN queues:

```
show data qos queue
Global statistics for LAN Queues:
No available queue statistics.
```

```
Global statistics for WAN Queues:
GigabitEthernet 0/0:
No available queue statistics.

Fiber 0/1:
No available queue statistics.

EFM 0/2:
No available queue statistics.

ATM 0/2:
No available queue statistics.

Global statistics for  Cellular 0/0 Queues:
No available queue statistics.

Note: Queue name may be truncated (limited to 20 characters).
```

show data route-map

This command displays the route map.

Syntax

```
show data route-map <Route-Map Name>
```

Command Mode

Basic User and Privileged User

Example

This example displays NAT activity and statistics:

```
show data route-map plist1 vrf vrfnam1
```

show data spanning-tree

This command displays the status and parameters of Spanning Tree Protocol including system status and all the relevant interfaces.

Syntax

```
show data spanning-tree
```

Command	Description
`info <Slot/Port>`	Displays only system Spanning Tree information, per Slot/Port.
`interface-info {fastethernet|gigabitethernet} <Slot/Port>`	Displays spanning-tree information per Fast Ethernet interface or per Gigabit Ethernet interface, per Slot/Port.

Command Mode

Basic User and Privileged User

Example

This example displays the status and parameters of STP per Fast Internet interface, Slot 1, Port 1:

```
show data spanning-tree interface-info fastethernet 1/1
    Interface 1/1 Spanning-tree Status
    ---------------------------------
    In this Interface the spanning tree is Disabled!!
```

This example displays the status and parameters of STP per Gigabit Ethernet interface, Slot 0, Port 0:

```
show data spanning-tree interface-info gigabitethernet 0/0
    No spanning tree on this interface
```

show data tacacs

This command displays information about TACACS (Terminal Access Controller Access Control System) authentication protocol, used for centralized username and password verification.

Syntax

```
show data tacacs config
```

Command Mode

Basic User and Privileged User

Example

This example displays information about TACACS:

```
show data tacacs config
```

show data track

This command displays the status of active tracks, a specific track ID, a specific interface or a specific IP address, and track failures.

Syntax

```
show data track {<Track ID> history|<Track ID> rtt-history|brief}
```

Command	Description
`<Track ID> history [failures]`	Display status history of a specific track ID. You optional view track failure history: `show data track <track ID> history failures [<last x hours>]`: Displays track failures (when and duration) for a specified track and optionally, in the last x hours (1-72).
`<Track ID> rtt-history`	Display a graph of track average RTT during THE last 60 minutes and 72 hours of a specific track ID.
`brief {<IP address>|failures|interface}`	Displays the status ("up" or "down") of all active trackings. The output can be filtered by: ■ IPv4 (A.B.C.D): Displays brief tracks status of specific target IP v4 address. ■ IPv6 (X:X::X:X): Displays brief tracks status of specific target IP v6 address. ■ `failures`: Displays brief

Command	Description
	tracks failures ✓ `show data track brief failures`: Displays when the last failures occurred for each track. ✓ `show data track brief failures <last x hours>`: Displays how many times a track failed and for how long (total), in the last x hours (1-720). ✓ `show data track brief failures <IP address>`: Displays when the last failure occurred for each track for a specified IP address. ✓ `show data track brief failures interface <Interface>`: Displays when the last failure occurred for each track for a specified interface. ■ `interface` : Display brief tracks status of specific output in interface.

Command Mode

Basic User and Privileged User

Related Commands

clear counters track

Example

- This example displays the state of all tracks:

```
show data track brief
Track  State    Min / 60sec. Avg / Max  RTT (m.s)    Target        Interface
Description
1      Up       1      1              118              10.4.4.60             VLAN 1
 "vlan1_local_test"
2      Down  3      3              239              1.1.1.1               GigabitEthernet
0/0   "rrr"
3     Up        1      2              135              2001::31              VLAN 1
 "track_3"
4     Up       41     45             212              8.8.8.8               VLAN 1
```

- This example displays the state of all tracks filtered by interface GE 0/0:

```
show data track brief interface gigabitethernet 0/0
Track    State    Min / 60sec. Avg / Max  RTT (m.s)    Target                Interface
       Description
1      Up      41   50        1020          8.8.8.8               GigabitEthernet 0/0
3      Up      41   48        1020          8.8.4.4               GigabitEthernet 0/0
"this_is_a_long_track_description"
11     Down    3    3         239           1.1.1.1               GigabitEthernet 0/0      "rrr"
```

- This example displays when the last failures occurred for each track:

```
# show data track brief failures
track 1 has no failures (target 8.8.8.8, Description "ping_google")
track 2 failed in the last 24 hours (target 8.8.4.4, Description)
track 10 never been UP (target 1.11.2.22, Description)
track 3 failed in the last hour (target 8.8.8.8, Description)
```

- This example displays how many times a track failed and for how long (total), in the last x hours (1-720):

```
# show data track brief failures 24
track 1 failed 2 times for a total of 40 seconds (target 8.8.8.8, Description "ping
google")
track 2 had no failures (target 10.1.1.1, Description)
track 3 Never been UP (target 10.2.1.1, Description)
track 4 failed 5 times for a total of 70 seconds (target 8.8.4.4, Description
"google 2")
```

- This example displays failures (when and duration) for a specified track and optionally, in last x hours (1-72):

```
# show data track 2 history failures 72
Failed at 01-01-2003@05:16:23 for 1 second
Failed at 01-01-2003@15:29:59 for 1 second
Failed at 01-01-2003@22:58:39 for 1 second
Failed at 01-02-2003@00:09:20 for 1 second
```

show data vrrp

This command displays the status of Virtual Router Redundancy Protocol (VRRP).

Syntax

```
show data vrrp
```

Command	Description
`brief`	Displays a brief status of VRRP.
`interface {atm|bvi|cellular|dot11radio| efm|fiber|gigabitethernet|gre| ipip|ipipv6|ipv6ip|l2tp|loopback| pppoe|pptp|vlan|vti}`	Displays VRRP status per interface.

Command Mode

Basic User and Privileged User

Example

This example displays a brief status of VRRP:

```
show data vrrp brief
Interface Grp Pri Time,msec  Own Pre State  Master addr Group addr
```

This example displays the VRRP status for a cellular interface:

```
show data vrrp interface cellular 0/0
```

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 resets in the debug file.

Syntax

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

Command	Description

`list`	Displays a list of logged device resets. Each logged reset is numbered sequentially, displaying the duration (in seconds) that the device was operational (up time) before the reset, the reason for the reset, when it occurred, and the software version, for example:
	`***** Reset *****`
	`Reset Counter:23`
	`Up Time (seconds): 3844`
	`Reset Reason: Web Reset`
	`Reset Time: 26.8.2020 9.25.44`
	`SwVersion: 724A-356-833`
	`**********`
	If the reset was caused due to an error (i.e., crash), "Exception" (instead of "Reset") is displayed at the beginning of the logged reset, 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 reset, specified by its Counter number (use the above command to view all the logged resets 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:
	`# show debug-file reset-info reset-counter 23`
	`Reset Files [syslog]`
	`** Summary **`
	`***** Reset *****`
	`Reset Counter:23`

Command	Description
	Up Time (seconds): 3844 Reset Reason: Web Reset Reset Time: 26.8.2020 9.25.44 SwVersion: 724A-356-833 ********** # show debug-file reset-info reset-counter 23 syslog

Command Mode

Basic and Privileged User

Example

This example displays the list of logged device resets:

```
# show debug-file reset-info list
** Current Reset Counter [25] **

***** Exception *****
Reset Counter:24
Exception Reason: CMX Kernel Panic
EXCEPTION TIME : 4.9.2020 10.21.46
**********

***** Reset    *****
Reset Counter:23
Up Time (seconds): 3844
Reset Reason: Web Reset
Reset Time: 26.8.2020 9.25.44
SwVersion:  724A-356-833
**********

***** Reset    *****
Reset Counter:22
Up Time (seconds): 3844
Reset Reason: CLI Reset
Reset Time: 20.7.2020 13.6.12
SwVersion:  724A-356-833
**********
```

show global-mac-table

This command displays the pool of (eight) MAC addresses with their prefixes (automatically generated or manually configured) and shows if they are being used by an underlying interface.

Syntax

```
show global-mac-table
```

Command Mode

Basic and Privileged User

Related Commands

- To configure the prefix of the MAC addresses in the pool: `set admin-global-mac`
- To enable and associate a MAC address from the pool with an underlying interface: `(conf-if-<interface>)# mac auto`

Example

```
# show global-mac-table
Global Mac Table:
[ 0]: status:    occupied  mac:02:90:8f
[ 1]: status:    free   mac:02:91:8f
[ 2]: status:    free   mac:02:92:8f
[ 3]: status:    free   mac:02:93:8f
[ 4]: status:    free   mac:02:94:8f
[ 5]: status:    free   mac:02:95:8f
[ 6]: status:    free   mac:02:96:8f
[ 7]: status:    free   mac:02:97:8f
```

show ini-file

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

Syntax

```
show ini-file
```

Command Mode

Basic and Privileged User

Example

```
show ini-file
;**************
;** Ini File **
;**************

;Board: Mxx
;HW Board Type: 69  FK Board Type: 84
;Serial Number: 8906721
;Customer SN:
;Slot Number: 1
;Software Version: 7.20A.140.586
;DSP Software Version: 5011AE3_R => 721.09
;Board IP Address: 192.168.0.2
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 192.168.0.1
;Ram size: 512M   Flash size: 128M   Core speed: 300Mhz
;Num of DSP Cores: 1  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;;;Key features:;Board Type: M500L ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;Eth-Port=32 ;DATA features: Routing
FireW
all&VPN WAN BGP Advanced-Routing 3G FTTX-WAN T1E1-Wan-Trunks=2 ;DSP
Voice features: ;Channel Type: DspCh=30 ;E1Trunks=4 ;T1Trunks=4 ;FXSPorts=4
;FXOPo
rts=4 ;Control Protocols: MGCP MEGACO H323 SIP SBC=4 ;Default
features:;Coders: G711 G726;

;------  HW components------
;
; Slot # : Module type : # of ports
;-----------------------------------------
;     2 : FXS        : 4
;     3 : FXO        : 4
;-----------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.31.2.44
EnableSyslog = 1
```

```
TelnetServerIdleDisconnect = 120
--MORE--
```

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 resets (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
arp	See show network arp below
available-app-interfaces	See show network available-app-interfaces below
dhcp clients	See show network dhcp clients on the next page
nqm	See show network nqm on page 139
tls	See show network tls on page 139

Command Mode

Basic and Privileged User

show network arp

This command displays the Address Resolution Protocol (ARP) table.

Syntax

```
show network arp
```

Command Mode

Basic and Privileged User

Example

```
show network arp
IP Address   MAC Address        Interface     Type
10.15.0.1    00:1c:7f:3f:a9:5d  eth0.1        reachable

End of arp table, 1 entries displayed
```

show network available-app-interfaces

This command displays all defined VRF and IP address source network interfaces, including their alias names.

Syntax

show network available-app-interfaces

Command Mode

Basic and Privileged User

Related Command

To configure aliases, use the `alias` command (see alias on page 599).

Note

If no IP route has been configured, the 'Source Address' column displays "None" in the output of this command.

Example

The example below shows the "SIP" application bound to the main VRF, the source IP address is the GigabitEthernet 0/0 interface (10.10.10.1), and the destination is IP address 11.11.11.100.

```
MP5XXNG(config-data)# do show network available-app-interfaces

VRF IFs:  VRF Alias              Address Family                    Vrf Name          IF Status
          ------------------------------------------------------------------------------------------
          "main-vrf-ipv4"        IPv4                              main-vrf          UP
          "main-vrf-ipv6"        IPv6                              main-vrf          UP
          "1234567890123456"     IPv4                              2                 UP
          "voip"                 IPv4                              vrf_voip          UP

IP  IFs:  IP Alias               IP Address          Device IF Name      Vrf Name          IF Status
          ------------------------------------------------------------------------------------------
          "1234567890123450"     10.2.2.2            VLAN 2              main-vrf          UP
          "vlan_1"               10.4.4.61           VLAN 1              2                 UP


Applications binding: (Current source interface resolved in the vrf according to app. destination address)
        App name          VRF Alias                App Dst Address                  Source Address
        ------------------------------------------------------------------------------------------
        SIP               "main-vrf-ipv4"          11.11.11.100                    10.10.10.1
```

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 nqm

This command displays the latest results of previous Network Quality Monitoring (NQM) probing sessions.

Syntax

```
show network nqm <Indexed Sender Number>
```

Command Mode

Basic User and Privileged User

Example

This example displays the latest results of previous Network Quality Monitoring (NQM) probing sessions:

```
show network nqm 0 2

|    Probe Time    | Valid | RTT |  PL  |  PL  | Total | Jit. | Jit. | Total | MOS | MOS |
|                  |       |     | Tx   | Rx   |  PL   | Tx   | Rx   | Jit.  | CQ  | LQ  |
|------------------|-------|-----|------|------|-------|------|------|-------|-----|-----|
|04-25-2017@09:45:22|  yes  |  10 |    0 |    0 |     0 |   24 |    4 |    28 | 4.2 | 4.2 |
|04-25-2017@09:46:22|  yes  |  11 |    0 |    0 |     0 |    3 |    5 |     8 | 4.2 | 4.2 |

there are 3 entries in the log, displaying last 2 entries
```

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 network wan-bindings

This command displays information about the WAN interface bindings.

Syntax

```
show network wan-bindings
```

Command Mode

Basic User and Privileged User

Example

This example displays information about the WAN interface bindings:

```
show network wan-bindings
```

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).
`data [interface|no-switchports |static-routes| tracks]`	Displays the device's data configuration (`configure data`). Optionally, you can filter the output, using the following command options: ■ `interface`: Displays only configuration of a specific interface. ■ `no-switchports`: Displays all configuration except configuration related to the switch ports (e.g., `flowcontrol auto`). ■ `static-routes`: Displays only static routes configuration. ■ `tracks`: Displays only tracks configuration.
`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

Command	Description
	defined by a URL (TFTP, HTTP or HTTPS).
`network`	Displays the device's network configuration (`configure network`).
`system`	Displays the device's system configuration (`configure system`).
`troubleshoot`	Displays the device's troubleshooting configuration (`configure troubleshoot`).
`voip`	Displays the device's VoIP configuration (`configure voip`).

Command Mode

Basic and Privileged User

Note

- The Local Users table (in which management users are configured, as described in user on page 291) 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 stored on the device.

Syntax

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

Command	Description
services	Displays registered storage services, e.g., for CDRs.
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 on the next page
alarms-history	See show system alarms-history on page 148
assembly	See show system assembly on page 148
clock	See show system clock on page 149
cpu-util	See show system cpu-util on page 150
fax-debug-status	See show system fax-debug-status on page 151

Command	Description
feature-key	See show system feature-key on page 151
floating-license	See show system floating-license on page 152
floating-license reports	See show system floating-license reports on page 153
log	See show system log on page 154
ntp-status	See show system ntp-status on page 154
radius servers status	See show system radius servers status on page 155
temperature	See show system temperature on page 156
uptime	See show system uptime on page 157
utilization	See show system utilization on page 157
version	See show system version on page 159

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            |
| 0/0              | 1         | WAN-Copper            |
| 0/2              | 1         | WAN-A/VDSL            |
| 1                | 1-8       | LAN-GE                |
| 2                | 1-4       | BRI NT

USB Port 1: Empty
```

```
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 (data or voice) CPU utilization in the last 72 hours, 60 minutes, and 60 seconds. **Note:** This command is applicable only to Mediant 500/500L/800 MSBR.

Command Mode

Basic and Privileged User

Example

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

show system cwmp

This command displays the status of the DSL Forum's TR-069, CPE WAN Management Protocol (CWMP), for example, the Auto-Configuration Server's (ACS's) URL. CWMP is implemented for CPE-ACS communications. The command also displays the ACS hardware version.

Syntax

```
show system cwmp
```

Command	Description
`deviceinfo hardwareversion`	Displays the ACS hardware version.
`status`	Display the status of the ACS connection.

Command Mode

Basic User and Privileged User

Example

This example displays the status of the ACS connection:

```
show system cwmp status
CPE Connection-Request URL:
ACS URL:
Connection Status: Not applicable
Provisioning Code: 000.000.000.000
```

This example displays the version of the ACS hardware:

```
show system cwmp deviceinfo hardwareversion
HardwareVersion: M500L-4S4O-4LFW-CA1SF-1U
```

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 history.

Syntax

```
show system log
```

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

Command Mode

Basic and Privileged User

Related Commands

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

Example

This example displays the logged messages:

```
show system log
Jan  4 00:44:39 local0.notice [S=4666] [BID=5b1035:208]  HTTPTaskHCTL - Run
selfCheck
Jan  4 00:45:40 local0.notice [S=4667] [BID=5b1035:208]  HTTPTaskHCTL - Run
selfCheck
```

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 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 technical-information

This command displays a multitude of information on the device, which can help with troubleshooting. Typically, AudioCodes support may request that you send its output for troubleshooting.

The command's output includes all the information that the following `show` commands display:

- `show system version`
- `show system assembly`
- `show data ip route`
- `show data ip interface brief`
- `show run`
- `debug reset-history`

The command also includes system ini file content and all data directory content from flash.

Syntax

```
show system technical-information
```

Command Mode

Basic and Privileged User

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 for the Voice application and the Data-Router application (in percentage).

Syntax

```
show system utilization
```

Command	Description
`history {at-start|data|voice}`	■ `at-start`: Displays CPU utilization (in percentage) measured five minutes after the device resets. ■ `data|voice`: Displays CPU utilization (in percentage) of voice or data-router: ✓ 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

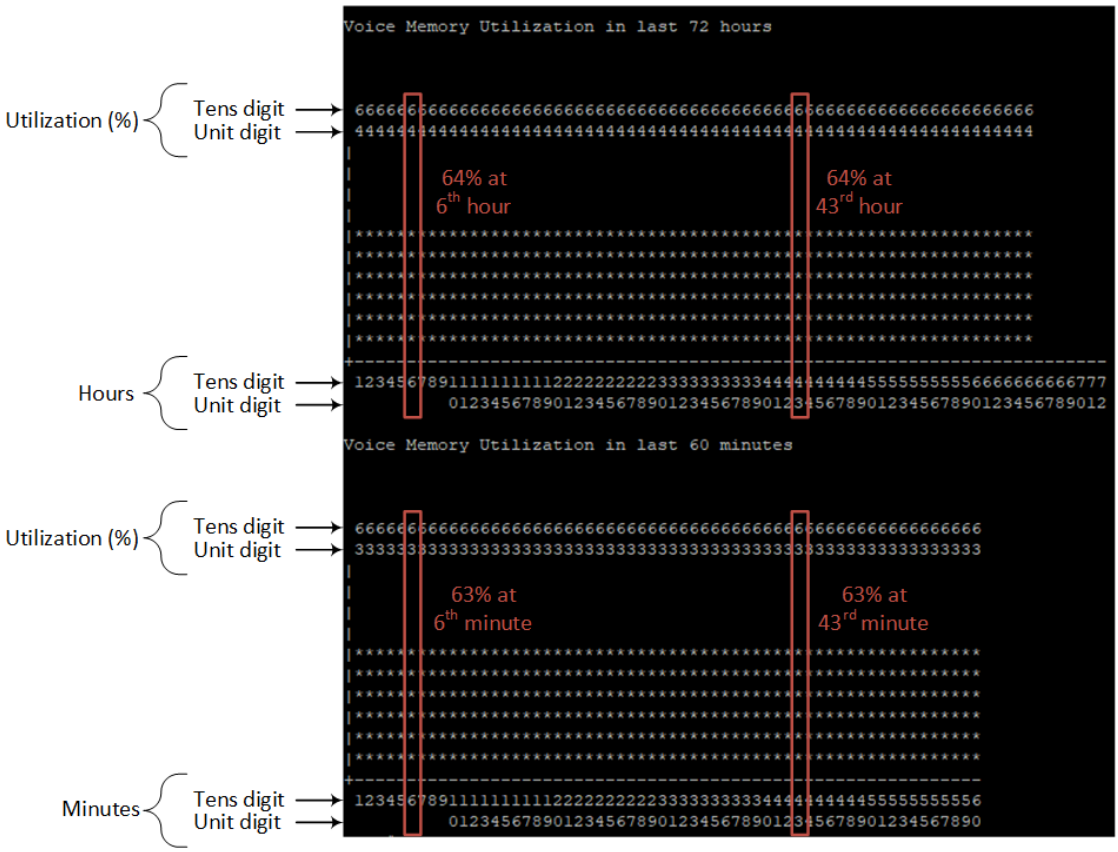
Basic and Privileged User

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`:



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 and terminates users that are currently logged into the device's CLI and applies to users logged into the CLI through RS-232 (console), Telnet, or SSH.

For each logged-in user, the command displays the type of interface (console, Telnet, or SSH), user's username, remote IP address from where the user logged in, and the duration (days and time) of the session. Each user is displayed with a unique index (session ID).

Syntax

```
show users
```

Command Mode

Basic and Privileged User

Note

The device can display management sessions of up to 24 hours. After this time, the duration counter is reset.

Example

Displaying all active calls:

```
show users
[0] console    Admin     local          0d00h03m15s
[1] telnet     John      10.4.2.1       0d01h03m47s
[2]* ssh       Alex      192.168.121.234  12d00h02m34s
```

The current session from which the show command was run is displayed with an asterisk (*).

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 167
coders-stats	See show voip coders-stats on page 168
cpu-stats	See show voip cpu-stats on page 168
dsp	See show voip dsp on page 169
e911	See show voip e911 on page 171
ids	See show voip ids on page 171
interface	See show voip interface on page 172

Command	Description
ip-group	See show voip ip-group on page 174
ldap	See show voip ldap on page 176
other-dialog	See show voip other-dialog statistics on page 177
proxy	See show voip proxy sets status on page 177
realm	See show voip realm on page 178
register	See show voip register on page 179
subscribe	See show voip subscribe on page 181
tdm	See show voip tdm on page 182

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 below
history	See show voip calls history on page 164
statistics	See show voip calls statistics on page 165

Command Mode

Basic and Privileged User

show voip calls active

This command displays active calls.

Syntax

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

Command	Description
(Carriage Return)	Displays the total number of active calls and detailed call information.
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.
`match`	Filters the output according to a matched string.
`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} [<Session ID>] [match <String>]
```

Command	Description
`gw`	Displays historical Gateway CDRs.
`match`	Filters displayed output according to a string.
`sbc`	Displays historical SBC CDRs.
Session ID	(Optional) Displays historical SBC or Gateway CDRs of a specified SIP session ID.
`siprec`	Displays historical SIPRec CDRs.

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`	Displays SBC call statistics (see the example below).	
`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]:  0:00
Call attempts: 0
Incoming call attempts: 0
Outgoing call attempts: 0
Established calls: 0
Incoming established calls: 0
Outgoing established calls: 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
```

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 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).

Command	Description
`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 on the next page

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.

Syntax

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

Command	Description
e1-t1	Displays information on a specified E1/T1 interface.
bri	Displays information on a specified BRI interface.

Command	Description
fxs-fxo	Displays the current status, main PM parameters and main configuration parameters to a specific analog interface (FXS or FXO).
module	Defines the module slot index as shown on the front panel
port	Defines the module's analog port number (FXS/FXO) or trunk port number (E1/T1 or BRI) to display.

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

This example displays information of the E1/T1 interface of trunk port 1 of trunk module 3on the BRI interface:

```
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 interface bri

 show voip interface bri 2/1
----------------------------
     module/port:      2/1
     trunk number:     0
     protocol:         none
     state:            not active
     alarm status:     LOS 1,  LOF 0
     loopback status:  no loop

   performance monitoring was not started on this trunk.

   basic configuration:
     isdn-layer2-mode: BRI_L2_MODE_P2P
     trace-level:      no-trace

 show voip interface bri 2/2
----------------------------
     module/port:      2/2
     trunk number:     1
     protocol:         none
     state:            not active
     alarm status:     LOS 1,  LOF 0
     loopback status:  no loop

   performance monitoring was not started on this trunk.

   basic configuration:
     isdn-layer2-mode: BRI_L2_MODE_P2P
     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 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 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
Active incoming other dialogs: 0
Active outgoing other dialogs: 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	Displays registration status of user Accounts (Accounts table). ■ gw (Gateway accounts) ■ sbc (SBC accounts)
board	Displays registration status for the entire gateway.
db sbc	Displays SBC users registered with the device (SBC User Information table). ■ 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, including the IP Group to which the user belongs): ■ Active:YES = user was successfully registered. Active:NO = user was registered and is waiting for approval. **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	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. ■ 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

Command	Description
	registration status - REGISTERED / NOT REGISTERED).

Command Mode

Basic and Privileged User

Example

- Displaying registration status of SBC users of AOR "2017":

```
show voip register db sbc user 2017
*** SBC Registered Contacts for AOR '2017' ***
sip:2017@10.8.2.225:5080;expire=90; Active: YES; IPG#4; ResourceID#
(#983)
```

- 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: 4
Active incoming SUBSCRIBE dialogs: 6
Active outgoing SUBSCRIBE dialogs: 8
```

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
```

7 Clear Commands

This section describes the clear commands.

Syntax

```
# clear
```

This command includes the following commands:

Command	Description
alarms-history	See clear alarms-history on the next page
clear counters	See clear counters on the next page
clear data	See clear data on page 186
debug-file	See clear debug-file on the next page
clear-history	See clear history on page 187
clear ip	See clear ip on page 188
clear ipv6	See clear ipv6 on page 189
clear l2tp-server	See clear l2tp-server on page 191
clear pptp-server	See clear pptp-server on page 192
qos	See clear qos counters on page 192
storage-history	See clear storage-history on page 192
system	See clear system on page 193
system-log	See clear system-log on page 194
user	See clear user on page 194
voip	See clear voip on page 195

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 counters

This command deletes all interface counters or one specific interface counter.

Syntax

```
# clear counters
```

Command	Description
(Carriage Return)	Deletes all counters.
`atm <Group/Subinterface>`	Deletes the counters of Asynchronous Transfer Mode (ATM) on xDSL interface counters (per DSL line group and ATM sub-interface ID).
`bvi <Bridge Interface>`	Deletes the counters of the Bridge group Virtual Interface (BVI), per interface.

Command	Description
`cellular <Cellular Interface ID Number>`	Deletes the counters of the 3G Cellular interface, per interface ID number.
`dot11radio <Interface ID Number>`	Deletes the counters of the WiFi interface, per WiFi interface ID number.
`efm <Slot/Port.VLAN ID>`	Deletes the counters of the Ethernet in the First Mile interface, per interface slot and port (VLAN ID is optional).
`fiber <Slot/Port.VLAN ID>`	Deletes the counters of the Fiber interface, per interface slot and port (VLAN ID is optional).
`gigabitethernet <Slot/Port.VLAN ID>`	Deletes the counters of the Gigabit Ethernet interface, per interface slot and port (VLAN ID is optional).
`gre <Interface ID Number>`	Deletes the counters of the Generic Routing Encapsulation (GRE) tunneling interface, per GRE tunneling interface ID number.
`ipip <Interface ID Number>`	Deletes the counters of the IP in IP tunneling interface, per IP in IP tunneling interface ID number.
`ipipv6 <Interface ID Number>`	Deletes the counters of the IP in IP version 6 tunneling interface, per IP in IP version 6 tunneling interface ID number.
`ipv6ip <Interface ID Number>`	Deletes the counters of the IP version 6 in IP tunneling interface, per IP version 6 in IP tunneling interface ID number.
`l2tp <Interface ID Number>`	Deletes the counters of the Layer 2 Tunneling Protocol (L2TP), per L2TP tunneling interface number.
`loopback <Interface ID Number>`	Deletes the counters of the PPPoE interface / Loopback interface, per interface ID number.
`pppoe <Interface ID Number>`	Deletes the counters of the Point-to-Point Protocol over Ethernet (PPPoE) interface, per PPPoE interface ID number.
`pptp <Interface ID Number>`	Deletes the counters of the Point-to-Point Tunneling Protocol (PPTP) interface, per PPTP interface ID number.

Command	Description
`track [Track ID]`	Deletes the statistics of the maximum round-trip time (RTT) of packets for all Tracks or optionally, per Track ID. It clears (resets to zero) the minimum and maximum RTT counter displayed in the output of the command, show data track brief.
`vlan <Interface ID Number>`	Deletes the counters of the VLAN interface, per VLAN interface ID number.
`vti <Interface ID Number>`	Deletes the counters of the Virtual Tunnel Interface (VTI), per VTI number.

Command Mode

Privileged User

Example

This example clears all counters:

```
# clear counters
```

This example clears the counter of the PPTP interface whose ID is 0:

```
# clear counters pptp 0
```

clear data

This command deletes the data logs.

Syntax

```
# clear data
```

Command	Description
`dns-view counters`	Deletes the DNS counters.
`dsl-connection-attempts`	Deletes the data logs for DSL connection attempts.

Command	Description
`log-history`	Deletes buffered log messages relating to the data functionality of the device.
`mac-address-table <VLAN>`	Deletes the MAC table. Optional: Deletes per VLAN ID.
`crypto session [peer <IP Address>]`	Deletes all active IPSec security associations (SAs) or the active IPSec SA of a specified peer (IP address).

Command Mode

Privileged User

Example

This example deletes the buffer of log messages relating to the data functionality of the device:

```
# clear data log-history
```

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 ip

This command deletes IP information.

Syntax

```
# clear
```

Command	Description
`access-list {counters}`	Deletes IP access list counters.
`arp {<A.B.C.D.>|all|interface}`	Deletes a specific dynamic ARP entry in the format A.B.C.D., or the entire ARP cache, or the dynamic ARP cache of a specific interface.
`bgp {<*>|<1-65535>|<A.B.C.D>| <X:X::X:X>|dampening|external| peer-group|view}`	Deletes BGP information.
`dhcp {binding}`	Deletes items from the DHCP database.
`mroute <VRF Table Name>`	Deletes the multicast route table entries, or, optionally, for a specified Virtual Routing and Forwarding (VRF) table.

Command	Description
`nat translations`	Deletes the current NAT (Network Address Translation) connections.
`prefix-list <Prefix List Name>`	Deletes the counters for IP prefix lists or for a specified prefix list.
`vrf <VRF Table Name>`	Deletes IP information associated with a specified Virtual Routing and Forwarding (VRF) table.

Command Mode

Privileged User

Example

This example deletes

```
# clear ip nat translations
```

All NAT translations cleared.

This example deletes access list counters:

```
# clear access-list
```

clear ipv6

This command deletes IP version 6 configuration.

Syntax

```
# clear ipv6
```

Command	Description
`dhcpv6 binding {<XX:XX::XX>|all|interface}`	Deletes items from the DHCP version 6 database: ■ XX:XX:XX:XX

Command	Description
	(Deletes a specific IPv6 binding) ■ all (Deletes all automatic bindings) ■ interface (Deletes the binding from a specific interface)
neighbors {<XX:XX::XX>|all|interface<atm|bvi|cellular|efm | gigabitethernet|gre|ipip|l2tp| loopback|pppoe|pptp|vlan>}	Deletes IP version 6 entries from the neighbors table. ■ XX:XX:XX:XX (Deletes a specific IP version 6 entry from the neighbors table) ■ all (Deletes all IP version 6 entries from the neighbors cache) ■ interface (Deletes IP version 6 entries per interface)
prefix-list <Prefix List Name>	Deletes counters for IP version 6 prefix lists, or deletes counters for a specified IP version 6 prefix list.

Command	Description
`vrf <VRF Table Name>`	Deletes the counters on an IP version 6 prefix list associated with a specified VRF table.

Command Mode

Privileged User

Example

This example deletes counters for IP prefix lists:

```
# clear ip prefix-list
```

clear l2tp-server

This command deletes Layer 2 Tunneling Protocol (L2TP) server connections.

Syntax

```
# clear l2tp-server
```

Command	Description
`all`	Clears all L2TP server connections
`conn <Connection Number>`	Clears incoming L2TP server connections, per connection number.

Command Mode

Privileged User

Example

This example clears incoming L2TP server connection number 1:

```
# clear l2tp-server conn 1
```

clear pptp-server

This command deletes incoming Point-to-Point Tunneling Protocol (PPTP) VPN server connections.

Syntax

```
# clear pptp-server
```

Command	Description
`all`	Deletes all PPTP server connections.
`conn`	Deletes incoming PPTP server connections, per connection number.

Command Mode

Privileged User

Example

This example deletes incoming PPTP server connection number 1:

```
# clear # clear pptp-server conn 1
```

clear qos counters

This command deletes counter data related to quality of service.

Syntax

```
# clear qos counters
```

Command Mode

Privileged User

clear storage-history

This command deletes the locally stored CDRs.

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 service: cdr-storage-history Includes the following Command:	
	`all`	Deletes all stored CDR files
	`unused`	Deletes unused stored CDR 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

This command deletes the history of the CPU utilization.

Syntax

```
# clear system cpu-util history
```

Command Mode

Privileged User

Example

This example clears the history of system CPU utilization:

```
# clear system cpu-util history
Cleared CPU history
```

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.

Syntax

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

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 197
`statistics`	See clear voip statistics on page 198

Command Mode

Privileged User

clear voip calls

This command deletes all active calls.

Syntax

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

Command	Description
(Carriage Return)	If Session ID isn't specified, all active VoIP calls are cleared.
Session ID	(Optional) If Session ID is specified, the specified call is cleared.

Command Mode

Privileged User

Related Commands

show voip calls active

Example

Displaying and then clearing VoIP calls:

```
# 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
```

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
```

clear voip statistics

This command deletes calls statistics.

Syntax

```
# clear voip statistics
```

Command Mode

Privileged User

8 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 204
dir	See dir on page 210
erase	See erase on page 211
ethernet	See ethernet on page 212
nslookup	See nslookup on page 213
output-format	See output-format on page 215
ping	See ping on page 216
pstn	See pstn on page 219
reload	See reload on page 219
srd-view	See srd-view on page 222
system-snapshot	See system-snapshot on page 222
telnet	See telnet on page 224
traceroute	See traceroute on page 225
undebug	See undebug on page 227
usb	see usb on page 228
write	See write on page 229
write-and-backup	See write-and-backup on page 230

admin

This command provides various administration-related operations.

Syntax

```
admin
```

Command	Description
admin-global-mac	See admin-global-mac on the next page
register	See admin register|unregister below
state	See admin state on page 202
streaming	See admin streaming on page 204
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-global-mac

This command allows you to configure the MAC address prefix for eight MAC addresses in the pool, which can be used for underlying interfaces. The PPP interface gets its MAC address from the underlying interface (e.g., ppp0 and underlying giga 0/0). Therefore, after creating different interfaces with different MACs, you can create different PPPs and set its underlying to the interfaces with the different MACs.

Syntax

```
# admin-global-mac {<manually configured MAC prefix>|auto}
```

Command	Description
`auto`	The device automatically determines the prefix of the eight MAC addresses in the pool. The first MAC address has prefix 02:90:8f, the second has prefix 02:91:8f, and so on, until the last MAC address which has prefix 02:97:8f. The suffix is taken from the underlying interface (e.g., from gig 0/0).
<manually configured MAC prefix>	You can manually configure the prefix of the eight MAC addresses in the pool. Each MAC address in the pool is incremented by 1 in the second octets. For example, if configured to 09:11:2g, the second MAC has prefix 09:12:2g, the third MAC has prefix 09:13:2g, and so on. The suffix is taken from the underlying interface (e.g., from gig 0/0).

Command Mode

Privileged User

Related Commands

- To see if the MAC addresses in the pool are being used or not (by underlying interfaces): `show global-mac-table`

- To enable and associate a MAC address from the pool with an underlying interface:
  `(conf-if-<interface>)# mac auto`

Example

This example manually configures the prefix of the MAC addresses in the pool:

```
# (config-data)# admin-global-mac 09:11:2g
```

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)

Command	Description
	them when the 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>}
```

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. **Note:** ■ 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).
`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 reset.
`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.
`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).
`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).

Command	Description
system-log-persistent	Defines the file type as a persistent system log file. **Note:** The file can only be downloaded from the device (see the command 'to' 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 service: cdr-storage-history
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).
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

Command	Description
	logo in the device's Web interface. **Note:** The file can only be uploaded to the device (see the command 'from' below).
Download/Upload	
`from`	Uploads a file to the device.
`to`	Downloads a file from the device to a specified destination.
File Location	

URL	Defines the URL from which / to which to upload / download the file.
	The file transfer protocol can be one of the following:
	■ HTTP
	■ HTTPS
	■ SCP
	■ TFTP
	The source network interface (IP address alias/IP VRF alias) can also be specified using the `source` command:
	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>@<IP>/<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, connected to the device, 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.

Command Mode

Privileged User

Related Commands

- erase
- dir
- write

Note

- When you load 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 resets or powers off.
- For more information on the different file types, refer to the User's Manual.
- During firmware file (.cmp) load, a message is displayed showing load 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 load 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

- Copying firmware file from an HTTP server:

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

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

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

- Auxilliary file batch:

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

- Copying CLI-based configuration from TFTP server:

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

- Upgrading the device's firmware from a source URL file:

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

- Copying the dial plan file:

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

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 an Auxiliary file from the device's memory.

Syntax

```
# erase <Auxiliary File>
```

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), enter the write command after issuing the dir command.

Command Mode

Privileged User

Related Commands

- dir
- write

Example

- Viewing Auxilliary files:

```
# 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
```

- Erasing the CPT file from flash memory:

```
# erase call-progress-tones
# write
```

ethernet

This command configures ITU-T's Y.1731 feature which delivers fault and performance management to service providers managing extensive networks.

Syntax

```
# ethernet
```

Command	Description
`cfm lck {start level <1-7>period <1,60>|stop}`	Configures Connectivity Fault Management (CFM) and Locked Signal (LCK). ■ level (Configures the maintenance level for sending LCK frames) ■ period (Configure the LCK transmission period: 1 second or 60 seconds)
`y1731 1dm{domain <Domain Name>mpid<Endpoint ID>level <1-7>}|loss`	Configures ITU-T's Y.1731 feature's Frame Delay to a single delay measurement (1DM).

Command	Description
	■ domain (the name of the domain) ■ mpid (endpoint identifier) ■ level (Configures the maintenance level for sending frames) ■ loss (Configures ITU-T's Y.1731 feature's frame loss measurement)

Command Mode

Privileged User

Example

This example configures starting Ethernet CFM and LCK, level 1, period 60:

```
# ethernet cfm lck start level 1 period 60
```

This example configures ITU-T's Y.1731 Frame Delay to a single delay measurement (1DM) whose domain is MIKE, endpoint ID 1, level 1.

```
# ethernet y1731 1dm domain MIKE mpid 1 level 1
```

nslookup

This command queries the Domain Name System (DNS) to obtain domain name mapping or IP address mapping.

Syntax

```
nslookup indent.me|<Hostname> [source voip interface vlan <VLAN ID>] [type {a|aaaa|naptr|srv}
```

Command	Description
Hostname	Defines the host name.
`indent.me`	Displays the global IP address of the device that is sent in response to an ident.me request. **Note:** To configure the interface through which the device sends the global IP address, use the following command: ■ **MSBR:** `debug get-global-ip source data [source-address] interface <Interface><Number>` ■ **Mediant 500Li, Mediant 800Ci, and MP-5xx:** `debug get-global-ip network-source <Interface Name>`
`source voip interface vlan`	(Optional) Configures a VLAN ID (1 -3999).
`type`	(Optional) Defines the type of DNS: ■ a (Use a Host address) ■ aaaa (Use an IPv6 Address) ■ naptr (Use NAPTR - Naming Authority PoinTeR) ■ srv (Use Server selection)

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

Command Mode

Basic and Privileged User

Example

The following displays an example of an nslookup for Google:

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

The following displays an example of an nslookup for an indent.me request:

```
nslookup ident.me
ident.me resolved to 49.12.234.183
```

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 8.

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>} [ethernet mpid]  [source data {interface|source-address|vrf}] [repeat <Echo Requests>] [size <Payload Size>]  [summarized]
```

Command	Description
<IPv4 Address>	Configures an IPv4 IP address in dotted-decimal notation or as a hostname.
ipv6 <IPv6 Address>	Configures an IPv6 address as X:X::X:X or as a hostname.
<Hostname>	Configures a hostname or FQDN (.g., abc.com).

Command	Description
ethernet mpid <Endpoint ID> domain <CFM Domain Name>	Configures a Layer-2 ping - Ethernet Connectivity Fault Management (CFM) per IEEE 802.1ag. This is a loopback message.
`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).
`source data interface`	(Optional) Specifies the interface from where you want to send the ping packet. The source IP address is selected automatically. ■ bvi (bridge interface) ■ cellular (Cellular 3G interface) ■ gigabitethernet (Gigabit Ethernet interface) ■ gre (GRE tunnel interface) ■ ipip (IPIP tunnel interface) ■ ipipv6 (IPIPv6 tunnel interface) ■ ipv6ip (IPv6IP tunnel interface ■ l2tp (L2TP tunnel interface) ■ loopback (PPPoE interface) ■ pppoe (PPPoE interface) ■ pptp (PPTP tunnel interface) ■ vlan (VLAN interface) ■ vti (VTI tunnel interface)
`source data source-address`	(Optional) Specifies the source interface (IP address of the interface) from where you

Command	Description
	want to send the ping packet. ■ gigabitethernet (Gigabit Ethernet interface) ■ gre (GRE tunnel interface) ■ ipip (IPIP tunnel interface) ■ ipipv6 (IPIPv6 tunnel interface) ■ ipv6ip (IPv6IP tunnel interface ■ l2tp (L2TP tunnel interface) ■ loopback (PPPoE interface) ■ pppoe (PPPoE interface) ■ pptp (PPTP tunnel interface) ■ vlan (VLAN interface) ■ vti (VTI tunnel interface)
`source data vrf`	(Optional) Specifies the VRF name from where you want to send the ping packet.
`summarized`	Displays a summary of the ping results.

Command Mode

Basic and Privileged User

Note

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

Example

■ Pinging an FQDN:

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

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

```
ping 10.4.0.1 source data 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 IPv6 destination address:

```
ping ipv6 2001:15::300
```

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 resets the device with or without saving the configuration to flash memory.

Syntax

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

Command	Description
`if-needed [graceful]`	Resets the device only if you have configured parameters that require a device reset 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]`	Resets the device immediately and saves configuration (including Auxiliary files) to flash memory (before reset). The reset can be done immediately or upon certain conditions: ■ `reload now` : Resets the device immediately. ■ `reload now graceful <seconds>`: Resets the device only after the user-defined period (in seconds) elapses. ■ `reload now graceful if-no-calls`: ✓ If calls exist, the device doesn't reset and displays "Not Good (In Call)". ✓ If no calls exist, the device resets immediately and displays "OK". ✓ If the device is unable to restart (for whatever reason), it displays "Not Good".
`without-saving [in <Minutes>|graceful <Seconds>]`	Resets the device without saving configuration to flash memory. You can also configure a delay time before reset occurs: ■ `in`: Resets the device only after a user-defined period (in minutes). Use this before making changes to sensitive

Command	Description
	settings. If your changes cause the device to lose connectivity, wait for the device to restart with the previous working configuration. ■ `graceful`: Resets 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 resets 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 resets. To cancel the delayed reset, use the `no reload` command.

Command Mode

Privileged User

Related Command

`write`

`reload-timeout-for-emergency-call`

Example

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

```
# reload if-needed
```

run-startup-script

This command executes a loaded startup script.

Syntax

```
# run-startup-script
```

Command Mode

Privileged User

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
```

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>  [source data [interface|source-address|vrf]]
```

Command	Description
Address	Remote host IP address.
Port	(Optional) Remote host port number.
`interface {bvi|cellular|gigabitethern|gre|ipip|ipipv6|ipv6ip|l2tp|loopback|pppoe|pptp|vlan|vti}`	Defines the source interface and ID to bind to.
`source-address interface {bvi|cellular|gigabitethern|gre|ipip|ipipv6|ipv6ip|l2tp|loopback|pppoe|pptp|vlan| vti}`	Defines the source address interface to bind to.
vrf	Defines the virtual routing forwarding (VRF) name.

Command Mode

Privileged User

Example

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

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

- Invoking a Telnet session to a device located on the WAN using a WAN interface:

```
# telnet 10.10.10.2 23 source data interface gigabitethernet 0/0
```

- Invoking a Telnet session to a device located on the WAN using VRF:

```
# telnet 10.10.10.2 23 source data vrf Test
```

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>} [max-ttl <Hop Limit>] [proto udp|icmp] [resolve-to-name]
```

```
traceroute {ipv6 <IPv6 Address>|<IPv4 Address>} source data {source-address interface <Interface Type> <Slot/Port/VLAN>|vrf <VRF Name> [max-ttl <Hop Limit>] [proto udp|icmp] [resolve-to-name]
```

```
traceroute {ipv6 <IPv6 Address>|<IPv4 Address>} source network-source <IP address alias or VRF> [proto udp|icmp]
```

Command	Description
IPv4 Address or Hostname	The IPv4 address or hostname to which the trace is sent.
`source data source-address interface`	Source interface, for example, gigabitethernet 0/0.
`source data vrf`	Source VRF name.
`source network-source`	Source network (alias or VRF).
`max-ttl`	Defines the maximum number of hops to the destination (1-30; default is 30).
`proto {icmp|udp}`	Defines the protocol type. The default is UDP. IPv4 traceroute also supports icmp protocol type.
`resolve-to-name`	If a DNS server has been configured, this option displays the FQDN of each node on the path to the destination (where possible). After entering this command option, no other options can be entered.

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
```

undebug

This command disables debugging Border Gateway Protocol (BGP) functions.

Syntax

```
# undebug
```

Command	Description
`all bgp`	Disables debugging all BGP functions.
`bgp {events|filters| fsm|keepalives|updates zebra}`	Disables debugging specified BGP functions. - Disables BGP events. - Disables BGP filters. - Disables BGP FSM information. - Disables BGP keepalives. - Disables BGP updates. - Disables BGP Zebra information.
`vrf <VRF Table Name> {all|bgp <events|filters|fsm| keepalives|updates| zebra>}`	Disables debugging specified functions in the MSBR's VRF (Virtual Routing and Forwarding) table. - Disables VRF events. - Disables VRF filters. - Disables VRF FSM information. - Disables VRF keepalives. - Disables VRF updates.

Command	Description
	■ Disables VRF Zebra information.

Command Mode

Privileged User

Related Commands

debug

Example

This example disables debugging all BGP functions:

```
# undebug all bgp
 All possible debugging has been turned off
```

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`	Restores the device's configuration to factory defaults.

Command Mode

Privileged User

Note

- The `write` command does not reset the device. For parameters that require a reset for their settings to take effect, use the `reload now` command instead, or use it after the `write` command.
- The `write factory` command erases all current network configuration and thus, remote connectivity to the device (Telnet/SSH) may fail immediately after you run this command.
- When the `write factory` command is run, Auxiliary files are also erased.

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

9 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
additional-mgmt-if	See additional-mgmt-if
automatic-update	See automatic-update on page 234
cli-settings	See cli-settings on page 243
clock	See clock on page 250
configuration-version	See configuration-version on page 251
cwmp	See cwmp on page 252
feature-key	See feature-key on page 257
floating-license	See floating-license on page 258
http-services	See http-services on page 260
hw	See hw on page 265
hostname	See hostname on page 266
ldap	See ldap on page 267
mgmt-access-list	See mgmt-access-list on page 273
mgmt-auth	See mgmt-auth on page 274
ntp	See ntp on page 276
performance-profile	See performance-profile on page 278
provision	See provision on page 277

Command	Description
radius	See radius on page 280
sbc-performance-settings	See sbc-performance-settings on page 283
snmp	See snmp on page 284
user	See user on page 291
user-defined-failure-pm	See user-defined-failure-pm on page 294
web	See web on page 295
web-data	See web-data on page 297
web-if	See web-if on page 299
welcome-msg	See welcome-msg on page 301

Command Mode

Privileged User

10 automatic-update

This command configures the Automatic Update feature.

Syntax

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

Command	Description
File	Automatically uploads specified files to the device from a remote server. For more information, see Files on page 236.
`aupd-graceful-shutdown <Seconds>`	Enables the graceful lock period for Automatic Update and defines the period.
`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.
`http-user-agent`	Defines the information sent in the HTTP User-Agent header. For more information, see http-user-agent on page 239.
`network-source`	Defines the alias name representing a VRF or an IP address of the IPv6 source network interface that is used to bind to the Automatic Update mechanism.
`predefined-time`	Defines the time of day in the format hh:mm (i.e., hour:minutes).

Command	Description
`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 resets (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 239.
`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 241.
`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 seconds) between subsequent Automatic Update processes.
`verify-certificate {off|on}`	Enables verification of the server certificate over HTTPS. The device authenticates the certificate against the 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

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 loaded. 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 loaded.
`cas-table`	Defines the URL path to a remote server from where the Channel Associated Signaling (CAS) file can be loaded.
`cli-script`	Defines the URL path to a remote server from where the CLI Script file can be loaded.
`configuration-pkg`	Defines the URL path to a remote server from where the Configuration Package file can be uploaded. **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 loaded.
`dial-plan-csv`	Defines the URL path to a remote server from where the Dial Plan file (.csv) can be loaded.
`feature-key`	Defines the URL path to a remote server from where the License Key file can be loaded.
`firmware`	Defines the URL path to a remote server from where the software file (.cmp) file can be loaded. **Note:** This is a one-time file update; once loaded, the device does not load it again.

Command	Description
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 loaded.
network-source	Defines the alias name representing a VRF or an IP address of the source network interface that is used to open the connection with the remote server.
prerecorded-tones	Defines the URL path to a remote server from where the Prerecorded Tone file can be loaded.
startup-script	Defines the URL path to a remote server from where the Startup Script file can be loaded.
tls-cert	Defines the URL path to a remote server from where the TLS certificate file can be loaded.
tls-private-key	Defines the URL path to a remote server from where the TLS private key file can be loaded.
tls-root-cert	Defines the URL path to a remote server from where the TLS root CA file can be loaded (replaces existing files).
tls-root-cert-incr	Defines the URL path to a remote server from where the TLS root CA file can be loaded (incremental file load).
user-info	Defines the URL path to a remote server from where the User Info file can be loaded.
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 loaded.
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 loaded.
voice-configuration	Defines the URL path to a remote server from where the voice configuration file can be loaded.

Command	Description
`voice-prompts`	Defines the URL path to a remote server from where the Voice Prompts file can be loaded.
`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 loaded.
`web-logo`	Defines the URL path to a remote server from where the logo image file for the Web interface can be loaded.

Command Mode

Privileged User

Note

- You can use a placeholder ("<MAC>" or "<mac>") for the device's LAN MAC address in the URL path and filename of some of the URL parameters. For more information, see the *User's Manual*.
- You can use a placeholder ("WANMAC" or "<wanmac>") for the device's WAN MAC address in the URL path and filename of some of the URL parameters. For more information, see the *User's Manual*.
- 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-<MAC>.txt"
(auto-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 ■ 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>>
```

Command	Description	
<URL>	Defines the URL address of the provisioning server (HTTP/S, FTP, or TFTP).	
File Name <FILE>	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:	
	File Type (template-files-list)	Hard-coded String
	ini	device.ini
	init	deviceTemplate.ini
	cli	cliScript.txt
	clis	cliStartupScript.txt
	acmp	autoFirmware.cmp
	vp	vp.dat (applies only to Mediant 1000B)
	usrinf	userInfo.txt
	cmp	firmware.cmp
	fk	fk.ini

Command	Description	
	cpt	cpt.dat
	prt	prt.dat
	cas	cas.dat (applies only to Digital PSTN devices)
	dpln	dialPlan.dat
	amd	amd.dat
	sslp	pkey.pem
	sslr	root.pem
	sslc	cert.pem

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

11 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 246).
`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 resets. 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.

Command	Description
`direct-exec {off|on}`	Enables users with Security Administrator privileges to skip the `enable` command and start in enabled mode (Privileged User) by default upon CLI login. For more information on this mode, see Privileged User Mode on page 4.
`idle-timeout {off|on}`	Defines the maximum duration (in minutes) that a CLI session may remain idle, before being disconnected.
`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).
`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-if`	Defines the SSH Interfaces table (see ssh-if on page 248).
`ssh-last-login-message {off|on}`	Enables the display of the last address from which the user logged into the SSH server.
`ssh-max-binary-packet-size`	Defines the maximum SSH binary packet size.

Command	Description
`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).
`ssh-max-sessions`	Defines the maximum number of SSH sessions.
`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-if`	Defines the Telnet Interfaces table (see telnet-if on page 247).
`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-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.

Command	Description
	■ automatic: Whenever you manually change the height of the window (i.e., by dragging with the mouse), the new size is automatically saved. **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
```

telnet-if

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

Syntax

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

Command	Description
Index	Defines the table row index.
`network-source`	Defines the alias name representing a VRF or an IP address of the source network interface that is used to bind to the Telnet application (interface that the listening socket opens).
`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

Note

The command is applicable only to Mediant 500Li.

Example

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

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

ssh-if

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

Syntax

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

Command	Description
Index	Defines the table row index.
`network-source`	Defines the alias name representing a VRF or an IP address of the source network interface that is used to bind to the SSH application (interface that the listening socket opens).
`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

Note

The command is applicable only to Mediant 500Li.

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
```

12 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`	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.
`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.

