

# **Oracle® Communications Session Border Controller**

ACLI Reference Guide

Release S-CX6.4.0

*Formerly Net-Net Session Director*

## Notices

Copyright ©2014, 2012, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## 1 How to use the ACLI..... 17

The ACLI .....	17
Using the ACLI .....	17
Privilege Levels.....	17
Enabling Superuser Mode.....	17
System Access.....	18
Local Console Access.....	18
Remote Telnet Access.....	18
Remote SSH Access.....	18
ACLI Help and Display.....	18
Exiting the ACLI.....	19
Navigation Tips.....	19
Hotkeys.....	19
Command Abbreviation and Completion.....	20
Command Abbreviation.....	20
Tab Completion.....	20
Configuration Element and System Command Menus.....	20
Context-Sensitive Help.