Command Mode

Privileged User

Example

This example configures the date of the device.

```
(config-system)# clock
(clock)# date 23/11/2016
```

13 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
```

13 cwmp

This command configures TR-069.

Syntax

```
(config-system)# cwmp
(cwmp-tr069)#
```

Command	Description
`acs-password`	Defines the login password that the <device> uses for authenticated access to the ACS.
`acs-url`	Defines the URL address of the ACS to which the <device> connects. For example, http://10.4.2.1:10301/acs/.
`acs-url-provisioning-mode {automatic|manual}`	Defines the method for configuring the URL of the TR-069 ACS.
`acs-user-name`	Defines the login username that the <device> uses for authenticated access to the ACS.
`conf-change-notification {off|on}`	Enables the device to notify the TR-069 ACS of device configuration changes.
`connection-request-password`	Defines the connection request password used by the ACS to connect to the <device>.
`connection-request-user-name`	Defines the connection request username used by the ACS to connect to the <device>.
`cwmp-acl <ACL Name>`	Applies an ACL rule to TR-069 management.
`data-model {device|internetgatewaydevice}`	Defines the TR-069 Data Model: ■ device: Device (TR-181) ■ internetgatewaydevice: TR-098
`default-inform-interval`	Defines the inform interval (in seconds)

Command	Description
	at which the <device> periodically communicates with the ACS.
`delete-device-log`	Deletes the device's CWMP log records.
`disable-provisioning-code-limitation`	Disables reject ACS set request when configuration mode is Manual.
`display-allowed-acs-ips`	Displays the allowed IP addresses of the ACS. These are IP addresses that have been automatically added to the device's firewall (see the `port-restriction` command, below), which blocks all other IP addresses from accessing the TR-069 listening port. **Note:** This command is applicable only to MP-5xx, Mediant 500Li, and Mediant 800Ci.
`display-device-log`	Displays the device log records received by the ACS.
`idle-period > day-of-week`	Defines the day of the week on which the CPE allows file download from ACS.
`idle-period > end`	Defines the end time (in HH:MM format) of the idle period range during which the CPE allows file download from ACS.
`idle-period > start`	Defines the start time (in HH:MM format) of the idle range during which the CPE allows file download from ACS.
`ipv6`	Enables the use of an IPv6 or IPv4 address for the ACS. To allow only an IPv4 address: `no ipv6 enable` For a full description, refer to the User's Manual.
`period-inform-enable {off|on}`	Enables the device to send periodic inform messages to the ACS.
`network-source`	Defines the alias name representing a

Command	Description
	VRF or an IP address of the IPv4 source network interface that is used to bind to the TR-069.
`ntp-dependency {off|on}`	When the device is configured to connect securely to the TR-069 Auto Configuration Server (ACS) over TLS and to verify the certificate, you can enable this command to connect only when the device is synchronized with the NTP server.
`port`	Defines the local HTTP/S port used for TR-069. The default is 827547.
`port-restriction {off|on}`	Enables the device to restrict access to its embedded TR-069 server. When enabled, the device automatically configures the firewall with the ACS IP addresses (manually configured or DNS resolved if FQDN) to allow access to the TR-069 listening port (configured by [TR069HTTPPort]), blocking all other traffic to the port. **Note:** ■ The device can add up to six IP addresses o f the ACS to the firewall. ■ To view allowed IP addresses, use the command `display-allowed-acs-ips` (see above). ■ For this feature to be functional, you must also enable the firewall on the TR-069 interface. ■ This command is applicable only to MP-5xx, Mediant 500Li, and Mediant 800Ci.
`send-connection-request`	The device sends a connection request event toward the ACS.
`service {off|on}`	Enables <device> management through TR-069.

Command	Description
`socket-receive-timeout`	TR-069 socket receive timeout.
`source data {source-address|vrf}`	Defines the source interface through which the device connects (binds) to the TR-069 ACS. This can be the main VRF (default), a non-default VRF , or the Loopback interface: ■ Loopback interface: (cwmp-tr069)# source data source-address interface loopback <Index> ■ Main VRF: (cwmp-tr069)# source data ■ Non-default VRF: (cwmp-tr069)# source data vrf <VRF name> **Note:** ■ Configuring the source data doesn't require a device reset. ■ After you configure the source data, the device's TR-069 service disconnects from the ACS and closes all sockets (server and client). It then tries to connect to the ACS through the new source interface. ■ If you have configured a VRF or Loopback interface that doesn't exist, the 'ACS Connection Status' read-only field in the Web interface displays "Waiting for external IP address". ■ Connection URL and external IP address (with path) are changed according to source data.

Command	Description
`tcp-fragment {off|on}`	Enables the device to send outgoing TR-069 packets with the DF (Don't Fragment) flag in the IP header.
`tls-context <TLS Context ID>`	Assigns a TLS Context for TR-069 management.
`tr069-cwmp-wait-interval`	Defines the minimum interval (in seconds) that the <device> waits before attempting again to communicate with the ACS after the previous communication attempt failed.
`verify-certificate {off|on}`	Enables verification of the certificate during the TR-069 connection.
`verify-common-name {off|on}`	Enables verification of the common name during the TR-069 connection.

Command Mode

Privileged User

Example

This example enables TR-069.

```
(config-system)# cwmp
(cwmp-tr069)# service on
```

14 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
"r6wmr5to25smaB12d21aiSl94yMCf3lsfjBjagcch1kq9AZ9MJqqCOw44ywFcMIIbi
BaeNcsjh878ld1f2wKbY3lXJj1SOlcbiBfc6FBj1fROlJ9XvAw8k1lXdoFcOpeQJp2e
0sti1s0blNecypomhgU5yTlPREPQtl2e1wpiNgx7lRfeyXV?2s9@coFcOhdayWjWh
QuJeIgb5VbfyENc2w46O6OG3lf7NJnbkF5mxkka5xccyoVedYq1gMc"
```

15 floating-license

This command enables the Floating License 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.
`floating-license {off|on}`	Enables the Floating License 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-transcoding-sessions`	Defines a transcoding session limit for the customized Allocation Profile.

Command Mode

Privileged User

Example

This example enables the Floating License 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
```

16 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-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 configured in the HTTP Remote Hosts table for the specific remote Web service.

Command	Description
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 {disable|enable}	Enables the verification of the TLS certificate subject name (Common Name / CN or Subject Alternative Name / SAN) when connection with the host is based on HTTPSthat is

Command	Description
	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 <0-9>`	Defines the priority level of the host within the assigned group.
`rest-address`	Defines the IP address or FQDN of the remote HTTP host.

Command	Description
`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
```

16 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). **Note:** The command is applicable only to Mediant 800.
`usb-power {off|on}`	Shuts down (`off`) the USB port, by disconnecting power to the port.

Command Mode

Privileged User

Example

This example enables sending an alarm if a Power Supply module is removed or fails.

```
(config-system)# hw
(hw)# dual-powersupply-supported yes
```

17 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
```

18 ldap

This command configures LDAP and includes the following subcommands:

Syntax

```
(config-system)# ldap
```

Command	Description
`ldap-configuration`	See ldap ldap-configuration below
`ldap-server-groups`	See ldap ldap-server-groups on page 270
`settings`	See ldap settings on page 271

Command Mode

Privileged User

ldap ldap-configuration

This command configures the LDAP Servers table, which lets you define LDAP servers.

Syntax

```
(config-system)# ldap 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 269.

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 {no|yes}	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 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 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 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 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 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-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
```

19 mgmt-access-list

This command configures the Access List table, which lets you restrict access to the device's management interfaces (Web and CLI) by specifying IP addresses of management clients that are permitted to access the device.

Syntax

```
(config-system)# mgmt-access-list <Index>
(mgmt-access-list <Index>)# ip-address <IP address>
```

Command Mode

Privileged User

Example

This example allows the host at IP address 10.11.12.120 to connect to the management interface:

```
(config-system)# mgmt-access-list 0
(mgmt-access-list 0)# ip-address 10.11.12.120
```

20 mgmt-auth

This command configures various management settings.

Syntax

```
(config-system)# mgmt-auth
(mgmt-auth)#
```

Command	Description
`default-access-level`	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`.
`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|when-no-auth-server}`	Configures 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
```

21 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.
`ntp-as-oam {off|on}`	Defines the location of the Network Time Protocol (NTP).
`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).

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)# primary-server 10.15.7.8
(ntp)# update-interval 3600
```

21 provision

This command configures automatic provisioning of the device by a remote HTTP/S provisioning server (Remote Web Service).

Syntax

```
(config-system)# provision
```

Command	Description
`enable {off|on}`	Enables this automatic provisioning feature.
`max-retries`	Defines the maximum number of attempts to send the request before provisioning is considered a failure.
`retry-interval`	Defines the time (in seconds) between each sent HTTP request that failed.
`server-password`	Defines the password for authentication with the server.
`server-url`	Defines the provisioning server's URL path where the requests must be sent.
`server-username`	Defines the username for authentication with the server.

Command Mode

Privileged User

22 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
```

23 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-source`	Defines the alias name representing a VRF or an IP address of the IPv4 source network interface that is used to bind to the RADIUS application client.
`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.
`source data {interface|source-address} <Interface> <slot/port>.<VLAN ID>`	Defines the source interface for RADIUS.
`timeout-behavior`	Configures device behavior when RADIUS times out.
`vsa-access-level`	Defines the 'Security Access Level'

Command	Description
	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
```

24 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 reset 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
```

25 snmp

This command configures Simple Network Management Protocol (SNMP).

Syntax

```
(config-system)# snmp
```

Command	Description
alarm-customization	See snmp alarm-customization below
settings	See snmp settings on the next page
trap	See snmp trap on page 287
trap-destination	See snmp trap-destination on page 288
v3-users	See snmp v3-users on page 289

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.
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 settings

This command configures various SNMP settings.

Syntax

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

Command	Description
activate-keep-alive-trap [interval]	Enables a keep-alive trap for the agent behind NAT.
delete-ro-community-string	Deletes the read-only community string.
delete-rw-community-string	Deletes the read-write community string.
disable {no|yes}	Enables SNMP.
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
snmp-server-interface > ipv4-snmp-network-source	Defines the alias name that represents the VRF table or IP address of the IPv4 network interface that is used to bind to the SNMP application.
snmp-server-interface-ipv6 > ipv6-snmp-network-source	Defines the alias name that represents the VRF table or IP address of the IPv6 network interface that is used to bind to the SNMP application.
port	Defines the port number for SNMP requests and responses.
ro-community-string	Configures a read-only community string.
rw-community-string	Configures a read-write community string.
snmp-acl {community string}	Sets the configuration.
snmp-transport-type {IPv4|IPv6}	Defines the IP address version of the SNMP trap destinations.
sys-contact	Defines the contact person for this managed node (string) .
sys-location	Defines the physical location of the node (string).

Command	Description
`sys-name`	Defines the sysName as descibed in MIB-2 (string).
`sys-oid`	Defines the base product system OID - SNMP SysOid (string).
`trusted-managers {0-4} <IP Address>`	Defines the IP address of Trusted SNMP Managers.

Command Mode

Privileged User

Example

This example configures the SysOID:

```
(config-system)# snmp settings
(snmp)# sys-oid 1.3.6.1.4.1.5003.10.10.2.21.1.3
```

snmp trap

This command configures SNMP traps.

Syntax

```
(config-system)# snmp trap
(snmp-trap)#
```

Command	Description
`auto-send-keep-alive {disable|enable}`	Invokes a keep-alive trap and sends it every 9/10 of the time configured by the parameter NatBindingDefaultTimeout.
`community-string`	Defines the community string used in traps.
`manager-host-name`	Defines the FQDN of the remote host that is used as an SNMP Trap Manager.
`reset-community-string`	Returns to the default trap community string.

Command Mode

Privileged User

Example

This example configures the FQDN of the remote host used as the SNMP Trap Manager:

```
(config-system)# snmp trap
(snmp-trap)# manager-host-name John
```

snmp trap-destination

This command configures the SNMP Trap Destinations table, which configures SNMP trap destinations (Managers).

Syntax

```
(config-system)# snmp trap-destination <Index>
(trap-destination-<Index>)#
```

Command	Description
Index	Defines the table row index.
`ip-address`	Defines the SNMP manager's IP address.
`port`	Defines the SNMP manager's port.
`reset-trap-user`	Returns to the default trap user.
`send-trap {disable|enable}`	Enables the sending of traps to the SNMP manager.
`trap-user`	SNMPv3 USM user or SNMPv2 user to associate with this trap destination.

Command Mode

Privileged User

Example

This example demonstrates configuring a trap destination:

```
(config-system)# snmp trap-destination 0
(trap-destination 0)# ip-address 10.13.4.145
(trap-destination 0)# send-trap
```

snmp v3-users

This command configures the SNMPv3 Users table, which configures SNMPv3 users.

Syntax

```
(config-system)# 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|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 v3-users 0
(v3-users-0)# username JaneD
```

26 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`
	`db6bce85685c6634f6115456a083ea753f6d1`
	`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|master|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.

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!
```

26 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
```

27 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.
`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.
`enforce-password-complexity {0|1}`	Enforces definition of a complex login password.
`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.
`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]

Command	Description
	parameter).
`req-client-cert {off|on}`	Enables requirement of client certificates for HTTPS Web interface connections.
`secured-connection {http-and-https|https-only}`	Defines the protocol (HTTP or HTTPS) for accessing the Web interface.
`wan-http-allow {off|on}`	Enables WAN access to the management interface through HTTP.
`wan-https-allow {off|on}`	Enables WAN access to the management interface through HTTPS.
`web-hostname`	Defines a hostname (FQDN) for accessing the device's Web interface.

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
```

27 web-data

This command enables the Web interface to display pages for configuring some of the device's data-router functionality.

Syntax

```
(config-system)# web-data
(web-data)#
```

Command	Description
`web-data-config {off|on}`	Enables the Web interface to display additional pages for configuring certain data-router functionality. This is typically enabled when the device is also used as an analog telephone adapter (ATA).
`web-data-lan-if`	Defines the LAN interface (VLAN) of the device's data-router that is displayed on the Web interface's LAN Interface page.
`web-data-wan-if`	Defines the WAN interface of the device's data-router that is displayed on the Web interface's WAN Interface page. The default is "gigabitethernet 0/0".

Command Mode

Privileged User

Note

This functionality is applicable only to Mediant 500Li and Mediant 800Ci.

Example

This example enables display of data-router configuration pages in the Web interface:

```
(config-system)# web-data
(web-data)# web-data-config on
```

27 web-if

This command configures the Web Interfaces table, which lets you define additional Web interfaces (Web and REST), which binds the web interface to a selected Virtual Route Forward (VRF) / IP address, and with additional configuration (e.g., TLS certificate).

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 Web interface access.
`https-port`	Defines the device's LAN HTTPS port for Web interface access.
`network-source`	Defines the alias name that represents the IP address or VRF of the source network interface that is used to bind to the Web interface.
`require-client-certificate {no|yes}`	Enables requirement of client certificates for HTTPS Web 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)# network-source ITSP
(web-if-0)# tls-context-name ITSP
(web-if-0)# https-only-val https-only
(web-if-0)# activate
```

28 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>
```

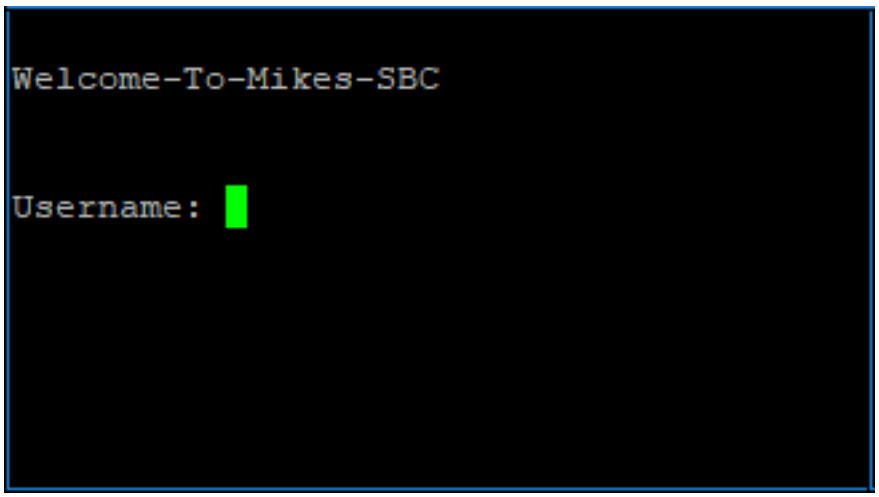
Command	Description
Index	Defines the table row index.
`text <Message>`	Defines the message (string) for the row.
`display`	Displays the banner message.

Command Mode

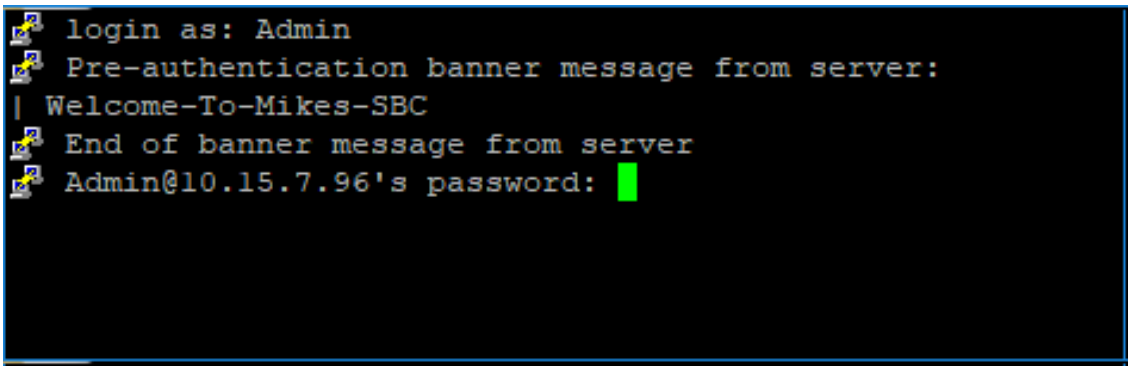
Privileged User

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:



- **SSH CLI:** The message is displayed after you enter your login username (before the login password prompt), as shown in the following example:



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

29 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 305
activity-trap	See activity-trap on page 307
cdr	See cdr on page 308
cdr-server	See cdr-server on page 316
pstn-debug	See pstn-debug on page 318
fax-debug	See fax-debug on page 319
logging	See logging on page 320
max-startup-fail-attempts	See max-startup-fail-attempts on page 323
pstn-debug	See pstn-debug on page 324
startup-n-recovery	See startup-n-recovery on page 325
syslog	See syslog on page 326
test-call	See test-call on page 330

Command Mode

Privileged User

30 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 CLI commands.
`config-changes {on|off}`	Enables logging notifications on parameters-value-change events.
`device-reset {on|off}`	Enables logging notifications on device-reset 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.
`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

Example

This example enables reporting of login and logout attempts:

```
(config-troubleshoot)# activity-log
(activity-log)# login-and-logout on
```

31 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
```

32 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 311).
`cdr-history-privacy [disable|hide-caller-and-callee]`	Enables the device to hide (by displaying an asterisk) the values of the Caller and Callee fields in CDRs that are displayed by the device: SBC CDR History table (Web), Gateway CDR History table (Web), `show voip calls history` (CLI), and `show voip calls active` (CLI).
`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.

Command	Description
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 {gzip|none|zip}	Defines the file compression type for 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-	Configures at what stage of the call

Command	Description
`call|connect-and-end-call|start-and-end-call}`	RADIUS accounting messages are sent to the RADIUS accounting server.
`rest-cdr-http-server`	Defines the REST server (by name) to where the device sends CDRs through REST API.
`rest-cdr-report-level {connect-and-end-call|connect-only|end-call|none|start-and-end-and-connect-call|start-and-end-call}`	Enables signaling-related CDRs to be sent to a REST server and defines the call stage 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 sb-cdr-format on page 313

Command	Value
show-title	See show-title on page 314

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 {local-storage-gw|radius-gw|syslog-gw}	Defines the type of CDRs that you want customized.
col-type	Defines the CDR field (column) that you want to customize.
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
```

sb-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.
`col-type`	Defines the CDR field (column) that you want to customize.
`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.
`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|SigSourcePort|SigDestPort|MediaType |AMD| % |SIPTrmReason|SIPTermDesc |PstnTermReason|LatchedRtpIp |LatchedRtpPort |LatchedT38Ip |LatchedT38Port |CoderTranscoding

32 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.
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

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)# name CDR-Server
(cdr-server-0)# activate
```

32 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
```

33 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
```

34 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>)#
```

Command	Description
Index	Defines the table row index.
`filter-type {any|classification|fxs-fxo|ip-group| ip-to-ip-routing|ip-to-tel|ip-trace|sip-interface|srd|tel-to-ip|trunk-bch|trunk-group-id|trunk-id|user}`	Type of logging filter.
`log-dest {debug-rec|local-storage|syslog}`	Log destination.
`log-type {cdr-only|none|pstn-trace|signaling|signaling-media|signaling-media-pcm}`	Log type.
`mode {disable|enable}`	Enables or disables the log rule.
`value`	Value of log filter (string).

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.

Syntax

```
(config-troubleshoot)# logging settings
(logging-settings)#
```

Command	Description
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-status {start|stop}	Starts and stops debug recording.
dbg-recint-name	Defines the local interface name.

Command	Description
`network-source`	Defines the alias name representing a VRF or an IP address of the source network interface that is used to bind to the Debug Recording application (the interface that the listening socket opens).

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
(logging-settings)# network-source debug1
```

35 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
```

36 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
```

37 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
```

38 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.
`ipv6-enable {on|off}`	Enables DNS-resolution into IPv6 addresses.
`log-level {alert| critical| debug-notrecommended | error| fatal| info-notrecommended | notice| warning}`	Defines the minimum severity level of messages included in the Syslog message that is generated by the device
`network-source`	Defines the alias name representing a VRF or an IP address of the source network interface that is used to bind to the Syslog client.
`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-ip`	Defines the syslog server's IP address or FQDN.
`syslog-optimization {disable|enable}`	Enables or disables bundling

Command	Description
	debug syslog messages for performance.
`system-persistent-log-size`	Defines the maximum size (in KB) of each 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-tlscontext`	Assigns a TLS Context when the TLS transport protocol is used for communication with the Syslog server.
`syslog-servers`	Defines multiple secondary syslog servers. For more information, see syslog-servers on the next page.
`system-log-size`	Defines the maximum size (in KB) of the local system log file.

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 can 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}`	Defines the type of information (only CDRs, only SDRs, or all) to send in the syslog.
`ip-address`	Defines the syslog server's IP address (IPv4 or IPv6) or FQDN.
`mode {off|on}`	Activates or deactivates the syslog server.
`port`	Defines the syslog server's port number.
`protocol {udp|tcp|tls}`	Defines the transport protocol for communicating with the Syslog server.
`severity-level {Alert|Critical| Debug|Emergency|Error|Informational|`	Defines the minimum severity

Command	Description
Notice|Warning}	level of messages included in the Syslog message.

Command Mode

Privileged User

Niotes

- To configure the primary syslog server, see syslog on page 326.
- 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 reset.

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 on
(syslog-servers-0)# severity-level Alert
```

39 test-call

This command configures test calls.

Syntax

```
(config-troubleshoot)# test-call
```

Command	Value
settings	See settings below
test-call-table	See test-call-table on the next page

Command Mode

Privileged User

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
```

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.

Command	Description
call-duration	Call duration in seconds (-1 for auto, 0 for 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.

Command	Description
play {disable|dtmf|prt}	Playback mode.
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

40 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 337
bind vrf	See bind vrf on page 339
dns	See dns on page 341
interface	See interface on page 346
nat-translation	See nat-translation on page 347
network-settings	See network-settings on page 349
nqm	See nqm on page 351
physical-port	See physical-port
poe-table	See poe-table on page 358
qos	See qos on page 359
sctp	See sctp on page 361
security-settings	See security-settings on page 363
tftp-server	See tftp-server on page 365
tls	See tls on page 366

Command Mode

Privileged User

41 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 a brief description for the rule.
`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.
`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)# network-interface-name ITSP
(access-list-0)# allow-type allow
(access-list-0)# packet-size 1500
```

41 bind vrf

This command provides support for binding the management servers (Web HTTP and HTTPS, Telnet, SSH, and SNMP) to a network source which can be a defined VRF, source address, or network interface.

Syntax

```
bind vrf <VRF Name> management-servers [Server Name]
bind vrf all-vrfs management-servers [Server Name]
bind source-address interface <Interface ID> management-servers [Server Name]
bind interface <Interface ID> management-servers [Server Name]
```

Arguments	Description
VRF Name	Defines the VRF name.
Interface ID	Defines the interface ID.
Server name	Management server that binds to network source. Available servers to bind are: ■ http ■ https ■ snmp ■ ssh ■ telnet If no server is specified, all management servers will be bind.

Default

Main VRF (default routing table)

Command Modes

Enable

Example

■ To bind all management servers to all VRFs:

```
(config-network)# bind vrf all-vrfs management-servers
```

- To bind the SNMP management server to the source address of VLAN 1 interface:

```
(config-network)# bind source-address interface vlan 1 management-servers snmp
```

- To remove an existing bind (return to default bind), use the no command:

```
(config-network)# no bind source-address interface vlan 1 management-servers snmp
```

42 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 343)
- srv2ip (see dns srv2ip on page 344)

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> data interface <ID>
```

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 DNS server.
`dns-default-secondary-server-ip`	Defines the IP address of the default secondary DNS server.

Command Mode

Privileged User

Example

This example configures the IP address of the default primary 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
```

43 interface

This command configures network interfaces and includes the following sub-commands:

- osn (see interface osn below)

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 of the OSN network interface:

```
(config-network)# interface osn
(conf-net-if-OSN)# native-vlan 1
```

44 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.
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.
network-source	Defines the alias name representing a VRF or an IP address of the source network interface that is used to bind to the SIP application.
src-start-port	Defines the optional starting port range (0-65535) of the IP interface, used as matching criteria for the NAT rule.
target-end-port	Defines the optional ending port range (0-65535) of the global address.
target-ip-address	Defines the global (public) IP address.
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
```

45 network-settings

This command configures the network settings.

Syntax

```
(config-network)# network-settings
(network-settings)#
```

Command	Description
`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.
`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 the SBA Management Interface.
`wan-copper-fiber-mode {single-copper|single-fiber|use-all}`	Enables 802.1Q-in-802.1Q (QinQ), as defined by IEEE 802.1ad, for a specific WAN interface -- copper (`single-copper`) or WAN fiber (`single-fiber`). QinQ expands VLAN space, by adding an additional 802.1Q tag to 802.1Q-tagged packets. **Note:** ■ The command is applicable only to Mediant 500Li and Mediant 800Ci. ■ This feature is supported only on the WAN interface (not LAN). ■ To disable QinQ, set the command to `use-all`. ■ For the parameter to take effect, a device reset is required.

Command Mode

Privileged User

Example

This example sending and receiving of ICMP Redirect messages:

```
(config-network)# network-settings
(network-settings)# icmp-disable-redirect 1
```

46 nqm

This command configures the device to monitor the quality of the network path (network quality monitoring - NQM) between it and other AudioCodes devices. The path monitoring is done by sending packets from a "sender" device to a "responder" device and then calculating the round-trip time (RTT), packet loss (PL), and jitter.

The command includes the following subcommands:

- probing-table (see nqm probing-table below)
- responder-table (see nqm responder-table on the next page)
- sender-table (see nqm sender-table on page 353)

NQM is applicable only to Mediant 800 MSBR.

nqm probing-table

This command configures the polling attributes (duration and frequency).

Syntax

```
(config-network)# nqm probing-table < Index >
(probing-table-<Index>)# < Command>
```

Command	Description
`duration`	Configures the duration of the probing session (in seconds).
`frequency`	Configures the time interval between the start of two consecutive probing sessions (in seconds).
`history-entries`	Configures the number of probing result entries to keep in the history file.
`life-span`	Configures the life span of this probe (in seconds).
`probe-name`	Configures a descriptive name for this probe.
`start-time`	Configures the start time of this probe.

Command Mode

Privileged User

Example

This example configures a row in the Probing table:

```
(config-network)# nqm probing-table 0
(probing-table-0)# probe-name voip_probe_1
(probing-table-0)# start-time now
```

nqm responder-table

This command adds a responder (IP address and port).

Syntax

```
(config-network)# nqm responder-table < Index >
(responder-table-<Index>)# < Command>
```

Command	Description
`active {0|1}`	Enables the Responder.
`local-port {3900|3910|3920|3930|3940|3950|3960|3970|3980|3990}`	Configures the local transport layer port number.
`responder-name`	Configures a descriptive name for the Responder.
`source-interface-name`	Configures a name for the source interface to listen on for incoming NQM packets.
`network-source`	Defines an alias name representing a

Command	Description
	VRF or an IP address of the source network interface that is used to bind to the NQM application (the source interface to listen for incoming NQM packets).

Command Mode

Privileged User

Example

This example configures a row in the Responder table:

```
(config-network)# nqm responder-table 0
(responder-table-0)# responder-name vmain_office_voip_responder_1
(responder-table-0)# local-port 3900;
(responder-table-0)# exit
```

nqm sender-table

This subcommand adds a sender (including RTT, PL, and jitter thresholds; associates probing definition; responder address; local interface).

Syntax

```
(config-network)# nqm sender-table < Index >
(sender-table-<Index>)# < Command>
```

Command	Description
`active {0|1}`	Enables the Sender.

Command	Description
cq-mos-threshold	Configures the minimum allowable Conversation Quality MOS.
jitter-threshold	Configures the maximum allowable Jitter (msec).
lq-mos-threshold	Configures the minimum allowable Listener Quality MOS.
packet-interval	Configures the interval between each packet transmitting (msec).
packet-timeout	Configures the receive timeout on expected packets.
packet-tos	Configures the TOS value in the IP header.
payload-size	Configures the size of the IP payload (bytes).
pl-threshold	Configures the maximum allowable Packet Loss.
probe-name	Configures the name of the corresponding probe in the Probing table.
rtt-threshold	Configures the maximum allowable Round Trip Time (msec).
sender-name	Configures a descriptive name for the Sender.
source-interface-name	Configures a name for the source interface.
network-source	Defines the alias name representing a VRF or an IP address of the source

Command	Description
	network interface that is used to bind to the NQM application (the source interface to listen for incoming NQM packets).
`target-ip-address`	Configures the target IP address.
`target-port {3900|3910|3920|3930| 3940|3950|3960|3970|3980|3990}`	Configures the target transport layer port number.

Command Mode

Privileged User

Example

This example configures a row in the Sender table to define a sender termination:

```
(config-network)# nqm sender-table 0
(sender-table-0)# sender-name main_office_voip_checker_1
(sender-table-0)# set target-ip 10.4.3.98
(sender-table-0)# set target-port 3900
```

A responder termination defined by the pair <target IP address, target port> can be defined only once for a single sender line; multipile senders can’t be defined to send packets to the same responder termination.

```
(sender-table-0)# probe-name voip_probe_1
```

A single row in the Probing table may be shared by several senders, thereby sharing and simplifying common attributes.

46 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. **Note:** The parameter is applicable only to Mediant 500Li.
`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
```

47 poe-table

This command configures the Power Over Ethernet Settings table, which lets you enable power on the Ethernet lines (PoE).

Syntax

```
(config-network)# poe-table < Index >
(poe-table-<Index>)# < Command >
```

Command	Description
`port-at-enable {disable|enable}`	Enables PoE according to IEEE 802.3at.
`port-enable {disable|enable}`	Enables PoE port.
`port-max-power`	Configures the PoE port's maximum power.

Command Mode

Privileged User

Note

This command is applicable only to Mediant 800 MSBR.

Example

This example enables PoE on port 0:

```
(config-network)# poe-table 0
(poe-table-0)# port-enable enable
(poe-table-0)# port-max-power 4000
```

48 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
```

48 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
```

49 security-settings

This command configures various TLS certificate security settings.

Syntax

```
(config-network)# security-settings
(network-security)#
```

Command	Description
`PEERHOSTNAMEVERIFICATIONMODE {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.
`SIPSREQUIRECLIENTCERTIFICATE {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.

Command	Description
	Note: For the parameter to take effect, a device reset is required.
`fips140mode {off|on}`	Enables FIPS 140-2 conformance mode for TLS. **Note:** Applicable only to specific products.
`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
```

50 tftp-server

This command configures the device's TFTP server.

Syntax

```
(config-network)# tftp-server
```

Command	Description
`enable`	Enables the TFTP server.
`files`	Manages TFTP files.

Command Mode

Privileged User

Example

This example enables the TFTP server:

```
(config-network)# tftp-server enable
```

51 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 369.
`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 {1024|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}`	Determines whether the device allows or rejects peer certificates if it cannot connect to the OCSP server.
`ocsp-port`	Defines the OCSP server's TCP port number.
`ocsp-server {disable|enable}`	Enables or disables

Command	Description
	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 371.
`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 are rejected.
`trusted-root {clear-and-import|delete|detail|export|import|summary}`	Trusted root certificate actions -

Command	Description
	see trusted-root on page 372.

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 TLS certificates.

Syntax

```
(tls-<Index>)# certificate
```

Command	Description
Index	Defines the table row index.
`alternative-name-add {dns|email|ip-addr|uri}`	Defines the Subject Alternative Name (SAN) fields, which can be a DNS, e-mail, IP address or URI.
`alternative-name-clear`	Deletes all the Subject Alternative Name (SAN) fields.
`create-self-signed`	Creates a self-signed certificate (by the device) with the current key.
`delete`	Deletes the certificate.
`detail`	Displays certificate information.

Command	Description
`export`	Displays the certificate in the console ("BEGIN CERTIFICATE" to "END CERTIFICATE").
`import`	Imports a certificate. Type the certificate after the command.
`signature-algorithm {sha-1|sha-256|sha-512}`	Defines the signature algorithm.
`signing-request`	Creates a certificate signing request to send to the CA.
`status`	Displays active status of certificate (e.g., expiration day).
`subject {clear|copy|display|field-set}`	Operations on the certification subject name.

Command Mode

Privileged User

Example

This example displays information on a TLS certificate:

```
(config-network)# tls 0
(tls-0)# certificate details
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 0 (0x0)
  Signature Algorithm: sha1WithRSAEncryption
    Issuer: CN=ACL_5967925
    Validity
      Not Before: Jan  5 07:26:31 2010 GMT
      Not After : Dec 31 07:26:31 2029 GMT
    Subject: CN=ACL_5967925
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (1024 bit)
        Modulus:
```

```
            00:aa:1f:fa:82:5b:2b:2f:26:08:64:96:cb:50:a9:
            c2:5b:ec:57:66:58:16:aa:17:79:0a:0f:77:5d:dd:
            15:88:3c:b1:f7:c4:c4:b9:e8:a9:af:88:0f:fa:5e:
            85:be:1c:34:c1:15:5d:b5:07:93:e2:0d:2f:5e:2f:
            7e:f3:5c:ee:bf:c5:ac:43:8a:7b:f2:3e:0d:1b:c4:
            84:2e:07:53:b4:52:af:c8:d0:23:0b:f9:a2:ac:72:
            2e:f1:65:59:f1:0b:7a:d2:77:cd:e8:c9:5e:81:93:
            0b:f5:f2:93:85:5e:06:c5:9a:b8:3d:81:d9:b7:e7:
            4b:44:fe:9e:fd:53:e6:7d:d1
        Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
        3e:f5:97:07:96:e4:36:27:19:8b:e7:7d:5d:04:8c:ba:46:d8:
        d7:31:6c:75:2b:3a:c8:4d:6b:cb:56:d0:29:21:d1:7b:8b:79:
        57:6e:35:71:8e:e6:eb:5d:17:77:ac:b6:ec:20:6d:6a:9b:17:
        9a:28:17:e1:a1:d5:11:7e:a4:95:04:df:15:cb:84:e0:3a:7d:
        bd:15:2c:62:2e:f2:40:2f:00:6d:ba:28:16:fe:bd:87:86:d0:
        4b:a0:c0:a6:06:b8:22:4d:67:ed:af:1d:83:83:ae:92:c4:06:
        f3:e2:e5:8c:17:66:3c:ed:80:f0:96:a3:e0:95:e3:88:9e:61:
        d7:b8
```

private-key

This subcommand lets you do various actions on private keys.

Syntax

```
(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} 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.
`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.
`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

52 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 376
coders-and-profiles	See coders-and-profiles on page 446
gateway	See gateway on page 377
ids	See ids on page 463
interface	See interface on page 468
ip-group	See ip-group on page 478
media	See media on page 484
message	See message on page 498
proxy-set	See proxy-set on page 506
qoe	See qoe on page 510
realm	See realm on page 518
sbc	See sbc on page 522
sip-definition	See sip-definition on page 554
sip-interface	See sip-interface on page 581
srd	See srd on page 584
trunk-to-ip channels	See trunk-to-ip channels on page 586

Command Mode

Privileged User

53 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
```

54 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 393)
- dtmf-supp-service (see dtmf-supp-service on page 405)
- manipulation (see manipulation on page 414)
- routing (see routing on page 431)
- trunk-group (see trunk-group on page 440)
- trunk-group-setting (see trunk-group-setting on page 441)
- voice-mail-setting (see voice-mail-setting on page 442)

advanced

This command configures advanced gateway parameters.

Syntax

```
(config-voip)# gateway advanced
(gw-settings)#
```

Command	Description
`attempted-call-count-on-start {off|on}`	Enables the device to count calls only at call start stage for SNMP performance monitoring MIBs that count attempted calls (IP-to-Tel and Tel-to-IP), for example, acPMSIPAttemptedCallsTable.
`enable-rai {off|on}`	Enables generation of an RAI (Resource Available Indication) alarm if the device's busy endpoints exceed a user-defined threshold.
`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

Command	Description
	started after the first SIP 2xx response has 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 381
call-waiting	See call-waiting on page 382
caller-display-info	See caller-display-info on page 383
enable-caller-id	See enable-caller-id on page 384
enable-did	See enable-did on page 385
fxo-setting	See fxo-setting on page 386
fxs-setting	See fxs-setting on page 388
keypad-features	See keypad-features on page 389
metering-tones	See metering-tones on page 391
reject-anonymous-calls	See reject-anonymous-calls on page 392
tone-index	See tone-index on page 392

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.
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.

Command	Description
dst-number	Defines the destination telephone number to automatically 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
```

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}`	Determines whether the device disconnects a call when a dial tone is detected from the PBX.
`fxo-autodial-play-bsytn {off|on}`	Determines whether 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

Command	Description
	TimeForReorderTone).
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.
time-wait-b4-dialing	Defines the delay before the device starts dialing on the FXO line.
waiting-4-dial-tone	Determines whether or not the device waits

Command	Description
{disable|enable}	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	Enables 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.
fxs-emg-call-for-unreg-port	Enables the device to allow FXS endpoints (ports) to make emergency calls (Tel-to-IP) even if registration of a specific port to the SIP proxy server has failed.
fxs-ntt-	Enables the device to comply with the NTT Japan standard for

Command	Description
`polarity-reversal {off|on}`	line polarity reversal for IP-to-Tel calls (FXS).
`fxs-ntt-noid-interworking-mode {none|ip2tel}`	Enables mapping of the no-id cause value, which is the reason of the anonymous call, from IP (SIP From header) to FXS, for IP-to-Tel calls.

Command Mode

Privileged User

Example

This example configures a maximum of 10 streaming sessions for MoH:

```
(config-voip)# gateway 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

Command	Description
	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 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

Command	Description
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.
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".

Command	Description
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.
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.
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

Command	Description
	exists.
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.

Command	Description
epn-as-cpn-ip2tel {off|on}	Use endpoint number as calling number for 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.
handle-isdn-facility-on-disconnect {off|on}	Enables the device to handle (interwork) "known" Facility information elements (IE) that are included in incoming ISDN Disconnect messages.
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

Command	Description
	(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 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.
`isdn-send-progress-on-183-without-sdp {off|on}`	Enables interworking incoming SIP 183 without SDP responses and outgoing ISDN Q.931 Progress/Alerting messages, for Tel-to-IP 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|`	Send TBCT/ECT/RLT request only when

Command	Description
connect}	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.
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.
media-ip-ver-pref {ipv4-only| ipv6-only| prefer-ipv4| prefer-ipv6}	Select the preference of Media IP version.
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].

Command	Description
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-id	IP Group ID 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'.
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.
prefix-to-ext-line	Prefix to dial for external line.
q850-reason-code-2play-user-tone	Q850 Reason Code which cause playing special PRT Tone.
qsig-path-replacement	0 - Enable IP to QSIG transfer,1 - Enable QSIG to IP Transfer
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.

Command	Description
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 whether to disconnect call while receiving ISDN PROGRESS with Cause 0 - never, 1- disconnect if not Early media,2 - always
rmv-calling-name	If set to 1 - Removes Calling Name from IP->TEL calls.
rmv-cli-when-restr	Removes CLI from IP->TEL calls if received CLI is restricted
rtcp-act-mode	RTCP activation policy.
rtp-only-mode	immediately. -1 - takes the RTPONLYMODE global value per gatewa0 - 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
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

Command	Description
	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
tel-to-ip-dflt-redir-rsn	Tel2IP Default Redirect Reason
third-party-transcoding	Enables Third Party Call Control Transcoding 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-	Trunk Restart Mode on Power Up.

Command	Description
channel|per-trunk}	
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
usr2usr-hdr-frmt	(0): X-UserToUser, (1): format: User-to-UserUser with protocol discriminator, (2): format: User-to-User with 'encoding=hex' at the end, (3): format: User-to-User with text presentation
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 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

Command	Description
	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 408
supp-service-settings	See supp-service-settings on page 410

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.

Command	Description
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.

Command	Description
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.
second-dtmf-option-type	Defines the second preferred transmit DTMF negotiation method.

Command	Description
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.
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.
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).

Command	Description
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-ipgroupid	IP Group ID 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.
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-	Supplementary Service code for deactivating Call Forward

Command	Description
code	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.
estb-conf-code	Control Key activation for 3-way conference.
flash-key-seq-style {flash-hook| sequence-1| sequence-2 | sequence-3}	Flash key sequence. **Note:** The parameter is applicable only to FXS interfaces.
flash-key-toggle-to-secondary	Defines the flash-hook key with digit sequence for toggling from the primary call to the secondary call. **Note:** The parameter is applicable only to FXS interfaces.

Command	Description
flash-key-toggle-to-primary	Defines the flash-hook key with digit sequence for toggling from the secondary call to the primary call. **Note:** The parameter is applicable only to FXS interfaces.
flash-key-call-transfer	Defines the flash-hook key with digit sequence for initiating a call transfer. **Note:** The parameter is applicable only to FXS interfaces.
flash-key-conference	Defines the flash-hook key with digit sequence for initiating a three-way conference call. **Note:** The parameter is applicable only to FXS interfaces.
flash-key-bye-and-toggle	Defines the flash-hook key with digit sequence for ending the active call (sends a SIP BYE message) when you have two calls and one is on-hold. When the sequence is pressed, the previously held call becomes the active call. **Note:** The parameter is applicable only to FXS interfaces.
flash-key-bye-2-secondary	Defines the flash-hook key with digit sequence for ending the call that is currently on hold (sends a SIP BYE message). **Note:** The parameter is applicable only to FXS interfaces.
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.

Command	Description
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.
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.

Command	Description
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).
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 below
calling-name-map-tel2ip	See calling-name-map-tel2ip on the next page
cause-map-isdn2isdn	See cause-map-isdn2isdn on page 418
cause-map-isdn2sip	See cause-map-isdn2sip on page 418
cause-map-sip2isdn	See cause-map-sip2isdn on page 419
dst-number-map-ip2tel	See dst-number-map-ip2tel on page 420
dst-number-map-tel2ip	See dst-number-map-tel2ip on page 421
phone-context-table	See phone-context-table on page 422
redirect-number-map-ip2tel	See redirect-number-map-ip2tel on page 423
redirect-number-map-tel2ip	See redirect-number-map-tel2ip on page 425
settings	See settings on page 426
src-number-map-ip2tel	See src-number-map-ip2tel on page 428
src-number-map-tel2ip	See src-number-map-tel2ip on page 430

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.
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

Command	Description
	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	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.

Command	Description
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-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.
`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.

Command	Description
dst-host-pattern	Defines the Request-URI host name prefix, which appears in the incoming SIP INVITE message.
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.
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.

Command	Description
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

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).

Command	Description
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-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-	Tel to IP Source Number Mapping Dial Plan Index.

Command	Description
nb-map-dial-index	
tel2ip-src-nb-map-dial-mode	Tel to IP Source Number Mapping Dial Plan 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

Command	Description
	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-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.

Command	Description
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 {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 433
gw-routing-policy	See gw-routing-policy on page 434
ip2tel-routing	See ip2tel-routing on page 435
settings	See settings on page 436
tel2ip-routing	See tel2ip-routing on page 438

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-method	Tel to IP Alternative Routing Connectivity Method.
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..

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
```

55 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 448
audio-coders-groups	See audio-coders-groups on page 449
ip-profile	See ip-profile on page 451
tel-profile	See tel-profile on page 459

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 Audio Coders Groups table, which lets you define Audio Coders Groups. The table is a "parent" of the Coder Groups 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 the Coder Groups table, which lets you define audio coders. For more information, see audio-coders on the next page.
`coders-group-name`	Defines a name for the Coders Group.

Command Mode

Privileged User

Example

This example configures the name "ITSP" for the Coders Group 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 Groups table, which lets you define audio coders. The table is a "child" of the Audio 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 Audio Coders table with G.711:

```
(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 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`	Configures AMD (Answering Machine Detector) mode.
`amd-sensitivity-level`	Determines the AMD level of detection sensitivity.

Command	Description
amd-sensitivity-parameter-suite	Determines the serial number of the AMD sensitivity suite.
call-limit	Defines the maximum number of concurrent calls per IP Profile.
cng-mode	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.
data-diffserv	Defines the DiffServ value of MSRP traffic in the IP header's DSCP field.
disconnect-on-broken-connection	Defines the behavior when receiving an RTP broken notification.
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	Enables Early Media.
echo-canceller	Enables echo cancellation (i.e., echo from voice calls is removed).
enable-early-183	Enables Early 183.
enable-hold	Enables Call Hold service.
enable-qsig-tunneling	Enables QSIG Tunneling over SIP.
enable-symmetric-mki	Enables 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.

Command	Description
generate-srtp-keys	Configures generating new SRTP keys on SRTP negotiation mode.
ice-mode	Configures ICE Mode.
input-gain	Defines the voice TDM Input Gain.
ip-preference	Configures Profile Preference - the priority of the IP Profile.
is-dtmf-used	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	Defines the preference of the Media IP version.
media-security-behaviour	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	Enables Cisco compatible fax and modem bypass mode.
play-held-tone	Defines the SBC Play Held Tone.
play-rbt-to-ip	Enables a ringback tone playing towards IP.
profile-name	Configures a Profile Name (string).

Command	Description
prog-ind-to-ip	Determines whether to send the Progress Indicator to IP.
reliable-heldtone-source	Defines the SBC Reliable Held Tone Source.
remote-hold-Format	Defines the SBC Remote Hold Format.
reset-srtp-upon-re-key	Resets SRTP State Upon Re-key.
rtp-ip-diffserv	Defines the RTP IP DiffServ.
rtp-redundancy-depth	Defines the RTP Redundancy Depth - enables the device to generate RFC 2198 redundant packets.
rx-dtmf-option	Defines the supported receive DTMF negotiation method.
sbc-2833dtmf-payload	Defines the SBC RFC2833 DTMF Payload Type Value.
sbc-adapt-rfc2833-bw-voice-bw	Adapts RFC 2833 BW to Voice coder BW.
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	Defines the SBC Allowed Coders Mode.
sbc-allowed-media-types	Defines the SBC allowed media types (comma separated string).
sbc-alternative-dtmf-method	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	Defines the device's privacy handling of the P-asserted-Identity header. This indicates how the outgoing SIP message asserts identity.
sbc-diversion-mode	Defines the device's handling of the Diversion header.

Command	Description
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	Defines the coders included in the outgoing SDP answer (sent to the calling fax).
sbc-fax-behavior	Defines the offer negotiation method.
sbc-fax-coders-group-name	Defines the supported fax coders.
sbc-fax-offer-mode	Defines if the fax coders sent in the outgoing SDP offer.
sbc-fax-rerouting-mode	Enables the re-routing of incoming SBC calls that are identified as fax calls.
sbc-generate-noop	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	Generates silence RTP packets.
sbc-handle-xdetect	Defines the support of X-Detect handling.
sbc-history-info-mode	Defines the device's handling of the History-Info header.
sbc-isup-body-handling	Defines the ISUP Body Handling.
sbc-isup-variant	Defines the ISUP Variant.
sbc-jitter-compensation	Defines the SBC Jitter Compensation.
sbc-keep-routing-headers	Keeps the Record-Route and in-dialog Route headers from incoming request in the outgoing request.
sbc-keep-user-agent	Keeps the User-Agent header from the incoming request in the outgoing request.

Command	Description
sbc-keep-via-headers	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	Defines the transcoding method between SRTP and RTP.
sbc-media-security-method	Defines the SRTP method SDES/DTLS.
sbc-msrp-empty-message-format	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	Defines the device's MSRP role in SDP offer-answer negotiations ('a=setup' line) for MSRP sessions.
sbc-msrp-re-invite-update-supp	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	Enables the SBC to respond with multiple answers within the same dialog (non-standard).
sbc-multi-early-diag	Enables the SBC to respond with multiple SIP dialogs (forking).
sbc-play-rbt-to-transferee	Plays Ring Back Tone to transferred side on call transfer.
sbc-prack-mode	Defines the LEG's related PRACK behavior.
sbc-preferred-ptime	Defines the SBC Preferred Ptime.
sbc-receive-multiple-dtmf-methods	Enables the device to receive DTMF digits out-of-band (not with audio stream) using both the SIP INFO and RFC 2833 methods.
sbc-renumber-mid	Enables the device to change the value of the 'a=mid:n' attribute (where *n* is a unique value) to 0 (or next consecutive number), if it is present in the outgoing SDP offer.

Command	Description
sbc-rfc2833-behavior	Affects the RFC 2833 SDP offer/answer negotiation.
sbc-rmt-3xx-behavior	Defines the SBC Remote 3xx Behavior.
sbc-rmt-can-play-ringback	Configures remote endpoint capability to play a local ringback tone.
sbc-rmt-delayed-offer	Configures SBC remote delayed offer support.
sbc-rmt-early-media-resp	Defines the SBC remote early media response type.
sbc-rmt-early-media-rtp	Defines the SBC remote early media RTP mode.
sbc-rmt-early-media-supp	Defines SBC remote early media support.
sbc-rmt-mltple-18x-supp	Defines SBC remote multiple 18x support.
sbc-msrp-re-invite-update-supp	Defines if the remote MSRP endpoint supports the receipt of re-INVITE and UPDATE SIP messages.
sbc-rmt-re-invite-supp	Defines SBC remote re-INVITE support.
sbc-rmt-refer-behavior	Defines SBC remote refer behavior.
sbc-rmt-renegotiate-on-fax-detect	Defines if remote renegotiate when fax is detected.
sbc-rmt-replaces-behavior	Defines how the SBC manages REFER/INVITE with Replaces.
sbc-rmt-rfc3960-supp	Defines the SBC remote RFC 3960 gateway model support.
sbc-rmt-rprsntation	Defines how to represent the SBC's contact information to the remote side.
sbc-rmt-update-supp	Defines SBC remote UPDATE support.
sbc-rtcp-feedback	Defines RTCP feedback support.
sbc-rtcp-mode	Defines the SBC RTCP mode.

Command	Description
sbc-rtcp-mux	Defines support of RTP-RTCP multiplexing.
sbc-rtp-red-behav	Defines SBC RTP redundancy behavior.
sbc-sdp-handle-rtcp	Defines SBC SDP Handle RTCP.
sbc-sdp-ptime-ans	Defines SBC SDP Ptime answer.
sbc-sdp-remove-crypto-lifetime	Defines SBC SDP Remove Crypto Lifetime.
sbc-send-multiple-dtmf-methods	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	Defines SBC behavior with 'Session-Expires' header.
sbc-use-silence-supp	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 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	Activates Voice Quality Enhancement.
second-tx-dtmf-option	Defines the second priority DTMF methods, offered during the SIP negotiation.
signaling-diffserv	Defines the SIP Signaling DiffServ.
transcoding-mode	Defines the voice transcoding mode between the two SBC legs for the SBC application.
voice-volume	Defines the voice TDM output gain.

Command	Description
vxx-transport-type	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'.
digitmapping	Defines which digit map set to use (Primary or

Command	Description
	Secondary) for Tel-to-IP calls.
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).
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-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-	Defines the maximum delay (in msec) for the

Command	Description
delay	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.
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
```

56 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 465

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
```

57 interface

This command configures the PSTN interfaces.

Syntax

```
(config-voip)# interface
```

Command	Description
bri	See bri below
e1-t1	See e1-t1 on page 471
fxs-fxo	See fxs-fxo on page 475

Command Mode

Privileged User

bri

This command configures BRI interfaces.

Syntax

```
(config-voip)# interface bri <Slot (Module)/Port>
(bri <Slot/Port>)#
```

Command	Description
b-ch-negotiation	ISDN B-Channel negotiation mode.
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
isdn-bits-cc-behavior	Sets the ISDN Call Control

Command	Description
	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, and PROCEEDING

Command	Description
	messages
play-rbt-to-trk	Enable ringback tone playing towards trunk side.
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. ■ To start a PSTN trace for all trunks that have been configured with the **trace-level** command option, use

Command	Description
	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 <Slot (Module)/Port>
(e1-t1 <Slot/Port>)#
```

Command	Description
`b-ch-negotiation`	ISDN B-Channel negotiation mode
`b-channel-nego-for-trunk`	ISDN B-Channel negotiation mode for trunk.

Command	Description
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.
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

Command	Description
	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-location-to-isdn {not-included|user|private-net-serving-local-user|public-net-serving-local-user|transit|public-net-serving-remote-user|private-net-serving-remote-user|international|bewond-interworking}`	Defines the Location value (overwrites original) in the Progress Indicator information element (IE) for Q.931 messages that the device sends to the Tel side.
`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
`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

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-	Determines whether to enable the analog DC remover in

Command	Description
remover	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.
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.

Command	Description
`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.
`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
```

58 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}`	Enables classification of incoming SIP dialogs (INVITEs) to Server-type IP Groups based on Proxy Set (assigned using the IPGroup_ProxySetName parameter).
`contact-user`	Defines the user part of the From, To,

Command	Description
	and Contact headers of SIP REGISTER messages, and the user part of the Contact header of INVITE messages received from this IP Group and forwarded by the device to another IP Group.
`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.
`max-num-of-reg-users`	Defines the maximum number of users in this IP Group that can register with the device.

Command	Description
media-realm-name	Assigns a Media Realm to the IP Group.
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	Defines the shared password for authenticating the IP Group, when the device acts as an Authentication server.
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-	Defines the routing mode after a call

Command	Description
configured|proxy|routing-table|standard}	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-stateful-proxy|microsoft-server|not-configured}	Defines the device's operational 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

Command	Description
	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`	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.
`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 Media Optimization.
`topology-location {down|up}`	Defines the display location of the IP Group in the Topology view of the Web interface.

Command	Description
`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.
`username`	Defines the shared username for authenticating the IP Group, when the device acts as an Authentication server.
`uui-format {disable|enable}`	Enables the generation of the Avaya UCID value, adding it to the outgoing INVITE sent to this 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
```

59 media

This command configures media.

Syntax

```
(config-voip)# media
```

Command	Description
fax-modem	See fax-modem below
ipmedia	See ipmedia on page 486
rtp-rtcp	See rtp-rtcp on page 488
security	See security on page 490
settings	See settings on page 492
tdm	See tdm on page 494
voice	See voice on page 495

Command Mode

Privileged User

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).

Command	Description
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	Determines the depth of redundancy for non-V.21 T.38 fax packets.
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.

Command	Description
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-sse-payload-type-rx	Defines the received V.1501.1 SSE RTP payload type.
v21-modem-transport-type	Sets 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]
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
```

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.
EnableStandardSIDPayloadType	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 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

Command	Description
	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.
multicast-rtp {disable|enable}	Enables Multicast RTP. For configuring Trunk-to-IP channels for multicasting, see trunk-to-ip channels on page 586.
publication-ip-group-id	Defines the IP Group to where the device sends RTCP XR reports.
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.

Command	Description
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-tx	Defines the Tx RFC 2833 DTMF relay dynamic payload type for outbound calls.
telephony-events-payload-type-rx	Defines the Rx RFC 2833 DTMF relay dynamic payload type for outbound calls.
udp-port-spacing {10|4|5}	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	Defines the device

Command	Description
{mandatory|preferable|preferable-single-media}	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.
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.
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

Command	Description
	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.
`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

Command	Description
	other party.
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 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	Enables COT (Continuity Tones) detection and generation.
disable-nat-traversal {0|1|2|3|4}	Defines the NAT mode.

Command	Description
inbound-media-latch-mode	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	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
TDMBusClockSource {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

Command	Description
	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)# TDMBusClockSource 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].
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.

Command	Description
`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
```

60 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 500
message-policy	See message-policy on page 501
pre-parsing-manip-sets	See pre-parsing-manip-sets on page 503
settings	See settings on page 504

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
```

61 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.
`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.
`is-proxy-hot-swap {disable|enable}`	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.

Command	Description
`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.
`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 the next page.
`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.
`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.

Command	Description
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.
`proxy-address`	Defines the address of the proxy.
`transport-type {not-configured|tcp|tls|udp}`	Defines the transport type for communicating with 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
```

62 qoe

This command configures Quality of Experience (QoE).

Syntax

```
(config-voip)# qoe
```

Command	Description
additional-parameters	See additional-parameters call-flow-report on page 512
bw-profile	See bw-profile below
qoe-profile	See qoe-profile on page 512
qoe-settings	See qoe-settings on page 516
quality-of-service-rules	See quality-of-service-rules on page 515

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).
egress-video-bandwidth	Defines the major (total) threshold for outgoing video traffic (in Kbps).

Command	Description
`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|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
`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.
`tls{off|on}`	Enables a TLS connection with the OVOC server.
`server-name`	Defines the IP address or FQDN (hostname) of the OVOC server to where the quality experience reports are sent.
`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
```

63 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 the next page.
`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 520.

Command	Description
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.
tcp-port-range-start	Defines the starting 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
```

64 sbc

This command configures SBC tables.

Syntax

```
(config-voip)# sbc
```

Command	Description
classification	See classification below
dial-plan	See dial-plan <Index> on page 525
external-media-source	See external-media-source on page 528
malicious-signature-database	See malicious-signature-database on page 529
manipulation	See manipulation on page 530
routing	See routing on page 535
cac-profile	See cac-profile on page 545
settings	See settings on page 547

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	Defines the source transport type as a matching

Command	Description
{any|tcp|tls|udp}	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.
srd-name	Assigns an SRD to the rule 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 526.
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.

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.

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>	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	Description
<URL>	

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 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 532

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.
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	Determines whether additional

Command	Description
{disable|enable}	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 name - full name (usually in the From header).
src-ip-group-name	Defines the IP Group from where the incoming INVITE is received.

Command	Description
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

Command	Description
	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.
privacy-restriction-mode {dont-change-privacy|remove-restriction|restrict|transparent}	Defines user privacy handling (i.e., restricting source user identity in outgoing SIP dialogs).

Command	Description
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 538
sbc-alt-routing-reasons	See alt-routing-reasons on page 541
sbc-routing-policy	See sbc-routing-policy on page 544

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 the IP Group Set table. For more information, see ip-group-set-member on the next page.
name	Defines a descriptive name, which is used when associating the

Command	Description
	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.
`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 routing rule.
`cost-group`	Assigns a Cost Group to the routing rule for determining 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

Command	Description
	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.
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-

Command	Description
	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.
`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.
`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

Command	Description
	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.
`ldap-srv-group-name`	Assigns an LDAP Server Group to the Routing Policy.
`name`	Defines a

Command	Description
	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.
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.
`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`	Defines the call direction of the SIP request

Command	Description
{both|inbound|outbound}	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-error	When using UDP as the transport protocol, the retries failed transmissions to a proxy server according to the [ProxySet_FailureDetectionRetransmissions] parameter. However, when the failed attempt receives an ICMP error (which indicates Host Unreachable or Network Unreachable) as opposed to a timeout, it may be desirable to abandon additional retries in favor of

Command	Description
	trying the next IP address (proxy server) in the Proxy Set.
auth-chlng-mthd	Set to 0 to use a www-authenticate header or 1 to send a proxy-authenticate header in the message
auth-qop	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.
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-gruu	Obtain and use GRUU (Global Routable UserAgentURIs).
end-point-call-priority	Defines the ports call priority.
enforce-media-order	Arrange media lines according to the previous offer-answer (required by RFC 3264).
enforce-media-order	Enforces media order according to RFC 3264.
gw-direct-route-prefix	Defines the prefix for call redirection from SBC to Gateway.
keep-contact-user-in-reg	Keeps original Contact User in REGISTER requests.
lifetime-of-nonce	Defines the lifetime of the nonce in seconds.
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.
no-rtp-detection-timeout	Defines the timeout for RTP detection after call connect (msec).

Command	Description
num-of-subscribes	Defines the active SUBSCRIBE sessions limit.
p-assert-id	0 - As Is,1- Add P-Asserted-Identity Header, 2 - Remove P-Asserted-Identity Header
play-tone-on-connect-failure-behavior	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 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.
reserve-dsp-on-sdp-offer {off|on}	Enables the device to reserve (guarantee) DSP resources for a call on the SDP Offer.
sas-notice	If enabled - when SBC needs to terminates a REGISTER request, it adds a body (survivability notice) to the 200OK response.
sbc-100trying-upon-reinvite	Defines if the device sends a SIP 100 Trying response upon receipt of a re-INVITE request.
sbc-3xx-bhvt	Defines how the device passes Contact in 3xx responses.
sbc-broadworks-survivability	Indicates how the registration database is provisioned.
sbc-bye-auth	Allows the media to remain active upon receipt of a 401/407 response by sending a releaseNackEvent, rather than releaseEvent.
sbc-db-route-mode	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.

Command	Description
sbc-dialog-subsc-route-mode	Determines where in-dialog refresh subscribes are sent.
sbc-direct-media {off|on}	Enables direct media.
sbc-diversion-uri-type	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	Defines the handling method for 18X response to forking.
sbc-gruu-mode	Defines the GRUU behavior.
sbc-keep-call-id	Keeps original call Id for outgoing messages.
sbc-max-fwd-limit	Defines the limit of the Max-Forwards header.
sbc-media-sync	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	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 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

Command	Description
	Subscribe responses.
sbc-refer-bhvr	Defines handling of Refer-To in REFER requests.
sbc-remove-sips-non-sec-transp	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	Defines the RTCP mode.
sbc-server-auth-mode	Defines the authentication mode.
sbc-sess-exp-time	Defines the session refresh timer for requests in a dialog.
sbc-session-refresh-policy	Defines whether Remote or SBC should be refresher when SBC terminates the Session Expire refreshing.
sbc-shareline-reg-mode	Defines the registration handling mode in case of shared line manipulation.
sbc-subs-try	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	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

Command	Description
	URL database is used.
send-invite-to-all	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.
short-call-seconds	Defines the duration (in seconds) of an SBC call for it to be considered a short call and thus, included in the count of the performance monitoring SNMP MIBs for short calls.
sip-topology-hiding-mode	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 configured.
transcoding-m500l	Enables transcoding on Mediant 500L MSBR.
transcoding-mode	Defines the transcoding mode.
unclassified-calls	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
```

65 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 556
proxy-and-registration	See proxy-and-registration on page 558
settings	See settings on page 564
sip-recording	See sip-recording on page 577

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.
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.
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.
ignore-auth-stale	Enables the device to retry registering even if the last SIP 401\407 response included "stale=false".
ip-addrr-rgstrr	Defines the SIP Registrar IP address.
max-gen-reg-rate	Defines the max. generated Register requests per interval.
max-registration-backoff-time	Defines the Backoff mechanism that is applied between failed registration attempts initiated by the device.

Command	Description
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.
auth-password	Defines the password for authentication.
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.
redundant-routing-m	Defines the mode of redundant routing.
reg-on-conn-failure	Enables re-registration on TCP/TLS connection failure.
reg-on-invite-fail	Enable re-register upon INVITE transaction failure.
registrar-name	Defines the SIP Registrar name.

Command	Description
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 {not-use|for-account|for-every-register}	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-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	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	Enables use of Alternative Route Reasons Table for 3xx.
FarEndDisconnectSilenceMethod	Defines the far disconnect silence detection method.
FarEndDisconnectSilencePeriod	Defines the silence period detection time.
aaa-indications	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	Enables empty Authorization header to be added to Register request.

Command	Description
amd-beep-detection	Defines the AMD beep detection mode.
amd-mode	Defines the AMD mode.
anonymous-mode	Defines the "anonymous" mode.
app-sip-transport-type	Defines the SIP transport type.
application-profile	Defines the Application Profile.
authenticated-message-handling {no-changes-permitted| register-changes-permitted}	Defines if a Message Manipulation Set is run again on incoming authenticated SIP messages received after the device sends a SIP 401 response for challenging initial incoming SIP REGISTER requests.
broken-connection-event-timeout	Defines the duration the RTP connection should be broken before the Broken Connection event is issued [100ms].
busy-out	Enables trunks to be taken out of service in case of LAN down.
call-num-plybck-id	Defines the Calling Number Play Back ID.
call-pickup-key	Defines the key sequence for call pickup.
call-transfer-using-reinvites	Enables Call Transfer using re-INVITEs.
calls-cut-through	Enables call connection without on-hook/off-hook process 'Cut-Through'.
cdr-report-level	Defines the CDR report timing.
cdr-srvr-ip-adrr	Defines the Syslog server IP address for sending CDRs.
coder-priority-nego	Defines the coder priority in SDP negotiation.
crypto-life-time-in-sdp	Disables Crypto life time in SDP.
current-disc	Enables disconnect call upon detection of current disconnect signal.
default-record-uri	Defines the default record location URI

Command	Description
	used by Media Ctrl.
delay-after-reset	Defines the Gateway delay time after reset (seconds).
delay-b4-did-wink	Defines the delay between off-hook detection and Wink generation (FXS).
delayed-offer	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	Enables use of different RTP port after hold.
did-wink-enbl	Enables DID lines using Wink.
digit-delivery-2ip	Enables automatic digit delivery to IP after call is connected.
digit-delivery-2tel	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 broken notification.
disc-on-silence-det	Enables disconnect calls on a configured silence timeout.
disp-name-as-src-nb	Enables display name to be used as source number.
display-default-sip-port	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.

Command	Description
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 calls).
emerg-calls-regrt-t-out	Defines the regret time for Emergency calls.
emerg-nbs	Defines emergency numbers (Tel-to-IP calls).
emrg-spcl-rel-cse	set configuration
enable	Enables RADIUS.
enable-did	Enables DID for all FXS ports (that are not specifically enabled - see enable-did on page 385).
enable-ptime	Enables requirement of ptime parameter in SDP.
enable-sips	Enables SIP secured URI usage.
enbl-non-inv-408	Enables sending 408 responses for non-INVITE transactions.
enum-service-domain	Defines the ENUM domain for ENUM resolution.
fake-tcp-alias	Enables enforcement reuse of TCP/TLS connection.
fake-retry-after	Defines if the device, upon receipt of 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.
fax-re-routing	Enables rerouting of fax calls to fax destination.
fax-sig-method {no-fax|t.38-relay|g.711-transport| fax-	Defines fax signaling method.

Command	Description
fallback|g.711-reject-t.38}	
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-ignore-multiple-answers	Enables the device to use only the first SDP answer in the SIP dialog process and ignore any subsequent SDP answers that it may receive (e.g., SIP 183 with SDP and then a 200 OK with SDP, or two 183's with SDP). Therefore, even if a different SDP answer is received, the voice channel doesn't change.
gw-mx-call-duration	Limits the device call time duration (minutes).
handle-reason-header	
hist-info-hdr	Enables History-Info header support.
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

Command	Description
	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 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.

Command	Description
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 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.

Command	Description
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.
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.
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.

Command	Description
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.
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 resets 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.

Command	Description
replace-nb-sign-w-esc	Replaces the number sign (#) with the escape character %23 in outgoing SIP messages.
reset-srtp-upon-re-key	Resets SRTP State Upon Re-key.
resource-prio-req	Indicates whether or not Require header is able to contain the resource-priority tag.
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.

Command	Description
sdp-session-owner	Defines the SDP owner string.
sdp-ver-nego	Handle SDP offer/answer if SDP version was increased, otherwise takes SDP 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.
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|acc-remote-allow}	Defines 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.
sip-nat-detect	If not set, the incoming request will be

Command	Description
	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).
sync-ims-accounts	Enables synchronization of multiple Accounts per the IMS specification.
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

Command	Description
	port.
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).
uri-for-assert-id	Enables use of Tel uri or Sip uri for P-Asserted or P-Preferred headers.
use-aor-in-refer-to-header	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	Enables use of destination as connected number.
use-dtg	Enables use of DTG parameter.

Command	Description
use-tgrp-inf	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	Enables User-Information usage.
user-phone-in-from	Adds 'User=Phone' to From header.
user-phone-in-url	Adds User=Phone parameter to SIP URL.
usr-def-subject	Defines the SIP subject.
verify-rcvd-requri	Defines whether to verify Request URI Header in requests.
verify-rcvd-via	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	Enables X-Channel header.
zero-sdp-behavior	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
siprec-metadata-format {legacy|rfc7865}	Defines the format of the recording metadata that is included in SIP messages sent to the SRS.
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.
`condition-name`	Assigns a Message Condition rule to the SIP Recording rule.
`peer-ip-group-name`	Defines 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`	Defines the IP Group 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`	Defines the IP Group of the recording server (SRS).
`srs-red-ip-group-name`	Defines the IP Group of the redundant SRS in the active-standby pair for SRS redundancy.

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
```

66 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.
`enable-un-auth-registrs {disable|enable|not-`	Enables the device to accept REGISTER requests and register them in its registration database from

Command	Description
conf}	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.
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.
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.

Command	Description
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
```

67 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
```

67 trunk-to-ip channels

This command configures the Trunk-to-IP Channels table, which lets you route multicast voice traffic over T1/E1 (i.e., mapping between T1/E1 channel and multicast group). The source and destination of the traffic are multicast groups.

Syntax

```
(config-voip)# trunk-to-ip channels <Index>
(channels-<Index>)#
```

Command	Description
Index	Defines the table row index.
b-channel	Defines the B-channel.
coder {G711Alaw|G711Mulaw}	Defines the voice coder.
interface	Defines the local interface.
local-ip-address	Defines the local IP address(relevant only for RTPRxOnly).
local-udp-port	Defines the local UDP port (relevant only for RTPRxOnly).
remote-ip-address	Defines the remote IP address (relevant only for RTPTxOnly).
remote-udp-port	Defines the remote UDP port (relevant only for RTPTxOnly).
rtp-direction {RTPTxOnly|RTPRxOnly)	Defines the RTP direction: ■ RTPTxOnly: Trunk > RTP ■ RTPRxOnly: RTP > Trunk
trunk-id	Defines the trunk ID.

Command Mode

Privileged User

Related Commands

`multicast-rtp` - enables the Multicast media feature

Notes

For more information on configuring multicasting, refer to the documenting *Multicasting Traffic with E1-T1 Configuration Note*.

Example

This example configures multicasting:

- For the receiving MSBR (traffic from multicast group is forwarded to channel of the E1):

```
(config-voip)# trunk-to-ip channels 0
(channels-0)# trunk-id 4
(channels-0)# b-channel 1
(channels-0)# local-ip-address 239.5.1.2
(channels-0)# local-udp-port 10000
(channels-0)# rtp-direction RTPRxOnly
(channels-0)# activate
```

- For the sending MSBR (traffic from channel of the E1 is forwarded to multicast group):

```
(config-voip)# trunk-to-ip channels 0
(channels-0)# trunk-id 4
(channels-0)# b-channel 1
(channels-0)# remote-ip-address 239.0.1.2
(channels-0)# remote-udp-port 20000
(channels-0)# rtp-direction RTPTxOnly
(channels-0)# activate
```

Part VII

Data-Router Level Commands

68 Introduction

This part describes the commands located on the Data configuration level, which configures the data-router functionality. The commands of this level are accessed by entering the following command at the root prompt:

Syntax

```
# configure data
(config-data)#
```

Command Mode

Privileged User

69 WAN Access Commands

General WAN Commands

interface

This command enters a specific interface configuration. Use the `no` form of this command to delete a specific interface.

Syntax

```
interface atm <group/subinterface[.vlanID[.vlanID]]>
interface bvi <bridge interface>
interface cellular <slot/port>
interface dot1radio <wifi interface>
interface dsl <slot/port>
interface e1 <slot/port>
interface efm [<slot/port>.vlanID}
interface fastEthernet <slot/port>
interface fiber <slot/port> [.vlanID][.vlanID]>
interface gigabitEthernet <slot/port[.vlanID]>
interface gigabitEthernet <slot/port>
interface gre  <Tunnel GRE ID>
interface ipip <Tunnel IPIP ID>
interface l2tp <L2TP ID>
interface loopback <Loopback interface ID>
interface multilink <Multilink interface ID>
interface serial <slot/port>
interface shdsl <slot/port>
interface pppoe <PPPoE interface ID>
interface pptp <PPTP ID>
interface t1 <slot/port>
interface vlan <vlanID>
interface vti <VTI interface ID>
```

Command	Description
Slot	Defines the module slot index as shown on the front panel.
Port	Defines the port index within the selected module.
`atm`	Defines the DSL group and subinterface number, separated by a slash (e.g., 0/0), (Vlan ID and second

Command	Description	
	vlanID are optional).	
`bridge interface`	Defines the Bridge Virtual Interface for Layer 3.	
`bvi`	Defines the BVI bridge interface (1-255).	
`cellular`	Defines the cellular 3G/4G interface.	
`dot1radio`	Defines the Wi-Fi interface (1-4).	
`dsl`	Defines the ADSL/VDSL interface and slot/port.	
`e1`	Defines the E1 slot and port.	
`efm`	Defines the EFM interface slot and port (Vlan ID is optional).	
`fastEthernet`	Defines the FastEthernet interface slot and port.	
`fiber interface`	Defines the fibre interface (Vlan ID and second vlanID are optional). `l2tp id`	Defines the L2TP ID (0 - 99).
`loopback interface id`	Defines the Loopback interface ID (1 - 20).	
`multilink interface id`	Defines the Multilink interface ID (0 - 255).	
`pppoe`	Defines the PPPoE interface ID (0 - 7).	
`pptp`	Defines the PPTP ID (0 - 99).	
`serial <slot/port>`	Defines the serial interface slot/port.	
`shdsl`	Defines the SHDSL interface slot/port.	
`t1`	Defines the T1 slot and port.	
`tunnel gre id`	Defines the Tunnel GRE ID (1 - 255).	
`vlanID (VLAN interface)`	Defines the VLAN ID for Layer 3 interfaces available via the LAN switch.	
`vlan <ID>`	Defines the VLAN ID for a Layer 3 sub interface.	

Default

NA

Command Mode

Privileged User

Example

This example enters a specific interface configuration for the VLAN 6 menu.

```
(config-data)#interface vlan 6
```

This example configures a bridge interface.

```
(config-data)#interface bvi 10
```

interface vlan

This command defines the VLAN ID.

Syntax

```
interface vlan <vlan id>
```

Command	Description
`vlan id`	Defines the VLAN ID {1-3999[.vlanID}.

Default

NA

Command Mode

Privileged User

Example

This example defines the VLAN ID.

```
(config-data)#interface vlan 200.100
```

interface t1

This command defines the T1 interface slot and port.

Syntax

```
interface t1 [slot/port]
```

Command	Description
t1	Defines the T1 interface slot and port.

Default

NA

Command Mode

Privileged User

Example

This example defines the T1 slot and port.

```
(config-data)#interface t1 2/2
```

interface serial

This command defines the serial interface slot and port.

Syntax

```
interface serial [slot/port]
```

Command	Description
[slot/port]	Defines the serial interface slot and port.

Default

NA

Command Mode

Privileged User

Example

This example defines the serial slot and port.

```
(config-data)#interface serial 2/2
```

interface loopback

This command defines the loopback interface identifier.

Syntax

```
interface loopback <loopback interface id>
```

Command	Description
`loopback interface id`	Defines the loopback interface identifier (1-20).

Default

NA

Command Mode

Privileged User

Example

This example defines the loopback interface identifier.

```
(config-data)#interface loopback 10
```

interface multilink

This command defines the multilink interface identifier.

Syntax

```
interface multilink <multilink interface id>
```

Command	Description
multilink interface id	Defines the multilink interface identifier (0-255).

Default

NA

Command Mode

Privileged User

Example

This example defines the multilink interface identifier.

```
(config-data)#interface multilink 100
```

interface gigabitethernet

This command defines the GigabitEthernet interface slot and port.

Syntax

```
interface gigabitEthernet [slot/port.vlanID]
```

Command	Description
slot/port[.vlanID [.vlanID]]	Defines the GigabitEthernet interface slot and port (Vlan ID and second vlanID are optional).

Default

NA

Command Mode

Privileged User

Example

- This example enters a specific interface configuration for the WAN Interface menu.

```
(config-data)#interface gigabitEthernet 0/0
```

- This example enters a specific interface configuration for the sub-Interface 3 menu.

```
(config-data)#interface gigabitEthernet 0/0.3
```

- This example enters a specific interface configuration for the GigabitEthernet Physical Port 3 menu.

```
(config-data)#interface gigabitEthernet 4/3
```

interface fastethernet

This command defines the FastEthernet interface slot and port.

Syntax

```
interface fastethernet [slot/port]
```

Command	Description
`slot/port[.vlanID[.vlanID]]`	Defines the FastEthernet interface slot and port.

Default

NA

Command Mode

Privileged User

Example

This example enters a specific interface configuration for the FastEthernet Physical Port 3 menu.

```
(config-data)#interface fastEthernet 5/3
```

interface efm

This command defines the EFM interface slot and port.

Syntax

```
interface efm [slot/port.vlanID]
```

Command	Description
slot/port.vlanID	Defines the EFM interface slot and port.

Default

NA

Command Mode

Privileged User

Example

This example defines the EFM interface slot and port.

```
(config-data)#interface efm 5/3.1
```

interface e1

This command defines the E1 interface slot and port.

Syntax

```
interface E1 [slot/port]
```

Command	Description
slot/port.vlanID	Defines the E1 interface slot and port.

Default

NA

Command Mode

Privileged User

Example

This example defines the E1 interface slot and port.

```
(config-data)#interface e1 5/3
```

interface bvi

This command defines the BVI bridge interface.

Syntax

```
interface bvi [bridge interface id]
```

Command	Description
`bridge interface ID`	Defines the BVI bridge interface.

Default

NA

Command Mode

Privileged User

Example

This example configures a bridge interface.

```
(config-data)#interface bvi 10
```

interface pppoe

This command creates a PPP-over-Ethernet (RFC 2516) interface.

Syntax

```
interface pppoe <PPPoE Interface ID>
```

Command	Description
`PPPoE Interface ID`	Defines the PPPoE Interface ID in the range of 0-7.

Default

NA

Command Mode

Privileged User

Example

This example creates a PPP-over-Ethernet interface.

```
(config-data)# interface pppoe 2
```

alias

This command configures alias names for the device's Virtual Routing and Forwarding (VRF) and IP address interfaces. The alias is used to bind a specific management application (i.e. RADIUS, LDAP, SSH, SNMP, Telnet, Web Interfaces, and Syslog) to a source network interface. If the network interface name is not defined for one of these management interfaces, the default VRF named "main-vrf" (IPv4 or IPv6) is used by default. However, for the voice interface, SIP Interfaces and Media Realms must be assigned a network interface (i.e., alias name of VRF or IP address).

The alias configuration is optional and must be done if the VRF or IP address is used by one of the above-mentioned management applications. If the interface is used for other purposes, such as data routing, the alias of the interface does not need to be configured.

Syntax

```
alias <IP Address Alias Name>
```

```
ipv4-alias|ipv6-alias <VRF Alias Name)
```

Command Mode

Privileged User

Related Commands

All VRFs and IP addresses that are configured with alias names can be displayed using the command, `show network available-app-interface` (see show network available-app-interfaces on page 137).

Example

- Defines an IPv4 address with alias on interface VLAN 1:

```
(config-data)# interface vlan 1
(conf-if-VLAN 1)# ip address 10.4.4.61 255.255.0.0 alias ip_vlan1
```

- Defines an IPv6 address with alias on interface VLAN 1:

```
(config-data)# interface vlan 1
(conf-if-VLAN 1)# ip address 2000:3000::10/64 alias ipv6_vlan1
```

- Defines a VRF with an IPv4 alias:

```
(config-data)# ip vrf voip ipv4-alias voip_v4
```

- Defines a VRF with an IPv6 alias:

```
(config-data)# ip vrf voip ipv6-alias voip_v6
```

desc

This command sets the description of the specified interface. This descriptive name can be used to associate the interface with other commands.

Syntax

```
desc <string>
```

Command	Description
`string`	Specifies the interface description using an alphanumerical string (up to 255 characters).

Default

NA

Note

- Use inverted commas when using the space character as part of the description.
- The string is limited to 255 characters.

Command Mode

Privileged User

Example

- This example sets the description on the Gigabit Ethernet interface to "MyGbE":

```
#configure data
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# desc MyGbE
```

- This example references the Gigabit Ethernet interface using its descriptive name "MyGbE":

```
# show data interfaces desc MyGbE
```

or

```
(config-data)# interface desc MyGbE
(conf-if-GE 0/0)#
```

ip address

This command defines the primary IP address on the specified Layer 3 interface. Use the no form of this command to remove a configured IP address.

Syntax

```
ip address <ip address> <subnet mask> {alias} <alias name>
```

Command	Description
`<ip address>`	Defines a valid IPv4 address. IP addresses must be expressed in dotted-decimal notation (for example, 10.1.2.3).
`<subnet mask>`	Defines the subnet mask that corresponds to a range of IP addresses. Subnet masks must be expressed in dotted-decimal notation (e.g., 255.255.255.0).
`alias`	Defines an alias name for the IP address.

Default

NA

Command Mode

Privileged User

Note

For more information on alias names, see alias on page 599.

Example

- Configures IP address 10.4.2.3/255.255.0.0 on VLAN 6.

```
(config-data)# interface vlan 6
(conf-if-VLAN 6)# ip address 10.4.2.3  255.255.0.0
```

- Configures IPv4 address 10.4.4.61/255.255.0.0 with alias on interface VLAN 1:

```
(config-data)# interface vlan 1
(conf-if-VLAN 1)# ip address 10.4.4.61 255.255.0.0 alias ip_vlan1
```

duplex

This command configures the duplex mode on the specified Layer 2 interface.

Syntax

```
duplex half|full|auto
```

Command	Description
`half`	Forces half duplex operation.
`full`	Forces full duplex operation.
`auto`	Enables AUTO duplex configuration.

Default

Duplex is set to auto.

Command Mode

Privileged User

Example

This example forces full duplex operation on GigabitEthernet 4/2 interface.

```
(conf-if-GE 4/2)# duplex full
```

vrrp

This command provides for automatic assignment of available routers to participating hosts. This increases the availability and reliability of routing paths through automatic default gateway selections on a LAN.

The protocol achieves this by creating virtual routers, comprised of master and backup routers. VRRP routers use multicast to notify its presence in the LAN (never forwarding outside of the LAN).

VRRP is based on RFC 2338, 3768.

Syntax

IPv4:

```
vrrp <VRID> ip <ip address>
vrrp <VRID> ip <ip address> secondary
vrrp <VRID> priority <priority>
vrrp <VRID> preempt
vrrp <VRID> timers advertise <time in seconds>
```

IPv6:

```
vrrp <VRID> ipv6 ip <ip address>
vrrp <VRID> ipv6 ip <ip address> secondary
vrrp <VRID> ipv6 priority <priority>
vrrp <VRID> ipv6 preempt
vrrp <VRID> ipv6 timers advertise <time in seconds>
```

Command	Description
ip	Sets the primary IP address for the VRID.
secondary	Sets secondary IP address for the VRID.
priority	Sets the priority for VRID. The range is 1-254.

Command	Description
`preempt`	Sets preemption for lower priority Master.
`timers advertise`	Sets interval timer for advertising the Master VRID

Default

NA

Command Mode

Privileged User

Note

- To delete an IPv6 VRRP: `no vrrp <VRID> ipv6`
- The device uses VRRPv2 for IPv4, and VRRPv3 for IPv6.

Example

The following is an example of how this command can be used.

```
# configure data
(config-data)# interface VLAN 1
(conf-if-VLAN 1)# vrrp 1 ip 10.100.1
(conf-if-VLAN 1)#  vrrp 1 prioity 200
```

Cellular Modem Configuration Commands

This section defines cellular modem configuration.

interface cellular 0/0

On Mediant 800 MSBR devices with the appropriate hardware revision, this command allows defining an Internet connection via a cellular 3G modem connected to the USB port.

The command creates the cellular interface and enters the “conf-cellular” CLI context, where additional settings are available.

Syntax

```
interface cellular 0/0
```

Default

By default, the cellular interface is not configured.

Note

The shutdown, route default, napt, ppp user, ppp authentication commands are applicable in the “conf-cellular” CLI context.

Command Mode

Privileged User

Example

This example defines a cellular interface:

```
(config-data)# interface cellular 0/0
(conf-cellular)#
```

adv

This command enables advanced configurations.

Syntax

```
adv
```

Command Mode

Privileged User

Example

This example sets the device to advanced configuration:

```
(config-data)# interface cellular 0/0
(conf-cellular)# adv
(adv-cell-config)#
```

hdlc

This command sets the HDLC framing link type for PPP mode.

Syntax

```
hdlc asynchronous | synchronous
```

Command	Description
asynchronous	Sets the HDLC asynchronous framing.
synchronous	Set HDLC synchronous framing (default)

Default

The default setting is "synchronous".

Command Mode

Privileged User

Example

This example sets the HDLC asynchronous framing:

```
(config-data)# interface cellular 0/0
(conf-cellular)# adv
(adv-cell-config)# hdlc asynchronous
```

modem-details

This command sets the modem Vendor ID number and Product ID number configuration, according to the connected USB device. It can be used with "option" driver update and/or, "USB modeswitch" commands.

Syntax

```
modem-details default-product-id [default product id - HEX]
modem-details modem-product-id [modem product id - HEX]
modem-details vendor-id [product id - HEX]
```

Command	Description
default-product-id - HEX	Sets the default Product-ID (as 4 HEX digits) when the dongle is plugged in.

Command	Description
`modem-product id - HEX`	Sets the modem Product-ID (as 4 HEX digits) when the dongle is plugged in.
`vendor-id - HEX`	Sets the supported Vendor ID (as 4 HEX digits) when the dongle is plugged in.

Command Mode

Privileged User

Example

This example sets the supported Vendor ID:

```
(config-data)# interface cellular 0/0
(conf-cellular)# adv
(adv-cell-config)# modem-details vendor-id AAFF
```

option

This command sets the "option" serial driver support using the parameters set in the modem-details sub-menu (Vendor-id/Modem product-id).

The USB device manufacturer should advise that it is able to work with the "option" driver.

Syntax

```
option enable
```

Command Mode

Privileged User

Example

This example enables serial driver support:

```
(config-data)# interface cellular 0/0
(conf-cellular)# adv
(adv-cell-config)# modem-details vendor-id AAFF
(adv-cell-config)# modem-details product-id 12AB
(adv-cell-config)# modem-details default-product-id 34BC
```

```
(adv-cell-config)# option enable

Setting modem details is mandatory before running the command "option enable":

(adv-cell-config)# option enable
Please set all modem details to enable option driver support
```

usb-modeswitch

This command sets the USB modeswitch settings. When a USB device is plugged in for the first time, it might perform like a flash storage. The MSBR should make the storage device disappear and changes it to a communications device to work with it under the Cellular interface.

The usb_modeswitch command can send a provided message to the device, to initiate the mode switching. Using the parameters in the “modem- details” command, and the usb-modeswitch sub-menu, it changes the device "default-product-id" to the "modem-product-id" and the “default-vendor id” to “vendor-id”.

Syntax

```
usb-modeswitch configuration-id [index]
usb-modeswitch enable
usb-modeswitch message [message text}
```

Command	Description
`configuration-id`	Defines an optional configuration-id to the modeswitch parameters
`configuration-id index`	Defines the Configuration index.
`enable`	Enables the USB modeswitch.
`message`	Defines an optional USB modeswitch message.
`message text`	Defines the actual USB modeswitch message text.

Command Mode

Privileged User

Example

This example enables the USB modeswitch on the following modem-details:

```
(config-data)# interface cellular 0/0
(conf-cellular)# adv
(adv-cell-config)# modem-details vendor-id AAFF
(adv-cell-config)# modem-details product-id 12AB
(adv-cell-config)# modem-details default-product-id 34BC
(adv-cell-config)# usb-modeswitch enable
Setting modem details is mandatory before running the command "usb-
modeswitch enable":
(adv-cell-config)# usb-modeswitch enable
Please set all modem details to enable USB modeswitch operation
```

sim

This command defines the PIN code for the SIM card and unlocks the SIM card, for cellular interfaces.

Syntax

```
(config-data) # interface cellular 0/0
(conf-cellular-0/0)# adv
(adv-cell-config)#
```

Command	Description
`sim-lock-status`	Displays the SIM card lock status.
`sim-pin-code-change`	Defines a new PIN code for the SIM card when the current PIN code is known.
`sim-pin-code-unlock`	Unlocks a locked SIM card using the PIN code.
`sim-puk-code-unlock`	Unlocks a locked SIM card when the PIN code is unknown, using the Personal Unlocking Key (PUK) code and then defines a new PIN code. After three wrong attempts for the pin code, the SIM card locks. The only way to unlock it is by using the PUK code, which appears on the printed label on the card.

Note

This command is applicable only to Mediant 500Li and Mediant 800Ci.

Command Mode

Privileged User

Example

- This example changes the PIN code of the SIM card from 2222 to 1111:

```
(config-data) # interface cellular 0/0
(conf-cellular-0/0)# adv
(adv-cell-config)# sim-pin-code-change 2222 1111
```

- This example changes the PIN code of the SIM card to 1111 when the current PIN code is unkown and the card has been locked by the PUK code (51174269):

```
(config-data) # interface cellular 0/0
(conf-cellular-0/0)# adv
(adv-cell-config)# sim-puk-code-unlock  51174269 1111
```

apn

This command sets the Access Point Name (APN) used by the cellular interface.

Syntax

```
apn <apn-string>
```

Default

The default APN is “uinternet”.

Command Mode

Privileged User

Note

The command is applicable only to PPP-based cellular modems.

Example

This example sets the APN:

```
(config-data)# interface cellular 0/0
(conf-cellular)# apn internetg
```

backup monitoring

This command selects which of the device's other interfaces, needs to be monitored.

This command configures the cellular 3G connection in “backup” mode, where the connection is initiated only if another interface goes down.

To return to “primary” mode – where the cellular 3G connection is always up – use the “no” form of this command.

This command is available in the “conf-cellular” configuration context.

Syntax

```
backup monitoring <if-type> <if-index>
```

Command	Description
`if-type`	Defines the Interface Type, e.g. GigabitEthernet or ATM
`if-index`	Defines the Interface Index, e.g. 0/0

Default

The default operation mode is primary WAN, i.e. “no backup monitoring”.

Command Mode

Privileged User

Example

This example sets cellular backup mode:

```
(config-data)# interface cellular 0/0
(conf-cellular)# backup monitoring GigabitEthernet 0/0
```

conditional-apn

This command defines the variable APN by operator name.

Syntax

```
conditional-apn operator <Name> apn <APN for specified Operator>
```

Command Mode

Privileged User

Note

The command is applicable only to PPP-based cellular modems.

Example

This example configures a conditional APN.

```
(config-data)# interface cellular 0/0
(conf-cellular)# conditional-apn operator ITSP-1 apn ORANGE
```

crypto

This command defines encryption and decryption of the cellular interface.

Syntax

```
crypto
```

Command	Description
`map <tag>`	Assigns a Crypto Map. .
`vpn-client <IP Address>`	Connects to a VPN server.
`vpn-server map`	Creates a VPN server.

Command Mode

Privileged User

Example

This example connects the cellular interface to VPN server 100.1.3.4:

```
(config-data)# interface cellular 0/0
(conf-cellular)# crypto vpn-client 100.1.3.4
```

firewall

This command enables a firewall on the cellular interface.

Syntax

```
firewall enable
```

Command Mode

Privileged User

Example

This example enables the firewall on the cellular interface:

```
(config-data)# interface cellular 0/0
(conf-cellular)# firewall enable
```

initstr

This command sets the initialization string for the cellular modem.

Syntax

```
initstr <init-string>
```

Default

The default initialization string is “AT&F”.

Command Mode

Privileged User

Note

The command is applicable only to PPP-based cellular modems.

Example

This example sets the initialization string:

```
(config-data)# interface cellular 0/0
(conf-cellular)# initstr ATC0D0
```

ipv6

This command sets the cellular interface for IPv6.

Syntax

```
ipv6 {address|dhcp-client|enable|nd}
```

Command	Description
`address`	Defines an IPv6 address. You can use the following optional commands: ■ `ipv6 address autoconfig`: The device automatically acquires an IPv6 address using stateless auto-configuration on the cellular interface. This is instead of using a DHCPv6 server. ■ `ipv6 address autoconfig extnd-prfx-lan`: The device (per RFC 7278) takes the prefix received in an ICMPv6 Router Advertisement message received on the WAN side and uses it for SLAAC on the LAN side (as if it were a prefix for Prefix Delegation / PD). This means that the 64-bit prefix received on the WAN interface is used as-is for SLAAC on the LAN side. ■ `ipv6 address dhcp`: Obtains the IPv6 address from the DNS server that is associated with the cellular interface.
`dhcp-client pd`	The device as a DHCPv6 client receives a prefix (on its WAN interface) for delegation and uses it to perform SLAAC connectivity on its LAN side (sending prefix in ICMPv6 Router Advertisement message).
`enable`	Enables IPv6 on the cellular interface.

Command	Description
`nd autoconfig default-route`	

Command Mode

Privileged User

Note

- The command is applicable only to PPP-based cellular modems.
- To disable IPv6: `no ipv6 enable`

Example

This example enables RFC 7278 support where the device uses prefixes received in Router Advertisment ICMPv6 message, for SLAAC on its LAN side as-is:

```
(config-data)# interface cellular 0/0
(conf-cellular-0/0)# ipv6 enable
(conf-cellular-0/0)# ipv6 address autoconfig extnd-prfx-lan
(conf-cellular-0/0)# ipv6 nd autoconfig default-route
```

On any given LAN interface:

```
ipv6 enable
ipv6 nd ra interval 15 10
ipv6 nd pd Cellular 0/0/1 ::/64
no ipv6 nd ra suppress
```

Once configured, the device does the following:

- Generates an IPv6 address addr1 using EUI64 (and MAC address of the cellular interface) and installs <addr1>/128 on its cellular interface, which creates a native connected route on that subnet (128) is created.
- Generates an IPv6 adddress addr2 using EUI64 (and MAC address of LAN interface) and installs <add2>/64 on the LAN interface, which creates a native connected route on that subnet (64).
- Sets the default gateway to the source address of the original Router Advertisement ICMPv6 message on which the prefix was received on the WAN side (cellular network).
- Sends the RA on the LAN interface with the prefix received on the Router Adv. message received on the WAN side (cellular network). The prefix has both its flags of onlink and autoconf turned on ("1").

Any host connecting to the device on its LAN side can either set its IPv6 address as “automatic”, which uses the prefix along with EUI64 to generate a Global Unicast address for the host itself, or configure a static address based on the prefix that the RA includes.

mode dhcp

This command defines the mode of the cellular modem as DHCP.

Syntax

```
mode
```

Command	Description
dhcp	Defines the cellular interface as Ethernet using DHCP.

Command Mode

Privileged User

Example

This example defines the cellular interface as PPP:

```
(config-data)# interface cellular 0/0
(conf-cellular)# mode dhcp
```

mtu

This command defines the Maximum Transmission Unit (MTU) of the cellular interface. The value is usually negotiated automatically.

Syntax

```
mtu
```

Command	Description
<128 - 9999>	Defines MTU in bytes.
auto	MTU is defined automatically.

Default

auto.

Command Mode

Privileged User

Example

This example defines MTU automatically.

```
(config-data)# interface cellular 0/0
(conf-cellular)# mtu auto
```

napt

This command enables the NAPT mode. This setting is mandatory unless your service provider supports routable addresses for your LAN hosts.

Syntax

```
napt
```

Command Mode

Privileged User

Note

The command is applicable only to PPP-based cellular modems.

pcui

This command defines the PCUI port index for communication with the MSBR.

Syntax

```
pcui <port index>
pcui send <send text> expect <expect text> reboot
```

Command	Description
`port index`	Defines the TTY port index.
`send text`	Defines the AT command format.
`expect text`	Defines the expected string to match.
`reboot (optional)`	Reboot on match. (optional)

Command Mode

Privileged User

Note

The command is applicable only to PPP-based cellular modems.

Example

This example sets the PCUI port index for communication with the MSBR.

```
(config-data)# interface cellular 0/0
(conf-cellular)# pcui send AT+CSQ expect OK reboot
```

Use the "show data cellular pcui" command to see the output from the PCUI port.

pdn-policy

This command configures the priority for automatically connecting to a cellular network (instead of manually selecting the provider).

Syntax

```
(conf-cellular-0/0)# pdn-policy
(cell-pdn-policy)#
```

Command	Description
`evaluation-time`	Defines the duration (in seconds) that a carrier's (profile's) signal strength is below the defined threshold (see `rule reception`), for triggering the

Command	Description
	device to disconnect from the cellular provider and connect to the provider with the next highest priority.
`mode priority`	Enables the policy prioritization mode (by default, enabled).
`mode scan-priority`	Enables the device to choose a cellular network (profile) based on strongest signal strength (RSRP level). The device does this upon startup. Once a cellular network is chosen, the device doesn't change the cellular network (even if another network later has a stronger signal strength). **Note:** ■ The device may take up to two minutes to scan the different cellular networks to identify which has the highest RSRP level. ■ For this feature, the device only checks profiles that are configured with `mcc` and `mnc` values. ■ If connectivity is lost with the chosen profile (or registration fails), the device falls back to the default profile. ■ When enabled, all the other commands described in this table are not relevant.
`priority <1-16> <Profile Name>`	Defines the priority of the profile (cellular provider), where 1 is the highest and 16 the lowest. The device always tries to connect to the profile with the highest priority.

Command	Description
`rule reception {gsm rssi|lte rsrp}`	Defines the GSM or LTE signal strength (reception) threshold (in dBm). If the signal strength of the cellular provider is less than this threshold for a duration defined by `evaluation-time`, the device disconnects from the provider and connects to the provider with the next highest priority profile (see `priority`). ■ GSM: `rule reception gsm rssi <RSSI in -dBm>` ■ LTE: `rule reception lte rsrp <RSRP in -dBm>`

Related Commands

- `pdn-policy`
- `profile`

Note

- This command is applicable only to Mediant 500Li and Mediant 800Ci.
- This command is applicable only to the integrated cellular modem (LTE).

Command Mode

Privileged User

Example

This example defines "Provider1" with highest priority and a policy that if the RSRP threshold is below -100 dBm for at least 120 seconds, the device connects to the provider with the next highest priority ("Provider2"):

```
(config-data)# interface cellular 0/0
(conf-cellular-0/0)# pdn-policy
(cell-pdn-policy)# rule reception lte rsrp -100
(cell-pdn-policy)# evaluation-time 120
(cell-pdn-policy)# priority 1 Provider1
```

```
(cell-pdn-policy)# priority 2 Provider2
(cell-pdn-policy)# exit
```

phone

This command sets the telephone number (dial-string) used by the cellular interface.

Syntax

```
phone <phone-string>
```

Default

The default phone number is “*99#”.

Command Mode

Privileged User

Note

The command is applicable only to PPP-based cellular modems.

Example

This example sets the phone number:

```
(config-data)# interface cellular 0/0
(conf-cellular)# phone *99#
```

pin

This command sets the 4-digit Personal Identification Number (PIN) code required for the SIM card installed in the modem.

Use the "no" form of this command to remove the PIN.

This command is available in the “conf-cellular” configuration context.

Syntax

```
pin <code>
```

Default

The default setting is "no pin".

Command Mode

Privileged User

Example

This example sets the PIN code:

```
(config-data)# interface cellular 0/0
(conf-cellular)# pin 1234
```

ppp authentication

This command enables PPP authentication and defines the supported authentication protocols for PPP over cellular interface.

Syntax

```
ppp authentication <protocol>
```

Command	Description
pap	Defines the Password Authentication Protocol as PPP authentication protocol. This is for normal login -when a connection has been made the host sends the username and password.
chap	Defines the Challenge Handshake Authentication Protocol as PPP authentication protocol. With CHAP, the authenticator (i.e. the server) sends a randomly generated "challenge" string to the client, along with its hostname. The client uses the hostname to look up the appropriate secret, combines it with the challenge, and encrypts the string using a one-way hashing function. The result is returned to the server along with the client's hostname.
ms-chap	Defines the Microsoft Challenge Handshake Authentication Protocol as PPP authentication protocol.
ms-chap2	Defines the Microsoft Challenge Handshake Authentication Protocol 2 as PPP authentication protocol.

Default

All four authentication protocols are set as on (no limit is placed on which and how many authentication is used - all four can be activated on the same interface).

You can disable some protocol using “no ppp authentication <protocol>” command

Command Mode

Privileged User

Note

The command is applicable only to PPP-based cellular modems.

For disabling authentication protocol, use the command “no ppp authentication <protocol>”.

Example

This example disables the authentication protocol.

```
(config-data)# interface cellular 0/0
(conf-cellular)# no ppp authentication chap
```

ppp user

This command defines the username and password for authentication of the PPP connection for PPP over cellular interface.

Syntax

```
ppp user <Username>
```

Command	Description
obscured-pass	Copy the password from existing configuration
pass	Defines the password for the PPP connection.

Command Mode

Privileged User

Note

The command is applicable only to PPP-based cellular modems.

Example

This example configures a PPP username "JohnD" and password "1234".

```
(config-data)# interface cellular 0/0
(conf-cellular)# ppp user JohnD pass 1234
```

profile

This command defines a profile for cellular modems that use DHCP.

For Mediant 500Li and Mediant 800Ci, you can configure multiple profiles per cellular interface. Each profile can represent a specific LTE provider.

For the MSBR series, you configure only one profile per cellular interface.

Syntax

```
profile
```

Command	Description
<Provider>	Name of the profile (provider). If a profile is created without a name, the profile is automatically assigned the name "default". **Note:** This is applicable only to Mediant 500Li and Mediant 800Ci.
`apn`	Defines the APN for the profile. **Note:** For the SIM card installed in the Mediant 5G-EA cellular modem, you can define up to two APNs.
`authentication {chap|mschapv2|none|pap|pap-chap}`	Defines the authentication method. **Note:** Typically, `pap-chap` (i.e., both PAP and CHAP enabled) is applicable only to Mediant 5G-EA.
`mcc <MCC> [mnc <MNC>]`	Defines the provider's MCC (mobile country code) and MNC (mobile network code).
`obscured-pass`	Defines an obscured password for the profile.

Command	Description
password	Defines a password for the profile.
user	Defines a username for the profile.

Related Commands

- pdn-policy
- profile-selection

Note

- This command is applicable only to the integrated cellular modem (LTE).

Command Mode

Privileged User

Example

- This example configures two LTE provider profiles:

```
(conf-cellular-0/0)# profile Provider1
(profile-#company1)# apn net.com
(profile-#company1)# authentication pap
(profile-#company1)# mcc 425 mnc 07
(profile-#company1)# exit

(conf-cellular-0/0)# profile Provider2
(profile-#company2)# apn abc.com
(profile-#company2)# authentication pap
```

- Configuring two APNs:

```
(config-data)# interface cellular 0/0/1
(conf-cellular-0/0/1)# profile
(profile-#company1)# apn sphone
(profile-#company1)# exit
(conf-cellular-0/0/1)# exit

(config-data)#  interface cellular 0/0/2
(conf-cellular-0/0/2)# profile
(profile-#company1)# apn spone2
```

```
(profile-#company1)# exit
(conf-cellular-0/0/2)# exit
```

profile-selection

This command defines the method for selecting an LTE provider (profile), which can be done manually or automatically based on policy priority.

Syntax

```
profile-selection {fixed|policy priority}
```

Command	Description
`fixed <Profile Name>`	Manually chooses the cellular provider (by profile name).
`policy priority`	Enables automatic selection of the cellular provider based on priorities (see `pdn-policy`).

Related Commands

- `pdn-policy`
- `profile`

Note

- This command is applicable only to the integrated cellular modem (LTE).
- This command is applicable only to Mediant 500Li and Mediant 800Ci.

Command Mode

Privileged User

Example

- To manually choose the cellular provider "Provider1":

```
(conf-cellular-0/0)# profile-selection fixed Provider1
```

- To enable automatic cellular provider selection based on priority rules:

```
(conf-cellular-0/0)# profile-selection policy priority
```

sim disable-nr5g-mode

This command restricts the M5G-EA cellular module to operate in either 5G Non-Standalone (NSA) or 5G Standalone (SA) mode.

Syntax

```
sim disable-nr5g-mode {nsa|sa}
```

Command	Description
nsa	Disables NSA and restricts operation to SA.
sa	Disables SA and restricts operation to NSA.

Default

By default, both modes are enabled and the module automatically chooses a mode according to the cellular network.

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example restricts operation to SA mode:

```
(config-data)# interface cellular 0/0
(conf-cellular-0/0)# sim disable-nr5g-mode nsa
```

sim roaming

This command enables and disables cellular data roaming for cellular interfaces (SIM).

Syntax

```
sim roaming
```

Command Mode

Privileged User

Example

This example disables cellular data roaming:

```
(config-data) # interface cellular 0/0
(conf-cellular-0/0)# no sim roaming
```

sms

This command provides support for sending an SMS text message through a 3G cellular connection. Cellular connectivity is achieved by attaching a third-party, 3G cellular modem to the device's USB port.

Syntax

```
sms <mobile number> "<message text>"
```

Command	Description
`<mobile number>`	Defines the destination phone number.
`<message text>`	Defines the message text which can include up to 127 characters and must be enclosed in double quotes (").

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example sends a text message to a mobile phone.

```
(config-data)# interface cellular 0/0
(conf-cellular)# shutdown
(conf-cellular)# sms 0546342171 "Hello John Doe!"
```

tty

This command selects the serial instance (TTY) for the cellular modem. Most modems provide multiple serial interfaces for diagnostic purposes, usually only one is appropriate for Internet access. TTY is the serial port used to communicate with the modem (which is typically determined automatically). However, in case the device cannot communicate with the serial modem, you can use a different serial port (according to the Linux guide provided by the manufacturer of the cellular dongle modem).

Setting “tty first” will use the first responsive serial interface. Setting “tty last” will use the highest numbered interface (default). Alternatively, a serial interface can be selected by number.

- The recommended setting for Sierra Wireless 308 modems is "tty 2".
- The recommended setting for Huawei E160 / E182E modems is "tty 0".
- The recommended setting for all other modems is the default "tty last".

Syntax

```
tty <tty-value>
```

Command	Description
<tty-value>	Defines the “first”, “last” or a number between 0 and 11. If set to first, the first responsive serial interface is used. If set to last, the highest numbered interface is used.

Default

The default TTY value is “last”.

Command Mode

Privileged User

Note

The command is applicable only to PPP-based cellular modems.

Example

This example sets the TTY instance:

```
(config-data)# interface cellular 0/0
(conf-cellular)# tty 0
```

vendor

This command defines the vendor and model specific settings of the cellular modem. These are specific commands used by external dongles that don't follow the norm.

Syntax

```
vendor <Vendor ID>
```

Command Mode

Privileged User

Note

The command is applicable only to PPP-based cellular modems.

Example

This example defines the vendor of the cellular modem.

```
(config-data)# interface cellular 0/0
(conf-cellular)# vendor netgear 341u
```

ADSL/VDSL Commands

The following describes ADSL/VDSL commands.

interface dsl 0/0

Asymmetric Digital Subscriber Line (ADSL) and VDSL (Very high-speed DSL) are popular WAN access technologies using copper wire pairs.

On appropriate hardware variants of the device, this command defines the physical properties of the ADSL/VDSL interface.

Once the physical layer is configured:

- For ADSL, proceed to ATM interfaces using the command `interface atm`.
- For VDSL, proceed to configure EFM using the command `interface efm`.

- The DSL interface automatically detects the signal on the interface and based on the signal it chooses the DLS mode (ADSL or VDSL).

Syntax

```
interface dsl <slot>/<port>
```

Command	Description
<slot>	Defines the location of the ADSL/VDSL hardware mezzanine. Must be 0.
<port>	Defines the location of the ADSL/VDSL hardware mezzanine. Must be 0.

Default

By default, the DSL interface is not defined.

Command Mode

Privileged User.

Example

The example below describes how to define the DSL interface.

```
(config data)# interface dsl 0/0
```

annex

This command selects Annex A (DSL over POTS) or Annex B (DSL over ISDN) for the ADSL/VDSL interface.

Syntax

```
interface dsl <slot>/<port>
(conf-if-dsl <slot/port>)# annex {a|b}
```

Command	Description
a	Selects G.991.2 regional annex A.
b	Selects G.991.2 regional annex B

Default

The default setting is annex a.

Command Mode

Privileged User

Example

This example selects regional annex B:

```
(conf-if-dsl 0/0)# annex b
```

Fiber Optic Commands

The commands below describe Fiber Optic.

interface fiber

This command enters a specific interface configuration. Use the no form of this command to delete a specific interface.

Syntax

```
interface fiber <slot/port>
interface fiber <slot/port[.vlanID]>
```

Command	Description
slot	Defines the module slot index as shown on the front panel.
port	Defines the port index within the selected module.
vlanID	Defines the VLAN ID for a Layer 3 sub interface.

Default

NA

Command Mode

Privileged User

Example

This example enters a specific interface configuration for the WAN Interface menu.

```
(config-data)#interface fiber 0/3
```

This example enters a specific interface configuration for the sub-Interface 3 menu.

```
(config-data)#interface fiber 0/3.3
```

SHDSL Commands

The commands below describe SHDSL.

interface SHDSL 0/0

Symmetric High-speed Digital Subscriber Line (SHDSL, sometimes called G.SHDSL) is a popular WAN access technology using copper wire pairs.

The purpose of this command is to configure physical-layer properties of SHDSL, such as the number of wire-pairs in use. See the sub-commands "mode" and "group" for additional information.

Once the physical layer is configured, proceed to ATM interfaces using the command "interface atm".

Syntax

```
interface shdsl <slot>/<port>
```

Command	Description
slot	Defines the location of the SHDSL hardware mezzanine. Must be 0.
port	Defines the location of the SHDSL hardware mezzanine.

Default

The system will attempt to detect the correct configuration automatically, by sensing line connectivity and negotiating connection parameters with the Internet Service Provider.

Command Mode

Privileged User

Example

The example below describes how to define the SHDSL interface.

```
(config-data)# interface shdsl 0/0
```

mode

This command selects the SHDSL mode of operation (ATM or EFM).

Syntax

```
interface shdsl 0/0
mode {atm|efm}
```

Command	Description
atm	Selects ATM mode of operation.
efm	Selects Ethernet-in-the-First-Mile (EFM) operation.

Default

The default setting is ATM.

Command Mode

Privileged User

Example

This example defines ATM on the SHDSL interface:

```
(conf-shdsl)# mode atm
```

group

This command defines an SHDSL group of wires. Use the "no" form of this command to delete a previously-defined group.

Syntax

```
interface shdsl 0/0
[no] group <group-id>
```

Command	Description
`<group-id>`	Defines the range as 0 to 3.

Default

By default, four SHDSL groups are defined, each with a single wire-pair; the system will attempt to detect changes on the physical medium and adapt configuration accordingly.

Command Mode

Privileged User

Example

This example defines one group:

```
(conf-shdsl)# group 0
```

pairs

This command selects the wire-pairs which participate in an SHDSL group.

Syntax

```
interface shdsl 0/0
group <group-id>
pairs <list of wire-pair numbers>
```

Command	Description	
`list of wire-pair numbers`	Defines the wire-pair numbers (0 to 3), separated by commas. Examples:	
	pairs 0	Defines a simple two-wire connection using the first wire pair.
	pairs 0,1	Defines a multiple pair (m-pair) connection using wire pairs.

Command	Description	
	pairs 0,1,2,3	Defines a multiple pair (m-pair) connection using all four wire-pairs. Pair 0 is the master pair for this group.

Default

By default, four SHDSL groups are defined, each with a single wire-pair; the system will attempt to detect changes on the physical medium and adapt configuration accordingly.

Command Mode

Privileged User

Example

This example defines a group of two wire-pairs:

```
(conf-shdsl-0)# pairs 0,1
```

termination

This command selects the type of line termination on an SHDSL group.

Syntax

```
interface shdsl 0/0
group <group-id>
termination {cpe|co}
```

Command	Description
cpe	Selects STU-R mode (SHDSL Remote Terminal)
co	Selects STU-C mode (SHDSL Central Office Terminal) Note: CO mode is unsupported and available for diagnostic purposes only; the system cannot be used as a DSLAM.

Default

The default is CPE mode.

Command Mode

Privileged User

Example

This example defines CPE mode:

```
(conf-shdsl-0)# termination cpe
```

linerate

This command selects the line rate of each wire-pair in an SHDSL group.

Syntax

```
interface shdsl 0/0
group <group-id>
linerate auto
linerate kbps <min-rate> <max-rate>
```

Command	Description
auto	Automatically negotiates the Line rate. Up to 5696 Kbps per wire-pair.
<min-rate>	Defines the minimum line rate in kilobits per second. The lowest supported rate is 432 Kbps.
<max-rate>	Defines the maximum line rate in kilobits per second. The highest supported rate is 5696 Kbps.

Default

The default is setting is auto.

Command Mode

Privileged User

Example

This example selects automatic line rate:

```
(conf-shdsl-0)# linerate auto
```

annex

This command selects the regional annex (as defined in ITU-T Recommendation G.991.2) for an SHDSL group.

Syntax

```
(config data)# interface dsl <slot/port>
(conf-if-dsl <slot/port>)# annex [a/b]
```

Command	Description
a	Selects G.991.2 regional annex A.
b	Selects G.991.2 regional annex B.

Default

The default setting is annex a.

Command Mode

Privileged User

Example

This example selects regional annex A:

```
(conf-hdsl-0/0)# annex a
```

interface atm

This command defines an ATM sub-interface for Internet access over SHDSL. An ATM sub-interface provides IP services over a Permanent Virtual Circuit (PVC) defined by the ATM network administrator.

Syntax

```
interface atm <group-id>/<sub-id>
```

Command	Description
group-id	Defines the number of the SHDSL group (0-3) defined by the "group"

Command	Description
	command.
sub-id	Defines the sub-interface number (0 to 7). Note: The system supports up to a total of eight ATM interfaces in all SHDSL groups.

Default

By default, no ATM interfaces are defined.

Command Mode

Privileged User

Example

This example defines an ATM interface:

```
(config-data)# interface atm 0/0
```

pvc

This command defines the Permanent Virtual Circuit (PVC) associated with an ATM sub-interface.

Syntax

```
interface atm <group-id>/<sub-id>
pvc <vpi>/<vci>
```

Command	Description
<vpi>	Defines the Virtual Path Identifier code (0 to 256).
<vci>	Defines the Virtual Connection Identifier code (32 to 65535).

Default

By default, no ATM interfaces are defined.

Command Mode

Privileged User

Example

This example defines an ATM interface with VPI 8, VCI 48:

```
(conf-atm0/0)# pvc 8/48
```

encapsulation

This command defines the type of IP encapsulation used on an ATM sub-interface.

Syntax

```
interface atm <group-id>/<sub-id>
encapsulation {ipoa|ethoa|pppoa}-{mux|snap}
encapsulation pppoe
encapsulation pppoe-mux
```

Command	Description
ipoa	Selects the IP-over-ATM, in RFC 2684 "Routed" mode.
ethoa	Selects the Ethernet-over-ATM, in RFC 2684 "Bridged" mode.
pppoa	Selects PPP over ATM client (defined in RFC 2364)
snap	Selects AAL5 LLC/SNAP mode. A LLC header is used to describe the type of payload transmitted
mux	Selects AAL5 VC-multiplexed mode, data is not prepended with an LLC header
pppoe	Selects PPPoE over ATM in LLC/SNAP mode (i.e., PPPoE client on top of ethoa-snap encapsulation)
pppoe-mux	Selects PPPoE over ATM in VC-multiplexed mode (PPPoE client on top of ethoa-mux encapsulation)

Default

By default, no ATM interfaces are defined.

Command Mode

Privileged User

Example

This example defines an ATM interface with RFC 2684 "Routed" encapsulation, with LLC/SNAP headers:

```
(conf-atm0/0)# encapsulation ipoa-snap
```

ubr / cbr / vbr

This command defines the ATM service class for an ATM sub-interface.

Syntax

```
interface atm <group-id>/<sub-id>
ubr <peak-kbps>
cbr <peak-kbps>
vbr <peak-kbps> <sustained-kbps> <burst-cells>
```

Command	Description
`ubr`	Defines Unspecified Bit Rate; no bandwidth is reserved for this interface. Traffic may be limited by a peak rate.
`cbr`	Defines Constant Bit Rate; bandwidth is reserved according to the specified rate. Traffic cannot exceed the specified rate.
`vbr`	Defines Variable Bit Rate; bandwidth is reserved according to the configured sustained rate. Traffic may exceed the sustained rate up to the peak rate, but is further limited by a maximum number of burst cells.
`<peak-kbps>`	Defines the Maximum data rate in kilobits per second
`<sustained-kbps>`	Defines the Sustained data rate in kilobits per second
`<burst-cells>`	Defines the maximum number of cells allowed in excess of the sustained rate

Default

The default setting is UBR with unlimited traffic rate.

Command Mode

Privileged User

Example

This example defines an ATM interface with a constant bit-rate traffic class, allowing bandwidth of 4 megabits per second:

```
(conf-atm0/0)# cbr 4096
```

ppp user

This command defines the PPPoA / PPPoE username and password for an ATM sub-interface.

Syntax

```
interface atm <group-id>/<sub-id>
ppp user <username> pass <password>
```

Command	Description
<username>	Defines the PPP user name.
<password>	Defines the PPP password.

Default

This command has no defaults.

Command Mode

Privileged User

Example

This example defines a PPPoA ATM interface:

```
(conf-atm0/0)# ppp user admin pass 12345
```

T1 WAN Commands

This section describes the commands for the T1 WAN interface. The T1 WAN interface is one of three WAN interfaces of the Mediant 500 MSBR and Mediant 800 MSBR.

The other WAN interfaces are SHDSL and the Ethernet WAN interface (see the relevant sections above).

The T1 WAN interface supports up to two physical T1 ports; 0 and 1.

This section includes the following topics:

- T1 Physical Interfaces. See below.
- Serial Interfaces. See Serial Interfaces on page 650.
- Multilink Interfaces (MLP over T1 WAN). See Multilink Interfaces (MLP over T1 WAN) on page 660.

The commands described in the previous sections are also applicable to the T1 WAN interface.

T1 Physical Interfaces

This section describes the WAN T1 Physical Interface commands.

You can configure the WAN T1 physical interface and the WAN serial interface on the same physical WAN port, where the same identifier <slot>-<port> is specified for both interfaces. In the examples described in this section and in section 41.5.15, <slot> / <port> is specified as either '0/0' and '0/1'.

channel-group

This command specifies the active TDM slots within the T1 frames.

Syntax

```
channel-group <slot number>,<slot number>
channel-group <slot number>-<slot number>
```

Command	Description
<slot number>	Defines the slot number within the range 1-24.

Default

By default all slots are active → 1-24.

Command Mode

Privileged User

Example

This example sets active slots 2, 4 and 17, 18, 19 on t1 port 0/0.

```
(conf-if-t1 0/0)# channel-group 2, 4, 17-19
```

clock-source

This command specifies the clock source on the current T1 interface.

Syntax

```
clock-source <source>
```

Command	Description
<source>	Defines the source of the clock: 'internal' – clock is taken locally from WIC itself 'line' – clock is taken from the line i.e., from the remote side

Default

By default, the clock source is 'line'.

Command Mode

Privileged User

Example

This example sets clock source to the internally generated on T1 Port 0/1:

```
(conf-if-t1 0/1)# clock-source internal
```

framing-method

This command specifies the framing method on the current T1 interface.

Syntax

```
framing-method <framing mode>
```

Command	Description
<framing mode>	Defines the framing method: 'esf' – extended super frame (F24) 'sf' – superframe (D4)

Default

By default, the framing method is 'esf'.

Command Mode

Privileged User

Example

This example sets the framing method to superframe (D4) on t1 port 0/0:

```
(conf-if-t1 0/0)# framing-method sf
```

line-code

This command specifies the line coding on the current T1 interface.

Syntax

```
line-code <line code>
```

Command	Description
<line code>	Defines the line code: 'ami' – Alternate Mark Inversion encoding 'b8zs' – Bipolar Eight Zero Substitution encoding

Default

By default, the framing method is 'bz8s'.

Command Mode

Privileged User

Example

This example sets the line code to 'ami' on t1 port 0/1:

```
(conf-if-t1 0/1)# line-code ami
```

line-buildout-loss

This command specifies the buildout loss on the current T1 interface.

Syntax

```
line-buildout-loss <loss>
```

Command	Description
<loss>	Defines the line buildout loss [dB]: ■ 0 dB ■ -7.5 dB ■ -15 dB ■ -22.5 dB

Default

By default, the line buildout loss is 0 dB.

Command Mode

Privileged User

Example

This example sets the line buildout loss to -7.5 dB on t1 port 0/0:

```
(conf-if-t1 0/0)# line-buildout-loss -7.5
```

max-cable-loss

This command specifies the loss due to cable length on the current T1 interface.

Syntax

```
max-cable-loss <loss>
```

Command	Description
<loss>	Defines the cable loss [dB]: 0.6 dB – Cable length 0-133ft 1.2 dB – Cable length 134-266ft 1.8 dB – Cable length 267-399ft 2.4 dB – Cable length 400-533ft 3 dB – Cable length 534-655ft

Default

By default, the maximum cable loss is 0.6 dB.

Command Mode

Privileged User

Example

This example sets the cable loss to 3 dB on T1 Port 0/1:

```
(conf-if-t1 0/1)# max-cable-loss 3
```

loopback

This command specifies loopback on the current T1 WAN interface.

Syntax

```
loopback <traffic source> <loopback location>
loopback <traffic source> <loopback location> <timeout>
```

Command	Description
<traffic source>	Defines the traffic source to be looped back: 'remote' – loopback ingress traffic. 'local' – loopback egress traffic.
<loopback location>	Defines where the loop is performed in the T1 WAN Interface: 'line' – loop is done in the csu.
<timeout>	On the local loopback only. Specifies the timeout (in seconds) after the local loopback releases.

Command	Description
	Default timeout is 180 seconds.

Default

By default, there is no loopback.

Command Mode

Privileged User

Example

This example set the remote line loopback on T1 Port 0/0.

```
(conf-if-t1 0/0)# loopback remote line
```

ber-test

This command specifies the Bit Error Rate test on the current T1 WAN interface.

Syntax

The syntax for this command includes several variations:

```
ber-test <channels group> <error rate> <pattern type>
ber-test <channels group> <error rate> <pattern type> <timeout>
ber-test <channels group> <error rate> <pattern type> forever
```

Command	Description
<channels group>	Specifies the slot number within the range 1-24, on which the BER test runs. (See channel-group command for examples).
<error rate>	Specifies the rate of injected errors to the BER interface: 0 – no errors injected. 1 – inject errors in rate of 10^{-1}. 2 – inject errors in rate of 10^{-2}. 3 – inject errors in rate of 10^{-3}. 4 – inject errors in rate of 10^{-4}. 5 – inject errors in rate of 10^{-5}. 6 – inject errors in rate of 10^{-6}.

Command	Description
	7 – inject errors in rate of 10^{-7}.
<pattern type>	Specifies the pattern type: '1-2' - select 01 Sequence as BER pattern '1-4' - select 0001 Sequence as BER pattern '1-8' - select 00000001 Sequence as BER pattern '3-24' - select 3 '1's with 21 '0's Sequence as BER pattern 'all-0' - select all 0 Sequence as BER pattern 'all-1' - select all 1 Sequence as BER pattern 'qrss' - select Quasi-Random Signal Sequence as BER pattern
<timeout>	Specifies the time that the BER test will run for, in seconds. The default value is 180 seconds. For running the BER test with no time limitation, select the 'forever' value for this field.

Default

By default, the BER test is not active.

Note

- This command is supported on the T1-WAN interface only.
- The user needs to make a loopback at the FarEnd, to have synchronous BER test patterns.
- Running the BER test with an error rate of 10^{-1} might cause the data not to synchronize. So the BER won`t count bits or errors.

Command Mode

Privileged User

Example

This example starts the BER test for Channels 1-20 and Channel 22, with error rate of 10^{-3} and pattern type QRSS, which has no timeout:

```
(conf-if-t1 0/0)# ber-test 1-20, 22 3 qrss forever
```

This example starts the BER test for Channels 1,2 and 10-15, no errors injected, pattern type 3-24, and default timeout (180 seconds):

```
(conf-if-t1 0/0)# ber-test 1, 2, 10-15 0 3-24
```

Serial Interfaces

This section describes the WAN serial interface commands.

You can configure the WAN serial interface and the WAN T1 physical interface on the same physical WAN port, where the same identifier <slot>-<port> is specified for both interfaces. In the examples described in this section and in Section 41.5.14, <slot> / <port> is specified as either '0/0' and '0/1'.

serial-protocol

This command specifies the encapsulating protocol on the serial interface.

Syntax

```
serial-protocol <protocol>
```

Command	Description
`protocol *bundle id parameter is for mlp only.`	Defines the encapsulating protocol: ■ 'hdlc' – set hdlc protocol ■ 'ppp' – set ppp protocol ■ 'mlp' – set multilink ppp protocol and associates the serial interface to a logical bundle id.

Default

By default, there is no encapsulating protocol set on the serial interface.

Command Mode

Privileged User

Example

This example sets PPP as the encapsulating protocol on the serial interface 0/0:

```
(conf-if-serial 0/0)#serial-protocol ppp
```

To remove the protocol, type 'no' at the prefix of the command.

This example sets HDLC as the encapsulating protocol on the serial interface 0/0:

```
(conf-if-serial 0/0)#serial-protocol hdlc
```

To remove the protocol, type ‘no’ at the prefix of the command.

This example sets MLP as the encapsulating protocol on the serial interface 0/1 and associates the serial interface to a logical bundle identified by id 0:

```
(conf-if-serial 0/1)#serial-protocol mlp 0
```

To remove the protocol, type ‘no’ at the command prefix.

ip address (HDLC over T1)

This command specifies the IP address and subnet mask of the HDLC serial interface.

Syntax

```
ip address <a.b.c.d> <e.f.g.h>
```

Command	Description
a.b.c.d	Defines the static local IP address set on this HDLC serial interface.
e.f.g.h	Defines the static subnet mask set on this HDLC serial interface.

Default

By default, the IP address is 1.1.1.1 and the subnet mask is 255.255.255.0.

Command Mode

Privileged User

Example

This example sets IP address 223.4.5.6 on HDLC encapsulated serial interface 0/0:

```
(conf-if-serial-hdlc 0/0)# ip address 223.4.5.6 255.255.255.252
```

ip dns-server (HDLC over T1)

This command specifies the primary and secondary DNS servers to be used by this HDLC serial interface.

Syntax

```
ip dns-server <a.b.c.d> [e.f.g.h]
```

Command	Description
a.b.c.d	Defines the IP address of the primary DNS server.
e.f.g.h	Defines the IP address of the secondary DNS server.

Default

By default, no DNS servers are defined for the HDLC serial interface.

Command Mode

Privileged User

Example

This example sets IP address 223.4.5.6 on the HDLC encapsulated serial interface 0/0:

```
(conf-if-serial-hdlc 0/0)# ip dns-server 10.1.1.10 10.1.1.11
```

ip mtu (HDLC over T1)

This command specifies the maximum transfer unit value to be used by this HDLC serial interface.

Syntax

```
ip mtu <mode> <value>
```

Command	Description
<mode>	Defines the mtu mode to be used: 'automatic' – Sets to default value 1500 bytes. 'manual' – Sets manually according to the following value.
<value>	Defines the MTU in manual mode (68-1500).

Default

By default the mtu is set to 1500 bytes.

Command Mode

Privileged User

Example

This example sets the mtu to 1400 bytes:

```
(conf-if-serial-hdlc 0/0)# ip mtu manual 1400
```

ip address (PPP over T1)

This command specifies the IP addressing mode of the PPP serial interface.

Syntax

```
ip address <mode> <a.b.c.d> <e.f.g.h>
```

Command	Description
Mode	Defines the PPP IP addressing modes: 'automatic' – IP address will be accepted from peer during IPCP negotiation. 'manual' – set local static IP address and optional subnet mask. 'unnumbered' – use unnumbered mode (PPP serial interface uses LAN interface ip address).
a.b.c.d	Defines the static local IP address set on this PPP serial interface – relevant for manual mode only.
e.f.g.h	Defines the optional static subnet mask set on this PPP serial interface - relevant for manual mode only.

Default

By default the IP addressing is automatic.

Command Mode

Privileged User

Example

This example sets IP address 223.4.5.6 on PPP encapsulated serial interface 0/0:

```
(conf-if-serial-ppp 0/0)# ip address manual 223.4.5.6
```

This example sets IP addressing mode to automatic on PPP encapsulated serial interface 0/0:

```
(conf-if-serial-ppp 0/0)# ip address automatic
```

ip dns-server (PPP over T1)

This command specifies the primary and secondary DNS servers to be used by this PPP serial interface.

Syntax

```
ip dns-server <mode> <a.b.c.d> <e.f.g.h>
```

Command	Description
mode	Defines the DNS servers addressing modes: 'automatic' – DNS servers' IP addresses will be accepted from peer during PPP negotiation. 'manual' – set static DNS servers' IP address
a.b.c.d	Defines the IP address of the primary DNS server - relevant only for manual mode.
e.f.g.h	Defines the IP address of the optional secondary DNS server- relevant only for manual mode.

Default

By default no DNS servers are defined for the PPP serial interface.

Command Mode

Privileged User

Example

This example sets the static DNS servers' IP addresses on the PPP encapsulated serial interface 0/0:

```
(conf-if-serial-ppp 0/0)# ip dns-server manual 10.1.1.10 10.1.1.11
```

ip mtu (PPP over T1)

This command specifies the maximum transfer unit value to be used by this PPP serial interface.

Syntax

```
ip mtu <mode> <value>
```

Command	Description
mode	Defines the MTU mode to be used: 'automatic' – Set to default value 1500 bytes. 'manual' – Set manually according to following value.
value	Defines the MTU in manual mode (68-1500).

Default

By default, the MTU is set to 1500 bytes.

Command Mode

Privileged User

Example

This example sets the mtu to 1400 bytes:

```
(conf-if-serial-ppp 0/0)# ip mtu manual 1400
```

authentication chap (PPP/MLP over T1)

This command enables Challenge Handshake Authentication Protocol (CHAP) to be used by this PPP/MLP serial interface.

Syntax

```
authentication chap
```

Command	Description
'no' at prefix of command	Disables CHAP on this PPP/MLP serial interface.

Default

By default CHAP is enabled

Command Mode

Privileged User

Example

This example enables CHAP:

```
(conf-if-serial-ppp 0/0)# authentication chap
```

authentication pap (PPP/MLP over T1)

This command enables Password Authentication Protocol (PAP) to be used by this PPP/MLP serial interface.

Syntax

```
authentication pap
```

Command	Description
'no' at prefix of command	Disables PAP on this PPP/MLP serial interface.

Default

By default, PAP is enabled.

Command Mode

Privileged User

Example

This example enables PAP on the MLP serial interface 0/0:

```
(conf-if-serial-mlp 0/0)# authentication pap
```

authentication ms-chap (PPP/MLP over T1)

This command enables Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) to be used by this PPP/MLP serial interface

Syntax

```
authentication ms-chap
```

Command	Description
'no' at prefix of command	Disables MS-CHAP on this PPP/MLP serial interface.

Default

By default, MS-CHAP is enabled.

Command Mode

Privileged User

Example

This example enables MS-CHAP:

```
(conf-if-serial-ppp 0/0)# authentication ms-chap
```

authentication ms-chap2 (PPP/MLP over T1)

This command enables Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAP2) to be used by this PPP/MLP serial interface.

Syntax

```
authentication ms-chap2
```

Command	Description
'no' at prefix of command	Disables MS-CHAP2 on this PPP/MLP serial interface.

Default

By default, MS-CHAP2 is enabled.

Command Mode

Privileged User

Example

This example describes MS-CHAP2:

```
(conf-if-serial-ppp 0/0)# authentication ms-chap2
```

authentication username (PPP/MLP over T1)

This command sets the username to be used by this PPP/MLP serial interface during the authentication phase of the PPP negotiation.

Syntax

```
authentication username <username>
```

Command	Description
username	Defines the username string

Default

By default, the username is set to ‘user’.

Command Mode

Privileged User

Example

This example sets the username on the PPP serial interface 0/0:

```
(conf-if-serial-ppp 0/0)# authentication username JohnA
```

authentication password (PPP/MLP over T1)

This command sets the password to be used by this PPP/MLP serial interface during the authentication phase of the PPP negotiation.

Syntax

```
authentication password <password>
```

Command	Description
<password>	Defines the password string

Default

By default, password is set to 'password'.

Command Mode

Privileged User

Example

This example sets the password on the MLP serial interface 0/1:

```
(conf-if-serial-mlp 0/1)# authentication password qwerty
```

multilink bundle-id (MLP over T1)

This command associates the current MLP serial interface to a virtual bundle id. Setting more than one serial interface to the same bundle id bonds both interfaces under the same virtual bundle.

You can configure an identical virtual bundle for the MLP over T1 serial WAN interface and the Multilink WAN interface, where <bundle-id> is specified for both interfaces. In the example below, <bundle-id> is specified as '8'.

Syntax

```
multilink bundle-id <id>
```

Command	Description
<id>	Defines the bundle-id (0-255).

Default

No default value exists; you must specify a bundle id.

Command Mode

Privileged User

Example

This example associates a MLP serial interface 0/1 to logical bundle 0:

```
(conf-if-serial-mlp 0/1)#multilink bundle-id 8
```

Multilink Interfaces (MLP over T1 WAN)

This section describes the Multilink interfaces commands. The multilink interface holds all relevant data characteristics for a virtual bundle of MLP interface/s.

napt

This command sets the NAPT (Network Address Port Translation) on the Multilink interface.

Syntax

```
napt
```

Default

By default T1 interfaces use NAPT.

Command Mode

Privileged User

Example

This example sets the Multilink interface 0 to use NAPT:

```
(conf-if-multilink 0)#napt
```

ppp bundle-id

This command associates the current multilink interface with a virtual bundle id number.

You can configure an identical virtual bundle for the multilink WAN interface and the MLP over T1 serial WAN interface, where the identifier <bundle-id> is specified for both interfaces. In the example below, <bundle-id> is specified as '8'.

Syntax

```
ppp bundle-id <id>
```

Command	Description
<id>	Defines the bundle-id (0-255).

Default

By default, the bundle id is set to the multilink interface number.

Command Mode

Privileged User

Example

This example associates a multilink interface 1 with virtual bundle id 8:

```
(conf-if-multilink 1)# ppp bundle-id 8
```

ppp fragments-enable

This command will cause each transmitted packet to be fragmented among the virtual bundle's serial interfaces, thus reaching maximum bandwidth utilization.

Syntax

```
ppp fragments-enable
```

Command	Description
'no' at prefix of command	Disables fragmentation on this multilink interface.

Default

By default, fragmentation is disabled.

Command Mode

Privileged User

Example

This example enables fragmentation on interface multilink 0:

To disable fragmentation, type 'no' at the command prefix.

```
(conf-if-multilink 0)# fragments-enable
```

ppp mrru

This command sets the maximum reconstructed receive unit that is negotiated during the ppp session setup.

Syntax

```
ppp mrru <size>
```

Command	Description
<size>	Defines the mru size (68-1500).

Default

By default, mrru is set to 1500 bytes.

Command Mode

Privileged User

Example

This example sets the mrru to 500 bytes on multilink interface 1:

```
(conf-if-multilink 1)# ppp mrru 500
```

ip address

This command specifies the IP addressing mode of this multilink interface.

Syntax

```
ip address <mode> <a.b.c.d> <e.f.g.h>
```

Command	Description
mode	Defines the MLP IP addressing modes as follows: 'automatic' – IP address will be accepted from peer during PPP negotiation. 'manual' – set local static IP address and optional subnet mask. 'unnumbered' – use unnumbered mode (MLP serial interface uses LAN interface ip address).
a.b.c.d	Defines the static local IP address set on this MLP multilink interface – relevant for manual mode only.
e.f.g.h	Defines the optional static subnet mask set on this MLP multilink interface - relevant for manual mode only.

Default

By default the IP addressing is automatic.

Command Mode

Privileged User

Example

This example sets the IP address 223.4.5.6 on multilink interface 0:

```
(conf-if-multilink 0)# ip address manual 223.4.5.6
```

This example sets the IP addressing mode to automatic on multilink interface 0:

```
(conf-if-multilink 0)# ip address automatic
```

ip dns-server

This command specifies the primary and secondary DNS servers to be used by this multilink interface.

Syntax

```
ip dns-server <mode> <a.b.c.d> <e.f.g.h>
```

Command	Description
mode	The DNS servers addressing modes are: 'automatic' – DNS servers' IP addresses will be accepted from peer during PPP negotiation. 'manual' – Sets static DNS servers' IP address
a.b.c.d	Specifies the IP address of the primary DNS server - relevant only for the manual mode.
e.f.g.h	Specifies the IP address of the optional secondary DNS server- relevant only for the manual mode.

Default

By default, no DNS servers are defined for the multilink interface.

Command Mode

Privileged User

Example

This example sets static DNS servers' IP addresses on multilink interface 0:

```
(conf-if-multilink 0)# ip dns-server manual 10.1.1.10 10.1.1.11
```

Backup Group Commands

The commands below describe Backup Group.

backup-group

A backup group defines a set of interfaces so that only one of the interfaces is active at any given moment. Other interfaces in the group are automatically disabled.

By default, the interface marked as "priority 1" will be activated; if the active interface loses connectivity, the device attempts to bring up the next interface in the group. As soon as the higher-priority interface regains connectivity, the lower-priority interface will be disabled.

To associate interfaces with a backup group, use the "backup monitoring group" command in interface context.

Syntax

```
backup-group <group-name> [ primary-wan ]
 description <desc-text>
 exit
```

Command	Description
group-name	Defines the name of the backup group.
primary-wan	Marks the group as controlling the primary WAN connection. This setting affects SIP connectivity; when the primary WAN interface changes, registration will be performed via the new interface. This is an optional field.
desc-text	A description of the backup group.

Default

By default, no backup groups are defined.

Command Mode

Privileged User

Example

This example defines a backup group:

```
(config-data)# backup-group abc primary-wan
(backup-group)# description WAN-group
```

backup monitoring group

This command associates an interface with a backup group. Interfaces in a backup group are automatically enabled and disabled based on the connectivity status of other interfaces in the group. See the command "backup-group" for additional information.

To remove an interface from a backup group, use the "no" form of this command.

Syntax

```
backup monitoring group <group-name> priority {1|2|3}
```

Command	Description
group-name	Name of the backup group (defined by the backup-group command).
1, 2, 3	Sets the interface priority in the backup group.

Default

By default, interfaces are not associated with a backup group.

Command Mode

This command is available in interface configuration context.

Example

This example associates an interface with a backup group:

```
(conf-atm0/0)# backup monitoring group abc priority 1
```

70 Layer-2 (LAN) Commands

Wi-Fi Commands

The following describes Wi-Fi commands.

radio shutdown

This command provides support for enabling or disabling Wi-Fi functionality. The no radio shutdown disables the Wi-Fi interface.

Syntax

```
radio shutdown
no radio shutdown
```

Default

This command is applicable to Mediant 500 MSBR and Mediant 800/B MSBR.

Command Mode

Privileged User

Example

This example enables Wi-Fi functionality on the device.

```
(config-data)# radio shutdown
```

LAN Port Redundancy

You can configure the device for LAN port redundancy, where one of the ports is active while the other is the backup port (only one of them forwards packets). You can configure multiple groups of active-backup LAN ports.

Port backup operates in non-retrieve mode. The active port remains active until its link fails at which stage a switch-over to the backup port is done. When the first port link comes up again, no switch over (back) is made to this port, and it remains as the backup port.

After a device reset, if both ports have a link, the first port that was configured becomes the active port.

Port redundancy is configured as follows:

```
conf d
interface <first LAN port>
port-redundancy <second LAN port>
```

Example of two groups of LAN port redundancy pairs:

```
# conf d
(config-data)# interface fastethernet 1/1
(conf-if-FE 1/1)# port-redundancy fastethernet 1/2
(conf-if-FE 1/1)# ex
(config-data)# interface fastethernet 1/3
(conf-if-FE 1/3)# port-redundancy fastethernet 1/4
(conf-if-FE 1/3)# do show data port-redundancy
Port Redundancy Status
---------------------------
First Port   FastEthernet 1/1
Second Port   FastEthernet 1/2
Active Port   FastEthernet 1/1

Port Redundancy Status
---------------------------
First Port   FastEthernet 1/3
Second Port   FastEthernet 1/4
Active Port   FastEthernet 1/4
```

Data Services Commands

The following describes Data Services commands.

layer-2-only

This command allows the device's underlying interfaces (e.g., Gigabit Ethernet) using PPPoE to start the establishment of the PPPoE connection after Layer 2 of the underlying interface (e.g., when the cable is connected). This is instead of waiting for the PPPoE process to start after Layer 3 of the underlying interface has established.

Syntax

```
layer-2-only
```

Default

By default, this is disabled.

Command Mode

Privileged User

Example

This example enables this feature on the Gigabit Ethernet interface 0/0 using PPPoE:

```
# configure data
(config-data)# interface pppoe 0
(conf-pppoe-0)# underlying gigabitethernet 0/0
((conf-pppoe-0)# layer-2-only
```

mac auto

This command enables and associates a MAC address from the pool of MAC addresses with an underlying interface.

Syntax

```
mac auto
```

Default

By default, this is disabled.

Command Mode

Privileged User

Related Commands

- To configure the prefix of the MAC addresses in the pool: `set admin-global-mac`
- To see if the MAC addresses in the pool are being used or not (by underlying interfaces): `show global-mac-table`

Example

This example enables and associates a MAC address from the pool of MAC addresses on the Gigabit Ethernet 0/0 underlying interface for PPPoE:

```
(config-data) interface gigabitethernet 0/0
(conf-if-GE 0/0)# mac auto
```

```
(config-data)# interface pppoe 0
(conf-pppoe-0)# underlying gigabitethernet 0/0
```

shutdown

This command disables the specified interface. Use the no form of this command to enable the interface.

Syntax

```
shutdown
no shutdown
```

Default

When creating a new interface, it is disabled by default.

Command Mode

Privileged User

Example

This example enables VLAN 6.

```
(conf-if-VLAN 6)# no shutdown
```

speed

This command configures the speed on the specified switchport interface.

Syntax

```
speed 10
speed 100
speed auto
```

Command	Description
10	Forces 10 Mbps operation.
100	Forces 100 Mbps operation.

Command	Description
auto	Automatically detects switchport speed.

Default

Speed is set to auto.

Command Mode

Privileged User

Example

This example sets the speed to 100 on GigabitEthernet 4/2.

```
(conf-if-GE 4/2)# speed 100
```

Switch Port Interface Commands

The following describes Switch Port Interface commands.

switchport mode

This command configures the VLAN Trunking mode.

Syntax

```
switchport mode access
switchport mode trunk
switchport mode transparent
```

Command	Description
access	Sets the port to access mode.
trunk	Sets the port to trunk mode.
transparent	Set the port to transparent mode (Q-in-Q)

Default

Switchport mode is set to trunk.

Command Mode

Privileged User

Example

This example sets the switchport mode to static access on GigabitEthernet 4/2:

```
(config-data)# interface gigabitethernet 0/1
(conf-if-GE 0/1)# switchport mode access
```

switchport access vlan

This command configures the specified switch port interface as a static-access member of a VLAN.

Syntax

```
switchport access vlan <vlan id>
```

Command	Description
<vlan id>	Defines a valid VLAN interface ID. Range is 1 to 3999.

Default

A single VLAN interface is available (VLAN 1).

Note

If the port is in the trunk mode, this command will not alter the switchport mode to ‘Access’. Instead it will save the value to be applied when the port does switch to Access mode.

Command Mode

Privileged User

Related Commands

switchport mode

Example

This example sets the switchport mode to static access and makes the GigabitEthernet interface 4/2 port a member of VLAN 3:

```
(config-data)# interface gigabitethernet 4/2
(conf-if-GE 4/2)# switchport access vlan 3
```

switchport trunk allowed vlan

This command is used to configure the VLANs available on the trunk (when the interface is in trunking mode).

Syntax

```
switchport trunk allowed vlan add <vlan id>
switchport trunk allowed vlan remove <vlan id>
```

Command	Description
`add`	Adds an entry to the list of allowed VLANs.
`remove`	Removes an entry from the list of allowed VLANs.
`<vlan id>`	Specifies a valid VLAN interface ID. Range is 1 to 3999.

Default

NA

Note

VLAN ID values range from 1 to 3999.

Command Mode

Privileged User

Related Commands

switchport mode

Example

This example adds VLAN 3 to the VLAN trunk defined for GigabitEthernet 4/2:

```
(conf-if-GE 4/2)# switchport trunk allowed vlan add 3
```

switchport trunk native vlan

This command sets the native VLAN to the interface when set to Trunking mode.

Syntax

```
switchport trunk native vlan <vlan id>
```

Command	Description
<vlan id>	Specifies a valid VLAN interface ID. Range is 1 to 3999.

Default

This is set to VLAN 1 (the default VLAN).

Note

- VLAN ID values range from 1 to 3999.
- Configure which VLAN the interface uses as its native VLAN when in Trunking mode. Packets from this VLAN leaving the interface will not be tagged with the VLAN number. Any untagged packets received on the interface are considered to be tagged with VLAN ID.

Command Mode

Privileged User

Related Commands

switchport mode

Example

This example sets the native VLAN on GigabitEthernet 4/2 to 3.

```
(config-data)# interface gigabitethernet 4/2
(conf-if-GE 4/2)# switchport trunk native vlan 3
```

Port Monitoring Commands

Port monitoring allows the user to reflect traffic from each Ethernet LAN port to any other single LAN or microprocessor port. Monitoring of traffic is useful when trying to analyze the traffic or when debugging network problems. The device allows monitoring of egress traffic, ingress traffic, or both directions.

port-monitor

This command configures source ports. This is performed after you have chosen your destination port.

Syntax

```
port-monitor <type> <slot/port> <direction>
```

Command	Description
Type	Defines the source Interface type FastEthernet/GigabitEthernet.
slot/port	Defines the source Interface slot number and port number.
direction	Defines the monitoring direction (ingress, egress, or both-direction).

Related Commands

`port-monitor-save-after-reset`

Example

This example defines a key to a peer ip.

```
(conf-if-GE 4/3)# port-monitor GigabitEthernet 4/1 ingress
(conf-if-GE 4/3)# port-monitor FastEthernet 5/2 egress
(conf-if-GE 4/3)# port-monitor GigabitEthernet 4/4 both-direction
```

port-monitor-save-after-reset

This command saves your port monitoring (mirroring) configuration (see the port-monitor command in Section port-monitor above) so that it is maintained even after a device reset.

Syntax

```
port-monitor-save-after-reset
```

Related Commands

`port-monitor`

Example

This example configures port monitoring and saves the configuration defines a key to a peer ip.

```
(conf-if-GE 4/3)# port-monitor GigabitEthernet 4/4 both-direction
(conf-if-GE 4/3)# exit
(config-data)# port-monitor-save-after-reset
```

Spanning Tree Commands

The section below describes Spanning Tree commands.

Spanning Tree General Commands

The sub-section below describes Spanning Tree General commands.

spanning-tree

This command enables / disables the spanning tree in the system.

Syntax

```
spanning-tree
no spanning-tree
```

Command Mode

Privileged User

Example

This example enables the spanning-tree:

```
(config data)# spanning-tree
```

spanning-tree priority

This command sets the priority of the device.

Syntax

```
spanning-tree priority <value>
```

Command	Description
<value>	The range is 0 - 61440 in multiples of 4096

Default

32768

Note

Under configure terminal.

Command Mode

Privileged User

Example

This example sets the device priority to 4096.

```
(config data)# spanning-tree priority 4096
```

spanning-tree hello-time

This command sets the hello_time spanning-tree parameter of the device.

Syntax

```
spanning-tree hello-time <value>
```

Command	Description
<value>	The range is 1-10 seconds.

Default

2 seconds

Note

Under configure terminal

Command Mode

Privileged User

Example

This example sets the hello-time to 1 second:

```
(config data)# spanning-tree hello-time 1
```

spanning-tree max-age

This command sets the maximum-age spanning-tree parameter of the device.

Syntax

```
spanning-tree max-age <value>
```

Command	Description
<value>	The range is 6 - 40 seconds.

Default

20 seconds

Note

Under configure terminal

(FORWARD_DELAY-1)X2 >= MAX_AGE

Command Mode

Privileged User

Example

This example sets the max-age to 10:

```
(config data)# spanning-tree max-age 10
```

spanning-tree forward-delay

This command sets the forward-delay spanning-tree parameter of the device.

Syntax

```
spanning-tree forward-delay <value>
```

Command	Description
<value>	Defines the time set in the range of 4 – 30 seconds.

Default

15 seconds

Note

- Under configure terminal
- (FORWARD_DELAY-1)X2 >= MAX_AGE

Command Mode

Privileged User

Example

To set the device forward-delay to 5:

```
(config data)# spanning-tree forward-delay 5
```

Spanning Tree Interface Commands

The sub-section below describes Spanning Tree Interface commands.

spanning-tree

This command enables/disables the spanning tree on a specific interface.

Syntax

```
spanning-tree
no spanning-tree
```

Default

NA

Note

Under configure terminal

Command Mode

Privileged User

Examples:

To enable the spanning-tree on interface 5/1:

```
(conf-if-FE 5/1)# spanning-tree
```

To disable the spanning-tree on interface 5/1:

```
(conf-if-FE 5/1)# no spanning-tree
```

spanning-tree priority

This command sets the priority of the interface.

Syntax

```
spanning-tree priority <value>
```

Command	Description
<value>	Sets the value in the range of 0-240. Must be a multiple of 16.

Default

NA

Note

Under configure terminal

Command Mode

Privileged User

Example

This example sets the device priority to 16.

```
(conf-if-FE 5/1)# spanning-tree priority 16
```

spanning-tree cost

This command sets the cost of the interface.

Syntax

```
spanning-tree cost <value>
```

Command	Description
<value>	Defines the value in the range of 1-200,000,000.

Default

NA

Note

Under configure terminal

Command Mode

Privileged User

Example

This example sets the unit cost to 10000:

```
(conf-if-FE 5/1)# spanning-tree cost 10000
```

spanning-tree edge

This command sets the edge configuration of the interface.

Syntax

```
spanning-tree edge auto
spanning-tree edge enable
spanning-tree edge disable
```

Command	Description
auto/enable/disable	Defines the value as: ■ auto: auto detect ■ enable: enable edge ■ disable: disable edge

Default

NA

Command Mode

Privileged User

Example

This example sets the unit edge to 'auto':

```
(conf-if-FE 5/1)# spanning-tree edge auto
```

spanning-tree point-to-point

This command sets the point-to-point configuration of the interface.

Syntax

```
spanning-tree point-to-point auto
spanning-tree point-to-point enable
spanning-tree point-to-point disable
```

Command	Description
auto/enable/disable	Defines the value as: ■ auto: auto detect ■ enable: enable point-to-point ■ disable: disable point-to-point

Default

NA

Note

Under configure terminal.

Command Mode

Privileged User

Example

This example sets the unit point-to-point to auto:

```
(conf-if-FE 5/1)# spanning-tree point-to-point auto
```

LLDP and LLDP-MED Commands

The Link Layer Discovery Protocol (LLDP) is a Layer-2 protocol that advertises or discovers neighbors on IEEE 802 local area networks.

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that functions between endpoint devices and network devices.

lldp run

This command enables LLDP on LAN ports.

Syntax

```
lldp run
```

Default

NA

Command Mode

Privileged User

Example

This example enables LLDP on LAN ports:

```
(config-data)# lldp run
```

lldp holdtime

This command sets the aging timeout for LLDP peers.

Syntax

```
lldp holdtime <seconds>
```

Command	Description
seconds	Sets the aging timeout for LLDP peers in seconds.

Default

NA

Command Mode

Privileged User

Example

This example sets the aging timeout for LLDP peers to 10 seconds:

```
(config-data)# lldp holdtime 10
```

lldp location

This command sets the device's location.

Syntax

```
lldp location civic
lldp location coordinate
lldp location elin <ELIN emergency number>
lldp location none
```

Command	Description
`location`	■ Use one of the following: ■ civic: Use RFC 4776 civic address ■ coordinate: Use RFC3825 coordinate information ■ elin: Use ELIN emergency number ■ none: No location information

Default

NA

Command Mode

Privileged User

Example

This example enables the use of the RFC 4776 civic address:

```
(config-data)# lldp location civic
```

lldp network-policy

This command sets the LLDP network policy.

Syntax

```
lldp network-policy profile <profile number>
```

Command	Description
`profile number`	■ Defines the profile number (1-4).

Default

NA

Command Mode

Privileged User

Example

This example sets the LLDP network policy profile to 1:

```
(config-data)# lldp network-policy profile 1
```

lldp set-lan-as-client

This command enables LLDP client on its LAN ports.

Syntax

```
lldp set-lan-as-client
```

Default

NA

Command Mode

Privileged User

Example

This example enables LLDP client on its LAN ports:

```
(config-data)# lldp set-lan-as-client
```

lldp timer

This command sets LLDP transmission interval.

Syntax

```
lldp timer <transmission interval>
```

Command	Description
`transmission interval`	■ Defines the transmission interval in seconds.

Default

NA

Command Mode

Privileged User

Example

This example sets the LLDP transmission interval to 10 seconds:

```
(config-data)# lldp timer 10
```

71 Layer-3 Commands

IPv6 Commands

This version provides support for IPv6 (voice and data-routing functionalities) on the MSBR product series. This support is provided only if the Software License Key installed on the device includes the new Feature Key "IPv6" for enabling IPv6.

ipv6 enable

This command provides support for enabling IPv6 per data-router interface. When the IPv6 feature is included in the Software License Key, IPv6 is disabled per interface, by default. An IPv6-disabled interface will not have global IPv6 addresses enabled, nor will it have link-local addresses.

The show data ipv6 route command does not display routes of IPv6 interfaces that are disabled, but the interface is displayed by the show running config command. Configuration of IPv6 addresses can be done at any stage, but will only be active if IPv6 is enabled on the required interface.

Syntax

```
# ipv6 enable
# no ipv6 enable
```

Note

- This command is applicable only to data-router functionality.
- IPv6 support is available only if the installed Software License Key contains the IPv6 Feature Key. This flag does not replace the need of the Feature Key.
- By default, all data interfaces begin with IPv6 disabled.

Command Mode

Privileged User

Example

This example enables IPv6.

```
(config-data)# interface gigabitethernet 0/0
(config-if-GE 0/0)# ipv6 address 2010:18::40:81/640
(config-if-GE 0/0)# ipv6 enable
```

IPv6 Static Routes Commands

The following describes IPV6 Static Routes commands.

ipv6 route

This command provides support for configuring IPv6 static routes (destination prefix).

Syntax

ipv6 route vrf <VRF anme> <IPv6 destination address>/<prefix> <IPv6 gateway address> <interface name> <interface ID> [<metric value>] [track <track ID>] [description <string>]

ipv6 route <IPv6 destination address>/<prefix> [<next hop>] <interface name> <interface ID> [<metric value>] [track <track ID>] [description <string>]

This syntax describes a route that depends also on the source prefix of the packets:

Ipv6 route [vrf <VRF name>] source <IP source prefix>|local-voip destination <IP destination prefix> [<next hop>] <interface type> <interface ID> [<metric value>] [track <track ID>] [output-vrf <name>] [description <string>]

Command	Description
`VRF Name`	Defines the vrf name.
`IPv6 source prefix or local-voip`	Defines the IP source prefix as X:X::X:X/M MSBR in single network mode can also be set with local-voip to define the route source address to all VoIP packets generated locally by the MSBR
`IPv6 destination prefix`	Defines an IPv6 prfix as X:X::X:X/M.
`next hop`	Defines the next hop for routing
`metric value`	Defines the priority (0 - 255) of the route in the routing table. The smaller the value, the higher the priority of the route.
`track id`	Defines the option to make the route dependable on the configured track. (1-100). Up to two tracking objects can be configured (`track <first track number> track <second track number>`) and in this scenario, the route will only be active if both

Command	Description
	tracking objects are in "up" state.
output-vrf	Defines the outout vrf, for route leaking between vrfs.
description	Defines a route description.

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Interface	Description
a.b.c.d	Defines the IP address.

Note

- This command is applicable only to data-router functionality.
- IPv6 support is available only if the installed Software License Key contains the IPv6 Feature Key.

Command Mode

Privileged User

Example

- This example configures an IPv6 static route.

```
(config-data)# ipv6 route 2001:10::/64 2050:8:: GigabitEthernet 0/0 1
```

- The IPv6 static route can be displayed using the regular show running-config command or the following new IPv6 command:

```
# show data ipv6 route [<ipv6-address[prefix]>] [connected] [kernel] [static]
[summary]
```

ipv6 access-list

This command adds an access list entry.

Syntax

```
# ipv6 access-list resequence <ipv6 access-list name> <starting rule number>
<step size>

# ipv6 access-list extended <extended IPv6 access-list number>

# ipv6 access-list <access-list ID> {deny|permit} <protocol> <address1>
<address2>

# ipv6 access-list <access-list ID> {deny|permit} <protocol> <address1>
<address2> <port desc>

# ipv6 access-list <access-list ID> {deny|permit} <protocol> <address1>
<address2> <port desc> <postacl>
```

Command	Description
`starting rule number`	Defines the starting rule number [1-2147483647].
`step size`	Defines the step size.
`protocol`	Can be any of the following: ■ tcp ■ udp ■ ah

Command	Description
	■ esp ■ gre ■ icmp ■ igmp ■ ipv6 ■ [0-255] ipv6 protocol number
address1	Can be any of the following: ■ any - any host ■ host – single host ■ local ■ A:B:C::D/P - Defines the network IPv6 address and prefix.
address2	Can be any of the following: ■ any ■ host ■ local ■ A:B:C::D/P - Defines the network IPv6 address and prefix ■ eq ■ range
port desc	Can be any of the following: ■ eq - Defines a single port ■ range - Defines a range of ports ■ dscp - Match by Differentiated Services Code Point value and mask ■ established - Accept connection ■ log - Log matches ■ stateless - Accept packet
port number	Defines the port number [1-65535].

Command	Description
`extended IPv6 access-list number`	Defines the extended IPv6 access-list number in number (100-9999) or word format.
`postacl`	■ dscp - Match by Differentiated Services Code Point value and mask ■ established - Accept connection ■ log - Log matches ■ stateless - Accept packet

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example adds an access list entry.

```
(config-data)# ipv6 access-list extended 100
```

Acquiring IPv6 Address from DHCPv6 Server

ipv6 address dhcp

This command provides support for configuring the device as a DHCPv6 client to obtain an IPv6 address from a DHCPv6 server, according to RFC 3315. The device as a DHCPv6 client also supports the Rapid Commit option. This option lets the device quickly obtain configuration parameters from the DHCP server through a rapid two-message exchange (solicit, reply), instead of the usual four-message exchange (solicit, advertise, request, reply).

Use no ipv6 address to disable this command.

Syntax

```
# ipv6 address dhcp [rapid-commit]
# no ipv6 address
```

Note

- This command is applicable only to data-router functionality.
- The installed Software License Key must contain the IPv6 Feature Key.
- Rapid Commit must be supported and enabled on the DHCP server as well.
- The received IPv6 address can be viewed using the show data interfaces <interface> command.

Command Mode

Privileged User

Example

This example configures the device as a DHCPv6 client.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 address dhcp
```

Acquiring IPv6 Address from Router Advertisement

ipv6 address autoconfig

This command provides support for automatically acquiring an IPv6 address using stateless auto-configuration on a specified WAN interface. This is instead of using a DHCPv6 server for acquiring an IPv6 address.

Syntax

```
# ipv6 address autoconfig
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example automatically acquires an IPv6 address.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 address autoconfig
```

IPv6 Prefix Delegation

ipv6 nd pd

This command sets the IPv6 Prefix Delegation (PD). Use the no form of this command to remove the prefix from database.

Syntax

```
# ipv6 nd pd <interface> <no-import-to-ra>

# no ipv6 pd
```

Command	Description
<interface>	Configures the WAN interface from which the PD is received.
<no-import-to-ra>	Prefix from PD is added to DHCP server only (and not to RA).

Note

- This command is applicable only to data-router functionality.
- The IPv6 prefix must be /64.
- Prefix from PD added to DHCP server only:

```
ipv6 nd pd GigabitEthernet 0/0 ::2:0:0:0:0/64 no-import-to-ra
```

- Prefix from PD added to RA and DHCP server:

```
ipv6 nd pd GigabitEthernet 0/0 ::2:0:0:0:0/64
```

Command Mode

Privileged User

Example

This example sets the IPv6 PD.

```
(config-data)# interface VLAN 99
(conf-if-VLAN 99)# ipv nd pd gig 0/0 1::1/64 no-import-to-ra
```

IPv6 Router Advertisement Daemon Commands

This command provides support for the Router Advertisement Daemon for automatic configuration of IPv6 addresses, according to RFC 4861. The IPv6 Router Advertisement (RA) implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes, using the Neighbor Discovery Protocol (NDP), as specified in RFC 4861. The RA process is used for stateless auto-configuration of network hosts on IPv6 networks.

ipv6 nd managed-config-flag

This command sets the advertised "Managed address configuration" flag, which indicates hosts should use DHCPv6 for address configuration.

The no option sets the value to default (0).

Syntax

```
# ipv6 nd managed-config-flag
# no ipv6 nd managed-config-flag
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example sets the advertised "Managed address configuration" flag.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 nd managed-config-flag
```

ipv6 nd ns-interval

This command sets the advertised “Retrans Timer” (interval between retransmitted Neighbor Solicitation messages) value. The no option disables retransmit advertisements.

Syntax

```
# ipv6 nd ns-interval <1000-3600000 msec>
# no ipv6 nd ns-interval
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example sets the advertised "Retrans Timer" value.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 nd ns-interval 1000
```

ipv6 nd other-config-flag

This command sets the advertised "Other configuration" flag (indicating hosts should use DHCPv6 for non-IPv6 address, e.g., NTP address). The no option sets the value to the default (0).

Syntax

```
# ipv6 nd other-config-flag
# no ipv6 nd other-config-flag
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example sets the advertised "Other configuration" flag.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 nd other-config-flag
```

ipv6 nd prefix

This command sets the IPv6 prefix. Use the no form of this command to remove the prefix from database.

Syntax

```
# ipv6 nd prefix <prefix> <default> <no-import-to-dhcps> <valid lifetime>
<preferred lifetime> <no-advertise> <on-link|off-link> <infinite> <no-
autoconfig|autonomous>

# no ipv6 nd prefix
```

Command	Description
`<prefix>`	Configures the IPv6 Routing Prefix Advertisement
`<default>`	Configures default timers (`valid lifetime` is 86400 sec and `preferred lifetime` is 14400 sec) and the prefix is added to Router Advertisement (RA) and DHCP server (without `no-import-to-dhcps`).
`<no-import-to-dhcps>`	Prefix is added only to RA.
`<valid lifetime>`	The valid range is 0-4294967295 seconds (default 86400). It can have the symbolic value of 'infinity'.
`<infinite>`	Configures `valid lifetime` for the first `infinite`, and `preferred lifetime` for the second `infinite` (if added).
`<preferred lifetime>`	The valid range is 0-4294967295 seconds (default 14400). It can have the symbolic value of 'infinity'.
`<off-link>`	Do not use `prefix` for on-link determination
`<no-autoconfig>`	Do not use `prefix` for auto-configuration

Note

- This command is applicable only to data-router functionality.
- The IPv6 prefix must be /64.
- The off-link and no-autoconfig parameters can appear in any combination. Both parameters can have the symbolic 'infinity' value.

Command Mode

Privileged User

Example

This example sets the IPv6 prefix.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 nd prefix 8/64 10000 50000 on-link autonomous
```

ipv6 nd prefix <X:X::X:X> no-advertise

This command saves this prefix, but does not advertise it. The no option means the device advertises the prefix (default):

Syntax

```
# ipv6 nd prefix <X:X::X:X> no-advertise
# no ipv6 nd prefix
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example saves the IPv6 prefix but does not advertise it.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 nd prefix 0:1::2:5 no advertise
```

ipv6 nd ra

The no version of this command removes the RA parameters from the database.

Syntax

```
# no ipv6 nd ra
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example removes the RA parameters from the database.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# no ipv6 nd ra
```

ipv6 nd ra lifetime

This command sets the advertised “Router Lifetime” value.

Syntax

```
#  ipv6 nd ra lifetime <0-9000 sec (default 1800)>
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example sets the advertised “Router Lifetime” value.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 nd ra lifetime 5000
```

ipv6 nd ra interval

This command sets the IPv6 Router Advertisement minimum / maximum interval.

Syntax

```
# ipv6 nd ra interval <4-1800 sec>
# ipv6 nd ra interval <4-1800 sec> <[3-(0.75*MaxRAInterval) sec]>
```

Note

- This command is applicable only to data-router functionality.
- The minimum interval is set to 0.33 x maximum interval.

Command Mode

Privileged User

Example

This example sets the IPv6 Router Advertisement maximum interval..

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 nd ra interval 180
```

ipv6 nd ra propagate-mtu

This command informs the LAN interface which WAN interface's MTU size to use in the IPv6 Router Advertisement message. This is configured on the LAN interface.

Syntax

```
# ipv6 nd ra propagate-mtu <WAN Interface Name>
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example uses the MTU of the Gigabit Ethernet WAN interface for the IPv6 Router Advertisement.

```
(config-data)# interface vlan 1
(conf-if-VLAN 1)#ipv6 nd ra propagate-mtu gigabitethernet 0/0
```

ipv6 nd ra suppress

This command suppresses IPv6 Router Advertisements. The no version of this command enables IPv6 Router Advertisements.

Syntax

```
# ipv6 nd ra suppress
# no ipv6 nd ra suppress
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example suppresses IPv6 Router Advertisements.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 nd ra suppress
```

ipv6 nd reachable-time

This command sets the advertised “Reachability time” (time a neighbor is considered reachable after receiving a reachability confirmation) value. The no option sets the value to default (0).

Syntax

```
# ipv6 nd reachable-time <0-3600000 msec>
# no ipv6 nd reachable-time
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example sets the advertised “Reachability time" value.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 nd reachable-time 2000
```

ipv6 nd router-preference

This command sets advertised “Router preference” value. The no option sets the value to default (Medium).

Syntax

```
# ipv6 nd router-preference {High|Low|Medium (default)}
# no ipv6 nd router-preference
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example sets the advertised “Router preference" value.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 nd router-preference High
```

interface

This command enters the WAN interface that is connected to the WAN. The DHCPv6 client's default behavior is to set a default route through the interface running the client and connected to DHCPv6 server. However, that behavior can be overridden by the following CLI commands:

Syntax

```
# interface <WAN interface>
```

Command Mode

Privileged User

Example

In this example, a host is connected to the LAN interface of MSBR on VLAN 1 and the auto-created default route is cancelled.

```
MSBR# configure data
MSBR(config-data)# interface vlan 1
MSBR(conf-if-VLAN 1)# no ipv6 nd autoconfig default-route
```

QoS Commands

The QoS Configuration commands include the following:

bandwidth (queue)

This command sets the maximum bandwidth of a queue.

Syntax

```
bandwidth <minimum bandwidth in kbps>
bandwidth <minimum bandwidth in kbps> <maximum bandwidth in kbps>
bandwidth percent <minimum bandwidth in percent>
bandwidth percent <minimum bandwidth in percent> <maximum bandwidth in percent>
```

Command	Description
`minimum bandwidth in kbps`	Defines the minimum bandwidth of the queue in kbps.

Command	Description
`maximum bandwidth in kbps`	Defines the maximum bandwidth of the queue in kbps.
`minimum bandwidth in percent`	Defines the minimum bandwidth of the queue in percent (0-100).
`maximum bandwidth in percent`	Defines the maximum bandwidth of the queue in percent (0-100).

Default

NA

Command Mode

Privileged User

Example

This example configures the wan output service map default queue minimum bandwidth to 60 percent of bandwidth and maximum bandwidth to 80 percent of bandwidth.

```
(conf-s-map-q)# bandwidth percent 60 80
```

bandwidth (service-map)

This command sets the maximum bandwidth of a service-map.

Syntax

```
bandwidth <bandwidth in kbps>
bandwidth unlimited
bandwidth automatic
```

Command	Description
`< bandwidth in kbps >`	Defines the maximum bandwidth of the service-map.
`unlimited`	Defines the bandwidth is unlimited.
`automatic`	Defines the bandwidth is set automatically.

Default

NA

Command Mode

Privileged User

Example

This example configures the wan output service map maximum bandwidth to 100000 kbps.

```
(conf-s-map)# bandwidth 100000
```

qos match-map

This command enters a specific match-map configuration. Use the no form of this command to delete a specific match-map.

Syntax

```
qos match-map input <match-map name> <interface type> <interface ID>
qos match-map output <match-map name> <interface type> <interface ID>
```

Command	Description
match-map name	Defines the name of the match map to configure
interface type interface ID	Defines the interface type and ID, as described in the below table.

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]

Interface Type (ifname)		Interface ID
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

This example enters a specific match-map input configuration that applies only to Gigabit Ethernet 0/0:

```
(config data)# qos match-map input sip_incoming gigabitethernet 0/0
```

This example enters a specific match-map input configuration that applies only to VLAN ID 7:

```
(config-data)# qos match-map output sip_outgoing vlan 7
```

match priority

This command defines the priority to match on the specified match-map. Use the no form of this command to remove a match priority.

Syntax

```
match priority <priority value>
```

Command	Description
priority value	Defines a priority value to match (0-7).

Default

NA

Command Mode

Privileged User

Example

This example configures the priority 5 match-map to match traffic with priority value 5.

```
# configure data
(config-data)# qos match-map input qqq gigabitethernet 0/0
(conf-m-map)# match priority 5
```

match precedence

This command defines the precedence to match on the specified match-map. Use the no form of this command to remove a match precedence.

Syntax

```
match precedence routine
match precedence priority
match precedence network
match precedence internet
match precedence immediate
match precedence flash-override
match precedence flash
match precedence critical
match precedence <precedence value>
```

Command	Description
routine	Matches packets with routine precedence (0).
priority	Matches packets with priority precedence (1).

Command	Description
network	Matches packets with network control precedence (7).
internet	Matches packets with internetwork control precedence (6).
immediate	Matches packets with immediate precedence (2).
flash-override	Matches packets with flash override precedence (4).
flash	Matches packets with flash precedence (3).
critical	Matches packets with critical precedence (5).
<precedence value>	Defines the precedence value (0-7).

Default

NA

Command Mode

Privileged User

Examples:

This example configures the precedence match-map to match traffic with flash precedence (3):

```
(conf-m-map)# match precedence flash
```

match length packet

This command defines the packet length to match on the specified match-map. Use the no form of this command to remove a match packet length.

Syntax

```
match length packet <min packet length> <max packet length>
```

Command	Description
min packet length	Defines the minimum packet length in bytes to match.
max packet length	Defines the maximum packet length in bytes to match.

Default

NA

Command Mode

Privileged User

Examples:

This example configures the match-map to match traffic with packet length between 40 to 150 bytes.

```
(conf-m-map)# match length packet 40 150
```

match length data

This command defines the data length to match on the specified match-map. Use the no form of this command to remove a match data length.

Syntax

```
match length data <min data length> <max data length>
```

Command	Description
`min data length`	Defines the minimum data length in bytes to match.
`max data length`	Defines the maximum data length in bytes to match.

Default

NA

Command Mode

Privileged User

Examples:

This example configures the match-map to match traffic with data length between 40 to 150 bytes.

```
(conf-m-map)# match length data 40 150
```

match dscp

This command defines the dscp to match on the specified match-map. Use the no form of this command to remove a match dscp.

Syntax

```
match dscp ef
match dscp default
match dscp cs7
match dscp cs6
match dscp cs5
match dscp cs4
match dscp cs3
match dscp cs2
match dscp cs1
match dscp af43
match dscp af42
match dscp af41
match dscp af33
match dscp af32
match dscp af31
match dscp af23
match dscp af22
match dscp af21
match dscp af13
match dscp af12
match dscp af11
match dscp <dscp value>
```

Command	Description
ef	Matches packets with EF dscp (101110)
default	Matches packets with default dscp (000000)
cs7	Matches packets with CS7(precedence 7) dscp (111000)
cs6	Matches packets with CS6(precedence 6) dscp (110000)
cs5	Matches packets with CS5(precedence 5) dscp (101000)
cs4	Matches packets with CS4(precedence 4) dscp (100000)
cs3	Matches packets with CS3(precedence 3) dscp (011000)

Command	Description
cs2	Matches packets with CS2(precedence 2) dscp (010000)
cs1	Matches packets with CS1(precedence 1) dscp (001000)
af43	Matches packets with AF43 dscp (100110)
af42	Matches packets with AF42 dscp (100100)
af41	Matches packets with AF41 dscp (100010)
af33	Matches packets with AF33 dscp (011110)
af32	Matches packets with AF32 dscp (011100)
af31	Matches packets with AF31 dscp (011010)
af23	Matches packets with AF23 dscp (010110)
af22	Matches packets with AF22 dscp (010100)
af21	Matches packets with AF21 dscp (010010)
af13	Matches packets with AF13 dscp (001110)
af12	Matches packets with AF12 dscp (001100)
af11	Matches packets with AF11 dscp (001010)
dscp value	Defines the differentiated services codepoint value (0-63).

Default

NA

Command Mode

Privileged User

Example

This example configures the dscp match-map to match traffic with AF31 dscp (011010).

```
(conf-m-map)# match dscp af31
```

match any

This command configures the specified match-map to match any packet.

Syntax

```
match any
```

Default

NA

Command Mode

Privileged User

Example

This example configures the match-map to match any packet.

```
(conf-m-map)# match any
```

match access-list

This command defines the access-list to match on the specified match-map. Use the no form of this command to remove a match access list.

Syntax

```
match access-list <access-list name>
```

Command	Description
< access-list >	Defines the name of the access-list this match-map should match.

Default

NA

Command Mode

Privileged User

Example

This example configures the sip_incoming match-map to match traffic from access-list acl_sip.

```
(conf-m-map)# match access-list acl_sip
```

set queue

This command defines the queue to set on the specified match-map. Use the no form of this command to remove a set queue.

Syntax

```
set queue <queue name>
```

Command	Description
`queue name`	Defines the queue name that all traffic that matches this match-map belongs to.

Default

NA

Command Mode

Privileged User

Example

This example configures the sip_incoming match-map to belong to the sip_queue queue.

```
# configure data
(config-data)# qos match-map input mmap3
(conf-m-map)# set queue sip_queue
```

qos service-map

This command enters a specific service-map configuration.

Syntax

```
qos service-map lan input
qos service-map lan output
qos service-map gigabitethernet <slot/port> {input|output}
qos service-map atm <slot/port> {input|output}
qos service-map cellular <slot/port> {input|output}
qos service-map efm <slot/port> {input|output}
qos service-map serial <slot/port> {input|output}
qos service-map multilink <1-255> {input|output}
qos service-map fiber <slot/port> {input|output}
```

Command	Description
`input`	Defines inbound traffic.
`output`	Defines outgoing traffic.
`slot/port`	Defines the interface slot and port.

Default

NA

Command Mode

Privileged User

Example

This example enters a LAN output service map.

```
(config-data)# qos service-map lan output
```

qos priority-retain

This command, when enabled, does not adjust 802.1p priority bits per the DSCP values.

Syntax

```
qos priority-retain
```

Default

NA

Command Mode

Privileged User

Example

This example does not adjust 802.1p priority bits per the DSCP values.

```
(config-data)# qos priority-retain
```

set precedence

This command defines the precedence to set on the specified match-map. Use the no form of this command to remove a set precedence.

Syntax

```
set precedence routine
set precedence priority
set precedence network
set precedence internet
set precedence immediate
set precedence flash-override
set precedence flash
set precedence critical
set precedence <precedence value>
```

Command	Description
routine	Matches packets with routine precedence (0).
priority	Matches packets with priority precedence (1).
network	Matches packets with network control precedence (7).
internet	Matches packets with internetwork control precedence (6).
immediate	Matches packets with immediate precedence (2).
flash-override	Matches packets with flash override precedence (4).
flash	Matches packets with flash precedence (3).
critical	Matches packets with critical precedence (5).

Command	Description
`precedence value`	Defines the Precedence value (0-7).

Default

NA

Command Mode

Privileged User

Examples:

This example configures the precedence match-map to set traffic that matches this match-map to the flash precedence (3):

```
# configure data
(config-data)# qos match-map input mmap2
(conf-m-map)# set precedence flash
```

set dscp

This command defines the dscp to set on the specified match-map. Use the no form of this command to remove a set dscp.

Syntax

```
set dscp ef
set dscp default
set dscp cs7
set dscp cs6
set dscp cs5
set dscp cs4
set dscp cs3
set dscp cs2
set dscp cs1
set dscp af43
set dscp af42
set dscp af41
set dscp af33
set dscp af32
set dscp af31
set dscp af23
```

```
set dscp af22
set dscp af21
set dscp af13
set dscp af12
set dscp af11
set dscp <dscp value>
```

Command	Description
ef	Matches packets with EF dscp (101110).
default	Matches packets with default dscp (000000).
cs7	Matches packets with CS7(precedence 7) dscp (111000).
cs6	Matches packets with CS6(precedence 6) dscp (110000).
cs5	Matches packets with CS5(precedence 5) dscp (101000).
cs4	Matches packets with CS4(precedence 4) dscp (100000).
cs3	Matches packets with CS3(precedence 3) dscp (011000).
cs2	Matches packets with CS2(precedence 2) dscp (010000).
cs1	Matches packets with CS1(precedence 1) dscp (001000).
af43	Matches packets with AF43 dscp (100110).
af42	Matches packets with AF42 dscp (100100).
af41	Matches packets with AF41 dscp (100010).
af33	Matches packets with AF33 dscp (011110).
af32	Matches packets with AF32 dscp (011100).
af31	Matches packets with AF31 dscp (011010).
af23	Matches packets with AF23 dscp (010110).
af22	Matches packets with AF22 dscp (010100).
af21	Matches packets with AF21 dscp (010010).
af13	Matches packets with AF13 dscp (001110).
af12	Matches packets with AF12 dscp (001100).

Command	Description
af11	Matches packets with AF11 dscp (001100).
< dscp value>	Defines the differentiated services codepoint value (0-63).

Default

NA

Command Mode

Privileged User

Example

This example configures the dscp match-map to set traffic that matches this match-map to the AF31 dscp (011010):

```
# configure data
(config-data)# qos match-map input mmap2
(conf-m-map)# set dscp af31
```

set priority

This command defines the priority to set on the specified match-map. Use the no form of this command to remove a set priority.

Syntax

```
set priority <priority value>
```

Command	Description
< priority value>	Defines the priority value. The range is between 0-7.

Default

NA

Command Mode

Privileged User

Example

This example configures the match-map priority value to 5.

```
# configure data
(config-data)# qos match-map input mmap3
(conf-m-map)# set priority 5
```

policy

This command defines the policy of the specified queue.

Syntax

```
policy fairness
policy fifo
policy random-detect
policy strict-priority
```

Command	Description
`fairness`	Defines that the queue is configured with fairness policy.
`fifo`	Defines that the queue is configured with first in first out policy.
`random-detect`	Defines that the queue is configured with random early detection policy.
`strict-priority`	Defines that the queue is configured with strict scheduling priority policy.

Default

NA

Command Mode

Privileged User

Example

This example configures the wan output service map policy to fifo.

```
(conf-s-map-q)# policy fifo
```

priority

This command defines the priority to set on the specified queue.

Syntax

```
priority <priority value>
```

Command	Description
`priority value`	Defines the priority value in the range of 0 to 7.

Default

NA

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example configures the wan output service map priority to 4.

```
(conf-s-map-q)# priority 4
```

queue

This command enters a specific queue configuration. Use the no form of this command to delete a specific queue.

Syntax

```
queue <queue name>
queue default
```

Command	Description
`queue name`	Defines the name of the queue to configure.

Command	Description
default	Defines the behavior of traffic when it doesn't match any queue.

Default

NA

Command Mode

Privileged User

Example

This example enters a wan output service map queue called sip_wan_outgoing configuration menu.

```
(conf-s-map)# queue sip_wan_outgoing
```

This example enters a lan output service map default queue configuration menu.

```
(conf-s-map)# queue default
```

priority

This command provides support for scenarios where the device is used as a bridging device (Layer 2) and IEEE 802.1p priority marking for the bridged traffic is required. When this is used, outgoing packets belonging to a specified VLAN interface are marked with the configured priority value.

Syntax

```
priority <priority level>
```

Command	Description
priority level	Defines the priority level which can be any value from 0 (lowest) through 7 (highest).

Default

NA

Command Mode

Privileged User

Example

This example sets the priority level to "7".

```
(config-data)# interface vlan 1
(conf-if-VLAN 1)# priority 7
```

wfq_mode

This command defines how Weighted Fair Queuing (WFQ) is displayed (bytes, percentage, or weight).

Syntax

```
wfq_mode {bytes|percent|weight}
```

Command	Description
`bytes`	WFQ is displayed in bytes.
`percentage`	WFQ is displayed in percentage.
`weight`	WFQ is displayed in weight.

Default

`weight`

Command Mode

Privileged User

Note

The command is applicable only to Mediant 500Li and Mediant 800Ci.

Example

This example configures WFQ to be displayed in percentage:

```
(config-data)# qos service-map gigabitethernet 0/0 output(conf-s-map)# wfq_mode
percent
```

Data Routing Commands

Each routing protocol is available only if it is included in the Feature key supplied with the system.

Border Gateway Protocol (BGP) is the main routing protocol of the Internet. It is used to distribute routing information among Autonomous Systems. (For more information, refer to the protocol's RFC at http://www.ietf.org/rfc/rfc1771.txt).

Open Shortest Path First Protocol (OSPF) is an Interior Gateway Protocol (IGP) used to distribute routing information within a single Autonomous System. (For more information, refer to the protocol's RFC at http://www.ietf.org/rfc/rfc2328.txt.)

The feature's routing engine is based on the Quagga GNU routing software package. By using the BGP and OSPF protocols, this routing engine enables the device to exchange routing information with other routers within and outside an Autonomous System.

Static Routing Commands

Static Routing occurs when the router uses pre-defined, user-configured routing entries to forward traffic. Static routes are usually manually configured by the network administrator and added to the routing table.

A common use of static routes is for providing an instruction on how to forward traffic when no other route exists.

Static routes have a much lower administrative distance in the system than the dynamic routing protocols, and in most scenarios are prioritized over the dynamic routes.

ip route ip address

This command configures routing rules.

Syntax

```
ip route <ip address> <ip destination mask> [next-hop ip address] <interface>
<interface ID> [<metric value>] [track <track id>] [bfd-neighbor <neighbor ID>]
[output-vrf <vrf_id>] [description <string>]
```

Command	Description
`ip address`	Defines IP Destination prefix in the format of a.b.c.d.
`ip`	Defines the IP Destination prefix mask.

Command	Description
`destination mask`	
`interface`	Defines source interface name and id.
`metric`	Defines the metric (priority) value for this route (0-255).
`next-hop`	Defines the next hop for routing
`track`	Defines the track to be used for this route. Up to two tracking objects can be configured (`track <first track number> track <second track number>`) and in this scenario, the route will only be active if both tracking objects are in "up" state.
`output-vrf`	Defines the output vrf name for route leaking between vrfs.
`bfd-neighbor`	Defines the ID of a BFD neighbor to attach the route to.
`desciption`	Define a description name for this route

Interface Type (ifname)		Interface ID
`gigabitethernet`	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
`cellular`	Cellular interface ID	0/0
`gre`	Tunnel GRE ID	[1-255]
`ipip`	Tunnel IPIP ID	[1-255]
`l2tp`	L2TP ID	[0-99]
`pppoe`	PPPoE interface ID	[1-3]
`pptp`	PPTP ID	[0-99]
`vlan`	Vlan ID	[1-3999]
`loopback`	Loopback ID	[1-5]
`bvi`	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

This example adds a route to 10.20.0.0/16 through gateway 10.10.0.1 and interface vlan 1:

```
(config-data)# ip route 10.20.0.0 255.255.0.0 10.10.0.1 vlan 1
```

This example adds a track dependent route:

```
(config-data)# ip route 10.30.5.0 255.255.255.0 10.8.0.1 vlan 4 track 2
```

ip route source

This command configures source-based routing to specific destinations. Source-based routing can include VLANs.

Syntax

```
ip route source  < IP source prefix>|local-voip destination <IP source prefix> [next-hop ip address] <interface> <interface id> [<metric value>] [track <track id>] [bfd-neighbor <neighbor ID>] [output-vrf <vrf_id>] [description <string>]
```

Command	Description
`IP source prefix local-voip`	Defines the IP source prefix (a.b.c.d/p). MSBR in single network mode can also be set with local-voip to define the route source address to all VoIP packets generated locally by the MSBR
`IP source prefix`	Defines the ip destination prefix (a.b.c.d/p)
`next-hop`	Defines the next hop for routing
`metric value`	Defines the metric (priority) value for this route (0-255).
`track id`	Defines the track ID (1-100). Up to two tracking objects can be configured (`track <first track number> track`

Command	Description
	<second track number>) and in this scenario, the route will only be active if both tracking objects are in "up" state.
output-vrf	Defines the output vrf name for route leaking between vrfs.
bfd-neighbor	Defines the ID of a BFD neighbor to attach the route to.
desciption	Define a description name for this route

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Note

This command is applicable to Mediant MSBR devices.

Command Mode

Privileged User

Example

The following are examples of how this command can be used:

```
(config-data) # ip route source 10.3.0.0/16 destination 0.0.0.0/0 10.4.5.0 gre 18
track 5 track 6
```

ip redirects

This command enables Internet Control Message Protocol (ICMP) Redirect messages configuration.

Syntax

```
ip redirects send
ip redirects receive
```

Command	Description
`receive`	Enables receiving ICMP Redirect messages.
`send`	Enables sending ICMP Redirect messages.

Default

NA

Command Mode

Privileged User

Example

This example enables the receiving of ICMP Redirect messages:

```
(config-data)# ip redirects receive
```

ip port-triggering

This command enables the tftp and l2tp port-triggering.

Syntax

```
ip port-triggering {l2tp|tftp}
```

Command	Description
l2tp	Enables l2tp port-triggering.
tftp	Enables tftp port-triggering.

Default

NA

Command Mode

Privileged User

Example

This example enables l2tp port-triggering:

```
(config-data)# ip port-triggering l2tp
```

ip port-map

This command enables Application-Level Gateway (ALG) configuration commands.

Syntax

```
ip port-map sip disable
ip port-map sip <start_dest_port> [end_dest_port]
ip port-map rtsp disable
ip port-map rtsp <start_dest_port> [end_dest_port]
ip port-map pptp disable
ip port-map pptp <start_dest_port> [end_dest_port]
ip port-map msn disable
ip port-map msn <start_dest_port> [end_dest_port]
ip port-map mgcp disable
ip port-map mgcp <start_dest_port> [end_dest_port]
ip port-map l2tp disable
ip port-map l2tp <start_dest_port> [end_dest_port]
ip port-map ike disable
ip port-map ike <start_dest_port> [end_dest_port]
ip port-map h323_ras disable
```

```
ip port-map h323_ras <start_dest_port> [end_dest_port]
ip port-map h323_cs disable
ip port-map h323_cs <start_dest_port> [end_dest_port]
ip port-map ftp disable
ip port-map ftp <start_dest_port> [end_dest_port]
ip port-map dns disable
ip port-map dns <start_dest_port> [end_dest_port]
ip port-map dhcpv6 disable
ip port-map dhcp disable
ip port-map aim disable
ip port-map aim <start_dest_port> [end_dest_port]
```

Command	Description
start_dest_port	Defines the Destination Port (1-65535).
end_dest_port	Defines the End Destination Port (1-65535).

Default

NA

Command Mode

Privileged User

Example

The following is an example of how this command is used:

```
(config-data)# ip port-map sip 1000 1200
```

Dynamic Routing Commands

The following commands relate to Dynamic Routing.

router bgp vrf

This command enables a BGP protocol process with the specified asn.

Syntax

```
router bgp [vrf <VRF name>] <AS Number> [view <view name>]
no router bgp asn
```

Command	Description
VRF name	Defines the VRF name.
AS number	Defines the Autonomous System number (1 - 65355).
View name	Defines the viewname.

Default

NA

Command Mode

Privileged User

Example

This example enables the BGP protocol process with the specified ASnumber.

```
(config data)# router bgp vrf qwsa 100 view vname
```

ip as-path

This command defines a new as-path access list.

Syntax

```
ip as-path [vrf <VRF name>]  access-list word {permit|deny} line
ip as-path access-list word {permit|deny}line

no ip as-path access-list word
no ip as-path access-list word {permit|deny}line
```

Command	Description
VRF name	Defines the VRF name.
word	Defines the regular expression access list name.
permit	Specifies packets to forward.
deny	Specifies packets to reject.
line	Defines regular expression to match the BGP as-path.

Default

NA

Command Mode

Privileged User

Example

This example defines a new as-path access list.

```
(config data) # ip as-path access-list acc_list1 permit line 1
```

ip community-list

This command adds a community list entry.

Syntax

```
ip community-list [vrf <VRF name>] <community list number standard>
{permit|deny} [AA:NN]
ip community-list <community list number expanded> {permit|deny} line
ip community-list expanded name {permit|deny} line
ip community-list standard name {permit|deny} [AA:NN]
no ip community-list community-option
```

Command	Description
VRF name	Defines the VRF name.
community list number standard	Defines community list number standard [1-99]
community list number expanded	Defines community list number expanded [100-500]
expanded	Adds an expanded community list entry.
standard	Adds a standard community list entry.
name	Defines a community list name.
line	Defines an ordered list as a regular expression.

Command	Description
permit	Specifies a community to accept.
deny	Specifies a community to reject.

Default

NA

Command Mode

Privileged User

Example

This example adds a community list entry.

```
(config data) # ip community-list standard comm1 permit
```

ip extcommunity-list standard

This command defines a new standard extcommunity-list.

Syntax

```
ip extcommunity-list standard name {permit|deny} [AA:NN][AA:NN] [AA:NN]
[AA:NN]
no ip extcommunity-list name
no ip extcommunity-list standard name
```

Command	Description
VRF name	Defines the VRF table name.
name	Defines a community list name.
permit	Specifies a community to accept.
deny	Specifies a community to reject.
AA:NN	Defines the extended community attribute in 'rt aa:nn_or_IPaddr:nn' OR 'soo aa:nn_or_IPaddr:nn' format.

Default

NA

Command Mode

Privileged User

Example

This example defines a new standard extcommunity-list.

```
(config data) ip extcommunity-list standard comm1 permit
```

ip extcommunity-list vrf

This command defines a new standard extcommunity-list, associated with a defined VRF.

To delete the extended community list, use the no form of this command.

Syntax

```
ip extcommunity-list vrf <VRF name> <standard list number> {permit|deny}
[AA:NN]

ip extcommunity-list vrf <VRF name> standard <extended list name> {permit|deny}
[AA:NN][AA:NN][AA:NN][AA:NN]

ip extcommunity-list vrf <VRF name> <expanded list number> {permit|deny} [line]

ip extcommunity-list vrf <VRF name> expanded <extended list name>
{permit|deny} [line]

no ip extcommunity-list <VRF name> <standard list number> {permit|deny}
[AA:NN]

no ip extcommunity-list <VRF name> <extended list name> {permit|deny} [line]

no ip extcommunity-list <VRF name> expanded <extended list name>
{permit|deny} [line]

no ip extcommunity-list <VRF name> standard <extended list name> {permit|deny}
[AA:NN]
```

Command	Description
VRF name	Defines the VRF table name.
name	Defines a community list name.
standard list number	Defines a standard list number from 1 to 99 that identifies one or more permit or deny groups of extended communities.
expanded list number	Defines an expanded list number from 100 to 500 that identifies one or more permit or deny groups of extended communities.
extended list name	Defines Extended Community list name.
permit	Specifies a community to accept.
deny	Specifies a community to reject.
AA:NN	Defines the extended community attribute in 'rt aa:nn_or_IPaddr:nn' OR 'soo aa:nn_or_IPaddr:nn' format.
line	Defines an ordered list as a regular-expression.

Default

NA

Command Mode

Privileged User

Example

This example defines a new standard extcommunity-list.

```
(config data) ip extcommunity-list vrf VRF_list1 18 permit 2
```

ip extcommunity-list expanded

This command defines a new expanded extcommunity-list.

Syntax

```
ip extcommunity-list expanded name {permit|deny} line
ip extcommunity-list number-range-1 {permit|deny} line
ip extcommunity-list number-range-2 {permit|deny} line
ip extcommunity-list number-range-1 {permit|deny} [AA:NN][AA:NN] [AA:NN]
[AA:NN]
no ip extcommunity-list expanded name
```

Command	Description
name	Defines a community list name.
permit	Specifies a community to accept.
deny	Specifies a community to reject.
line	Defines a string expression of extended communities attribute.
number-range-1	Defines a community number in AA:NN format or internet|local-AS, no-advertise, no-export - (1 - 99)
number-range-2	Defines a community number in AA:NN format or internet|local-AS, no-advertise, no-export - (100 - 500)
AA:NN	Defines the extended community attribute in 'rt aa:nn_or_IPaddr:nn' OR 'soo aa:nn_or_IPaddr:nn' format.

Default

NA

Command Mode

Privileged User

Example

This example defines a new expanded extcommunity-list.

```
(config data) # ip extcommunity-list expanded commname permit
```

ip pim

This command configures Protocol Independent Multicast (PIM).

Syntax

Sets static RP address for router, should be configured on all related PIM routers.

```
ip pim rp-address <ip> group <Multicast group prefix>
```

Sets router to be a candidate RP, chosen by priority.

Sets router to be a candidate RP, Advertising Interval in seconds.

When the interface is used, the RP candidate will be set to interface IP.

```
ip pim rp-candidate {IP|Interface} priority <0-255> time <0-3600>
```

Sets router to be a BSR candidate, chosen by priority when Interface is used – the BSR candidate will be set to interface IP.

```
ip pim bsr-candidate {IP|Interface}  priority <0-255>
```

Sets threshold for moving to shortest path tree between the multicast server and the client.

- infinity - Never switch to shortest path
- packets – Move to shortest path tree when number of packets threshold was crossed during the specified interval
- rate - Move to shortest path tree when packet rate threshold was crossed during the specified interval

```
ip pim spt-threshold infinity
OR
ip pim spt-threshold packets <number of packets> interval <sec>
OR
ip pim spt-threshold rate <kpps> interval <sec>
```

Default

NA

Command Mode

Privileged User

Example

This is an example of how this command can be used.

```
(config data) ip pim rp-address 10.12.15.91 group 100.1012.15
```

ip prefix-list

This command configures the IPv4 prefix-based filtering mechanism.

Syntax

```
ip prefix-list <prefix list name> {permit|deny}  [a.b.c.d/m|any]
ip prefix-list <prefix list name> description
ip prefix-list <prefix list name> seq <seqnumber> [permit|deny] [a.b.c.d/m|any]
ip prefix-list <prefix list name> [vrf <VRF name>] [seq <prefix-list seq number>]
{permit|deny}<prefix to filter> [le <len>] [ge <len>]
no ip prefix-list <name>
```

Command	Description
a.b.c.d/m	Defines the IP prefix network/length.
any	Defines any prefix match.
description	Defines up to 80 characters describing this prefix-list.
VRF name	Defines the vrf name.
prefix list name	Defines the name of a prefix list.
seqnumber	Defines the sequence number. Range is [1-4294967295].
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
le <len>	The prefix list is applied if the prefix length is less than or equal to the le prefix length. Not used if "prefix to filter" is set to "any" (0-32).
ge <len>	The prefix list is applied if the prefix length is greater than or equal to the ge prefix length. Not used if "prefix to filter" is set to "any"(0-32).

Default

NA

Command Mode

Privileged User

Example

This example configures prefix-based filtering mechanism

```
(config-data)# ip prefix-list iplist permit any
```

ipv6 prefix-list

This command configures the IPv6 prefix-based filtering mechanism.

Syntax

```
ipv6 prefix-list <prefix list name> {deny|permit} [X:X::X:X/M] [le <maximum prefix length> ] [ge <minimum prefix length>]

ipv6 prefix-list <prefix list name> {deny|permit} any

ipv6 prefix-list <prefix list name> description <description field>

ipv6 prefix-list <prefix list name> seq <seqnumber> {deny|permit} [X:X::X:X/M] [le <maximum prefix length> ] [ge <minimum prefix length>]

ipv6 prefix-list <prefix list name> seq <seqnumber> {deny|permit}any

ipv6 prefix-list <prefix list name> vrf <VRF table name> {deny|permit} [X:X::X:X/M] [le <maximum prefix length> ] [ge <minimum prefix length>]

ipv6 prefix-list <prefix list name> vrf <VRF table name> {deny|permit} any

ipv6 prefix-list <prefix list name> vrf <VRF table name> description <description field>

ipv6 prefix-list <prefix list name> vrf <VRF table name> [seq <prefix-list seq number>] {deny|permit} [X:X::X:X/M] [le <maximum prefix length>] [ge <minimum prefix length>]

ipv6 prefix-list <prefix list name> vrf <VRF table name> [seq <prefix-list seq number>] {deny|permit} any

ipv6 prefix-list sequence-number [vrf <VRF table name>]
```

Command	Description
a.b.c.d/m	Defines the IP prefix network/length.
any	Defines any prefix match.
description	Defines up to 80 characters describing this prefix-list.
VRF name	Defines the vrf name.
prefix list name	Defines the name of a prefix list.
seqnumber	Defines the sequence number. Range is [1-4294967295].
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
le <len>	The prefix list is applied if the prefix length is less than or equal to the le prefix length. Not used if "prefix to filter" is set to "any".
ge <len>	The prefix list is applied if the prefix length is greater than or equal to the ge prefix length. Not used if "prefix to filter" is set to "any".

Default

NA

Command Mode

Privileged User

Example

This example configures prefix-based filtering mechanism

```
(config-data)# ip prefix-list iplist permit any
```

key chain

This command configures the key string for RIPv2 authentication

Syntax

```
key chain <name> [vrf <VRF name>]
no router <name>
```

Command	Description
VRF name	Defines the vrf name.
key chain name	Defines the key chain name.

Default

NA

Command Mode

Privileged User

Example

This example configures the key string for RIPv2 authentication.

```
(config-data)# key chain kcname
```

router-id

This command specifies the router ID (as an IP address)

Syntax

```
router-id <a.b.c.d> [vrf <vrf name>]
no ip router-id
```

Command	Description
a.b.c.d	Defines the local IP address
VRF name	Defines the vrf name (up to 64 bytes).

Default

NA

Command Mode

Privileged User

Example

This example specifies the router ID as an IP address.

```
(config-data)# router-id 10.15.4.12
```

aggregate-address

This command specifies an aggregate address for both IPv4 and IPV6.

Syntax

```
aggregate-address a.b.c.d/M
aggregate-address a.b.c.d/m summary-only
aggregate-address a.b.c.d/m summary-only as-set
aggregate-address a.b.c.d/m as-set
aggregate-address a.b.c.d/m as-set summary-only
aggregate-address a.b.c.d a.b.c.d
aggregate-address a.b.c.d a.b.c.d summary-only
aggregate-address a.b.c.d a.b.c.d summary-only as-set
aggregate-address a.b.c.d a.b.c.d as-set
aggregate-address a.b.c.d a.b.c.d as-set summary-only
aggregate-address x:x::x:x/m
```

Command	Description
a.b.c.d	Defines an IPv4 IP address or subnet mask.
a.b.c.d/m	Defines an IPv4 IP address/network prefix.
x:x::x:x/m	Defines an IPv6 aggregate address.
as-set	Resulting routes include As Set.
summary-only	Defines aggregated routes are not announced.

Default

NA

Command Mode

Privileged User

Example

This example specifies an aggregate address.

```
# configure data
(config-data)# router bgp 1
(conf-router)# aggregate-address 10.21.3.150 255.255.0.0
```

redistribute kernel

This command redistributes the kernel route to the BGP process.

Syntax

```
redistribute kernel
```

Default

NA

Command Mode

Privileged User

Example

This example redistributes the kernel route to the BGP process.

```
(config-data)# router bgp 1
(conf-router)# redistribute kernel
```

bgp scan-time

This command configures the background scanner interval.

Syntax

```
bgp scan-time <scanner interval>
```

Command	Description
scanner interval	Defines the scanner interval in seconds (5-60).

Default

NA

Command Mode

Privileged User

Example

This example configures the background scanner interval to 20 seconds.

```
# configure data
(config-data)# router bgp 2
(conf-router)# bgp scan-time (20)
```

bgp network import-check

This command configures BGP to check if the network route exists in IGP.

Syntax

```
bgp network import-check
```

Command Mode

Privileged User

Example

This example specifies an aggregate address.

```
# configure data
(config-data)# router bgp 1
(conf-router)# bgp network import-check
```

bgp router-id

This command overrides the configured router identifier.

Syntax

```
bgp router-id a.b.c.d
```

Command	Description
a.b.c.d	Defines the manually configured router identifier.

Default

NA

Command Mode

Privileged User

Example

This example overrides the configured router identifier.

```
# configure data
(config-data)# router bgp 2
(conf-router)# bgp router-id 10.13.12.2
```

bgp log-neighbor-changes

This command logs BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems.

Syntax

```
bgp log-neighbor-changes
```

Default

NA

Command Mode

Privileged User

Example

This example logs BGP neighbor status changes.

```
# configure data
(config-data)# router bgp 2
(conf-router)# bgp log-neighbor-changes
```

bgp graceful-restart

This command defines graceful restart capability parameters.

Syntax

```
bgp graceful-restart [stalepath-time <delay value>]
```

Command	Description
delay value	Defines the delay value in seconds [1-3600].

Default

NA

Command Mode

Privileged User

Example

This example defines graceful restart capability parameters.

```
# configure data
(config-data)# router bgp 2
(conf-router)# bgp graceful-restart
```

bgp fast-external-failover

This command immediately resets a session if a link to a directly connected external peer goes down.

Syntax

```
bgp fast-external-failover
```

Default

NA

Command Mode

Privileged User

Example

This example resets a session if a link to a directly connected external peer goes down.

```
# configure data
(config-data)# router bgp 2
(conf-router)# bgp fast-external-failover
```

bgp enforce-first-as

This command configures a BGP routing process to remove updates received from external BGP peers that do not list their Autonomous System (AS) number as the first AS path segment in the AS_PATH attribute of the incoming route.

Syntax

```
bgp enforce-first-as
```

Default

NA

Command Mode

Privileged User

Example

This example is an example of how this command is used.

```
# configure data
(config-data)# router bgp 2
(conf-router)# bgp enforce-first-as
```

bgp deterministic-med

This command selects the best Multi_Exit_Disc (MED) path from paths advertised from the neighboring AS.

Syntax

```
bgp deterministic-med
```

Default

NA

Command Mode

Privileged User

Example

This example is an example of how this command is used.

```
# configure data
(config-data)# router bgp 2
(conf-router)# bgp deterministic-med
```

bgp default local-preference

This command configures the default local preference value.

Syntax

```
bgp default local-preference {ipv4-unicast|local-preference <local preference value>}
```

Command	Description
`local preference value`	Defines the default local preference value [0-4294967295].

Default

NA

Command Mode

Privileged User

Example

This example defines the default local preference value.

```
# configure data
(config-data)# router bgp 2
(conf-router)# bgp default local-preference 100
```

bgp dampening

This command enables route-flap dampening. Flapping routes trigger instability in the routing table. Routers running BGP have a mechanism designed to reduce the destabilizing effect of flapping routes.

Syntax

```
bgp dampening
bgp dampening <half life time>
bgp dampening [<half life time>] <re-use limit> [<start suppress> <suppress duration>
```

Command	Description
`half life time`	Defines the amount of time that must pass to decrease the penalty by one half [1-45].
`re-use limit`	Defines the value to start reusing a route [1 – 20000]. This value is compared to the penalty value to resolve route reusability. If the penalty is greater than the suppress limit, the route is suppressed. Otherwise, it is reused.
`start suppress`	Defines the value that specifies the penalty that will be used if a route is suppressed [1 – 20000].
`suppress duration`	Defines the maximum duration in minutes that a route will be suppressed [1-255].

Default

NA

Command Mode

Privileged User

Example

The following is an example of how this command is used.

```
# configure data
(config-data)# router bgp 2
(conf-router)# bgp dampening 1 1000 1000 100
```

bgp confederation peers

This command splits an autonomous system into smaller autonomous systems or combines several autonomous systems into one.

Syntax

```
bgp confederation peers <AS number>
bgp confederation peers <AS number> [<AS number>]
[<AS number>][<AS number>]
```

Command	Description
AS number	Defines the Autonomous System numbers for BGP peers that belong to the confederation [1-65535].

Default

NA

Command Mode

Privileged User

Example

This example specifies four other confederations as members of autonomous system 2.

```
# configure data
(config-data)# router bgp 2
(conf-router)# bgp confederation identifier 65018 65020 65022 65024
```

bgp confederation identifier

This command splits an autonomous system into smaller autonomous systems or combines several autonomous systems into one.

Syntax

```
bgp confederation identifier <AS number>
```

Command	Description
AS number	Defines the Autonomous System numbers for BGP peers that belong to the confederation [1-65535].

Default

NA

Command Mode

Privileged User

Example

This example specifies confederation 200 belongs to autonomous system 18.

```
# configure data
(config-data)# router bgp 200
(conf-router)# bgp confederation identifier 18
```

bgp router-id

This command specifies the router-ID.

Syntax

```
bgp router-id a.b.c.d
no bgp router-id
```

Command	Description
a.b.c.d	Defines the Router Identifier.

Default

Router identifier value is selected as the largest IP address of the interfaces.

Command Mode

Privileged User

Example

This example sets the Router Identifier.

```
(config data) # bgp router-id 10.13.22.130
```

bgp cluster-id

This command configures the Route-Reflector Cluster-id.

Syntax

```
bgp cluster-id [a.b.c.d|Cluster id number]
no bgp cluster-id
```

Command	Description
a.b.c.d	Defines the Route-Reflector Cluster-id in IP address format.
Cluster ID Number	Defines the Route-Reflector Cluster-id as 32 bit quantity - Range [1-4294967295]

Default

Router identifier value is selected as the largest IP address of the interfaces.

Command Mode

Privileged User

Example

This example sets the Cluster ID.

```
(config-data)# router bgp 1
(conf-router)# bgp cluster-id 10.13.22.130
```

bgp client-to-client reflection

This command configures client-to-client route reflection.

Syntax

```
bgp client-to-client reflection
```

Default

NA

Command Mode

Privileged User

Example

This example configures client-to-client route reflection.

```
(config data) # bgp client-to-client reflection
```

bgp bestpath as-path

This command specifies that the length of confederation path sets and sequences that should be taken into account during the BGP best path decision process.

Syntax

```
bgp bestpath as-path {confed|ignore}
```

Command	Description
confed	Compare path lengths including confederation sets & sequences in selecting a route.
ignore	Ignores as-path length when selecting a router.

Default

NA

Command Mode

Privileged User

Example

This example ignores as-path length in selecting a router.

```
(config data) # bgp bestpath as-path ignore
```

bgp bestpath compare-routerid

This command compares the router-id for identical EBGP paths.

Syntax

```
bgp bestpath compare-routerid
```

Default

NA

Command Mode

Privileged User

Example

This example compares the router-id for identical EBGP paths.

```
(config data) # bgp bestpath compare-routerid
```

bgp bestpath med confed

This command allows BGP to select the best path when multiple BGP routes to the same destination exist.

Syntax

```
bgp bestpath med confed [missing-as-worst]
```

Command	Description
missing-as-worst	Treats the missing MED as the least preferred one.

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use the command.

```
(config data) # bgp med confed missing-as-worst
```

bgp bestpath med missing-as-worst

This command treats the missing Multi Exit Discriminator (MED) attribute in a path as having a value of infinity and as the least preferred one.

Syntax

```
bgp bestpath med missing-as-worst [confed]
```

Command	Description
confed	Compares MEDs among confederation paths.

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use the command.

```
(config data) # bgp bestpath med missing-as-worst confed
```

bgp always-compare-med

This command allows comparing MEDs from different neighbors.

Syntax

```
bgp always-compare-med
```

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use the command.

```
(config data) # bgp always-compare-med
```

distance

This command defines an administrative distance.

Syntax

```
distance <admin distance> <a.b.c.d/M>
```

Command	Description
admin distance	Defines the Administrative Distance [1-255].
a.b.c.d/M	Defines the IP source prefix.

Default

NA

Command Mode

Privileged User

Example

This example sets the Administrative Distance to 90.

```
(config data) # distance 90
```

distance bgp

This command allows the use of external, internal, and local administrative distances that could be a better route than other external, internal, or local routes to a node.

Syntax

```
distance bgp <external distance> <internal distance> <local routes>
```

Command	Description
`external distance`	Defines distance for routes external to the AS [1-255].
`internal distance`	Defines distance for routes internal to the AS [1-255].
`local routes`	Defines distance for local routes [1-255].

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use this command.

```
(config data) # distance bgp 200 200 100
```

redistribute static

This command redistributes the static route to the BGP process.

Syntax

```
redistribute static
```

Default

NA

Command Mode

Privileged User

Example

This example redistributes the static route to the BGP process.

```
(config-data)# router bgp 1
(conf-router)# redistribute static
```

redistribute connected

This command redistributes the connected route to the BGP process.

Syntax

```
redistribute connected
redistribute connected route-map <Pointer to route-map entries>
```

Command	Description
`pointer to route-map entries`	Defines the Router Identifier.

Default

NA

Command Mode

Privileged User

Example

This example redistributes the connected route to the BGP process.

```
(config-data)# router bgp 1
(conf-router)# redistribute connected
```

redistribute ospf

This command redistributes the OSPF route to the BGP process.

Syntax

```
redistribute ospf [metric <metric value>] [route-map <string>]
redistribute ospf [route-map <string>] [metric <metric value>]
```

Command	Description
`metric value`	Defines the metric value [0-4294967295].
`route-map string`	Defines the Route Map reference.

Default

NA

Command Mode

Privileged User

Example

This example redistributes the OSPF route to the BGP process.

```
(config-data)# router bgp 1
(conf-router)# redistribute ospf
```

neighbor remote-as

This command creates a new neighbor who's remote -as is as number. This command must be the first command used when configuring a neighbor.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|x:x::x:x} remote-as <AS number>
```

Command	Description
a.b.c.d|x:x::x:x	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
AS number	Defines the AS number <1-65535>.
peer	Defines this field as an IPv4 address.

Default

NA

Command Mode

Privileged User

Note

In all neighbor commands, the neighbor ip-address/word maybe described as peer.

Example

In This example, the router in AS-1, is trying to peer with AS-2 at 10.0.0.1.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.0.0.1 remote-as 2
```

neighbor shutdown

This command shuts down the peer.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|x:x::x:x} shutdown
```

Command	Description
a.b.c.d|x:x::x:x	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

In This example, the peer is shutdown.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.30.5.118 shutdown
```

neighbor enforce-multihop

This command enforces BGP neighbors to perform a multihop.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|x:x::x:x}  enforce-multihop
neighbor string enforce-multihop
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use this command.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.21.5.120 enforce-multihop
```

neighbor dont-capability-negotiate

This command allows not to perform capability negotiation.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} dont-capability-negotiate
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use this command.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.21.5.120 dont-capability-negotiate
```

neighbor disable-connected-check

This command enables one-hop away EBGP peer using a loopback address.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X}  disable-connected-check
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use this command.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.21.5.120 disable-connected-check
```

neighbor ebgp-multihop

This command allows ebgp neighbors that are not on directly connected networks.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} ebgp-multihop
```

Command	Description
`a.b.c.d|X:X::X:X`	Defines the IP address of the neighbor (IPv4 or IPv6).
`neighbor tag`	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This example allows an ebgp neighbor.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.21.5.120 ebgp-multihop
```

neighbor description

This command sets the description of the peer.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} description line
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
line	Defines the neighbor description (up to 80 characters).

Default

NA

Command Mode

Privileged User

Example

This following example sets the description of the peer

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.5.20.110 description main server
```

neighbor fall-over bfd

This command sets BFD for a Border Gateway Protocol (BGP).

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|x:x::x:x} fall-over bfd interval <value> min_rx
<value> multiplier <value>
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).

Command	Description
neighbor tag	Defines the neighbor tag.
interval	Interval (in msec) for outgoing BFD messages. The interval is increased if the remote system requires it.
min_rx	Minimum interval (in msec) between BFD messages. The remote system uses this interval for sending messages in case its interval is lower.
multiplier	Maximum number of packets that can be missed before the session status is considered down.

Default

NA

Command Mode

Privileged User

Example

This example sets BFD for a BGP.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.30.5.118 fall-over bfd interval 1000 min_rx 1000
multiplier 3
```

neighbor version

This command set the BGP version to match a neighbor.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} version version
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
version	Defines the version. It can be either 4 or 4-.

Command	Description
	BGP version 4- is similar but the neighbor speaks the old Internet-Draft revision 00's Multiprotocol Extensions for BGP-4.

Default

4

Command Mode

Privileged User

Example

In This example, the BGP version is set.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.5.20.110 version 4
```

neighbor interface ifname

This command sets up the ifname of the interface used for the connection. This command is deprecated and may be removed in a future release. Its use should be avoided.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} interface ifname
neighbor peer {<neighbor tag>|a.b.c.d|X:X::X:X} interface ifname
```

Command	Description
`a.b.c.d|X:X::X:X`	Defines the IP address of the neighbor (IPv4 or IPv6).
`neighbor tag`	Defines the neighbor tag.
`Ifname`	Defines an Interface name

Default

NA

Command Mode

Privileged User

Example

This example sets up the ifname of the interface used for the connection.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.5.20.100 interface vlan 4
```

neighbor next-hop-self

This command specifies an announced route's next hop as being equivalent to the address of the bgp router.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} next-hop-self
no neighbor peer next-hop-self
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This example specifies an announced route's next hop.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.12.50.103 next-hop-self
```

neighbor update-source

This command specifies the IPv4 source address to use for the BGP session to this neighbor.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} update-source <interface> <interface ID>
neighbor peer {<neighbor tag>|a.b.c.d|X:X::X:X} update-source
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

This example specifies the IPv4 source address to use.

```
(config-data)# router bgp 1
(conf-router)# neighbor 192.168.0.1 update-source vlan2
```

neighbor unsuppress-map

This command selectively advertises routes that were previously suppressed by the aggregate-address command.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} unsuppress-map <map name>
```

Command	Description
`a.b.c.d|X:X::X:X`	Defines the IP address of the neighbor (IPv4 or IPv6).
`map name`	Defines the name of the route map.
`neighbor tag`	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This is an example of how this command can be used.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.14.3.118 unsuppress-map gmap
```

neighbor transparent-nexthop

This command is used to keep the nexthop value of the route, even if the peer is an external BGP peer.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} transparent-nexthop
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This is an example of how this command can be used.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.14.3.11 transparent-nexthop
```

neighbor transparent-as

This command is used to specify not to append your AS path number even if the peer is an external BGP peer.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} transparent-as
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This is an example of how this command can be used.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.14.3.11 transparent-as
```

neighbor timers

This command sets the timers for a specific BGP neighbor. Keepalive messages are sent by a router to inform another router that the BGP connection between the two is still active.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} timers connect <timer>
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X}  timers <keepalive> <holdtime>
```

Command	Description
`a.b.c.d|X:X::X:X`	Defines the IP address of the neighbor (IPv4 or IPv6).
`neighbor tag`	Defines the neighbor tag.
`timer`	Defines the connect timer (0-65535).
`keepalive`	Defines the frequency (in seconds) with which keepalive messages are sent to its peer (0–65535).
`holdtime`	Defines the interval (in seconds) after not receiving a keepalive message (0-65535).

Default

NA

Command Mode

Privileged User

Example

This is an example of how this command can be used.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.14.3.118 timers connect 500
```

neighbor soft-reconfiguration inbound

This command allows inbound soft reconfiguration for a neighbor.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} soft-reconfiguration inbound
```

Command	Description
`a.b.c.d|X:X::X:X`	Defines the IP address of the neighbor (IPv4 or IPv6).
`string`	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This is an example of how this command can be used.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.14.3.118 soft-reconfiguration inbound
```

neighbor default-originate

This command announces default routes to the peer. The BGPD's default is to not announce the default route (0.0.0.0/0) even it is in the routing table.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X}  default-originate [route map <route map name>]
neighbor peer {<neighbor tag>|a.b.c.d|X:X::X:X} default-originate
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor	Defines the neighbor tag.
route map name	Defines the route map name.

Default

NA

Command Mode

Privileged User

Example

This example announces default routes to the peer.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.14.3.118 default-originate
```

neighbor capability route-refresh

This command advertises the route-refresh capability to this neighbor.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} capability route-refresh|dynamic
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} capability orf prefix-list
{both|receive|send}
neighbor peer {<neighbor tag>|a.b.c.d|X:X::X:X} default-originate
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor string	Defines the neighbor tag.
route-refresh	Advertises the route-refresh capability to this neighbor.
dynamic	Advertises the dynamic capability to this neighbor.
orf	Advertises the Outbound Route Filter (ORF) capability to the

Command	Description
	peer.
prefix-list	Advertises the prefix list ORF capability to this neighbor.
both	Enables the capability to SEND and RECEIVE the ORF to/from this neighbor.
receive	Enables the capability to SEND the ORF to this neighbor.
send	Enables the capability to RECEIVE the ORF from this neighbor

Default

NA

Command Mode

Privileged User

Example

This example announces default routes to the peer.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.14.3.118 capability route-refresh
```

neighbor port

This command defines the neighbor's BGP port.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} port <port number>
no neighbor a.b.c.d port <port number>
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
port number	Defines the port number (0 – 65535).

Default

NA

Command Mode

Privileged User

Example

This example defines the neighbor's BGP port.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.14.3.118 port 100
```

neighbor send-community

This command sends the community attribute to the neighbor.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} send-community
{both|stabdard|extended}
neighbor peer {<neighbor tag>|a.b.c.d|X:X::X:X} send-community
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
both	Sends standard and extended community attributes.
standard	Sends standard community attributes.
extended	Sends extended community attributes.

Default

NA

Command Mode

Privileged User

Example

This example sends the community attribute to this neighbor.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.15.3.111 send-community
```

neighbor route-server-client

This command configures a neighbor as a Route Server client.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} route-server-client
```

Command	Description
`a.b.c.d|X:X::X:X`	Defines the IP address of the neighbor (IPv4 or IPv6).
`neighbor tag`	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This example configures a neighbor as a Route Server client.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.15.3.111 route-server-client
```

neighbor route-reflector-client

This command configures a neighbor as a Route Reflector client.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} route-reflector-client
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This example configures a neighbor as a Route Reflector client.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.15.3.111 route-reflector-client
```

neighbor remove-private-AS

This command removes the private AS number from outbound updates.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} remove-private-AS
neighbor string remove-private-AS
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This example removes the private AS number from outbound updates.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.15.3.111 remove-private-AS
```

neighbor weight

This command specifies a default weight value for the neighbor's routes.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} weight weight
neighbor peer {<neighbor tag>|a.b.c.d|X:X::X:X} weight weight
```

Command	Description
`a.b.c.d|X:X::X:X`	Defines the IP address of the neighbor (IPv4 or IPv6).
`neighbor tag`	Defines the neighbor tag.
`weight`	Defines the weight value in the range of 0 – 65535.

Default

NA

Command Mode

Privileged User

Example

This example specifies a default weight value for the neighbor's routes.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.15.5.110 weight 1000
```

neighbor passive

This command enables open messages not to be sent to this neighbor.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} passive
neighbor string passive
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This example enables open messages not to be sent to this neighbor.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.15.5.110 passive
```

neighbor password

This command sets the password for the secured BGP session.

Syntax

```
neighbor {<neighbor tag> | a.b.c.d | X:X::X:X} [password
String]
```

Command	Description
a.b.c.d | X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
password string	Defines password for a neighbor.

Default

NA

Command Mode

Privileged User

Example

This example sets a password for a secured session with neighor 10.15.5.110.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.15.5.110 password 12345678
```

neighbor override-capability

This command enables the override capability negotiation result.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} override-capability
```

Command	Description
`a.b.c.d|X:X::X:X`	Defines the IP address of the neighbor (IPv4 or IPv6).
`neighbor tag`	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This example enables the override capability negotiation result.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.15.5.110 override-capability
```

neighbor maximum-prefix

This command specifies a maximum number of prefixes accepted from this peer.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} <prefix limit>  [<threshold>] [restart <restart interval>|warning-only]
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
prefix limit	Defines the maximum number of prefix limits (1 – 4294967295).
threshhold	Defines the threshold value (%) at which to generate a warning message.
restart interval	Defines the restart interval in minutes (1-65535).
warning only	Enables to only give a warning message when the limit has exceeded.

Default

NA

Command Mode

Privileged User

Example

This example specifies the maximum number of prefixes accepted from this peer.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.15.5.110 maximum-prefix 10000
```

neighbor route-map name

This command applies a route-map on the neighbor.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} route-map name {in|out|export|import}
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
name	Defines the name of the route-map.
in	Applies a map to incoming routes.
out	Applies a map to outbound routes.
export	Applies a map to routes coming from the route-server client.
import	Applies a map to routes going into the client's table.

Default

NA

Command Mode

Privileged User

Example

This example applies a route-map on the neighbor.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.12.5.101 route-map routename in import
```

neighbor peer-group

This command joins a specific peer to peer group word.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} peer-group <peer group name>
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
peer group name	Defines the peer group name.

Default

NA

Command Mode

Privileged User

Example

This example joins a specific peer to group1.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.12.5.101 peer-group group1
```

neighbor local-as

This command specifies a local Autonomous System number.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} local-as <AS number> [no-prepend]
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
AS number	Defines a local AS number (1-65535).
no-prepend	Does not prepend local-as to updates from BGP peers.

Default

NA

Command Mode

Privileged User

Example

This example configures the router to not prepend the Autonomous System number 200 to routes that are received from external peers.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.12.5.10 remote-as 100
(conf-router)# neighbor 10.12.5.10 local-as 200 no-prepend
```

neighbor interface

This command defines the Layer 3 interface.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} interface <if name> <interface ID>
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]

Interface Type (ifname)		Interface ID
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use this command.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.12.5.10 interface gre 100
```

neighbor strict-capability-match

This command strictly compares negotiation match.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} strict-capability-match
neighbor peer {<neighbor tag>|a.b.c.d|X:X::X:X} strict-capability-match
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

This example strictly compares negotiation match.

```
(config-data)# router bgp 1
(conf-router)# neighbor 15.13.4.15 strict-capability-match
```

neighbor attribute-unchanged

This command allows for the BGP attribute to be propagated unchanged to this neighbor.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} attribute-unchanged
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} attribute-unchanged [[as-path] [med] [next-hop]]
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} attribute-unchanged [[as-path] [next-hop] [med]]
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} attribute-unchanged [[next-hop] [as-path][med]]
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} attribute-unchanged [[next-hop] [med] [as-path]]
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} attribute-unchanged [[med] [next-hop] [as-path]]
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} attribute-unchanged [[med] [as-path] [next-hop]]
```

Command	Description
`a.b.c.d|X:X::X:X`	Defines the IP address of the neighbor (IPv4 or IPv6).
`neighbor tag`	Defines the neighbor tag.
`as-path`	Defines the AS-path attribute.
`next-hop`	Defines the Next Hop attribute.
`med`	Defines the Med attribute.

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use this command.

```
(config-data)# router bgp 1
(conf-router)# neighbor 15.13.4.15 attribute-unchanged
```

neighbor allowas-in

This command specifies the number of times that the AS path of a received route may contain the recipient BGP speaker's AS number and still be accepted.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} allowas-in [<number>]
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
number	Defines the number of occurrences of the AS number (1-10)

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use this command.

```
(config-data)# router bgp 1
(conf-router)# neighbor 15.13.4.15 allowas-in 5
```

neighbor advertisement-interval

This command defines the minimum interval between sending BGP routing updates.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} advertisement-interval <time>
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
time	Defines the time in seconds (0-600).

Default

NA

Command Mode

Privileged User

Example

This example sets the minimum interval between sending BGP routing updates to 100.

```
(config-data)# router bgp 1
(conf-router)# neighbor 15.13.4.15 advertisement-interval 100
```

neighbor activate

This command enables the Address Family for the neighbor.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} activate
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use this command.

```
(config-data)# router bgp 1
(conf-router)# neighbor 15.13.4.15 activate
```

neighbor prefix-list name

This command specifies a prefix-list for the peer.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X} prefix-list name {in|out}
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
in	Filters incoming updates.
out	Filters outgoing updates.
name	Defines the name of the prefix list in string format.

Default

NA

Command Mode

Privileged User

Example

This example specifies a prefix-list for the peer.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.15.5.110 prefix-list plist in
```

neighbor filter-list name

This command establishes BGP filters.

Syntax

```
neighbor {<neighbor tag>|a.b.c.d|X:X::X:X}  filter-list name [in|out]
```

Command	Description
a.b.c.d|X:X::X:X	Defines the IP address of the neighbor (IPv4 or IPv6).
neighbor tag	Defines the neighbor tag.
in	Filters incoming updates.
out	Filters outgoing updates.
name	Defines the as-path access list name.

Default

NA

Command Mode

Privileged User

Example

This example establishes BGP filters.

```
(config-data)# router bgp 1
(conf-router)# neighbor 10.15.5.100 filter-list flist in
```

network

This command enables the Address Family for the neighbor.

Syntax

```
network a.b.c.d [backdoor][[mask <network mask>][route-map <route-map name>]
network a.b.c.d/m [backdoor][route-map <route-map name>]
```

Command	Description
a.b.c.d	Defines the IP address of the network.
a.b.c.d/M	Defines the IP prefix network/length.
backdoor	Enables a BGP backdoor route.
mask	Enables a network mask.
route-map	Enables a route-map to modify the attributes.
route-map name	Defines the name of the route-map.
network mask	Defines a network mask in the format of a.b.c.d .

Default

NA

Command Mode

Privileged User

Example

The following is an example of how to use this command.

```
(config-data)# router bgp 1
(conf-router)# network 15.13.4.15 backdoor
```

BGP Protocol

The following commands relate to BGP Protocol.

Route Map Configuration

BGP Route Map Configuration includes the following commands:

route-map

This command configures the order entry in route map name with a match policy of "permit" or "deny".

Syntax

```
route-map <route map name> [vrf <VRF name>] {deny|permit} <order or sequence number of route map>
no route-map <route map name>
```

Command	Description
VRF name	Defines the vrf name.
Route map name	Defines the Route Map name.
order or sequence number of route map	Defines the sequence to insert into/delete from existing route-map entry. Range is [1-65535].

Default

NA

Command Mode

Privileged User

Example

This example configures the order entry in route map rmname.

```
(config-data)# route-map rmname permit 1
```

route-map-static

This command configures the static route-map.

Syntax

```
route-map-static <static route-map tag>
```

Command	Description
static route-map tag	Defines the static route-map tag.

Default

NA

Command Mode

Privileged User

Example

This example configures the static route-map.

```
(config-data)# route-map-static srmap
```

match as-path

This command defines the AS path access-list name.

Syntax

```
match as-path word
```

Command	Description
word	Defines the as-path access-list name.

Default

NA

Command Mode

Privileged User

Example

This example defines the AS path access-list name.

```
(config-data)# route-map rmap permit 1
(conf-router)# match as-path spname
```

set as-path prepend

This command sets the as-path prepend string for the BGP as-path attribute.

Syntax

```
set as-path prepend as-path
```

Command	Description
as-path	Defines the as-number in the range of 1 – 65535.

Default

NA

Command Mode

Privileged User

Example

This example sets the as-path prepend string for the BGP as-path attribute.

```
(config-data)# route-map qqq permit 1
(conf-route-map)# set as-path prepend 1
```

OSPFv2 Protocol

The following describes OSPF Version 2 protocol commands.

General Configuration

OSPF Version 2 is a routing protocol which is described in RFC 2328. OSPF is an IGP (Interior Gateway Protocol). Compared with RIP, OSPF can provide scalable network support and faster convergence times. OSPF is widely used in large networks such as ISP (Internet Service Provider) backbone and networks.

OSPF General Configuration includes the following commands:

router ospf

This command enables or disables the OSPF process.

Syntax

```
router ospf [vrf <VRF name>]
no router ospf
```

Command	Description
VRF name	Defines the VRF name.

Default

NA

Command Mode

Privileged User

Example

This example enables the OSPF process.

```
(config-data)# router ospf
```

OSPF Router Configuration

OSPF Router Configuration includes the following commands:

ospf router-id

This command sets the router-ID of the OSPF process.

Syntax

```
ospf router-id a.b.c.d
no ospf router-id
```

Command	Description
a.b.c.d	Defines the Router-ID in IP address format.

Default

NA

Command Mode

Privileged User

Example

This example sets router-ID of the OSPF process.

```
(config-data)# router ospf
(conf-router)# ospf router-id 10.24.5.100
```

ospf abr-type

This command sets the ospf abr-type.

Syntax

```
ospf abr-type type
no ospf abr-type type
```

Command	Description
no	Disables the router-ID of the OSPF process.
type	Refers to abr-type ■ cisco (according to cisco implementation) ■ ibm (according to IBM implementation) ■ shortcut (shortcut abr) ■ standard (standard behavior RFC 2328) **Note:** "Cisco" and "IBM" types are equivalent.

Default

NA

Command Mode

Privileged User

Example

This example sets the ospf abr-type according to the IBM implementation.

```
(config-data)# router ospf
(conf-router)# ospf abr-type ibm
```

ospf rfc1583compatibility

This command enables the rfc1583compatibility flag.

Syntax

```
ospf rfc1583compatibility
no ospf rfc1583compatibility
```

Default

NA

Command Mode

Privileged User

Example

This example enables the rfc1583compatibility flag.

```
(config-data)# router ospf
(conf-router)# ospf rfc1583compatibility
```

log-adjacency-changes

This command configures OSPF to log changes in adjacency.

Syntax

```
log-adjacency-changes [detail]
no log-adjacency-changes [detail]
```

Default

NA

Command Mode

Privileged User

Example

This example configures OSPF to log changes in adjacency.

```
(config-data)# router ospf
(conf-router) # log-adjacency-changes detail
```

passive-interface

This command suppresses routing updates on an interface.

Syntax

```
passive-interface GigabitEthernet <slot/port[.vlanID]>
passive-interface GigabitEthernet <slot/port>
passive-interface vlan <vlanID>
no passive-interface interface
```

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

This example suppresses routing updates on an interface.

```
(config-data)# router ospf
(conf-router)# passive-interface GigabitEthernet 0/0.4
```

timers throttle spf

This command sets the initial delay, the initial-holdtime and the maximum-holdtime between when SPF is calculated and the event which triggered the calculation.

Syntax

```
timers throttle spf delay initial-holdtime max-holdtime
no timers throttle spf
```

Command	Description
`delay`	Defines a number between 0 – 600000 delay in milliseconds from 1st change received until SPF calculation.
`initial-holdtime`	Defines the initial holdtime between 0 – 600000 in milliseconds between consecutive SPF calculation.
`maximum-holdtime`	Defines the maximum holdtime between 0 – 600000 in milliseconds.

Default

NA

Command Mode

Privileged User

Example

This example sets the delay to 200 ms, the initial holdtime is set to 400 ms and the maximum holdtime is set to 10 seconds.

```
(config-data)# router ospf
(conf-router) # timers throttle spf 200 400 10000
```

max-metric router-lsa

This command sets the time (seconds) to advertise self as stub-router.

Syntax

```
max-metric router-lsa {on-startup|on-shutdown} number
max-metric router-lsa administrative
no max-metric router-lsa [on-startup|on-shutdown|administrative]
```

Command	Description
on-startup	Defines the time (seconds) to advertise self as stub-router.
on-shutdown	Defines the time (seconds) to wait till full shutdown.
number	Defines the time (seconds) in the range of 5 – 86400.

Default

NA

Command Mode

Privileged User

Example

This example sets the time (seconds) to advertise self as stub-router.

```
(config-data) router ospf
(conf-router) # max-metric router-lsa administrative
```

auto-cost reference-bandwidth

This command sets the reference bandwidth for cost calculations, where this bandwidth is considered equivalent to an OSPF cost of 1, specified in Mbits/s.

Syntax

```
auto-cost reference-bandwidth number
no auto-cost reference-bandwidth
```

Command	Description
number	Defines the reference bandwidth in terms of megabits per second in the range of 1 – 4294967.

Default

100Mbit/s (i.e. a link of bandwidth 100Mbit/s or higher will have a cost of 1. Cost of lower bandwidth links will be scaled with reference to this cost).

Command Mode

Privileged User

Example

This example sets the reference bandwidth for cost calculations.

```
(config-data)# router ospf
(conf-router) # auto-cost reference-bandwidth 1000
```

network

This command specifies the OSPF enabled interface(s). If the interface has an address from range 192.168.1.0/24 then the command below enables ospf on this interface so the router can provide network information to the other ospf routers via this interface.

Syntax

```
network a.b.c.d/m area a.b.c.d
network a.b.c.d/m area number
no network a.b.c.d/m area a.b.c.d
no network a.b.c.d/m area number
```

Command	Description
a.b.c.d/M	Defines the OSPF network prefix.
area a.b.c.d	Defines the OSPF area ID in IP address format.
number	Defines the OSPF area ID as a decimal value in the range of 0 – 4294967295.

Default

NA

Command Mode

Privileged User

Example

If the interface has an address from range 192.168.1.0/24, then the command below enables ospf on this interface so that the router can provide network information to the other ospf routers via this interface.

```
(config-data)# router ospf
(conf-router) # network 192.168.1.0/24 area 0.0.0.0
```

area

This command summarizes intra-area paths from specified area in one Type-3 summary-LSA announced to other areas.

Syntax

```
area a.b.c.d range a.b.c.d/m
area number range a.b.c.d/m
no area a.b.c.d  range a.b.c.d /m
no area number range a.b.c.d/m
```

Command	Description
a.b.c.d	Defines the OSPF area in IP address format.
number	Defines the OSPF area ID as a decimal value in the range of 0 – 4294967295.
range	Summarizes routes matching address/mask (border routers only).
a.b.c.d/M	Defines the area range prefix.

Default

NA

Command Mode

Privileged User

Example

This example summarizes intra-area paths from the specified area in one Type-3 summary-LSA announced to other areas.

```
(config-data)# router ospf
(conf-router)# area 0.0.0.10 range 10.0.0.0/8
```

area ip-address|number range a.b.c.d/m not-advertise

This command filters intra area paths which are not advertised in other areas.

Syntax

```
area ip-address a.b.c.d range a.b.c.d/m not-advertise
area number number range a.b.c.d/m not-advertise
no area peer range a.b.c.d/m not-advertise
```

Command	Description
a.b.c.d	Defines the OSPF area in IP address format
number	Defines the OSPF area ID as a decimal value. Range is in between 0 – 4294967295.
a.b.c.d/M	Defines the area range prefix.
not-advertise	Defines not to advertise this range.

Default

NA

Command Mode

Privileged User

Example

This example filters intra area paths and is not advertised into other areas.

```
(config-data)# router ospf
(conf-router)# area ip-address 10.21.5.100 range 10.0.0.0/8 not-advertise
```

area ip-address|number range a.b.c.d/m substitute a.b.c.d/M

This command substitutes a summarized prefix with another prefix.

Syntax

```
area ip-address a.b.c.d range a.b.c.d/m substitute a.b.c.d/m
area number number range a.b.c.d/m substitute a.b.c.d/m
no area a.b.c.d range a.b.c.d/m substitute a.b.c.d/m
```

Command	Description
a.b.c.d	Defines the OSPF area in IP address format.
number	Defines the OSPF area ID as a decimal value. The range is 0 – 4294967295.
a.b.c.d/m	Defines the area range prefix.
substitute	Announces the area range as another prefix.
a.b.c.d/m	Announces network prefix instead of range.

Default

NA

Command Mode

Privileged User

Example

This example substitutes a summarized prefix with another prefix.

```
(config-data)# router ospf
(conf-router)# area ip-address 10.5.10.105 range 10.0.0.0/8 substitute 11.0.0.0/8
```

area ip-address|number shortcut

This command configures the area as Shortcut capable.

Syntax

```
area ip-address a.b.c.d shortcut {default|enable|disable}
area number <number> shortcut
no area ip-address a.b.c.d shortcut
no area number <number> shortcut
```

Command	Description
a.b.c.d	Defines the OSPF area in IP address format.
number	Defines the OSPF area ID as a decimal value in the range of 0 – 4294967295.
default	Sets the default shortcutting behavior
enable	Enables shortcutting through the area
disable	Disables shortcutting through the area

Default

NA

Command Mode

Privileged User

Example

This example configures the area as Shortcut capable.

```
(config-data)# router ospf
(conf-router)# area number 1000 shortcut enable
```

area ip-address|number stub

This command configures the area to be a stub area.

Syntax

```
area ip-address a.b.c.d stub
area number number stub
```

```
no area ip-address a.b.c.d stub
no area number number stub
```

Command	Description
a.b.c.d	Defines the OSPF area in IP address format.
Number	Defines the OSPF area ID as a decimal value in the range of 0 – 4294967295.

Default

NA

Command Mode

Privileged User

Example

This example configures the area to be a stub area.

```
(config-data)# router ospf
(conf-router)# area number 1000 stub
```

area ip-address|number stub no-summary

This command prevents an OSPFD ABR from injecting inter-area summaries into the specified stub area.

Syntax

```
area ip-address <a.b.c.d> stub no-summary
area number number stub no-summary
no area ip-address <a.b.c.d> stub no-summary
no area number number stub no-summary
```

Command	Description
a.b.c.d	Defines the OSPF area in IP address format
number	Defines the OSPF area ID as a decimal value in the range of 0 – 4294967295.

Command	Description
no-summary	Determines not to inject inter-area routes into the stub.

Default

NA

Command Mode

Privileged User

Example

This example prevents an OSPFD ABR from injecting inter-area summaries into the specified stub area.

```
(config-data)# router ospf
(conf-router)# area number 1000 stub no-summary
```

area ip-address|number default-cost

This command sets the cost of default-summary LSAs announced to stubby areas.

Syntax

```
area ip-address <a.b.c.d> default-cost <0-16777215>
area number number default-cost <0-16777215>
no area ip-address <a.b.c.d> default-cost <0-16777215>
```

Command	Description
a.b.c.d	Defines the OSPF area in IP address format.
number	Defines the OSPF area ID as a decimal value in the range of 0 – 4294967295.
<0-16777215>	Defines the stub's advertised default summary cost.

Default

NA

Command Mode

Privileged User

Example

This example sets the cost of default-summary LSAs announced to stubby areas.

```
(config-data)# router ospf
(conf-router)# area number 2000 default-cost 1000
```

area ip-address|number filter-list prefix NAME in/out

This command filters Type-3 summary-LSAs to/from area using prefix lists.

Syntax

```
area ip-address <a.b.c.d>  filter-list prefix NAME in
area ip-address <a.b.c.d> filter-list prefix NAME out
area number number filter-list prefix NAME in
area number number filter-list prefix NAME out
no area ip-address <a.b.c.d> filter-list prefix NAME in
no area ip-address <a.b.c.d> filter-list prefix NAME out
no area number number filter-list prefix NAME in
no area number number filter-list prefix NAME out
```

Command	Description
a.b.c.d	Defines the OSPF area in IP address format.
number	Defines the range of the area number 0 – 4294967295.
prefix	Filters prefixes between OSPF areas.
NAME	Defines the IP prefix list name.
in	Filters networks – sent out to this area
out	Filters networks – sent out from this area

Default

NA

Command Mode

Privileged User

Example

This example filters Type-3 summary-LSAs to/from area using prefix lists.

```
(config-data)# router ospf
(conf-router)# area number 1000 filter-list prefix NAME in
```

area ip-address|number authentication

This command specifies that simple password authentication should be used for the given area.

Syntax

```
area ip-address <a.b.c.d> authentication
area number number authentication
no area ip-address <a.b.c.d> authentication
no area number number authentication
```

Command	Description
a.b.c.d	Defines the OSPF area in IP address format.
number	Defines the area number in the range of 0 – 4294967295.

Default

NA

Command Mode

Privileged User

Example

This example specifies that simple password authentication should be used for the given area.

```
(config-data)# router ospf
(conf-router)# area number 1000 authentication
```

area ip-address|number authentication message-digest

This command specifies that OSPF packets must be authenticated with MD5 HMACs within the given area.

Syntax

```
area ip-address <a.b.c.d> authentication message-digest
area number number authentication message-digest
```

Command	Description
a.b.c.d	Defines the OSPF area in IP address format.
number	Defines the area number in the range of 0 – 4294967295.

Default

NA

Command Mode

Privileged User

Example

This example specifies that OSPF packets must be authenticated with MD5 HMACs within the given area.

```
(config-data)# router ospf
(conf-router)# area number 1000 authentication message-digest
```

redistribute kernel

This command redistributes routes of the specified protocol or kind into OSPF.

Syntax

```
redistribute kernel
redistribute kernel route-map
redistribute kernel metric-type {1|2}
redistribute kernel metric-type {1|2} route-map word
redistribute kernel metric <0-16777214>
```

```
redistribute kernel metric-type {1|2} metric <0-16777214> metric <0-16777214>
route-map word
no redistribute kernel
```

Command	Description
metric	Defines the metric for redistributed routes
metric-type	Defines the OSPF exterior metric type for registered routes
1|2	Sets the OSPF exterior type - 1- metric, 2-metrics
word	Describes the pointer to route-map entries

Default

NA

Command Mode

Privileged User

Example

This example redistributes routes of the specified protocol or kind into OSPF.

```
(config-data)# router ospf
(conf-router)# redistribute kernel
```

redistribute rip

This command redistributes information from RIP.

Syntax

```
redistribute rip [metric <default metric>] [route-map <pointer>]
redistribute rip [route-map <pointer>][metric <default metric>]
no redistribute rip
```

Command	Description
metric	Defines the metric for redistributed routes.

Command	Description
default metric	Defines the default metric [0-4294967295].
route-map	Defines the route map reference.
pointer	Defines the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes routes from RIP.

```
(config-data)# router bgp 3
(conf-router)# redistribute rip
```

redistribute connected

This command redistributes routes of the specified protocol or kind into OSPF.

Syntax

```
redistribute connected
redistribute connected route-map
redistribute connected metric-type {1|2}
redistribute connected metric-type {1|2} route-map word
redistribute connected metric <0-16777214>
redistribute connected metric-type {1|2} metric <0-16777214> metric <0-16777214> route-map word
no redistribute connected
```

Command	Description
metric	Defines the metric for redistributed routes.
metric-type	Defines the OSPF exterior metric type for registered routes.

Command	Description
1|2	Sets the OSPF exterior type - 1- metric, 2-metrics.
word	Describes the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes routes of the specified protocol or kind into OSPF.

```
(config-data)# router ospf
(conf-router)# redistribute connected
```

redistribute static

This command redistributes routes of the specified protocol or kind into OSPF.

Syntax

```
redistribute static
redistribute static route-map
redistribute static metric-type {1|2}
redistribute static metric-type {1|2} route-map word
redistribute static metric <0-16777214>
redistribute static metric-type {1|2} metric <0-16777214> metric <0-16777214>
route-map word
no redistribute static
```

Command	Description
metric	Defines the metric for redistributed routes.
Metric-type	Defines the OSPF exterior metric type for registered routes.
1|2	Sets the OSPF exterior type - 1- metric, 2-metrics.
word	Describes the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes routes of the specified protocol or kind into OSPF.

```
(config-data)# router ospf
(conf-router)# redistribute static
```

redistribute bgp

This command redistributes routes of the specified protocol or kind into OSPF.

Syntax

```
redistribute bgp
redistribute bgp route-map
redistribute bgp metric-type {1|2}
redistribute bgp metric-type {1|2} route-map word
redistribute bgp metric <0-16777214>
redistribute bgp metric-type {1|2}  metric <0-16777214> metric
<0-16777214> route-map word
no redistribute bgp
```

Command	Description
`metric`	Defines the metric for redistributed routes
`metric-type`	Defines the OSPF exterior metric type for registered routes
`1|2`	Sets the OSPF exterior type - 1- metric, 2-metrics
`word`	Describes the pointer to route-map entries

Default

NA

Command Mode

Privileged User

Example

This example redistributes routes of the specified protocol or kind into OSPF.

```
(config-data)# router ospf
(conf-router)# redistribute bgp
```

timers bgp

This command adjusts the BGP routing timers.

Syntax

```
timers bgp <keepalive interval> <hold time>
```

Command	Description
`keepalive interval`	Defines the Keepalive interval [0-65535].
`hold time`	Defines the Hold time.

Default

NA

Command Mode

Privileged User

Example

This example adjusts the BGP routing timer.

```
(config-data)# router bgp 3
(conf-router)# timers bgp 100 200
```

default-information originate

This command originates an AS-External (type-5) LSA describing a default route into all external routing capable areas, of the specified metric and metric type.

Syntax

```
default-information originate
default-information originate metric <0-16777214>
default-information originate metric <0-16777214> metric-type {1|2}
default-information originate metric <0-16777214> metric-type (1|2) route-map word
default-information originate always
default-information originate always metric <0-16777214>
default-information originate always metric <0-16777214> metric-type {1|2}
default-information originate always metric <0-16777214> metric-type {1|2}route-map word
no default-information originate
```

Command	Description
always	Sets always advertise default route.

Default

NA

Command Mode

Privileged User

Example

This command distributes a default route.

```
(config-data)# router ospf
(conf-router) # default-information originate
```

default-metric

This command sets the metric of redistributed routes.

Syntax

```
default-metric <0-16777214>
no default-metric
```

Command	Description
<0-16777214>	Defines the default metric.

Default

NA

Command Mode

Privileged User

Example

This example sets the metric of redistributed routes to 1000.

```
(config-data)# router ospf
(conf-router)# default-metric 1000
```

distance

This command defines an OSPF administrative distance.

Syntax

```
distance <1-255>
no distance <1-255>
distance ospf {intra-area|inter-area|external} <1-255>
no distance ospf
```

Command	Description
<1-255>	Defines the administrative distance.

Default

NA

Command Mode

Privileged User

Example

This example defines an OSPF administrative distance of 100.

```
(config-data)# router ospf
(conf-router)# distance 100
```

OSPF Interface Configuration

OSPF Interface Configuration includes the following commands:

ip ospf authentication-key auth_key

This command sets the OSPF authentication key to a simple password. After setting AUTH_KEY, all OSPF packets are authenticated.

Syntax

```
ip ospf authentication-key auth_key [a.b.c.d]
no ip ospf authentication-key [a.b.c.d]
```

Command	Description
auth_key	Defines the OSPF password (key).
a.b.c.d	Address of the interface

Default

NA

Command Mode

Privileged User

Example

This example sets the OSPF authentication key to a simple password.

```
(config-data)# interface vlan1
(conf-if-VLAN 1)# ip ospf authentication-key passx
```

ip ospf authentication message-digest

This command specifies that MD5 HMAC authentication must be used on this interface.

Syntax

```
ip ospf authentication message-digest [a.b.c.d]
```

Arguments	Description
a.b.c.d	Address of the interface.

Default

NA

Command Mode

Privileged User

Example

This example specifies that MD5 HMAC authentication must be used on this interface.

```
(config-data)# interface vlan1
(conf-if-VLAN 1)# ip ospf authentication message-digest
```

ip ospf message-digest-key KEYID md5 KEY

This command sets the OSPF authentication key to a cryptographic password.

Syntax

```
ip ospf message-digest-key KEYID md5 KEY [a.b.c.d]
no ip ospf message-digest-key
```

Command	Description
KEYID	Defines the KEYID in the range of 1 – 255.
KEY	Defines the OSPF password.
a.b.c.d	Address of the interface.

Default

NA

Command Mode

Privileged User

Example

This example sets the OSPF authentication key to a cryptographic password.

```
(config-data)# interface vlan1
(conf-if-VLAN 1)# ip ospf message-digest-key 100 md5 ABCD1234
```

ip ospf cost

This command sets the link cost for the specified interface.

Syntax

```
ip ospf cost number [a.b.c.d]
no ip ospf cost <cost> [a.b.c.d]
```

Command	Description
`number`	Defines the cost in the range of 1 – 65535.
`a.b.c.d`	Address of the interface.

Default

NA

Command Mode

Privileged User

Example

This example sets the link cost for the specified interface and address.

```
(config-data)# interface vlan1
(conf-if-VLAN 1)# ip ospf cost 1000 10.10.10.1
```

ip ospf dead-interval

This command sets the number of seconds for RouterDeadInterval timer value used for Wait Timer and Inactivity Timer.

Syntax

```
ip ospf dead-interval number [a.b.c.d]
ip ospf dead-interval minimal hello-multiplier <2-20> [a.b.c.d]
no ip ospf dead-interval [a.b.c.d]
```

Command	Description
number	Defines the seconds in the range of 1- 65535.
<2-20>	Defines the number of hellos to send each second.
a.b.c.d	Address of the interface.

Default

NA

Command Mode

Privileged User

Example

This example sets the number of seconds for RouterDeadInterval timer value to 1000.

```
(config-data)# interface vlan1
(conf-if-VLAN 1)# ip ospf dead-interval 1000
```

ip ospf hello-interval

This command sets the number of seconds for HelloInterval timer value.

Syntax

```
ip ospf hello-interval number [a.b.c.d]
no ip ospf hello-interval [a.b.c.d]
```

Command	Description
number	Defines the number of seconds in the range of 1- 65535.
a.b.c.d	Address of the interface.

Default

NA

Command Mode

Privileged User

Example

This example sets HelloInterval timer value to 1000 seconds.

```
(config-data)# interface vlan1
(conf-if-VLAN 1)# ip ospf hello-interval 1000
```

ip ospf network

This command explicitly sets the network type for the specified interface.

Syntax

```
ip ospf network {broadcast|non-broadcast|point-to-multipoint |point-to-point}
no ip ospf network
```

Command	Description
broadcast	Specifies the OSPF broadcast multi-access network.
non-broadcast	Specifies the OSPF NMBA network.
point-to-multipoint	Specifies the OSPF point-to-multipoint network.
point-to-point	Specifies the OSPF point-to-point network.

Default

NA

Command Mode

Privileged User

Example

This example explicitly sets the network type for the specified interface.

```
(config-data)# interface vlan1
(conf-if-VLAN 1)# ip ospf network point-to-point
```

ip ospf priority

This command sets the RouterPriority integer value.

Syntax

```
ip ospf priority number [a.b.c.d]
no ip ospf priority [a.b.c.d]
```

Command	Description
`number`	Defines the priority value in the range of 0-255.
`a.b.c.d`	Address of the interface

Default

1

Command Mode

Privileged User

Example

This example sets the RouterPriority integer value to 100.

```
(config-data)# interface vlan1
(conf-if-VLAN 1)# ip ospf priority 100
```

ip ospf retransmit-interval

This command sets the number of seconds for RxmtInterval timer value. This value is used when retransmitting Database Description and Link State Request packets.

Syntax

```
ip ospf retransmit-interval number [a.b.c.d]
no ip ospf retransmit interval [a.b.c.d]
```

Command	Description
number	Defines the number of seconds for the RxmtInterval timer value. Range is 1 – 65535.
a.b.c.d	Address of the interface.

Default

5 seconds

Command Mode

Privileged User

Example

This example sets the number of seconds for RxmtInterval timer value to 1000.

```
(config-data)# interface vlan1
(conf-if-VLAN 1)# ip ospf retransmit-interval 1000
```

ip ospf transmit-delay

This command sets the number of seconds for InfTransDelay value.

Syntax

```
ip ospf transmit-delay number [a.b.c.d]
no ip ospf transmit-delay [a.b.c.d]
```

Command	Description
number	Defines number of seconds for the InfTransDelay value in the range of <1-65535>.
a.b.c.d	Address of the interface

Default

1 second

Command Mode

Privileged User

Example

This example sets the number of seconds for InfTransDelay value to 1000.

```
(config-data)# interface vlan1
(conf-if-VLAN 1)# ip ospf transmit-delay 1000
```

ip ospf bfd

This command sets the number of seconds for the InfTransDelay value.

Syntax

```
ip ospf bfd interval <value> min_rx <value> multiplier <value>
```

Command	Description
interval	Defines the Interval (in msec) for outgoing BFD messages. The interval is increased if required by the remote system.
min_rx	Defines the interval (in msec) between BFD messages in milliseconds. The remote system uses this interval for sending messages if its interval is lower.
multiplier	Defines the maximum number of packets that can be missed before the session status is considered down.

Command Mode

Privileged User

Example

This example enables BFD for OSPF on VLAN 1 with an interval and min_rx of 200 msec and multiplier value of 3

```
(config-data)# interface vlan1
(conf-if-VLAN 1)# ip ospf bfd interval 200 min_rx 200 multiplier 3
```

OSPF6 Protocol

The following describes OSPF protocol for IPv6 commands.

router ospf6

This command enables or disables the OSPF6 process.

Syntax

```
router ospf6 [vrf <VRF name>]
no router ospf
```

Command	Description
VRF name	Defines the VRF name.

Default

NA

Command Mode

Privileged User

Example

This example enables the OSPF6 process.

```
(config-data)# router ospf6
```

area

This command filters OSPFv6 area parameters.

Syntax

```
area a.b.c.d filter-list prefix <ipv6 prefix-list name> {in|out}
area a.b.c.d range [X:X::X:X/M] [advertise|not-advertise]
```

Command	Description
a.b.c.d	Defines the OSPFv6 area in IP address format.
filter-list	Filter networks between OSPFv6 areas.
prefix	Filter prefixes between OSPFv6 areas.
ipv6 prefix-list name	Defines the name of an IPv6 prefix-list
range	Defines the configured address range.
in	The IPv6 prefix list is applied to IPv6 prefixes advertised to the relevant area from other areas.
out	The IPv6 prefix list is applied to IPv6 prefixes advertised out of the relevant area to other areas.
advertise	Set the address range status to “advertise” and generates a Type 3 summary link-state advertisement (LSA). (Optional)
not-advertise	Set the address range status to “DoNotAdvertise”. The Type 3 summary LSA is suppressed, and the component networks remain hidden from the other networks. (Optional)

Default

NA

Command Mode

Privileged User

Example

This example filters intra area paths and is not advertised into other areas.

```
(config-data)# router ospf6
(conf-router)# area ip-address 10.21.5.100 range 10:0::0:0/8 not-advertise
```

interface

This command selects an interface to configure.

Syntax

```
interface <interface name> <interface ID> area a.b.c.d
```

Command	Description
area	Defines the OSPF6 area ID.
interface name	Defines the interface name as one of the following: ■ bvi: Bridge interface ■ cellular: Cellular 3G interface ■ gigabitethernet: Gigabit Ethernet interface ■ gre: GRE tunnel interface ■ ipip: IPIP tunnel interface ■ l2tp: L2TP tunnel interface ■ loopback: PPPoE interface ■ pppoe: PPPoE interface ■ pptp: PPTP tunnel interface ■ vlan: VLAN interface
a.b.c.d	Defines the OSPFv6 area in IP address format.

Default

NA

Command Mode

Privileged User

Example

This example selects an interface to configure.

```
# configure data
(config-data)# router ospf6
(conf-router)# interface gre 1 area 10.21.5.100
```

redistribute

This command redistributes routes of the specified protocol or kind into OSPF6.

Syntax

```
redistribute {bgp|connected|kernel|ripng|static} [route-map <route-map name>]
```

Command	Description
bgp	Redistributes the bgp route.
connected	Redistributes the connected route.
kernel	Redistributes the kernel route.
ripng	Redistributes the ripng route.
static	Redistributes the static route.
route-map name	Defines the route-map name.

Default

NA

Command Mode

Privileged User

Example

This example redistributes the kernel route of the specified protocol or kind into OSPF6.

```
# configure data
(config-data)# router ospf
(conf-router)# redistribute kernel
```

Routing Information Protocol (RIP)

The following commands relate to Routing Information Protocol.

General Configuration

RIP General Configuration includes the following commands:

router rip

This command enables IPv4 RIP.

Syntax

```
router rip [vrf <VRF name>]
no router rip
```

Command	Description
VRF name	Defines the VRF name.

Default

NA

Command Mode

Privileged User

Example

This example enables RIP configuration mode.

```
(config-data)# router rip
```

router ripng

This command enables IPv6 RIPng.

Syntax

```
router ripng [vrf <VRF name>]
no router ripng
```

Command	Description
VRF name	Defines the VRF name.

Default

NA

Command Mode

Privileged User

Example

This example enables RIPng configuration mode.

```
(config-data)# router ripng
```

passive-interface

This command sets the specified interface to passive mode. On passive mode interfaces, all receiving packets are processed as normal and ripd does not send either multicast or unicast RIP packets except to RIP neighbors specified with the neighbor command. The interface may be specified as 'default' to make ripd default to passive on all interfaces. The default is to be passive on all interfaces.

Syntax

```
passive-interface {ifname|default}
no passive-interface ifname
```

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]

Interface Type (ifname)		Interface ID
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

This example sets the specified interface to passive mode.

```
(config-data)# router rip
(conf-router)# passive-interface vlan 2
```

ip split-horizon

This command controls the split-horizon on the interface. A Split horizon is a way of preventing a routing loop in a network. Information about the routing for a specific packet is never sent back in the direction from which it was received.

Default is ip split-horizon. If you don't perform split-horizon on the interface, please specify no ip split-horizon.

Syntax

```
ip split-horizon
no ip split-horizon
```

Default

NA

Command Mode

Privileged User

Example

This example sets split horizon on the VLAN 2 interface.

```
(config-data)# interface vlan 2
(conf-if VLAN 2)# ip split-horizon
```

RIP – Router Configuration

RIP Router Configuration includes the following commands:

network network

This command sets the RIP enable interface by network. The interfaces which have addresses matching the network are enabled. This group of commands either enables or disables RIP interfaces between numbers of a specified network address. For example, if the network for 10.0.0.0/24 is RIP enabled, this would result in all the addresses from 10.0.0.0 to 10.0.0.255 being enabled for RIP.

The no network command disables RIP for the specified network.

Syntax

```
network network a.b.c.d/m
no network network
```

Command	Description
a.b.c.d/m	Defines the IP prefix network/length

Default

NA

Command Mode

Privileged User

Example

This example sets the RIP enable interface by network.

```
(conf-router)# network network 10.4.4.10/16
```

network ifname

This command sets a RIP enabled interface by ifname. Both the sending and receiving of RIP packets will be enabled on the port specified in the network ifname command.

The no network ifname command disables RIP on the specified interface.

Syntax

```
network ifname
no network ifname
```

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

This example sets the RIP enable interface by ifname.

```
(conf-router)# network vlan 1
```

neighbor a.b.c.d

This command is used to specify neighbors when a neighbor can't process multicast. In some cases, not all routers are able to understand multicasting, where packets are sent to a network or a group of addresses. In a situation where a neighbor cannot process multicast packets, it is necessary to establish a direct link between routers. The neighbor command allows the network administrator to specify a router as a RIP neighbor.

The no neighbor a.b.c.d command will disable the RIP neighbor.

Syntax

```
neighbor a.b.c.d
no neighbor a.b.c.d
```

Command	Description
a.b.c.d	Defines the neighbor address.

Default

NA

Command Mode

Privileged User

Example

This example specifies a neighbor.

```
(conf-router)# neighbor 10.4.4.4
```

version version

This command sets the RIP version number.

Syntax

```
version version
no version
```

Command	Description
version	Defines the RIP version number – “1” or “2”

Default

- “2” for send
- Both “1” and “2” for receive

Command Mode

Privileged User

Example

This example sets RIP Version 2.

```
(conf-router) # version 2
```

redistribute kernel

This command redistributes routing information from kernel route entries into the RIP tables. The no redistribute kernel disables the routes.

Syntax

```
redistribute kernel
redistribute kernel metric <0-16>
redistribute kernel route-map [route-map]
no redistribute kernel
```

Command	Description
metric	Defines the Metric value (0 -16).
route-map	Defines the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes IPv4 routing information from kernel route entries.

```
# configure data
(config-data)# router rip
(conf-router)# redistribute kernel
```

redistribute static

This command redistributes routing information from static route entries into the RIP tables. The no redistribute static command disables the routes.

Syntax

```
redistribute static
redistribute static metric <metric value>
redistribute static route-map [route-map]
no redistribute static
```

Command	Description
metric	Defines the metric value (0 - 4294967295).
route-map	Defines the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes routing information from static route entries.

```
# configure data
(config-data)# router ospf
(conf-router) # redistribute static
```

redistribute connected

This command redistributes connected routes into the RIP tables.

The no redistribute connected command disables the connected routes in the RIP tables. The connected route on a RIP- enabled interface is announced by default.

Syntax

```
redistribute connected
redistribute connected [metric <metric value>]
redistribute connected [route-map [route-map]]
no redistribute connected
```

Command	Description
`metric value`	Defines the default metric value [0-4294967295].
`route-map`	Defines the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes connected routes into the RIP tables.

```
(conf-router) # redistribute connected
```

redistribute ospf

This command redistributes routing information from ospf route entries into the RIP tables. no redistribute ospf disables the routes.

Syntax

```
redistribute ospf
redistribute ospf metric <default metric>
```

```
redistribute ospf route-map [route-map]
no redistribute ospf
```

Command	Description
metric	Defines the metric value [0-4294967295].
route-map	Defines the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes ospf routes into the RIP tables.

```
(conf-router) # redistribute ospf
```

redistribute bgp

This command redistributes routing information from bgp route entries into the RIP tables. no redistribute bgp disables the routes.

Syntax

```
redistribute bgp
redistribute bgp metric <0-16>
redistribute bgp route-map [route-map]
no redistribute bgp
```

Command	Description
metric	Defines the metric value (0 -16).
route-map	Defines the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes bgp routes into the RIP tables.

```
(conf-router) # redistribute bgp
```

default-information originate

This command distributes a default route.

Syntax

```
default-information originate
```

Default

NA

Command Mode

Privileged User

Example

This example distributes a default route.

(conf-router)# default-information originate

distribute-list prefix

This command filters the RIP path and can apply access-lists to a chosen interface.

Syntax

```
distribute-list prefix [WORD] {in|out} ifname
```

Command	Description
WORD	Prefix list name

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

This example filters the RIP path for input packets of vlan 1.

```
(conf-router)# distribute-list prefix prefix1 in vlan 1
```

distance

This command sets the default RIP distance to a specified value.

Syntax

```
distance <1-255> [a.b.c.d/m]
no distance <1-255> [a.b.c.d/m]
```

Command	Description
a.b.c.d/m	Defines the IP prefix network/length.

Default

120

Command Mode

Privileged User

Example

This example sets the default RIP distance to 150.

```
(conf-router)# distance 150
```

timers basic

This command configures timers in the RIP protocol.

The no timers basic command resets the timers to the default settings listed below.

Syntax

```
timers basic [5-2147483647]
no timers basic
```

Command	Description
5-2147483647	Defines the Routing Table update timer value in seconds.

Default

The default Routing table update timer value in seconds is 30.

Command Mode

Privileged User

Example

This example updates the timer value to 50 seconds.

```
(conf-router)# timers basic 50
```

RIP – Interface Configuration

RIP Interface Configuration includes the following commands:

ip rip split-horizon

This command controls the split-horizon on the interface.

Syntax

```
ip rip split-horizon [poisoned-reverse]
no ip rip split-horizon
```

Default

NA

Command Mode

Privileged User

Example

This example sets the split-horizon on VLAN 1.

```
(conf-if-VLAN 1)# ip rip split-horizon
```

ip rip send version version

This interface command overrides the global rip version setting and selects which version of RIP packets are sent on this interface.

Syntax

```
ip rip send version version
```

Command	Description
`version`	Defines the RIP version number – “1” or “2”.

Default

Send packets according to the global version (Version 2).

Command Mode

Privileged User

Example

This example sets RIP Version 2 to send packets with.

```
(conf-if-VLAN 1)# ip rip send version 2
```

ip rip receive version version

This command overrides the global RIP version setting and selects which version of RIP packets are accepted on this interface.

Syntax

```
ip rip receive version version
```

Command	Description
`version`	Defines the RIP version number – “1” or “2”.

Default

Accept packets according to the global setting (1 and 2)

Command Mode

Privileged User

Example

This example sets RIP Version 2 to receive packets with.

```
(conf-if-VLAN 1)# ip rip receive version 2
```

ip rip authentication mode md5

This command sets the interface with RIPv2 MD5 authentication.

Syntax

```
ip rip authentication mode md5
no ip rip authentication mode md5
```

Command Mode

Privileged User

Example

This example sets the interface with RIPv2 MD5 authentication.

```
(conf-if-VLAN 1)# ip rip authentication mode md5
```

ip rip authentication mode text

This command sets the interface with RIPv2 simple password authentication.

Syntax

```
ip rip authentication mode text
no ip rip authentication mode text
```

Command Mode

Privileged User

Example

This example sets the interface with RIPv2 simple text authentication.

```
(conf-if-VLAN 1)# ip rip authentication mode text
```

ip rip authentication string

This command sets the authentication string.

Syntax

```
ip rip authentication string string
no ip rip authentication mode string
```

Command	Description
string	Defines the authentication string which must be less than 16 characters.

Command Mode

Privileged User

Example

This example sets the authentication string.

```
(conf-if-VLAN 1)# ip rip authentication string ripauthent
```

ip rip authentication key-chain

This command sets the authentication key-chain.

Syntax

```
ip rip authentication key-chain key-chain
no ip rip authentication key-chain key-chain
```

Command	Description
key-chain	Defines the name of the key chain.

Command Mode

Privileged User

Example

This example sets the authentication key-chain.

```
(conf-if-VLAN 1)# ip rip authentication key-chain 120
```

IP Route Map Configuration

RIP Route Map Configuration includes the following commands:

match community

This command matches a BGP community list.

Syntax

```
match community {<comm list std number>|<comm list exp number> |<comm list name>}
```

Command	Description
`comm list std number`	Defines the community list number (standard). Range is 1-99.
`comm list exp number`	Defines the community list number (expanded). Range is 100-500.
`comm list name`	Defines the community list name.

Command Mode

Privileged User

Example

This example matches a BGP community list.

```
(config-data)# route-map ww permit 1
(conf-route-map)# match community commlist1
```

match extcommunity

This command matches BGP/VPN extended community list.

Syntax

```
match extcommunity {<comm list std number>|<comm list exp number> |<comm list name>}
```

Command	Description
`comm list std number`	Defines the extended community list number (standard). Range is 1-99.
`comm list exp number`	Defines the extended community list number (expanded). Range is 100-500.

Command	Description
comm list name	Defines the extended community list name.

Command Mode

Privileged User

Example

This example matches a BGP/VPN extended community list.

```
(config-data)# route-map ww permit 1
(conf-route-map)# match extcommunity 1
```

match interface ifname

This command matches values from the routing table.

Syntax

```
match interface ifname
```

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Command Mode

Privileged User

Example

This example matches values from vlan 1.

```
(conf-route-map)# match interface vlan 1
```

match ip address prefix-list [WORD]

This command matches the IP address of the route.

Syntax

```
match ip address prefix-list plistname
```

Command	Description
plistname	Defines the prefix list string.

Command Mode

Privileged User

Example

This example matches entries of prefix-lists.

```
(conf-route-map)# match ip address prefix-list plist
```

match ip next-hop

This command matches the next-hop address of a route.

Syntax

```
match ip next-hop prefix-list plistname
```

Command	Description
plistname	Defines the prefix-list string.

Command Mode

Privileged User

Example

This example matches the next-hop address of a route.

```
(conf-route-map)# match ip next-hop prefix-list plist
```

match metric

This command matches the metric value of RIP updates.

Syntax

```
match metric <0-4294967295>
```

Command Mode

Privileged User

Example

This example matches the metric value of 100000.

```
(conf-route-map)# match metric 100000
```

set comm-list

This command sets the BGP community list (for deletion).

Syntax

```
set comm-list {<comm list std number>|<comm list exp number> |<comm list name>}
```

Command	Description
`comm list std number`	Defines the community list number (standard). Range is 1-99.
`comm list exp number`	Defines the community list number (expanded). Range is 100-500.
`comm list name`	Defines the community list name.

Command Mode

Privileged User

Example

This example sets a BGP community list.

```
(config-data)# route-map ww permit 1
(conf-route-map)# set comm-list 100
```

set ip next-hop

This command sets the next hop value in the RIPv2 protocol.

Syntax

```
set ip next-hop a.b.c.d
```

Command	Description
`a.b.c.d`	Defines the IP address.

Command Mode

Privileged User

Example

This example sets the next hop to 10.4.4.28.

```
(conf-route-map)# set ip next-hop 10.4.4.28
```

set metric

This command sets a metric value for matched routes when sending an announcement.

Syntax

```
set metric <0-4294967295>
```

Command Mode

Privileged User

Example

This example sets the metric value to 150000.

```
(conf-route-map)# match metric 150000
```

redistribute connected

This command redistributes connected routes into the RIPng tables.

The no redistribute connected command disables the connected routes in the RIP tables. The connected route on a RIP- enabled interface is announced by default.

Syntax

```
redistribute connected
redistribute connected metric <0-16>
redistribute connected route-map [route-map]
no redistribute connected
```

Command	Description
metric	Defines the metric value (0 -16).
route-map	Defines the pointer to route-map entries.

Command Mode

Privileged User

Example

This example redistributes connected routes into the RIPng tables.

```
# configure data
(config-data)# router ripng
(conf-router)# redistribute connected
```

RIPng

RIPng Router Configuration includes the following commands:

default-information originate

This command distributes a default route.

Syntax

```
default-information originate
```

Default

NA

Command Mode

Privileged User

Example

This example distributes a default route.

```
# configure data
(config-data)# router ripng
(conf-router)# default-information originate
```

default-metric

This command sets the metric of redistributed routes.

Syntax

```
default-metric <0-16777214>
no default-metric
```

Command	Description
<0-16777214>	Defines the default metric.

Default

NA

Command Mode

Privileged User

Example

This example sets the metric of redistributed routes to 1000.

```
# configure data
(config-data)# router ripng
(conf-router)# default-metric 1000
```

distribute-list prefix

This command filters the RIP path and can apply access-lists to a chosen interface.

Syntax

```
distribute-list prefix [WORD] {in|out} ifname
```

Command	Description
WORD	Prefix list name

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]

Interface Type (ifname)		Interface ID
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

This example filters the RIP path for input packets of vlan 1.

```
# configure data
(config-data)# router ripng
(conf-router)# distribute-list prefix prefix1 in vlan 1
```

network ifname

This command enables RIPng on a specified interface or network.

Syntax

```
network ifname/[X:X::X:X/M]
no network ifname/[X:X::X:X/M]
```

Interface Type (ifname)		Interface ID
[X:X::X:X/M]	IPv6 prefix network/length, e.g., 3ffe::/16	
gigabitethernet	GigabitEthernet interface slot and	[SLOT/PORT.VLANID]

Interface Type (ifname)		Interface ID
	port (VLAN ID is optional)	
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

This example sets the RIP enable interface by ifname.

```
# configure data
(config-data)# router ripng
(conf-router)# network vlan 1
```

passive-interface

This command suppresses routing updates on an interface.

Syntax

```
passive-interface ifname
no passive-interface ifname
```

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[Slot/Port.VLAN ID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

This example sets the specified interface to passive mode.

```
# configure data
(config-data)# router rip
(conf-router)# passive-interface vlan 1
```

route

This command sets up a static route.

Syntax

```
route <route map tag> deny <sequence>
route <route map tag> permit <sequence>
route <route map tag> vrf <VRF table> deny|permit <sequence>
```

Command	Description
route map tag	Defines the route map tag.
deny	Route map denies set operations.
permit	Route map permits set operations.
vrf	Associate with the defined VRF.
VRF table	Defines the VRF table name.
sequence	Defines the sequence to insert to/delete from an existing route-map entry. Range is 1-65535.

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[Slot/Port.VLAN ID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

The following is an example of how this command can be used.

```
# configure data
(config-data)# router ripng
(conf-router)# route AAAtag deny 10
```

route-map

This command sets up a route-map.

Syntax

```
route <rmap_name> in|out <ifname>
```

Command	Description
rmap_name	Defines the route map name.
in	Defines the route map for input filtering.
out	Defines the route map for output filtering.

Default

NA

Command Mode

Privileged User

Example

The following is an example of how this command can be used.

```
# configure data
(config-data)# router ripng
(conf-router)# route AAAmap in vlan 2
```

timers basic

This command configures timers in the RIPng protocol.

Syntax

```
timers basic <routing_table_timer> <routing_timeout_timer> <garbage_collection_timer>
```

Command	Description
routing_table_timer	Defines the Routing Table Update Timer value in seconds. Range is 5-2147483647.
routing_timeout_timer	Defines the Routing Information Timeout Timer. Range is 0-65535.
garbage_collection_timer	Defines the Garbage Collection Timer. Range is 0-65535.

Default

- The default Routing Table Update Timer value in seconds is 30.
- The default Routing Timeout Timer value in seconds is 180.
- The default Garbage Collection Timer.value in seconds is 120.

Command Mode

Privileged User

Example

This example updates the Routing Table Update Timer, Routing Timeout Timer, and Garbage Collection Timer.values to 50 seconds each.

```
# configure data
(config-data)# router ripng
(conf-router)# timers basic 50 50 50
```

redistribute bgp

This command redistributes routing information from bgp route entries into the RIPng tables. The no redistribute bgp disables the routes.

Syntax

```
redistribute bgp
redistribute bgp metric <0-16>
redistribute bgp route-map [route-map]
no redistribute bgp
```

Command	Description
metric	Defines the metric value (0 -16).
route-map	Defines the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes bgp routes into the RIPng tables.

```
# configure data
(config-data)# router ripng
(conf-router)# redistribute bgp
```

redistribute kernel

This command redistributes routing information from kernel route entries into the RIPng tables. The no redistribute kernel disables the routes.

Syntax

```
redistribute kernel
redistribute kernel metric <0-16>
redistribute kernel route-map [route-map]
no redistribute kernel
```

Command	Description
metric	Defines the Metric value (0 -16).
route-map	Defines the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes IPv6 routing information from kernel route entries.

```
# configure data
(config-data)# router ripng
(conf-router)# redistribute kernel
```

redistribute ospf6

This command redistributes routing information from ospf6 route entries into the RIPng tables. The no redistribute ospf6 command disables the routes.

Syntax

```
redistribute ospf6
redistribute ospf6 metric <0-16>
redistribute ospf6  route-map [route-map]
no redistribute ospf6
```

Command	Description
metric	Defines the metric value (0 -16).
route-map	Defines the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes ospf6 routes into the RIPng tables.

```
# configure data
(config-data)# router ripng
(conf-router)# redistribute ospf6
```

redistribute static

This command redistributes routing information from static route entries into the RIPng tables. The no redistribute static command disables the routes.

Syntax

```
redistribute static
redistribute static metric <0-16>
redistribute static route-map [route-map]
no redistribute static
```

Command	Description
`metric`	Defines the metric value (0 -16).
`route-map`	Defines the pointer to route-map entries.

Default

NA

Command Mode

Privileged User

Example

This example redistributes routing information from static route entries.

```
# configure data
(config-data)# router ripng
(conf-router)# redistribute static
```

Virtual Routing and Forwarding (VRF) Commands

These commands implement dynamic routing protocols (BGP, OSPF, PIM, and RIP) with Virtual Routing and Forwarding (VRF) tagging. One BGP, one OSPF, one PIM, and one RIP protocol can be enabled per VRF table. Up to five dynamic routing protocols can be enabled in all defined VRF tables.

ip vrf

This command enables a dynamic routing protocol on a VRF.

Syntax

```
ip vrf <vrf-name> {enable bgp|ospf|pim|rip] {ipv4-alias|ipv6-alias <alias name>}
no ip vrf <vrf-name>
```

Command	Description
`vrf-name`	Defines the VRF name (up to 64 bytes).
`enable {bgp|ospf|pim|rip}`	Enables a specific protocol on the VRF.
`ipv4-alias`	Defines an IPv4 alias name for the VRF.
`ipv6-alias`	Defines an IPv6 alias name for the VRF.

Default

NA

Note

- Up to 32 VRF's may be defined.
- A VRF which is associated with interfaces cannot be deleted (need first to disassociate the interfaces).

Command Mode

Privileged User

Related Commands

`ip route vrf`, `ip vrf forwarding`, `show ip vrf`

For more information on alias names, see alias on page 599.

To view VRFs and IP addresses that are configured with alias names, use the command `show network available-app-interface` (see show network available-app-interfaces on page 137).

Example

- Configures a VRF named "XXIP":

```
(config-data)# ip vrf XXIP
```

- Configures a VRF named "voip" with alias name "voip_v4":

```
(config-data)# ip vrf voip ipv4-alias voip_v4
```

ip vrf forwarding

This command associates an interface with a given vrf.

Syntax

```
ip vrf forwarding <string>
no ip vrf forwarding
```

Command	Description
`string`	Defines the VRF name.

Default

Interface is not associated with vrf.

Note

- This command is supported on all MSBR devices.
- The maximum number of interfaces per vrf is 20.
- The following interfaces are supported:
  - GigabitEthernet

- cellular
- gre
- ipip
- atm
- pppoe
- multilink
- vlan

Command Mode

Privileged User

Related Commands

ip vrf, show ip vrf

Example

This example associate interface VLAN 4 with vrf data:

```
# configure data
(config-data)# interface vlan 4
(conf-if-VLAN 4)# ip vrf forwarding data
```

ip route vrf

The command adds a static route into a VRF.

Syntax

The syntax of this command can include several interface types. The most common are as follows:

```
ip route vrf <vrf table name> <ip address> <prefix  mask> [gw ip address] ifname
<slot/port.VlanId> [metric value] [track <track id>] [bfd-neighbor <neighbor ID>]
[output-vrf <name>] [description <string>]
```

This syntax describes a route that depends also on the source prefix of the packets:

```
ip route vrf <VRF name> source <IP source prefix>|local-voip destination <IP
destination prefix> [<gateway>] <interface type> <interface ID> [<metric value>]
[track <track ID>] [output-vrf <name>] [description <string>]
```

Command	Description
`vrf table name`	Defines the VRF table name.
`IP source prefix or local-voip`	Defines the IP source prefix (a.b.c.d/p). MSBR in single network mode can also be set with local-voip to define the route source address to all VoIP packets generated locally by the MSBR
`IP destination prefix`	Defines the IP destination prefix (a.b.c.d/p).
`metric value`	Defines the metric value for this route (0-255).
`track`	Defines the track to be used for this route.
`track id`	Defines the Track ID (1-100).
`output-vrf`	Adds the ability to route traffic received by one VRF from some other VRF. It is configured with the output-vrf option added to the static route configuration.
`description`	Defines the description.
`bfd-neighbor`	Defines the ID of a BFD neighbor to attach the route to.

Interface Type (ifname)		Interface ID
`gigabitethernet`	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
`cellular`	Cellular interface ID	0/0
`gre`	Tunnel GRE ID	[1-255]
`ipip`	Tunnel IPIP ID	[1-255]
`l2tp`	L2TP ID	[0-99]
`pppoe`	PPPoE interface ID	[1-3]
`pptp`	PPTP ID	[0-99]

Interface Type (ifname)		Interface ID
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

N/A

Note

A route that points to an interface that is not associated with the given vrf will be disabled.

Command Mode

Privileged User

Related Commands

ip vrf, show ip route vrf, show data ip

Example

This example route packets received by vrf VOIP1, with destination prefix 10.4.0.0 from interface gi 0/0 (which belongs to vrf VOIP2) to the next hop 10.5.0.1:

```
(config-data)# ip route vrf VOIP1 10.4.0.0 255.255.0.0 10.5.0.1 gi 0/0 output-vrf
VOIP2
```

GRE and IPIP Tunnel Interface Commands

The section describes the GRE and IPIP Tunnel Interface commands.

interface gre|ipip

This command enters a specific WAN tunnel interface configuration. Use the no form of this command to delete the interface.

Syntax

```
interface gre <greID>
interface ipip <ipipID>
```

Command	Description
greID	Assigns a gre tunnel interface id in the range of 1-255.
ipipID	Assigns an ipip tunnel interface id in the range of 1-255.

Default

NA

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example enters a gre id 6 tunnel interface configuration:

```
(config data)# interface gre 6
```

napt

This command sets the NAPT (Network Address Port Translation) on the specified tunnel interface. Use the no form of this command to set route mode.

Syntax

```
napt
```

Default

By default, napt is used.

Command Mode

Privileged User

Example

This example sets the NAPT on GRE 6.

```
# configure data
(config-data)# interface gre 6
(conf-if-GRE 6)# napt
```

ip address

This command defines the local IP address of the specified tunnel interface. Use the no form of this command to remove a configured IP address.

Syntax

```
ip address <ip address>
```

Command	Description
`ip address`	Specifies a valid IPv4 address. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3).

Default

NA

Command Mode

Privileged User

Example

This example configures the IP address of 10.4.2.3 on interface GRE 6.

```
# configure data
(config-data)# interface gre 6
(conf-if-GRE 6)# ip address 10.4.2.3
```

tunnel destination

This command defines the destination IP address of the specified tunnel interface. Use the no form of this command to remove a configured IP address.

Syntax

```
tunnel destination <ip address>
```

Command	Description
`ip address`	Specifies a valid IPv4 address. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3).

Default

NA

Command Mode

Privileged User

Example

This example configures the tunnel destination IP address of 10.4.2.50 on interface GRE 6.

```
(config-data)# interface gre 6
(conf-if-GRE 6)# tunnel destination 10.4.2.50
```

GARP Commands

This section describes the GARP commands.

garp timer

This command configures the GARP timer.

Syntax

```
garp timer <Time>
```

Command	Description
`timer`	Defines the time in seconds (1-3600, default is 60).

Default

60 (seconds)

Note

- This command is applicable only to data-router functionality.
- This command is applicable only to Gigabit Ethernet and fiber WAN interfaces (VLAN 1 only).

Command Mode

Privileged User

Related Commands

garp enable

Example

This example configures the GARP timer to 6 seconds:

```
(config data)# garp timer 6
```

garp enable

This command enables GARP per interface.

Syntax

```
garp enable
no garp enable
```

Default

Disabled

Note

- This command is applicable only to data-router functionality.
- This command is applicable only to Gigabit Ethernet and fiber WAN interfaces (VLAN 1 only).

Command Mode

Privileged User

Related Commands

garp timer

Example

This example enables the GARP timer on the Gigabit 0/0 WAN interface:

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# garp enable
```

CLAT

This section includes the CLAT commands.

clat-enable

This command enables CLAT (customer-side translator) mechanism for 464XLAT on the specified interface.

Syntax

```
clat-enable
```

Default

NA

Command Mode

Privileged User

NA

Notes

To disable CLAT on the interface, use the `no` form of the command.

Related Commands

`router clat`: Configures CLAT.

Example

This example enables CLAT on VLAN 1:

```
#configure data
(config-data)# interface VLAN 1
(conf-if-VLAN 1)# clat-enable
```

router clat

This command configures the device for the CLAT (customer-side translator) mechanism for 464XLAT.

464XLAT provides a simple technique for an IPv4 client with a private address to connect to an IPv4 host over an IPv6 network. 464XLAT only supports IPv4 in the client-server model, where the server has a global IPv4 address. This means, it's not suited for IPv4 peer-to-peer communication or inbound IPv4 connections.

The architecture includes the following components:

- **PLAT (provider-side translator):** Translates N:1 global IPv6 addresses to global IPv4 addresses, and vice versa.
- **CLAT:** Translates private IPv4 addresses to global IPv6 addresses, and vice versa. **Only** this component is supported by the device.

Syntax

```
router clat {ipv4-dst-network|ipv6-dst-prefix|ipv6-src-prefix}
```

Command	Description
`ipv4-dst-network`	Defines the IPv4 destination network to reach via translation (using CLAT).
`ipv6-dst-prefix`	Defines the IPv6 destination prefix (PLAT prefix).
`ipv6-src-prefix`	Defines the IPv6 source prefix (CLAT prefix).

Note

- The IPv6 route must be entered in the destination prefix.
- Up to 5 destination networks can be added.
- The IPv6 source prefix can be added statically or by using prefix delegation interface
- This command is applicable only to Mediant 500Li and Mediant 800Ci.

Command Mode

Privileged User

Related Commands

clat-enable: Enables CLAT on a specific interface

Example

This example configures 464XLAT:

```
(config-data)# router clat
(conf-router-clat)# ipv4-dst-network 198.51.100.1
(conf-router-clat)# ipv6-dst-prefix 2001:db8:1234::198.51.100.1
(conf-router-clat)# ipv6-src-prefix 2001:db8:aaaa::192.168.1.2
```

DNS Server

The following describes the DNS Server commands.

dynamic-dns

This command defines Dynamic DNS (DDNS) service providers (IPv4 and IPv6). You can choose fixed providers (dtc.com, dyndns.org, and no-ip.com) or a user-defined provider. When the interface changes its state to or from connected, the DDNS checks if the address was changed, and sends an update if so.

Syntax

```
# dynamic-dns
(conf-dyndns)# service {custom <Name>|dtc.com|dyndns.org|no-ip.com}
```

```
(conf-dyndns)# service custom <Name>
(conf-<Name>) // see table below
```

Command	Description
`hostname`	Name registered in the DNS service.
`interface`	The interface to send the IP address.
`post-auth`	DNS service credentials.
`success-response`	Server success response strings

Command	Description
update-interval	Period to wait after each DNS update (in days).
url	Changes the URL of the message (after the "https://"). The URL to update the DDNS server when an IP changes must be specified using the following format in the HTTP request: [https/http]://[username]:[password]@[provider_url]?[post-auth]&[hostname=]&[ip=]&[ipv6=]
use-ipvx	In the URL, use ipvx instead of myipvx.
use_ssl_mode	Enables SSL.
username	DNS service credentials.

Command Mode

Privileged User

Note

The URL to update the DDNS server when an IP changes must be specified using the following format in the HTTP request:

[https/http]://[username]:[password]@[provider_url]?[post-auth]&[hostname=]&[ip=]&[ipv6=]

Example

This example defines a custom DDNS and the URL to update the DDNS in HTTP request is "https://www.exampledns.org/update?domains=mik&token=b77b7a89- 68d8- 4204- a29f-f9445583c81a&ip=172.17.119.13&ipv6=2000:3333::3:":

```
(config-data)# dynamic-dns
(conf-dyndns)# service custom MyDDNS
 (conf-MyDDNS)# interface Cellular 0/0/1
 (conf-MyDDNS)# update-interval 10
(conf-MyDDNS)# use_ssl_mode
(conf-MyDDNS)# no username
(conf-MyDDNS)# post-auth domains=mik&token=b77b7a89-68d8-4204-a29f-f9445583c81a
(conf-MyDDNS)# success-response ok OK
```

```
(conf-MyDDNS)# no shutdown
(conf-MyDDNS)# url www.exampledns.org/update
```

ip dns server

This command enables the DNS server on all Layer 3 interfaces. Use the `no` form of this command to disable the DNS server on all Layer 3 interfaces.

Syntax

```
ip dns server all auto
ip dns server all static
no ip dns server all auto
```

Command	Description
`auto`	Automatically sets the DNS server address by the response from the DHCP server. The interface must be set to obtain IP addresses from DHCP.
`static`	Statically sets the DNS server address by the configuration.

Default

NA

Related Commands

`ip host`

The `ip dns server` command is also available from the interface configuration subdirectory (see the `dns-server` command).

Command Mode

Privileged User

Example

This example enables a static DNS server for all Layer 3 interfaces:

```
(config-data)# ip dns server all static
```

ip host

This command adds an entry to the IP hostname table for all Layer 3 interfaces. Use the no form of this command to delete an entry from the IP Hostname table for all Layer 3 interfaces.

The following are the relevant specifications:

- RFC 1034
- RFC 1035
- RFC 2782 (SRV)
- RFC 3403 (NAPTR)

Syntax

```
ip host <name> <ip address> <ttl> <tracking ID>
ip host <name> srv <priority> <weight> <port> <target> <ttl>
ip host <name> naptr <order> <preference> <flags> regexp <regexp> <ttl>
ip host <name> naptr <order> <preference> <flags> service <service> regexp
<regexp> <ttl>
ip host <name> naptr <order> <preference> <flags> service <service>
replacement <replacement> <ttl>
```

Command	Description
name	Specifies the name of the host. Up to 63 characters.
ip address	Specifies the host's IPv4 (dotted decimal notation) or IPv6 address.
ttl	Defines Time-To-Live in seconds, range 0-2147483647.
priority	Defines the priority – a non-negative number with a range 0-65535.
weight	Defines the weight – a non-negative number with a range 0-65535.
port	Non-negative number, range 0-65535.
target	Domain name, up to 256 characters.
order	Non-negative number, range 0-65535.
preference	Non-negative number, range 0-65535.
flags	Currently four flags are defined: "S", "A", "U", and "P" (character-string).
service	Up to 64 characters and must start with an alphabetic (character-

Command	Description
	string).
tracking ID	If Tracking ID is configured, this DNS record is resolved only if the DNS server is unreachable. This is only relevant when a DNS server is configured. If not entered, the DNS record is always resolved.
regexp	Up to 256 characters (character-string).
replacement	Domain name, up to 256 characters.

Default

NA

Related Commands

ip dns server

Command Mode

Privileged User

Examples:

This example adds an entry with name ‘abcd’ and ip address ‘10.44.1.1’ to the IP Hostname table for all Layer 3 interfaces:

```
(config data)# ip host abcd 10.44.1.1 3600
```

This example (taken from RFC 2782) for adding SRV entry to the DNS server table for all Layer 3 interfaces:

```
(config data)# ip host _foobar._tcp srv 0 1 9 old-slow-box.example.com 3600
```

This example (taken from RFC 3403) for adding NAPTR entry to the DNS server table for all Layer 3 interfaces:

```
(config data)# ip host example.com naptr 100 50 A service z3950+N2L+N2C
replacement cidserver.example.com 3600
```

ip flow-export

This command defines the host/port to send flow statistics to. IP flow (NetFlow) is a feature that gives the ability to collect IP network traffic. The NetFlow records are generated from the firewall statistics. Since the NetFlow information is taken from the firewall, you must activate firewall capabilities on the monitored interface.

Syntax

```
ip flow-export enable
ip flow-export destination <a.b.c.d> <port>
ip flow-export version <version number> enable
ip flow-export source-address interface <interface name> <interface-id>
```

Command	Description
enable	Enables IP flow statistics.
destination	Specifies the NetFlow Destination server IP address.
port	Defines the NetFlow server port number (1-65535). The default port is 2055.
source-address	Sets the source of the NetFlow packets. If not specified, the source will be set according to the routing table interface.
version number	Enables NetFlow version number (5 or 9).
a.b.c.d	Defines the Netflow IP address.

Interface Name	Interface Type	Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]

Interface Name	Interface Type	Interface ID
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Command Mode

Privileged User

Example

This example enables IP flow statistics.

```
(config-data)# ip flow-export enable
```

ip fastpath

This command defines Acceleration settings.

Syntax

```
ip fastpath unilateral-timeout <seconds>
```

Command	Description
seconds	Defines Timeout in seconds (0 means connections will never time out).

Default

NA

Command Mode

Privileged User

Example

This example sets the connections so that they don't time out.

```
(config-data)# ip fastpath unilateral-timeout 0
```

dns-view

This command defines a DNS view.

Syntax

```
dns-view <view name>
```

Command	Description
`view name`	Defines the DNS view name.

Default

NA

Command Mode

Privileged User

Example

This example defines a DNS view.

```
(config-data)# dns-view view1
```

set server address

This command defines the DNS server to where the queries matching this DNS view are forwarded.

Syntax

```
# set server address <server ip address>
```

Command	Description
`server ip address`	Defines the server IP address which is one of the device's DNS server's IP address (configured as part of an interface properties); otherwise, the device will not forward to it.

Default

NA

Command Mode

Privileged User

Example

This example defines the DNS server to where the queries matching this DNS view are forwarded.

```
(config-data)# dns-view view1
(dns-view-view1)# set server interface 1.10.1.1
```

match source-address

This command defines the DNS queries by source address for the DNS view.

Syntax

```
# match source address <source IP address of DNS query> <source netmask of DNS query>
```

Default

NA

Command Mode

Privileged User

Example

This example defines the DNS queries by source address for the DNS view.

```
(config-data)# dns-view view1
(dns-view-view1)# match source address 1.1.1.1 12.1.1.1
```

set server interface

This command defines the interface associated with the DNS server.

Syntax

```
# set server interface <interface name> <slot / port /ID>
```

Command	Description
<interface name>	Defines the interface name which is the name of the interface that is configured with the desired DNS server (static or dynamic). This allows configuration of name servers received dynamically by DHCP or PPP.

Default

NA

Command Mode

Privileged User

Example

This example defines the interface.

```
(config-data)# dns-view view1
(dns-view-view1)# set server interface gigabitethernet 0/0
```

ip name-server

This command defines the DNS relay server's address on all Layer 3 interfaces. Use the no form of this command to the undefined DNS relay server's address on all Layer 3 interfaces.

Syntax

```
ip name-server <first ip address> all
ip name-server <first ip address> [<second ip address>|all]
```

Command	Description
`first ip address`	Specifies the primary DNS server address. Specifies a valid IPv4 (dotted-decimal notation) or IPv6 address.
`second ip address`	Specifies the secondary DNS server address. This field is not required when specifying a single IP address. It specifies a valid IPv4 (dotted-decimal notation) or IPv6 address.
`all`	Apply to all interfaces.

Default

NA

Related Commands

This command is also available from the interface configuration sub-directory.

Command Mode

Privileged User

Example

This example defines DNS relay servers 10.4.1.1 and 10.4.1.2 for all Layer 3 interfaces:

```
(config data)# ip name-server 10.4.1.1 10.4.1.2
```

ip max-conn

This command defines the maximum number of firewall connections per IP address.

Syntax

```
ip max-conn <number>
```

Command	Description
`number`	Sets the maximum number of firewall connections per IP address. (200-20000)

Default

NA

Command Mode

Privileged User

Example

This example sets the maximum number of firewall connections per IP address to 500:

```
(config data)# ip max-conn 500
```

DHCP Server

The following describes DHCP Server commands.

ip dhcp-server

This command enables the specified address of the DHCP relay server to be used on the specified interface or on all Layer 3 interfaces. It also provides support for the device to act as a DHCP server for Lync-enabled IP phones, by supporting DHCP Options 120 and 43. DHCP Option 120 enables SIP clients to discover a domain name system (DNS) FQDN (Fully-Qualified Domain Name) of a SIP server (SIP Server Discovery). For detailed information on DHCP Option 120, see RFC 3361. DHCP Option 43 enables devices to discover the Microsoft Lync Server Certificate Provisioning service. For detailed information on how to configure DHCP Option 120 and DHCP Option 43, see http://technet.microsoft.com/en-us/library/gg412828%28v=ocs.14%29.aspx.

Use the no form of this command to disable the address of the DHCP relay server on a specific interface or on all Layer 3 interfaces.

Not all the commands in this section have a no form. See the details in the commands syntax below. The no form for the ip dhcp-server <ip address> command is used to disable the DHCP relay server.

Syntax

```
# ip dhcp-server <ip address>{<interface> <interface ID>}
# ip dhcp-server all <interface> <interface ID>

# no ip dhcp-server <ip address>

# ip dhcp-server network <first ip address> <last ip address> <subnet mask>
# ip dhcp-server dns-server <dns ip address>
# ip dhcp-server netbios-name-server <wins ip address>
```

```
# ip dhcp-server lease <days> <hours> <minutes>

# ip dhcp-server boot-file-name <boot file name>
# no ip dhcp-server boot-file-name

# ip dhcp-server domain-name <domain name>
# no ip dhcp-server domain-name

# ip dhcp-server netbios-node-type <wins node type>
# no ip dhcp-server netbios-node-type

# ip dhcp-server ntp-server <ntp ip address>
# ip dhcp-server tftp-server <tftp ip address>

# ip dhcp-server tftp-server-name <tftp name>
# no ip dhcp-server tftp-server-name

# ip dhcp-server time-offset <time offset>
# no ip dhcp-server time-offset

# ip dhcp-server provide-host-name
# no ip dhcp-server provide-host-name

# ip dhcp-server sip-server <FQDN of SIP server - Option 120)
# ip dhcp-server lync-cert-provisioning <Microsoft Lync Server Certificate
Provisioning service - Option 43>

# ip dhcp-server option82
```

Command	Description
`ip address`	Specifies a valid IPv4 address. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3). Specifies a valid IPv4 address for the DHCP relay server.

`first ip address`
`last ip address`
`subnet mask`
	Specifies the address pool of the DHCP relay server (valid IPv4 address). IP addresses should be expressed in dotted decimal notation.

`dns ip address`	Specifies a valid IPv4 address for the dns server. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3). This parameter is optional.

Command	Description
`wins ip address`	Specifies a valid IPv4 address for wins server. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3). This parameter is optional.

`days`
`hours`
`minutes`
	Specifies the number of days and/or hours and/or minutes for server leases. This parameter is optional (default is 1 hour).

`boot file name`	Specifies the name of the configuration file that the DHCP client should download from the TFTP server. This parameter is optional. (BOOTP / DHCP Option 67).
`domain name`	Specifies the domain name that client should use when resolving hostnames via DNS. This parameter is optional. (BOOTP / DHCP Option 15).
`wins node type`	Specifies the NetBIOS (WINS) node type (i.e. 1 = B-node, 2 = P-node, 4 = M-node, 8 = H-node). This parameter is optional. (BOOTP / DHCP Option 46).
`ntp ip address`	Specifies a valid IPv4 address for NTP server. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3). This parameter is optional. (BOOTP / DHCP Option 42).
`tftp ip address`	Specifies a valid IPv4 address for TFTP server. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3). This parameter is optional. (BOOTP / DHCP Option 150).
`tftp name`	Specifies a TFTP server name. This parameter is optional. (BOOTP / DHCP Option 66).
`time offset`	Specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC). A positive offset indicates a location east of the zero meridian and a negative offset indicates a location west of the zero meridian. This parameter is optional. (BOOTP / DHCP Option 2).
`tr069-acs-server-name`	Supports sending a DHCP response with the URL of an Auto-Configuration Server (ACS) in reply to a DHCP request received from a client with the "dslforum.org" string in the Vendor Class Identifier (DHCP option 60). The device sends the URL in the Vendor Specific Information (DHCP option 43). This is applicable when the device is configured as a DHCP server and is used for TR-069 provisioning.

Command	Description
	Note: This command is applicable only to data-router functionality.
option82	Enables support for DHCP Option 82. This option is received from a DHCP relay agent that forwards client-originated DHCP packets to the device (acting as a DHCP server). When enabled, the device simply "echos" the information of Option 82 back to the DHCP client. The feature is enabled for the interface on which the DHCPv4 server is configured.

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Related Commands

This command is also available from the interface configuration sub-directory.

Command Mode

Privileged User

Example

- This example configures the DHCP relay address of 10.1.2.3 on VLAN 5:

```
# (config-data)# ip dhcp-server 10.1.2.3 vlan 5
```

- The following is an example of how to use tr069-acs-server-name parameter.

```
# (config-data)# interface vlan 10
# (conf-if-VLAN 10)# ip dhcp-server tr069-acs-server-name  srv_1
```

ipv6 dhcp-server dns-server

This command configures the DNS server IPv6 address that is sent by the device's DHCP server to the DHCP clients (workstations) on the LAN.

Syntax

```
# ipv6 dhcp-server dns-server {<static IPv6 address> | :: | auto}
```

Command	Description
`<static IPv6 address>`	Specifies a static IPv6 address (X:X::X:X) for the DNS server. This option can also operate with the `::` option (below).
`::`	The device sends its own link-local ipv6 address as the DNS server. This option can also operate with a static address (above).
`auto`	The device propagates the DNS server IPv6 address that us learned by the DHCPv6 client running on the WAN.

Note

This command is only applicable to MSBR devices.

Command Mode

Privileged User

Example:

The following example saves the IPv6 prefix but does not advertise it.

```
(config-data)# interface vlan 1
(conf-if-GE 0/0)# ipv6 dhcp-server dns-server 2001::1
```

ipv6 dhcp-server vrrp_id

This command configures Virtual Router Redundancy Protocol (VRRP) over IPv6. It associates the DHCPv6 server with the VRRP logical interface.

Syntax

```
# iipv6 dhcp-server vrrp_id <VRRP ID>
```

Command Mode

Privileged User

Example:

The following example configures VRRP ID 5 over IPv6:

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 dhcp-server vrrp_id 5
```

option

This command configures the Dynamic Host Configuration Protocol (DHCP) Server options. Use the no form of this command to remove the options.

Syntax

```
option <DHCP option code> {ascii string|hex string|ip address}
no option code <DHCP option code>
```

Command	Description
DHCP option code	Defines the DHCP option code.
ascii string	Defines an NVT ASCII character string. ASCII character strings that contain white space must be deliminated by quotation marks.
hex string	Defines dotted-hexadecimal data. Each byte in hexadecimal character strings is two hexadecimal digits - each byte can be separated by a period,

Command	Description
	colon, or white space.
ip address	Defines an IP address.

Default

The default instance number is 0.

Command Mode

DHCP pool configuration

Related Commands

ip dhcp pool

Usage Guidelines:

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options. The current set of DHCP options are documented in RFC 2131, Dynamic Host Configuration Protocol.

Examples:

This example configures DHCP Option 19, which specifies whether the client should configure its IP layer for packet forwarding. A value of “0” means disable IP forwarding; a value of “1” means enable IP forwarding. IP forwarding is enabled in This example:

(config-data)# ip dhcp pool gigabitethernet 0/0

```
# option code 19 hex 01
```

This example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in This example:

```
# option code 72 ip 172.16.3.252 172.16.3.253
```

service dhcp

This command enables the DHCP server on the specified interface or on all Layer 3 interfaces. Use the no form of this command to disable DHCP server on a specific interface or on all Layer 3 interfaces.

Syntax

```
service dhcp all
service dhcp gigabitethernet [slot/port.vlanID]
service dhcp vlan <vlan id>
```

Command	Description
`all`	Enables/disables all interfaces.
`slot/port.vlanID`	Defines the GigabitEthernet interface slot and port (Vlan ID is optional).
`vlan id`	Defines the VLAN interface.

Default

All interfaces are disabled.

Note

This command enables/disables the DHCP server created via the “ip dhcp pool” command.

Related Commands

Ip dhcp pool

The service dhcp command is also available from the interface configuration sub-directory.

Command Mode

Privileged User

Example

This example enables the DHCP server on VLAN 5:

```
(config data)# service dhcp vlan 5
```

DHCPv4 Client

This section describes DHCPv4 client commands

ip address dhcp

This command enables a DHCP client on the specified interface. Use the no form of this command to disable DHCP client functionality.

Syntax

```
ip address dhcp
no ip address dhcp
```

Default

NA

Note

The interface's IP address will be acquired via DHCP.

Command Mode

Privileged User

Example

This example configures a DHCP client on VLAN 6.

```
(config-data)# interface vlan 6
(conf-if-VLAN 6)# ip address dhcp
```

ip dhcp-client authentication key-id

This command configures authentication of DHCPv4 messages between the client and server. This command configures the authentication key (for up to two key IDs) that the device (as a DHCP client) sends in DHCP Option 90 (Management) to a DHCP server for authentication.

Syntax

```
ip dhcp-client authentication key-id <ID> key-string|obscured-key-string <Key Name>
```

Command	Description
key-id	Pre-configured unique identifier shared with server.
key-string	The actual key itself used to validate and sign DHCP messages.
obscured-key-string	The actual key itself used to validate and sign DHCP messages, but obscured (not displayed) for security.

Command Mode

Privileged User

Example

This example configures authentication for DHCPv4 messages on VLAN 3.

```
(config-data)# interface vlan 3
(conf-if-VLAN 3)# ipv6 dhcp-client authentication key-id 3 obscured-key-string
8JKQkJybmw==
(conf-if-VLAN 3)# no shutdown
(conf-if-VLAN 3)# exit
```

ip dhcp-client class-id

This command enables configuration of DHCP Option 60 (Vendor Class Identifier) to be sent by the client.

Syntax

```
ip dhcp-client class-id <string>
```

Command	Description
string	The “vendor class id” string (Option 60) to be sent in the DHCP negotiation.

Default

Option 60 is not sent by default

Command Mode

Privileged User

Related Commands

ip address dhcp

Example

This example configures a new VLAN interface, enables DHCP, and sets the vendor class string to “MSBR”.

```
(config-data)# interface vlan 3
(conf-if-VLAN 3)# ip address dhcp
(conf-if-VLAN 3)# ip dhcp-client class-id "MSBR"
(conf-if-VLAN 3)# no shutdown
(conf-if-VLAN 3)# exit
```

ip dhcp-client default-route

This command configures the device to accept the gateway received via DHCP as the default route for this interface or for a specific VRF on this interface.

Use the “no” form of this command to disregard the gateway received via DHCP.

Syntax

```
ip dhcp-client default-route [track <track id>] [vrf <VRF name>]
```

Command	Description
`default-route`	Defines the gateway received via DHCP as the default route on this interface.
`track id`	Defines a track ID that the default route depends on. The range is 1-100.
`vrf`	Defines the VRF (or "main-vrf").for which the gateway received via DHCP is the default route.

Default

no ip dhcp-client default-route

Command Mode

Privileged User

Related Commands

ip address dhcp

Example

This example configures a new vlan interface, enables dhcp & default gateway

```
(config-data)# interface vlan 3
(conf-if-VLAN 3)# ip address dhcp
(conf-if-VLAN 3)# ip dhcp-client default-route track 1
(conf-if-VLAN 3)# no shutdown
(conf-if-VLAN 3)# exit
```

ip dhcp-client retain-address

This command enables the device to not request the previous address obtained through DHCP.

Syntax

```
ip dhcp-client retain-address
```

Command Mode

Privileged User

Example

This example enables the device to not request the previous address obtained through DHCP for the Gigabit Ethernet interface.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ip dhcp-client retain-address
```

ip dhcp-client request

This command enables the configuration of DHCP Options (e.g., 160) for auto-provisioning the device (as a DHCP client).

For DHCP Option 160, the DHCP server can specify one of the following file combinations in each URL:

- Software file (.cmp) only
- Software file and ini file (.ini)
- Software file and Configuration Package file
- Software file and CLI Startup Script file

Syntax

```
ip dhcp-client request <DHCP Option>
```

Command	Description
DHCP Option	Defines the DHCP option sent in the DHCP negotiation.

Command Mode

Privileged User

Related Commands

ip address dhcp

Example

This example configures the device to send a DHCP Option 160 request to the DHCP server.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ip dhcp-client request 160
```

ip dhcp-client sip-server-address

This command enables the device to request the SIP server's IP address (and other information) in the sent DHCP Option 120 request as Request List Items in Option 55.

Use the “no” form of this command to disable.

Syntax

```
ip dhcp-client sip-server-address
```

Default

no ip dhcp-client sip-server-address

Command Mode

Privileged User

Example

This example enables the device to request the SIP server's IP address (and other information) in the sent DHCP Option 120 request as Request List Items in Option 55, for the Gigabit Ethernet interface:

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ip dhcp-client sip-server-address
```

ip dhcp-source-address

This command allows the user to configure the DHCP relay source address. This command is valid only in case of DHCP relay (remote).

Syntax

- Mediant 500Li, Mediant 800Ci, and MP-5xx:

```
ip dhcp-source-address interface
ip dhcp-source-address <IP Address>
```

- Mediant 500L MSBR, Mediant 500 MSBR, Mediant 500C MSBR, Mediant 800B MSBR, and Mediant 800C MSBR:

```
ip dhcp-source-address all <IP Address>
ip dhcp-source-address <Interface Name> <IP Address>
```

Command	Description
<IP Address>	Specifies a valid IPv4 address (in dotted decimal notation, for example, 10.1.2.3) for the DHCP relay source address.
`all`	Enables all interfaces. **Note:** Applicable only to Mediant 500L MSBR, Mediant 500 MSBR, Mediant 500C MSBR, Mediant 800B MSBR, and Mediant 800C MSBR.
`interface`	Uses the IP address of the LAN interface under which the command is run as the source address. **Note:** Applicable only to Mediant 500Li, Mediant 800Ci, and MP-5xx.
<Interface Name>	Defines the interface. **Note:** Applicable only to Mediant 500L MSBR, Mediant 500 MSBR, Mediant 500C MSBR, Mediant 800B MSBR, and Mediant 800C MSBR.

Default

NA

Notes

- The address should be of one of the local interfaces.
- If you don't configure `dhcp-source-address`, the default behavior is to use the source address of the WAN interface that is used to communicate with the DHCP server.

Command Mode

Privileged User

Related Commands

The `dhcp-source-address` command takes effect only when the DHCP Relay server is configured (see the `ip dhcp-server` command).

Example

- Mediant 500Li, Mediant 800Ci, and MP-5xx:

  This example configures VLAN 5 to relay DHCP requests to 10.5.5.11 and use the IP address of VLAN 5 as the source address on the relayed packets:

```
(config-data)# interface vlan 5
(conf-if-vlan 5)# ip dhcp-server 10.5.5.11
(conf-if-vlan 5)# ip dhcp-source-address interface
```

- Mediant 500L MSBR, Mediant 500 MSBR, Mediant 500C MSBR, Mediant 800B MSBR, and Mediant 800C MSBR:

  This example configures VLAN 5 to relay DHCP requests to 10.5.5.11 and use 10.4.4.11 as the source address on the relayed packets:

```
(config-data)# ip dhcp-server 10.5.5.11 vlan 5
(config-data)# ip dhcp-source-address vlan 5 10.4.4.11
```

ip dhcp pool

This command assigns a pool on a specified interface and enters the pool configuration.

Syntax

```
ip dhcp pool <interface name> <interface ID>
```

Command	Description
<interface name>	Defines interface naming on the interface command.

Interface Name	Interface Type	Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

NA

Related Commands

service dhcp

The ip dhcp pool command is also available from the interface configuration sub-directory. See ip dhcp-server.

Command Mode

Privileged User

Example

This example enters IP DHCP POOL on VLAN 5.

```
(config data)# ip dhcp pool vlan 5
```

boot-file-name

This command defines the name of the configuration file that the DHCP client should download from the TFTP server on the specified interface.

Syntax

```
boot-file-name <boot file name>
no boot-file-name
```

Command	Description
`boot file name`	Specifies the name of the configuration file that the DHCP client should download from the TFTP server. This parameter is optional. (BOOTP / DHCP Option 67).

Default

NA

Functional notes

NA

Command Mode

Privileged User

Related Commands

This command is also available from the interface configuration sub-directory. See ip dhcp-server.

Example

This example sets the name of the configuration file that should be downloaded.

```
(dhcp-conf-VLAN 5)# boot-file-name my-config
```

This example clears this parameter.

```
(dhcp-conf-VLAN 5)# no boot-file-name
```

domain-name

This command defines the domain name that client should use when resolving hostnames via DNS on the specified interface.

Syntax

```
domain-name <domain name>
no domain-name
```

Command	Description
`domain name`	Specifies the domain name that client should use when resolving hostnames via DNS. This parameter is optional. (BOOTP / DHCP Option 15).

Default

NA

Functional notes

NA

Command Mode

Privileged User

Related Commands

This command is also available from the interface configuration sub-directory. See ip dhcp-server.

Example

This example sets the domain name.

```
(dhcp-conf-VLAN 5)# domain-name domain.name.com
```

This example clears the domain name.

```
(dhcp-conf-VLAN 5)# no domain-name
```

dns-server

This command defines the DNS servers for the DHCP pool on the specified interface.

Syntax

```
dns-server <ip address>
```

Command	Description
<ip address>	Specifies a valid IPv4 address. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3).

Default

NA

Command Mode

Privileged User

Example

This example enters the ip dhcp pool on VLAN 5 and sets the DNS server to 10.1.2.3.

```
(dhcp-conf-VLAN 5)#dns-server 10.1.2.3
```

lease

This command defines the address lease time assigned to the DHCP pool on the specified interface.

Syntax

```
lease <days> [hours] [minutes]
```

Command	Description
<days>	Sets the number of days (mandatory). Range is 0 to 365.
<hours>	Sets the number of hours. Range is 0 to 23.
<minutes>	Sets the number of minutes. Range is 0 to 59.

Default

By default, the lease time is set to 1 hour.

Related Commands

This command is also available from the interface configuration sub-directory. See ip dhcp-server.

Command Mode

Privileged User

Example

This example enters ip dhcp pool on VLAN 5 and sets the lease time to 5 hours and 15 minutes.

```
(dhcp-conf-VLAN 5)# lease 0 5 15
```

netbios-name-server

This command defines a NetBIOS Windows Internet Naming Service (WINS) name servers assigned to the DHCP pool on the specified interface.

Syntax

```
netbios-name-server <ip address>
```

Command	Description
<ip address>	Specifies a valid IPv4 address. IP addresses should be expressed in dotted decimal notation (e.g., 10.1.2.3).

Default

NA

Related Commands

This command is also available from the interface configuration sub-directory. See

ip dhcp-server.

Command Mode

Privileged User

Example

This example enters ip dhcp pool on VLAN 5 and sets the NetBIOS name server to 10.1.2.3.

```
(dhcp-conf-VLAN 5)# netbios-name-server 10.1.2.3
```

netbios-node-type

This command specifies the NetBIOS (WINS) node type (i.e. 1 = B-node, 2 = P-node, 4 = M-node, 8 = H-node) on the specified interface.

Syntax

```
netbios-node-type <wins node type>
no netbios-node-type
```

Command	Description
<wins node type>	Specifies the NetBIOS (WINS) node type (i.e. 1 = B-node, 2 = P-node, 4 = M-node, 8 = H-node). This parameter is optional. (BOOTP / DHCP Option 46).

Default

NA

Functional notes

NA

Command Mode

Privileged User

Related Commands

This command is also available from the interface configuration sub-directory. See ip dhcp-server.

Example

This example sets the WINS note type to B-node (= 1).

```
(dhcp-conf-VLAN 5)# netbios-node-type 1
```

This example clears this parameter.

```
(dhcp-conf-VLAN 5)# no netbios-node-type
```

network

This command defines the network address and mask for the DHCP pool. This command is mandatory for assigning dhcp pool on the interface.

Syntax

```
network <first ip> <last ip> <mask>
```

Command	Description
<first ip>	First IP address in the range for this pool. Specifies a valid IPv4 address. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3).
<last ip>	Last IP address in the range for this pool. Specifies a valid IPv4 address. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3).
<mask>	Specifies the subnet mask that corresponds to a range of IP addresses. Subnet masks should be expressed in dotted decimal notation (for example, 255.255.255.0).

Default

NA

Related Commands

This command is also available from the interface configuration sub-directory.

Command Mode

Privileged User

Example

This example enters ip dhcp pool on VLAN 5 and sets the Network addresses and mask for the pool.

```
(dhcp-conf-VLAN 5)#network 10.4.60.1 10.4.60.5 255.255.0.0
```

override-router-address

This command overrides the router address assigned to the DHCP pool on the specified interface.

Syntax

```
override-router-address <IP Address>
```

Command	Description
<ip address>	Specifies a valid IPv4 address. IP addresses should be expressed in dotted decimal notation (e.g., 10.1.2.3).

Default

NA

Command Mode

Privileged User

Related Commands

This command is also available from the interface configuration sub-directory.

Examples:

This example overrides the router address to 10.1.2.3.

```
(dhcp-conf-VLAN 5)# override-router-address 10.1.2.3
```

provide-host-name

This command enables the device to provide host name if not specified by client on the specified interface. Use the no form of this command to disable this behavior.

Syntax

```
provide-host-name
no provide-host-name
```

Default

The device provides host name if not specified by the client.

Functional notes

NA

Command Mode

Privileged User

Related Commands

This command is also available from the interface configuration sub-directory. See ip dhcp-server.

Example

This example will enable the device to provide a host name.

```
(dhcp-conf-VLAN 5)# provide-host-name
```

This example disables this behavior.

```
(dhcp-conf-VLAN 5)# no provide-host-name
```

tftp-server

This command defines a TFTP server assigned to the DHCP pool on the specified interface.

Syntax

```
tftp-server <tftp ip address>
```

Command	Description
`tftp ip address`	Specifies a valid IPv4 address for TFTP server. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3). This parameter is optional. (BOOTP / DHCP Option 150).

Default

NA

Functional notes

NA

Command Mode

Privileged User

Related Commands

This command is also available from the interface configuration sub-directory. See ip dhcp-server.

Example

This example sets the TFTP server IP address.

```
(dhcp-conf-VLAN 5)# tftp-server 10.4.4.1
```

tftp-server-name

This command defines a TFTP server name assigned to the DHCP pool on the specified interface.

Syntax

```
tftp-server-name <tftp name>
no tftp-server-name
```

Command	Description
`tftp name`	Specifies a TFTP server name. This parameter is optional. (BOOTP / DHCP Option 66).

Defaults

NA

Functional notes

NA

Command Mode

Privileged User

Related Commands

This command is also available from the interface configuration sub-directory. See ip dhcp-server.

Example

This example sets the TFTP server name.

```
(dhcp-conf-VLAN 5)# tftp-server-name servername
```

This example clears the TFTP server name.

```
(dhcp-conf-VLAN 5)# no tftp-server-name
```

time-offset

This command defines the offset of the client's subnet in seconds from Coordinated Universal Time (UTC) on the specified interface.

Syntax

```
time-offset <time offset>
no time-offset
```

Command	Description
`time offset`	Specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC). A positive offset indicates a location east of the zero meridian and a negative offset indicates a location west of the zero meridian. This parameter is optional. (BOOTP / DHCP Option 2).

Default

NA

Functional notes

NA

Command Mode

Privileged User

Related Commands

This command is also available from the interface configuration sub-directory. See ip dhcp-server.

Example

This example sets the offset time to 500 seconds.

```
(dhcp-conf-VLAN 5)# time-offset 500
```

This example removes this parameter.

```
(dhcp-conf-VLAN 5)# no time-offset
```

service dhcp

This command enables the DHCP server on the interface. Use the no form of this command to disable the DHCP server.

Syntax

```
service dhcp
no service dhcp
```

Default

The DHCP server is disabled.

Note

This command enables/disables the DHCP server created via the ip dhcp pool and ip dhcp-server commands.

Related Commands

ip dhcp pool, Ip dhcp-server

The service dhcp command is also available from the main data configuration directory (see ip dhcp pool and ip dhcp-server).

Command Mode

Privileged User

Example

This example enables the DHCP server on VLAN 5:

```
(conf-if-VLAN 5)# service dhcp
```

DHCPv6 Client

This section describes DHCPv6 client commands.

ipv6 dhcp-client authentication

This command configures authentication of DHCPv6 messages between the client and server.

Syntax

```
ipv6 dhcp-client authentication realm <Realm Name> key-id <ID> key-string|obscured-key-string <Key Name>
```

Command	Description
realm	DHCP realm name. Enables re-use of the same key-id for different operators.
key-id	A number used by both client and server to identify the key used in signature calculation.
key-string	Defines the key used to sign the messages.

Command Mode

Privileged User

Example

This example configures authentication for DHCPv6 messages on VLAN 3.

```
(config-data)# interface vlan 3
(conf-if-VLAN 3)# ipv6 dhcp-client authentication realm real_new key-id 3
obscured-key-string 8JKQkJybmw==
(conf-if-VLAN 3)# no shutdown
(conf-if-VLAN 3)# exit
```

ipv6 dhcp-client cable-labs-opt-17

This command configures the device as a DHCPv6 client for sending vendor-specific sub-options 4-10 in DHCPv6 requests (Option 17), which provide device identification properties to the DHCP server.

The sub-options provided the following information:

- Sub-option code 4: Device serial number
- Sub-option code 5: Hardware version
- Sub-option code 6: Software version
- Sub-option code 7: Boot ROM version
- Sub-option code 8: Vendor OUI
- Sub-option code 9: Device model number
- Sub-option code 10: Vendor identifier

Syntax

```
ipv6 dhcp-client cable-labs-opt-17
```

Command Mode

Privileged User

Related Commands

ipv6 dhcp-client opt-17-sub-1 enterprise

Notes

By default, this command is on (sub-options 4-10 sent); If set to no, sub-options are not sent even if the command `ipv6 dhcp-client opt-17-sub-1 enterprise` is set.

Example

This example configures the DHCPv6 client to send Option 17 (with sub-options 4-10).

```
(config-data)# interface vlan 3
(conf-if-VLAN 3)#  ipv6 dhcp-client cable-labs-opt-17
(conf-if-VLAN 3)# no shutdown
(conf-if-VLAN 3)# exit
```

ipv6 dhcp-client force-dns

This command enforces the receipt of DNS information over DHCPv6.

As the DHCPv6 Solicit/Request includes Option 23 (DNS), the device reties the solicit if the DHCPv6 Advertise/Reply does not include a response for Option 23.

Syntax

```
ipv6 dhcp-client force-dns
```

Command Mode

Privileged User

Example

This example enforces the receipt of DNS information over DHCPv6.

```
(config-data)# interface vlan 3
(conf-if-VLAN 3)# ipv6 dhcp-client force-dns
(conf-if-VLAN 3)# no shutdown
(conf-if-VLAN 3)# exit
```

ipv6 dhcp-client ntp-server opt56

This command configures the device as a DHCPv6 client to send DHCP Option 56 (NTP Server) to the DHCP server to request the address of the NTP server.

Syntax

```
ipv6 dhcp-client ntp-server opt56
```

Command Mode

Privileged User

Example

This example configures the DHCPv6 client to send Option 56.

```
(config-data)# interface vlan 3
(conf-if-VLAN 3)#  ipv6 dhcp-client ntp-server opt56
(conf-if-VLAN 3)# no shutdown
(conf-if-VLAN 3)# exit
```

ipv6 dhcp-client opt-17-sub-1 enterprise

This command configures the device as a DHCPv6 client and configures the Enterprise number for sub-options 1 and 4-10 in DHCPv6 requests (Option 17). If not set, they are not sent. If set, they are sent under the enterprise set.

The sub-options provided the following information:

- Sub-option code 4: Device serial number
- Sub-option code 5: Hardware version
- Sub-option code 6: Software version
- Sub-option code 7: Boot ROM version
- Sub-option code 8: Vendor OUI
- Sub-option code 9: Device model number
- Sub-option code 10: Vendor identifier

Syntax

```
ipv6 dhcp-client opt-17-sub-1 enterprise
```

Command Mode

Privileged User

Related Commands

ipv6 dhcp-client cable-labs-opt-17

Notes

If the command `ipv6 dhcp-client cable-labs-opt-17` is set to `no`, sub-options 4-10 are not sent, even if the command `ipv6 dhcp-client opt-17-sub-1 enterprise` is set.

Example

This example configures the DHCPv6 client to send sub-options 1 and 4-10 in Option 17.

```
(config-data)# interface vlan 3
(conf-if-VLAN 3)#  ipv6 dhcp-client opt-17-sub-1 enterprise
(conf-if-VLAN 3)# no shutdown
(conf-if-VLAN 3)# exit
```

ipv6 dhcp-client pd

This command configures the DHCPv6 client to request an IPv6 prefix from a DHCPv6 server. This is referred to as prefix delegation.

Syntax

```
ipv6 dhcp-client pd {<Prefix Length>|rapid-commit}
```

Command	Description
`<Prefix Length>`	Defines the prefix length
`rapid-commit`	Enables the DHCPv6 client to obtain configuration parameters from a server through a rapid two-message exchange (solicit, reply).

Command Mode

Privileged User

Example

This example enables prefix delegation for a DHCPv6 client through VLAN 3.

```
(config-data)# interface vlan 3
(conf-if-VLAN 3)# ipv6 dhcp-client pd 10
(conf-if-VLAN 3)# no shutdown
(conf-if-VLAN 3)# exit
```

ipv6 dhcp-client prefix-len-128

This command changes the prefix length of an IPv6 address that has been acquired through DHCP to 128 bit (instead of the default, 64).

Syntax

```
ipv6 dhcp-client prefix-len-128
```

Default

64 (use the no command)

Note

The interface's IP address is acquired via DHCP.

Command Mode

Privileged User

Example

This example configures a DHCP client on VLAN 6.

```
(config-data)# interface vlan 6
(conf-if-VLAN 6)# ipv6 dhcp-client prefix-len-128
```

ipv6 dhcp-client vendor-class enterprise

This command configures the DHCPv6 Option 124, which indicates that the device is manufactured (vendor) by or supports this enterprise's actions.

Syntax

```
ipv6 dhcp-client vendor-class enterprise {<number> <string>|audc|broadband}
```

Command	Description
<Number> <String>	Defines the Enterprise Number as registered with IANA, and the string identifying the enterprise.
audc	Sets AudioCodes Enterprise Number 4923 and string "audiocodes.com".
broadband	Sets Broadband (ADSL) forum Enterprise Number 3561 and string "dslforum.org".

Command Mode

Privileged User

Example

This example configures the DHCP vendor class as that of AudioCodes.

```
(config-data)# interface vlan 3
(conf-if-VLAN 3)# ipv6 dhcp-client vendor-class audc
(conf-if-VLAN 3)# no shutdown
(conf-if-VLAN 3)# exit
```

ipv6 dhcp-client vendor-specific

This command enables the device as a DHCPv6 client to exchange vendor-specific information with the DHCP server, which is done using the DHCP Vendor-Specific Information Option.

Syntax

```
ipv6 dhcp-client vendor-specific
```

Command Mode

Privileged User

Example

This example enables the DHCP Vendor-Specific Information Option.

```
(config-data)# interface vlan 3
(conf-if-VLAN 3)#  ipv6 dhcp-client vendor-specific
(conf-if-VLAN 3)# no shutdown
(conf-if-VLAN 3)# exit
```

flowcontrol

This command configures a flow control mechanism to prevent buffer congestion and packet drop switch. In full duplex operation, the sender is notified to start or stop the transmission via a PAUSE frame, based on IEEE 802.3x standard. The Gigabit Ethernet switch can transmit, receive and react accordingly to 802.3x flow control frames. Flow control can be enabled or disabled per port.

Syntax

```
flowcontrol {auto|off|rx|rxtx|tx}
```

Command	Description
`flowcontrol auto`	Flow control auto mode.
`flowcontrol off`	Disables the interface to receive and send pause frames.
`flowcontrol rx`	Enables the interface to receive and process pause frames.
`flowcontrol rxtx`	Enables the interface to send and receive pause frames.
`flowcontrol tx`	Enables the interface to send pause frames to remote devices.

Note

- Supported interfaces: Gigabitethernet (0/0, 1/1, 1/2, 1/3, 1/4) and fiber 0/0
- Default values: All interfaces, except Fiber 0/1 by default are configured with `flowcontrol auto`; Fiber 0/1 is configured with `flowcontrol rxtx`.
- The flow control status for physical interfaces is displayed in the `show run` command:

  ```
  Flow Control: RXTX (Remote: RX)
  ```

  Where:

  - *Flow Control* indicates the ability to send (Tx) or receive (Rx) PAUSE frames from a local (device) perspective.
  - *Remote* indicates the partner port's ability to send or receive PAUSE frame.
- This command is applicable only to Mediant 500Li and Mediant 800Ci.

Command Mode

Privileged User

Example

This example configures enables the interface to receive and process pause frames:

```
# configure data
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# flowcontrol rx
```

ip dns randomization

This command supports DNS queries source port and Query ID randomization. The purpose is to prevent DNS spoofing attacks. There are two modes of operation:

- Forwarding Plan
- DNS proxy.

In Forwarding Plan mode (where an external DNS server on the MSBR's WAN side is advertised), only the source port will be randomized.

In DNS proxy mode (where MSBR itself is configured as DNS server on its LAN side), both DNS Query ID and source port used on the MSBR's WAN side, will be randomized.

Syntax

```
# ip dns randomization
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example activates the randomization feature on all DNS queries outgoing from the MSBR to the WAN side.

```
(config-data)# ip dns randomization
```

ip domain localhost

This command configures a DNS hostname for the device.

Syntax

```
# ip domain localhost <hostname>
```

The hostname can include placeholders for the device's MAC address and serial number. The placeholders are replaced by the actual MAC address and serial number of the device. The following placeholders (case-insensitive) can be used:

- For MAC address: {mac}
- For serial number: {sn}

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

- This example uses a placeholder for the MAC:

```
(config-data)# ip domain localhost msbr-{mac}
```

  The hostname is replaced by "msbr-11:11:11:11:11:11" if 11:11:11:11:11:11 is the device's MAC.

- This example uses a placeholder for the serial number:

```
(config-data)# ip domain localhost msbr-{sn}
```

  The hostname is replaced by "msbr-1343452" if 134452 is the device's serial number.

ip reassembly

This command defragments received fragmented IP packets from an interface and then reassembles the packets before forwarding them. The Wireshark packet analyzer is typically used to identify fragmented frames.

This capability is applied per interface and therefore, the CLI command must be set for the relevant IP interface. By default, this capability is disabled per interface.

Syntax

```
ip reassembly
no ip reassembly
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

The following is an example of how this command can be used.

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ip reassembly
```

ip tcp adjust-mss

This command configures the Maximum Segment Size (MSS) on a specific interface.

Syntax

```
ip tcp adjust-mss <mss value>
```

Command	Description
`mss value`	Sets the MSS value. Range is 0- 65535.

Note

MSS-value of 0 indicates that no MSS has been set.

Command Mode

Privileged User

Example

This example configures the tunnel interface.

```
# configure data
(config-data)# interface gre 1
(conf-if-GRE 1)# ip tcp adjust-mss 500
```

mtu

This command configures the Maximum Transmission Unit (MTU) on the specified interface.

Syntax

```
mtu auto
mtu dhcp
mtu <mtu value>
```

Command	Description
`auto`	Sets MTU automatically.
`dhcp`	Sets MTU by DHCP.
`mtu value`	Sets the MTU value. Range is 68 to 1500.

Default

MTU is set to auto (usually 1500).

Command Mode

Privileged User

Example

This example sets the MTU value to 770 bytes on VLAN 6.

```
(config-data)# interface vlan 6
(conf-if-VLAN 6)# mtu 770
```

network

This command allows selecting whether an interface is logically part of the LAN or part of the WAN.

QoS and NAPT functions handle traffic routed from LAN interfaces to WAN interfaces; port forwarding rules (static NAPT) work only on WAN interfaces; and the default firewall policy prevents inbound packets from WAN interfaces unless solicited by an active connection.

Syntax

```
network {lan|wan}
```

Command	Description
`lan`	Define a LAN interface.

Command	Description
wan	Define a WAN interface.

Default

VLAN interfaces default to LAN; all other interfaces default to WAN.

Command Mode

This command is available in interface configuration context.

Example

This example defines a LAN interface:

```
(config-data)# interface atm 0/0
(conf-atm0/0)# network lan
```

service tcp keepalives

This command controls the tcp keepalive functionality of newly created sockets.

Syntax

```
service tcp keepalives enable
service tcp keepalives interval <interval>
service tcp keepalives probe <probe>
service tcp keepalives time <time>
```

Command	Description
enable	Enables the TCP keepalive. The default value is "Disabled".
interval	Defines the interval between sub sequential keepalive probes in seconds. The default value is 75 seconds. The range is1-65355.
probe	Defines the number of unacknowledged probes to send before considering the connection inactive and notifying the application layer. The default value is 9 probes. The range is 1-65355.
time	Defines the interval between the last data packet sent and the first keepalive probe. The default value is 7200 seconds. The range is 1-65355.

Note

- This command is applicable only to data-router functionality.
- The default values are active only if keep-alive is enabled.

Command Mode

Privileged User

Example

This example enables tcp keepalives.

```
(config-data)# service tcp keepalives enable
```

IP Destination Reachability

The following describes IP Destination Reachability commands.

track

This command defines a tracking destination to be used by static routes or other configured elements. This command tracks a destination IP address from a given source interface. The tracking is done by sending ICMP probe packets and monitors the replies. If the destination is reachable, the Track Status is set to 'up'. When a configurable number of replies are not received, the Track Status is set to 'down'.

Syntax

```
track <Track ID> {icmpecho | icmp6echo} {<Destination Address>|dyn-dns-server} <Source Interface> <Interface ID> [source-ip-interface <Interface>] [interval <Value>] [retries <Value>] description <Description>
```

Command	Description
Destination Address	Defines the IP address of the tracked destination (IPv4 or IPv6).
`description`	(Optional) Defines a description (max. 64 bytes) of the tracking destination.
`dyn-dns-server`	The device automatically obtains the tracking destination for the specific source

Command	Description
	interface (instead of specifying an IP address). The destination is obtained from the DNS server that is associated with the source interface when using DHCP or PPP.
`icmpecho`	Tracking is done by sending ICMP probes and monitors the replies.
`icmpv6echo`	Tracking is done by sending ICMPv6 probes and monitors the replies
`interval`	Defines the interval (in seconds) between probes. Range is 1-3600. The default is 5 seconds.
`max-rtt`	Defines the maximum round-trip time (RTT) in milliseconds for each probe of the `retries` command, after which the track status changes to "down". For example, if configured to 2 ms and `retires` to 3, if 4 consecutive probes (3 additional attempts after the first one fails) where each is within 2 ms is unsuccessful, the status changes to "down". The default is 0 (disabled).
`retries`	Defines the number of consecutive failed retries probes (after first probe failed) before the track status changes to “down”. Range is 0 – 20. (Default value is 3). **Note:** The maximum time for each probe can also be configured, by the `max-rtt` command.
`retries-up`	If the tracking destination status is "down" and the device probes it successfully for this user-defined number of consecutive attempts, the track status changes to "up" (i.e., reachable). For example, if configured to 0, the first successful probe changes the status to "up". The default is 0.
Source Interface	Defines the interface name and ID (see table below).

Command	Description
source-ip-interface	Defines an interface whose IP address is used as the source IP address for the probes (see table below).
track id	Defines the track identifier to be used by other entities.
track protocol type	Defines the reachability by sending ping packets of either IPv4 or IPv6 (currently only probe type).

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

N/A

Command Mode

Privileged User

Related Commands

show data track brief, ip route

Examples:

- This example defines Track ID 5 for destination 10.30.4.5 from interface GigabitEthernet 0/0.

```
(config-data)# track 5 icmpecho 10.30.4.5 GigabitEthernet 0/0 description Track_Google_from_GE
```

- This example defines Track ID 5 for a destination obtained automatically from a DNS server from interface GigabitEthernet 0/0.

```
(config-data)# track 5 icmpecho dyn-dns-server GigabitEthernet 0/0 description Track_Google_from_GE
```

- This example defines Track ID 5 for destination 10.30.4.5 from interface GigabitEthernet 0/0 and source IP address of interface loopback 1.

```
(config-data)# track 5 IcmpEcho 10.30.4.5 GigabitEthernet 0/0 source-ip-interface loopback 1
```

bfd neighbor

This command is used to define a BFD neighbor. To set BFD OSPF timers, see ip ospf bfd on page 825.

Syntax

```
bfd neighbor <neighbor id> <ip address> <interface ID> interval <value> min_rx <value> multiplier <value> [multihop]
```

Command	Description
`neighbor id`	(1-20) Neighbor identifier
`ip address`	Address of the remote BFD device
`interface id`	Name and number of the outgoing interface
`interval`	(200-30000) Desired interval for outgoing bfd messages in milliseconds. The interval will be increased if the remote system requires it.

Command	Description
min_rx	(200-30000) Minimal interval between bfd messages in milliseconds. The remote system will use this interval for sending messages in case its interval is lower.
multiplier	(1-20) Maximum number of packets that can be missed before the session status is considered down.
multihop	Set the neighbor to multihop mode in case the remote device is not on the local LAN.

Default

N/A

Command Mode

Privileged User

Related Commands

show data bfd neighbors, ip route

Example

This example configures a BFD neighbor with ip address 192.168.0.100 on vlan 1

```
(config-data)# bfd neighbor 1 192.168.0.100 vlan 1 interval 200 min_rx 200
multiplier 3
```

ip sla responder udp-echo

This command configures the device as a responder to Cisco's IP Service Level Agreements (SLAs) UDP jitter test monitor protocol (MOS and QoS). The device replies with control packets and UDP echo measurement packets.

Up to one instance of the service (in one VRF) is supported. Up to 5 UDP measurement streams are supported.

Syntax

```
ip sla responder udp-echo [vrf <VRF Name>]
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Related Commands

`show data ip sla responder`

Example

The following is an example of how this command can be used.

```
(config-data)# ip sla responder udp-echo vrf LAB1
```

72 Security

The following describes Security commands.

ip synflood-protection

This command enables TCP SYN-flood protection.

Syntax

```
ip synflood-protection {enable|rate}
```

Command	Description
enable	Enables this command.
rate	Defines the rate The rate (your number is multiples by ten)

Default

NA

Command Mode

Privileged User

Example

This example enables TCP SYN-flood protection.

```
(config-data)# ip synflood-protection enable
```

web-restrict

This command blocks hostnames (Websites). You can block up to 100 hostnames.

Syntax

```
web-restrict <Hostname>
```

Default

NA

Command Mode

Privileged User

Example

This example blocks access to the Website "google.com".

```
(config-data)# web-restrict google.com
```

VPN Commands

The following describes VPN commands.

IPSec (crypto)

The sub-section below describes the IPSec commands.

Up to 16 IPSec (ISAKMP) tunnels.

crypto isakmp identity

This command configures the local identity, which is used by the peers to identify each other during ISAKMP negotiations for the IKEv2 tunnel.

Syntax

```
crypto isakmp identity [address|email|fqdn]
```

Command	Description
`address`	Defines the identity as an IP address in dotted-decimal notation.
`email`	Defines (string) the identity as a fully qualified email address.
`fqdn`	Defines (string) the identity as an FQDN.

Command Mode

Enabled configuration mode.

Example

This example configures a local identity by FQDN.

```
(config-data)# crypto isakmp identity fqdn abc.com
```

crypto isakmp keepalive

This command configures keep-alive settings for the IPSec tunnel.

Syntax

```
crypto isakmp keepalive
```

Command	Description
`retry-interval`	Defines the dead peer keep-alive retry-interval in seconds (default is 50 sec).
`threshold`	Defines the time in seconds after which the device considers itself "dead" (default is 100 sec). The threshold should be a multiple of the retry-interval. For example, if you configure the retry-interval to 60 seconds, then configure the threshold to 120.

Command Mode

crypto isakmp key are defined in enabled configuration mode.

Example

This example defines a keep-alive retry interval of 60 seconds, and a threshold of 120 seconds after which the device considers itself "dead".

```
(config-data)# crypto isakmp keepalive retry-interval 60
(config-data)# crypto isakmp keepalive threshold 120
```

crypto isakmp key

This command, when used in global configuration mode, configures a preshared authentication key. To delete a preshared authentication key, use the no form of this command.

Syntax

```
crypto isakmp key <key-string> address <peer-address-FQDN>
no crypto isakmp key <key-string> address <peer-address-FQDN>
```

Command	Description
<key-string>	Specifies the preshared key. Use any combination of alphanumeric characters up to 20 bytes. This preshared key must be identical at both peers.
address	Use this keyword if the remote peer Internet Security Association Key Management Protocol (ISAKMP) identity was set with its IP address or FQDN.
peer-address	Specifies the IP address or FQDN of the remote peer.

Default

There is no default preshared authentication key.

Command Mode

crypto isakmp key are defined in enabled configuration mode.

Example

This example defines a key to a peer ip.

```
(config-data)# crypto isakmp key 123456 address 100.100.100.2
```

crypto isakmp policy

This command, when used in global configuration mode, defines an Internet Key Exchange (IKE) policy. IKE policies define a set of parameters to be used during the IKE negotiation. To delete an IKE policy, use the no form of this command.

This command invokes the Internet Security Association Key Management Protocol (ISAKMP) policy configuration (config-isakmp) command mode.

To exit config-isakmp command mode, type ‘exit'.

You can configure multiple IKE policies on each peer participating in IPSec. When the IKE negotiation begins, it tries to find a common policy configured on both peers.

Syntax

```
crypto isakmp policy <id>
no crypto isakmp policy <id>
```

Command	Description
id	Uniquely identifies the IKE policy

This command puts you into the config-isakmp command mode.

```
(config-isakmp)# authentication <authentication method>
(config-isakmp)# encryption <encryption algorithm>
(config-isakmp)# hash <authentication algorithm>
(config-isakmp)# lifetime <second>
(config-isakmp)# group {1|2|3}
```

Command	Description
authentication {pre-share|rsa-sig}	Specifies the authentication method.
encryption {3des|aes|aes-gcm}	Specifies the encryption algorithm within an IKE policy. ■ 3des: Defines ESP with the 168-bit DES encryption algorithm (3DES or Triple DES). ■ aes {128|192|256}: Defines ESP with the 128-bit, 192-bit, or 256-bit AES encryption algorithm ■ aes-gcm {128|256}|: Defines AES-GCM with 128-bit or 256-bit secret keys with 16-byte ICV. This option is applicable to IKEv2 only.
group {1|14|15|16|19|2|20|21|5}	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash {md5|sha|sha256|sha384|sha512}	Specifies the hash algorithm within an IKE policy. ■ md5: Defines MD5 with the SHA (HMAC variant) authentication algorithm ■ sha: Defines ESP with the SHA (HMAC variant) authentication algorithm ■ sha256: Defines ESP with the 256-bit SHA (HMAC variant) authentication algorithm

Command	Description
	■ sha384: Defines ESP with the 384-bit SHA (HMAC variant) authentication algorithm ■ sha512: Defines ESP with the 512-bit SHA (HMAC variant) authentication algorithm
`ike {v1|v2}`	Defines the Internet Key Exchange (IKE) version.
`lifetime <seconds>`	Specifies the lifetime of an IKE SA.
`prf {sha256|sha384|sha512}`	Defines pseudo-random function (PRF) as the algorithm to derive keying material and hashing operations within an IKE policy. ■ sha256: Defines PRF with the 256-bit SHA (HMAC variant) authentication algorithm ■ sha384: Defines PRF with the 384-bit SHA (HMAC variant) authentication algorithm ■ sha512: Defines PRF with the 512-bit SHA (HMAC variant) authentication algorithm **Note:** PRF is applicable only to IKEv2.
`use-remote-id-any`	Allows the device to accept any remote-id presented by the peer to connect.The default is disabled (`no use-remote-id-any`).

Default

This command has no defaults.

Command Mode

crypto isakmp key are defined in enabled configuration mode.

Example

This example demonstrates how to configure an IKE policy:

```
(config-data)# crypto isakmp policy 50
(config-isakmp)# encryption aes 128
(config-isakmp)# authentication pre-share
(config-isakmp)# hash sha
(config-isakmp)# group 2
```

```
(config-isakmp)# ike v1
(config-isakmp)# lifetime 3600
```

crypto ipsec profile

This command configures an IPSec policy profile. To delete a IPSec policy profile, use the no form of this command.

Syntax

```
crypto ipsec profile <profile name>
no crypto ipsec profile
```

Command	Description
`profile name`	Defines the profile name.

Command Mode

The crypto isakmp key is defined in enabled configuration mode.

Example

This example configures an IPSec policy profile.

```
(config-data)# crypto ipsec profile p1name
```

crypto ipsec transform-set

This command, when used in global configuration mode, defines a transform set as acceptable combination of security protocols and algorithms for IPSec encapsulating security payload (ESP). To delete a transform set, use the no form of this command.

Syntax

```
crypto ipsec transform-set <transform-set-name>
<transform> <transform>
no crypto ipsec transform-set <transform-set-name>
```

Command	Description
transform-	Specifies the name of the transform set to create (or modify).

Command	Description
set-name	
transform	Specifies two "transforms". These transforms define the IPSec security protocols and algorithms. Accepted transform values are described in the "transform table".

Transform Type	Transform	Description
ESP Encryption Transform	esp-3des	Defines ESP with the 168-bit DES encryption algorithm (3DES or Triple DES).
	esp-aes	Defines ESP with the 128-bit AES encryption algorithm.
	esp-null	Defines null encryption algorithm.
	esp-gcm [128|192|256]	Defines ESP with 128, 192, or 256 bit AES encryption algorithm using the Galois Counter Mode (GCM) cipher (AES-GCM).
ESP Authentication Transform	esp-md5-hmac	Defines ESP with the MD5 (HMAC variant) authentication algorithm.
	esp-sha-hmac	Defines ESP with the SHA (HMAC variant) authentication algorithm.
	esp-sha256-hmac	Defines ESP with the SHA-256 (HMAC variant) authentication algorithm.
	esp-sha384-hmac	Defines ESP with the SHA-384 (HMAC variant) authentication algorithm.
	esp-sha512-hmac	Defines ESP with the SHA-512 (HMAC variant) authentication algorithm.
AH Transform	ah-md5-hmac	Defines AH with the MD5 (HMAC variant) authentication algorithm.
	ah-sha-hmac	Defines AH with the SHA (HMAC variant) authentication algorithm.
	ah-sha256-hmac	Defines AH with the SHA-256 (HMAC variant) authentication algorithm.

Transform Type	Transform	Description
	ah-sha384-hmac	Defines AH with the SHA-384 (HMAC variant) authentication algorithm.
	ah-sha512-hmac	Defines AH with the SHA-512 (HMAC variant) authentication algorithm.

This command puts you into the cfg-crypto-trans command mode

```
(cfg-crypto-trans)# mode <encapsulation-type>
```

Command	Description
encapsulation-type	Specifies the mode for a transform set: either tunnel or transport mode. If neither tunnel nor transport is specified, the default (tunnel mode) is assigned.

Default

This command has no defaults.

Command Mode

crypto ipsec transform-set are defined in enabled configuration mode.

Example

This example demonstrates how to configure a transform set:

```
(config data)# crypto ipsec transform-set abc esp-3des esp-sha-hmac
```

crypto map

To create or modify a crypto map entry and enter the crypto map configuration mode, use the crypto map global configuration command. To delete a crypto map entry or set, use the no form of this command.

Syntax

```
crypto map <map-name> <index> ipsec-isakmp
no crypto map <map-name> <index> ipsec-isakmp
```

Command	Description
map-name	Name that identifies the crypto map set
index	Uniquely number assigned to a crypto map entry

This command puts you into the config-crypto-map command mode:

```
(config-crypto-map)# set peer <peer-ip>
(config-crypto-map)# set transform-set <set-name>
(config-crypto-map)# set pfs {group1|group2|group5|same}
(config-crypto-map)# set security-association lifetime seconds <#>
(config-crypto-map)# match address <acl-name>
(config-crypto-map)# set tunnel start-action-mode {active|triggered|passive}
```

Command	Description
`set peer <peer-ip>`	Specifies an IPSec peer (IP address in dotted-decimal notation or an FQDN) in a crypto map entry.
`set transform-set <set-name>`	Specifies which transform sets can be used with the crypto map entry. The set-name will be compare with all transform-sets prefix
`set pfs <group1|group2|group5|same>`	Specifies that IPSec should ask for PFS when requesting new SAs for this crypto map entry, or that IPSec requires PFS when receiving requests for new SAs: ■ `group1` - Diffie-Hellman group 1 ■ `group2` - Diffie-Hellman group 2 ■ `group5` - Diffie-Hellman group 5 ■ `same` - Same Diffie-Hellman group as phase 1
`set security-association lifetime seconds <#>`	Specifies the lifetime of an IPSec SA.
`set tunnel start-action-mode {active|triggered|passive}`	Specifies the IPSec tunnel establishment mode: ■ `active` – (default) Once configured, the device immediately initiates establishment of an IPSec tunnel with the remote peer

Command	Description
	■ `trigger` – the device initiates establishment of an IPSec tunnel with the remote peer only if the device needs to send traffic through the tunnel (or the remote peer initiates it) ■ `passive` – the device establishes an IPSec tunnel only if the remote peer initiates it Using the `trigger` or `passive` mode prevents both peers from initiating the tunnel simultaneously.
`match address <acl-name>`	Specifies an extended access list for a crypto map entry. Only the first entry in the access list will be considered.

Default

IPSec SA lifetime default is 28800 seconds.

Command Mode

crypto map defined in enabled configuration mode.

Example

This example demonstrates how to configure a crypto map:

```
(config data)# crypto map mymap 1 ipsec-isakmp
(config-crypto-map)# set peer 1.2.3.4
(config-crypto-map)# set transform-set myset
(config-crypto-map)# set security-association lifetime seconds 28000
(config-crypto-map)# match address 101
(config-crypto-map)# set tunnel start-action-mode triggered
```

L2TP and PPTP Tunnel Interface Commands

The following describes the L2TP and PPTP Tunnel Interface commands.

description

This command sets the description on the specified tunnel interface.

Syntax

```
description <string>
```

Command	Description
`string`	Specifies the interface description using an alphanumerical string (up to 255 characters).

Default

NA

Note

- Use inverted commas when using the space character as part of the description.
- The string is limited to 255 characters.

Command Mode

Privileged User

Example

This example sets the description on L2TP 3.

```
(conf-if-L2TP 3)# description L2TP 3 interface
```

firewall enable

This command enables the firewall protection on the specified tunnel interface. Use the no form of this command to disable the firewall.

Syntax

```
firewall enable
```

Default

By default, firewall is enabled.

Command Mode

Privileged User

Example

This example enables the firewall on l2tp.

```
# configure data
(config-data)# interface l2tp 1
(conf-if-L2TP 6)# firewall enable
```

lcp-echo

This command configures the interface echo parameters. The echo is needed to keep the fw state alive, otherwise it is deleted after two minutes idle time and the connection will be blocked. This configuration will make ppp discover broken link in (interval x fails) seconds.

Syntax

```
lcp-echo <interval> <fails>
```

Command	Description
`interval`	Defines the interval in seconds (default value is 6 seconds).
`fails`	Defines the number of failed intervals to discover broken link (default value is 5 intervals).

Default

NA

Command Mode

Privileged User

Examples:

This example sets the echo interval and fails parameters to 10 and 5 respectively on L2TP 6:

```
(conf-if-L2TP 6)# lcp-echo 10 5
```

interface l2tp|pptp

This command enters a specific WAN ppp tunnel interface configuration. Use the no form of this command to delete the interface.

Syntax

```
interface l2tp <ID>
interface pptp <ID>
```

Command	Description
ID	Assigns the tunnel interface id in the range of 0-99.

Default

NA

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example enters an l2tp id 5 tunnel interface configuration:

```
(config data)# interface l2tp 5
```

mtu

This command configures the interface Maximum Transmission Unit (MTU) on the specified tunnel interface.

Syntax

```
mtu auto
mtu <mtu value>
```

Command	Description
auto	Sets MTU automatically.
value	Sets MTU value in the range of 68 to 1500.

Default

MTU is set to auto (usually 1476).

Command Mode

Privileged User

Example

This example sets the MTU value to 770 bytes on l2tp 6.

```
(conf-if-L2TP 6)# mtu 770
```

napt

This command sets the NAPT (Network Address Port Translation) on the specified tunnel interface. Use the no form of this command to set route mode.

Syntax

```
napt
```

Default

By default, NAPT is used.

Command Mode

Privileged User

Example

This example sets napt on l2tp 6.

```
(conf-if-L2TP 6)# napt
```

ppp user

This command defines the ppp username and password on the specified tunnel interface.

Syntax

```
ppp user <username> pass <password>
```

Command	Description
username	Defines the ppp username.
password	Defines the ppp password.

Default

NA

Command Mode

Privileged User

Example

This example sets the username and password on interface l2tp 6.

```
(conf-if-L2TP 6)# ppp user admin pass 1234
```

ppp authentication pap|chap|ms-chap|ms-chap-v2

This command enables several authentication protocols on the ppp protocol of the specified tunnel interface. Use the no form of this command to disable a specific authentication protocol.

Syntax

```
ppp authentication pap
ppp authentication chap
ppp authentication ms-chap
ppp authentication ms-chap-v2
```

Command	Description
pap	Defines the Password Authentication Protocol.

Command	Description
chap	Defines the Challenge Handshake Authentication Protocol.
ms-chap	Defines the Microsoft Challenge Handshake Authentication Protocol.
ms-chap-v2	Defines the Microsoft Challenge Handshake Authentication Protocol - Version 2.

Default

By default, all protocols are enabled.

Command Mode

Privileged User

Example

This example disable the pap protocol on interface l2tp 3.

```
(conf-if-L2TP 3)# no ppp authentication pap
```

shutdown

This command disables the specified interface. Use the no form of this command to enable the interface.

Syntax

```
shutdown
no shutdown
```

No arguments exist for this command.

Default

When creating a new interface, it is disabled by default.

Command Mode

Privileged User

Example

This example enables L2TP 3.

```
# configure data
(config data) # interface l2tp 3
(conf-if-L2TP 3)# no shutdown
```

tunnel destination

This command defines the end point host/ip address of the specified tunnel interface. Use the no form of this command to remove a configured IP address.

Syntax

```
tunnel destination <host name>
```

Command	Description
`host name`	Specifies a host name or a valid IPv4 address. IP addresses should be expressed in dotted decimal notation (for example, 10.1.2.3).

Default

NA

Command Mode

Privileged User

Example

This example configures the tunnel destination IP address of 10.4.2.50 on interface PPTP 6.

```
(conf-if-PPTP 6)# tunnel destination 10.4.2.50
```

l2tp-server

This command defines the L2TP VPN server.

Syntax

```
l2tp-server
```

Command Mode

Privileged User

Example

This example defines the L2TP VPN server:

```
(config data)# l2tp-server
no ppp encryption
   ip range 192.168.0.70 192.168.0.80
   ipsec key 123456
   no shutdown
   exit
```

pptp-server

This command enables the Point-to-Point Tunneling Protocol (PPTP) VPN server.

Syntax

```
pptp-server
```

Command Mode

Privileged User

Example

This example defines the L2TP VPN server:

```
(config data)# pptp-server
```

vpn-users

This command defines a VPN user.

Syntax

```
vpn-users
```

Command Mode

Privileged User

Example

This example defines a VPN user:

```
(config data)# vpn-users
(conf-vpnusers)user tom pass testpass
```

Port Security based on MAC Address

The following provides support for port access security based on MAC address. Only clients whose MAC addresses are defined for the device's port interface are allowed access to the port.

authentication static

This command defines a MAC address to allow access to one of the device's interfaces.

Syntax

```
# authentication static [mac <MAC address as xx:xx:xx:xx:xx:xx>|auto]
# no authentication static [mac <MAC address as xx:xx:xx:xx:xx:xx>|auto]
```

Command	Description
`auto`	Enables the device to authorize the first MAC address to access the Ethernet port.

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example defines a MAC address to allow access to one of the device's interfaces:

```
(config-data)# interface GigabitEthernet 0/1
(config-if-GE 0/1)# authentication static mac 01:23:45:67:89:ab
```

Access Control List (ACL) Commands

The following describes ACL commands.

access-list

Access list rules (ACL) are used in several system components for classifying IP traffic based on parameters such as addresses, protocols and ports. The primary usage of access lists is for filtering unwanted traffic on the system's interfaces.

You can assign up to 200 ACL rules to a single access group.

You can also configure multiple access lists (up to 16) per IPSec tunnel, enabling multiple sub-nets to "reside" behind an IPSec tunnel. For example, this multiple traffic selectors feature allows you to connect multiple subnets on both sides of the IPSec tunnel (remote and local). Per subnet-to-subnet connectivity rule, you can define a separate access list rule.

Access list processing is sequential; for each traffic flow, the list is scanned from the top until a matching rule is found. When configuring an access list, rules should be entered in appropriate order.

To attach an access list to an IP interface, see the "access-group" command documentation.

To remove an access list, use the "no" format of the command.

Syntax

```
access-list <acl-id> {permit|deny} <protocol> <source-selector> <dest-selector>
<options> <options>
```

For compatibility purposes, access lists numbered 1-99 and 1300-1999 are defined as limited ("basic") access lists. These access lists cannot contain protocol and port definitions.

Command	Description
`acl-id`	Defines the Access List name identifier for this access list. It can be a number or a name.
`permit|deny`	Defines the access to the packet: permit - Allows access to packets that match the criteria defined. deny - Blocks access to packets that match the source and destination IP addresses and service ports defined.
`protocol`	Defines a traffic protocol: ■ tcp ■ udp

Command	Description
	■ icmp ■ igmp ■ esp ■ ah ■ gre ■ ip ■ ip protocol number [0 – 255]
`source-selector` `dest-selector`	Defines the source address and destination address of packets sent or received by the device. Select an address or a name from the list to apply the rule on the corresponding host, or Any to apply the rule on all the device's LAN hosts. Select traffic by IP addresses and ports, in one of the following formats: any - Defines all traffic. host a.b.c.d - Defines Traffic to/from single host, specified by the IP address. When an access list (see configure data > access-list) is created for management using the protocols SNMP, Telnet, SSH or CWMP, it is possible to use a DNS name instead of an IP address. In this case, an FQDN can be configured for the host. local- Defines the Local IP address. a.b.c.d - Traffic to/from a subnet, specified by an IP address and a mask (e.g., 0.0.255.255). Note: The eq and range parameters are only used if <protocol> is set to "tcp" or "udp". eq <port> - Defines traffic to/from a single port. range <start> <end> - Defines traffic to/from multiple ports, specified by range. If the port selector is not defined, the rule will match all ports.
`dscp options`	The following options can be used: dscp - Match by Differentiated Services Code Point value and mask. Defines the packets by matching the Differentiated Services Code Point (DSCP) field of the IP header. The format of this option is: dscp <c> mask <m>

Command	Description
	The packet's DSCP value is compared to <c> under bit mask <m> (both must be specified in hexadecimal). For example: dscp 10 mask 3F established -Accepts connections. stateless - Accepts packets. log - Logs matches. precedence - Matches by IP Precedence value (0 high – 7 low) Note: "precedence" is applicable to MSBR devices – Mediant 500, Mediant 500L and Mediant 800.
`options`	Defines one or more of the following options: ■ stateless: Traffic matching is stateless, i.e., it does not keep track of the connection state. ■ log: Traffic matching this rule will be logged. established -Accepts connection

Default

The default access list behavior is "deny", i.e. if a flow doesn't match any of the rules it is assumed to be unwanted traffic.

Related Commands

SNMP Community strings can be associated with an ACL rule using the snmp-acl command.

Command Mode

Privileged User

Example

- Defines an access list that allows all TCP connections originating in a full subnet, with the exception of a single host:

```
(config-data)# access-list 2001 deny tcp host 10.31.4.50 any
(config-data)# access-list 2001 permit tcp 10.31.0.0 0.0.255.255 any stateless
```

- Multiple access lists per IPSec tunnel - example of connecting two subnets on each side of an IPSec tunnel, where the local subnets are 150.150.150.0/24 101.101.101.0/24, and the remote subnets are 200.200.200.0/24 201.201.201.0/24:

```
(config-data)# access-list 101 permit ip 150.150.150.0 0.0.0.255 200.200.200.0
0.0.0.255
(config-data)# access-list 101 permit ip 101.101.101.0 0.0.0.255 201.201.201.0
0.0.0.255
(config-data)# access-list 101 permit ip 150.150.150.0 0.0.0.255 201.201.201.0
0.0.0.255
(config-data)# access-list 101 permit ip 101.101.101.0 0.0.0.255 200.200.200.0
0.0.0.255
```

ip access-list extended

This command provides support for assigning an extended IP access-list number.

Syntax

```
ip access-list extended <access list id>
```

Command	Description
`access list id`	Defines the extended IP access-list number. The range is 100-9999.

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example defines an extended Access List with an access list number ID.

```
(config-data)# ip access-list extended 18
```

ip access-list standard

This command provides support for assigning a sequence number (ID) to an IP Access List rule and re-sorting the order of rules within an Access List.

Syntax

```
ip access-list standard <access list id>
```

Command	Description
access list id	Defines the standard IP access-list number. The range is 1-99.

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example defines an Access List with an access list number ID.

```
(config-data)# ip access-list standard 18
```

<rule id> deny|permit

This command defines a rule with a rule number for the Access List.

Syntax

```
<rule id> {permit|deny} <rule options... >
```

Command	Description
rule id	Defines the Rule ID. The range is 1 to 2147483647.

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example defines a rule with a rule number for the Access List.

```
(config-data)# ip access-list standard 1
(config-std-nacl)# 1 permit any
```

ip access-list resequence

This command re-sequences rule numbering of a specific Access List.

Syntax

```
ip access-list resequence <access list id> <starting rule number> <step increment>
```

Command	Description
access list id	Defines the Starting Rule Number. The range is 1-2147483647.

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example shows a configuration of Access List ID 1 with two rules (numbers 10 and 20):

```
(config-data)# ip access-list standard 1
(config-std-nacl)# 10 permit any
(config-std-nacl)# 20 permit host 3.3.3.3
```

To change the order of the rules so that the first rule is assigned number 100 and subsequent rules are assigned numbers incremented by 50:

```
(config-data)# ip access-list resequence 1 100 50
```

To view the rules and their changed sequence numbers:

```
# show data access-lists
...
Standard IP access list 1
```

```
1 100 permit  any   (0 matches)
1 150 permit  host 3.3.3.3   (0 matches)
```

ip access-group

This command associates an access list with an IP interface. Refer to the "access-list" command documentation for more information.

To remove an access list association, use the no format of the command.

Syntax

```
ip access-group <acl-id> in
ip access-group <acl-id> out
no ip access-group <acl-id>
```

Command	Description
`<acl-id>`	Identifies the access list to use (number or name).
`in`	The access list will control inbound traffic on the interface.
`out`	The access list will control outbound traffic on the interface.

Default

The default setting for IP interfaces is no access-group, i.e. unlimited traffic.

Command Mode

This command is issued in interface context.

Example

This example associates an access list with a VLAN interface:

```
(conf-if-VLAN 1)# ip access-group 2001 in
```

Firewall Commands

The following describes the Firewall commands.

firewall enable

This command enables the firewall protection on the specified tunnel interface. Use the no form of this command to disable the firewall.

Syntax

```
firewall enable
```

Default

By default, firewall is enabled.

Command Mode

Privileged User

Example

This example enables the firewall on GRE 6.

```
# configure data
(config-data)# interface gre 6
(conf-if-GRE 6)# firewall enable
```

mtu

This command configures the interface Maximum Transmission Unit (MTU) on the specified tunnel interface.

Syntax

```
mtu auto
mtu <mtu value>
```

Command	Description
`auto`	Sets MTU automatically.
`mtu value`	Sets MTU value. Range is between 68 and 1500.

Default

By default, MTU is set to auto (usually 1476).

Command Mode

Privileged User

Example

This example sets the MTU value to 770 bytes on GRE 6.

```
# configure data
(config-data)# interface gre 6
(conf-if-GRE 6)# mtu 770
```

desc

This command sets the description on the specified tunnel interface.

Syntax

```
desc <string>
```

Command	Description
`string`	Specifies the interface description using an alphanumerical string (up to 255 characters).

Default

NA

Note

- Use inverted commas when using the space character as part of the description.
- The string is limited to 255 characters.

Command Mode

Privileged User

Example

This example sets the description on GRE 6.

```
# configure data
(config-data)# interface gre 6
(conf-if-GRE 6)# desc gre 6 interface
```

shutdown

This command disables the specified tunnel interface. Use the no form of this command to enable the interface.

Syntax

```
shutdown
no shutdown
```

No arguments exist for this command.

Default

When creating a new interface, it is disabled by default.

Command Mode

Privileged User

Example

This example enables GRE 6.

```
# configure data
(config-data)# interface gre 6
(conf-if-GRE 6)# no shutdown
```

NAT Commands

The following describes NAT commands.

ip nat inside source static

NAT port-forwarding exposes a LAN service (IP address and port) to WAN users. The command creates a static translation rule, which maps a WAN port (on one or all WAN interfaces) to a LAN service.

To remove a port-forwarding rule, use the no format of the command.

Syntax

```
ip nat inside source static {tcp|udp} <lan-ip> <lan-port> <wan-ip> <wan-port>
ip nat inside source static {tcp|udp} <lan-ip> <lan-port> <wan-ip> range <wan-port-start> <wan-port-end>
ip nat inside source static {tcp|udp} <lan-ip> <lan-port> <if-name> <wan-port>
ip nat inside source static {tcp|udp} <lan-ip> <lan-port> <if-name> range <wan-port-start> <wan-port-end>
ip nat inside source static {tcp|udp} <lan-ip> same <wan-ip> <wan-port>
ip nat inside source static {tcp|udp} <lan-ip> same <wan-ip> range <wan-port-start> <wan-port-end>
ip nat inside source static {tcp|udp} <lan-ip> same <if-name> <wan-port>
ip nat inside source static {tcp|udp} <lan-ip> same <if-name> range <wan-port-start> <wan-port-end>
ip nat inside source static ip <lan-ip> <wan-ip>
ip nat inside source static ip <lan-ip> <if-name>
ip nat inside source static gre <lan-ip> <wan-ip>
ip nat inside source static {tcp|udp} <lan-ip> <lan-port> <wan-ip> <wan-port> same <if-name> <wan-port> match <access list name>
```

Command	Description
tcp	Defines forwarding for a TCP port.
udp	Defines forwarding for a UDP port.
lan-ip	Defines the IP address of LAN service host.
same	Sets the LAN port the same as the WAN port.
lan-port	Defines the port number (1-65535) of the LAN service.
match	Applies an access list rule to the NAT port forwarding rule. For configuring access list (ACL), use the command: (config-data)# access-list
wan-ip	Defines the WAN interface for this rule. Specify the IP address or 0.0.0.0 for all WAN interfaces.
wan-port	Defines the port number on WAN interface.
range	Performs port forwarding on a range of ports, rather than a single port.
acl-name	Access-list defining the LAN hosts affected by the NAT rule.

Command	Description
if-name	WAN interface name and index, to which NAT will be performed.
pool-name	IP address pool to be used on the WAN interface.

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

No port forwarding.

Command Mode

Privileged User

Example

The following example defines a port forwarding rule:

```
(config-data)# ip nat inside source static tcp 192.168.0.7 80 0.0.0.0 8080
```

The following example defines a port forwarding rule and applies an access list rule:

```
(config-data)# ip nat inside source static tcp 192.168.0.16 same gigabitethernet 0/0
8080 match PF-ACL
```

ip nat inside source static list

The command creates static NAT entries for LAN hosts. In this case, an access-list is used to define the LAN devices and an IP address pool defines the WAN addresses to be used.

Syntax

```
ip nat inside source list <acl-name> interface <if-name>
ip nat inside source list <acl-name> interface <if-name> pool <pool-name>
ip nat inside source list <acl-name> interface <if-name> pool <pool-name> port
<wan-port-start> <wan-port-end>
```

Command	Description
tcp	Defines forwarding for a TCP port.
udp	Defines forwarding for a UDP port.
lan-ip	Defines the IP address of LAN service host.
same	Sets the LAN port the same as the WAN port.
lan-port	Defines the port number (1-65535) of the LAN service.
wan-ip	Defines the WAN interface for this rule. Specify the IP address or 0.0.0.0 for all WAN interfaces.
wan-port	Defines the port number on WAN interface.
range	Performs port forwarding on a range of ports, rather than a single port.
acl-name	Access-list defining the LAN hosts affected by the NAT rule.
if-name	WAN interface name and index, to which NAT will be performed.
pool-name	IP address pool to be used on the WAN interface.

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

No NAT rules are defined.

Command Mode

Privileged User

Example

The following example defines a port forwarding rule:

```
(config-data)# ip nat inside source list NAT-ACL-NAME interface GigabitEthernet 0/0
```

ip nat inside destination

This command defines a load-balancing configuration, where several LAN hosts are handling access requests from the WAN.

To remove the NAT configuration, use the no format of the command.

Syntax

```
ip nat inside destination <ip-addr> port <port-num> pool <pool-name>
```

Command	Description
ip-addr	Defines the global IP address (WAN side).
port-num	Defines the port number on the WAN IP address.
pool-name	Defines the LAN hosts pool, which must be configured with the "ip nat pool <pool-name> rotary" command.

Default

No NAT rules are defined.

Command Mode

Privileged User

Example

This example defines a NAT setup where a number of LAN hosts are handling requests to a single WAN port:

```
(config-data)# ip nat inside destination 212.36.145.5 port 8000 pool lanpool
```

ip nat pool

This command defines a collection of IP addresses to be used for NAT purposes.

To remove a pool, use the no format of the command.

Syntax

```
ip nat pool <pool-name> <start-ip> <end-ip>
ip nat pool <pool-name> <start-ip> <end-ip> rotary
```

Command	Description
pool-name	Defines the name of the pool.
start-ip	Defines the starting IP address of the NAT address pool.

Command	Description
`end-ip`	Defines the last IP address of the NAT address pool.
`rotary`	Indicates that the pool refers to LAN hosts participating in a load-balancing scheme. See "ip nat inside destination" for additional information.

Default

No NAT pools are defined.

Command Mode

Privileged User

Example

This example defines a NAT pool consisting of one global IP address:

```
(config-data)# ip nat pool scarlet 212.34.156.1 212.34.156.1
```

ip nat translation

This command controls the life-time of dynamic NAT translations.

Syntax

```
ip nat translation udp-timeout <seconds>
ip nat translation tcp-timeout <seconds>
ip nat translation icmp-timeout <seconds>
```

Command	Description
`<seconds>`	Defines the number of seconds after which an idle NAT translation will expire.

Default

By default, UDP timeout is 120 seconds; TCP timeout is 3600 seconds; ICMP timeout is 6 seconds.

Command Mode

Privileged User

Example

This example defines the lifetime of idle UDP connections:

```
(config-data)# ip nat translation udp-timeout 360
```

802.1x LAN Port-based Authentication Commands

The 802.1x commands provide the support for functioning as an IEEE 802.1X authenticator. IEEE 802.1X (EAP-over-LAN, or EAPOL) is a standard for port-level security on secure Ethernet switches (wired or wireless). When equipment is connected to a secure port, no traffic is allowed until the identity of the equipment is authenticated.

dot.1x lan-authentication enable

This command enables 802.1X LAN port authentication. The no version of this command disables the command.

Syntax

```
dot1x lan-authentication enable
no dot1x lan-authentication enable
```

Command Mode

Privileged User

Example

This example enables 802.1 X LAN port authentication.

```
(config-data)# dot1x lan-authentication enable
```

dot1x radius-server

This command defines the RADIUS server for 802.1X authentication.

Syntax

```
dot1x radius-server host <a.b.c.d> auth-port <UDP port> key <shared secret
value>
dot1x radius-server host <a.b.c.d> auth-port <UDP port> obscured-key <shared
```

```
secret value>
dot1x radius-server local
```

Command	Description
a.b.c.d	Defines the RADIUS server IP address.
UDP port	Defines the UDP port to use.
shared secret value	Defines the shared secret value string.
key	Defines a shared secret.
obscured-key	Copies a shared secret from existing configuration.

Command Mode

Privileged User

Example

This example defines an external RADIUS server.

```
(config-data)# dot1x radius-server host 10.3.4.250 auth-port 1812 key 123456
```

dot1x reauth-time

This command enables each port to be re-authenticated after a user-defined interval (in seconds), following a successful authentication.

Syntax

```
dot1x reauth-time <seconds>
```

Command	Description
seconds	Defines the time to re-authenticate, in seconds.

Command Mode

Privileged User

Example

This example defines the time to re-authenticate in 3600.

```
(config-data)# dot1x reauth-time 3600
```

authentication dot1x

This command determines which client (based on MAC address) is allowed through a specific port after 802.1X authentication succeeds.

Syntax

```
authentication dot1x {single-host|multi-host}
```

Command	Description
`single-host`	Allows only the MAC address that successfully passed 802.1x authentication.
`multi-host`	Any MAC address is allowed after 802.1x authentication succeeds.

Note

The command is relevant for LAN interfaces only.

Command Mode

Privileged User

Example

The following is an example using this command.

```
(config-data)# interface GigabitEthernet 0/1
(conf-if-GE 0/1)# authentication dot1x single-host
```

dot1x supplicant

This command defines the device for IEEE 802.1x authentication as a client (supplicant). Once configured (and run `exit`), configuration is loaded and negotiation with the 802.1x authenticator (e.g., secure LAN switch) begins. If the supplicant's credentials are valid, the authenticator authorizes traffic on the secure port connected to the device.

Syntax

```
dot1x supplicant
(config-dot1x-supplicant)# set
```

Command	Description
`identity`	Defines the supplicant's identity string.
`mode {disable|md5|peap|tls}`	Disables the 802.1x supplicant mode or enables it using EAP-MD5, EAP-PEAP, or EAP-TLS.
`obscured-password`	Defines the supplicant's password (obscured).
`password`	Defines the supplicant's password.
`port-type`	Defines the supplicant's port type to run on.
`tls-ctx`	Defines the TLS Context (ID) for the supplicant.

Command Mode

Privileged User

Related Commands

`show data dot1x-supplicant-status`

Example

This example defines the 802.1x supplicant.

```
(config-data)# dot1x supplicant
(config-dot1x-supplicant)# set identity ipp
(config-dot1x-supplicant)# set mode tls
(config-dot1x-supplicant)# set password 123456
(config-dot1x-supplicant)# set port-type wan
(config-dot1x-supplicant)# set tls-ctx 1
```

802.1X On-board RADIUS Server Authentication Commands

The commands below provide support for an on-board RADIUS server that can be used for 802.1X wired (LAN) and wireless (Wi-Fi Protected Access II / WPA2) authentication. This supports both password-based authentication and certificate-based authentication.

dot1x local-user

This command defines the username and password.

Syntax

```
# dot1x local-user <username> obscured-password <password text>
# dot1x local-user <username> password <password text>
```

Command	Description
`obscured-password`	Copy the password from an existing configuration.
`password`	Enter password in plain text.
`password text`	Defines the actual password.

Command Mode

Privileged User

Example

This example defines the username and password.

```
(config-data)# dot1x local-user MD password 1234
```

interface dot11radio

This command defines the Wi-Fi interface.

Syntax

```
# interface dot11radio <number>
```

```
# interface dot11radio <number>
(conf-if-dot11radio <number>)# mfp
```

Command	Description
`mfp {disabled |optional |required}`	The device supports the IEEE 802.11w-2009 wireless

Command	Description
	encryption standard, which is based on the 802.11i framework and protects against subtle attacks on wireless LAN (WLAN) management frames (Protection Management Frames / PMF or also known as Management Frame Protection / MFP). ■ disabled: Disables MFP for the client (default). ■ optional: Sets MFP only with MFP-supporting clients. ■ required: clients are allowed to associate only if MFP is negotiated. If the devices do not support MFP, they are not allowed to join the network.

Command Mode

Privileged User

Example

This example defines the Wi-Fi interface.

```
(config-data)# interface dot11radio 1
```

This example enables PMF encryption on the Wi-Fi interface.

```
(config-data)# interface dot11radio 1
(conf-if-dot11radio 1)# mfp optional
```

security 802.1x

This command enables on-board RADIUS server for 802.1X security.

Syntax

```
# security 802.1x radius server local
```

Command Mode

Privileged User

Example

This example enables on-board RADIUS server for 802.1X security.

```
(config-data)# interface dot11radio 1
(config-if-dot11radio 1)# security 802.1x radius server local
```

security wpa

This command enables Wi-Fi security mode.

Syntax

```
# security wpa mode 802.1x
```

Command Mode

Privileged User

Example

This example enables Wi-Fi security mode.

```
(config-data)# interface dot11radio 1
(config-if-dot11radio 1) # security wpa mode 802.1x
```

security mode

This command defines Wi-Fi security mode to WPA2.

Syntax

```
# security mode wpa2
```

Command Mode

Privileged User

Example

This example defines Wi-Fi security mode to WPA2.

```
(config-data)# interface dot11radio 1
(config-if-dot11radio 1)# security mode wpa2
```

no shutdown

This command enables the interface.

Syntax

```
# no shutdown
```

Command Mode

Privileged User

Example

This example enables the interface.

```
(config-data)# interface dot11radio 1
(config-if-dot11radio 1)# no shutdown
```

Ethernet Commands

The following describes Ethernet commands.

ethernet l2tunnel

This command enables tunneling for different Layer-2 protocols.

Syntax

```
# ethernet l2tunnel {cdp|dtp|hex <hex protocol>| lacp|lldp|pagp|pvst-
plus|stp|udld|vtp}
```

Command	Description
hex protocol	Hexadecimal protocol number
cdp	Cisco Discovery Protocol
dtp	Dynamic Trunking Protocol
hex	Ethernet protocol type in hexadecimal
lacp	Link Aggregation Control Protocol
lldp	Link Layer Discovery Protocol
pagp	Port Aggregation Protocol
pvst-plus	Per-VLAN Spanning Tree Plus
stp	Spanning-Tree Protocol
udld	UniDirectional Link Detection
vtp	VLAN Trunking Protocol

Command Mode

Privileged User

Example

This example enables tunneling for cdp.

```
(config-data)# ethernet l2tunnel cdp
```

ethernet cfm

This command enables tunneling for IEEE 802.1ag Ethernet Connectivity Fault Management (CFM) protocols.

Syntax

```
# ethernet cfm aging-time <time in minutes>
# ethernet cfm debounce <packet number>
# ethernet cfm mep
```

Command	Description
`aging-time`	Sets the remote MEP aging time
`time in minutes`	Defines the actual aging time in minutes [1-9999].
`debounce`	Sets the status-reflection debounce counter.
`packet number`	Defines the number of port-down packets to receive before blocking ports.

Command Mode

Privileged User

Example

This example enables tunneling for cdp:

```
(config-data)# ethernet l2tunnel cdp
```

TACACS+ Commands

TACACS+ is a security protocol for centralized username and password verification. The following describes the TACACS+ commands.

tacacs-server

This command provides support for communicating with a TACACS+ server through the device's WAN interface.

Syntax

```
tacacs-server timeout |  source data source-address interface | source data vrf | source voip | port | obscured-key | host | key
```

Command	Description
`timeout`	Defines how much time to wait (in seconds) for a TACACS+ response before failing the authentication.
`source data source-address interface`	Defines the source interface ID.

Command	Description
source data vrf	Defines the VRF name.
host	Specifies the address (IP address or FQDN) of the TACACS+ server. **Note:** Up to two TACACS+ servers may be defined.
port	Specifies the TCP port number for the TACACS+ service.
key	Specifies the shared secret between the TACACS+ server and the device.
obscured-key	Copies the TACACS+ shared secret from an existing configuration.

Interface Type (ifname)		Interface ID
gigabitethernet	GigabitEthernet interface slot and port (VLAN ID is optional)	[SLOT/PORT.VLANID]
cellular	Cellular interface ID	0/0
gre	Tunnel GRE ID	[1-255]
ipip	Tunnel IPIP ID	[1-255]
l2tp	L2TP ID	[0-99]
pppoe	PPPoE interface ID	[1-3]
pptp	PPTP ID	[0-99]
vlan	Vlan ID	[1-3999]
loopback	Loopback ID	[1-5]
bvi	Bridge interface	[1-255]

Default

By default, no TACACS+ servers are defined.

The default TCP port is 49.

The default timeout is 5 seconds.

The default key is “MSBR”.

Note

This command is applicable to Mediant MSBR devices.

Command Mode

Privileged User

Example

The example below configures a TACACS+ server.

```
(config-data)# tacacs-server host 192.168.1.55
(config-data)# tacacs-server key Rumble
```

aaa authentication login tacacs+

This command enables usage of a TACACS+ server on the network to verify access to the device's Command-Line Interface.

To disable TACACS+ and return to local username/password verification, use the no form of this command.

Syntax

```
aaa authentication login tacacs+
aaa authentication login tacacs+ local
```

Command	Description
`local`	Specifies that if the TACACS+ server does not respond, password verification should fall back to locally-defined values.

Default

TACACS+ is disabled.

Command Mode

Privileged User

Example

The example below describes how to enable TACACS+ usage.

```
# configure data
(config-data)# aaa authentication login tacacs+
```

The example below configures authorization and authentication in the MSBR to work with TACACS+:

```
# configure data
(config-data)# aaa authentication login tacacs+
(config-data)# aaa authorization command tacacs+
(config-data)# tacacs-server host 192.162.0.199
(config-data)# tacacs-server key P@ssw0rd
```

aaa accounting exec start-stop tacacs+

This command enables TACACS+ for CLI session accounting.

To disable TACACS+ session accounting, use the "no" form of this command.

Syntax

```
aaa accounting exec start-stop tacacs+
```

Default

TACACS+ is disabled.

Command Mode

Privileged User

Example

The example below enables TACACS+ usage for session accounting.

```
(config-data)# aaa accounting exec start-stop tacacs+
```

aaa authentication login tacacs+ allow-console-bypass authentication

This command allows bypassing TACACS+ authentication when a user is connected using the serial port. After login, non-privileged commands will be allowed without negotiating with the TACACS+ Server. This does not affect TACACS+ users.

Syntax

```
aaa authentication login tacacs+ allow-console-bypass authentication
```

Default

TACACS+ is disabled.

Command Mode

Privileged User

Example

The example below allows bypassing TACACS+ authentication when a user is connected using the serial port.

```
(config-data)# aaa authentication login tacacs+ allow-console-bypass
authentication
```

aaa authentication login tacacs+ allow-console-bypass authentication authorization

This command allows bypassing TACACS+ enable authorization (privileged mode) when a user is connected using the serial port. After login, privileged commands will be allowed without negotiating with the TACACS+ Server. This will not affect TACACS+ users.

Syntax

```
aaa authentication login tacacs+ allow-console-bypass authentication
authorization
```

Default

TACACS+ is disabled.

Command Mode

Privileged User

Example

The example below allows bypassing TACACS+ enable authorization (privileged mode) when a user is connected using the serial port.

```
(config-data)# aaa authentication login tacacs+ allow-console-bypass
authentication authorization
```

aaa accounting command start-stop tacacs+

This command enables reporting of CLI start/stop times to a TACACS+ server on the network.

To disable TACACS+ command accounting, use the "no" form of this command.

Syntax

```
aaa accounting command start-stop tacacs+
```

Default

TACACS+ is disabled.

Command Mode

Privileged User

Example

The example below enables TACACS+ usage for command accounting.

```
(config-data)# aaa accounting command start-stop tacacs+
```

aaa authorization command tacacs+

This command enables usage of a TACACS+ server on the network to authorize each CLI command entered.

To disable TACACS+ per-command authorization, use the "no" form of this command.

Syntax

```
aaa authorization command tacacs+
```

Default

TACACS+ is disabled.

Command Mode

Privileged User

Example

The example below enables TACACS+ usage for per-command authorization.

```
(config-data)# aaa authorization command tacacs+
```

aaa authorization enable if-authenticated tacacs+

This command enters Privileged User mode automatically if authenticated by TACACS+.

Syntax

```
aaa authorization enable if-authenticated tacacs+
```

Default

TACACS+ is disabled.

Command Mode

Privileged User

Example

The example below enters Privileged User mode automatically if authenticated by TACACS+.

```
(config-data)# aaa authorization enable if-authenticated tacacs+
```

73 Performance Monitoring Commands

The following describes commands for monitoring performance.

pm sample-interval

This command configures sample intervals for performance monitoring (PM) statistics.

Syntax

```
# pm sample-interval seconds <first sample interval in seconds>
# pm sample-interval minutes <second sample interval in minutes>
```

Note

This command is applicable only to data-router functionality.

Command Mode

Privileged User

Example

This example configures the sample interval to 20 seconds.

```
(config-data)# pm sample-interval seconds 20
```

This page is intentionally left blank.

International Headquarters

Naimi Park
Ofra Haza 6
Or Yehuda, 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-18019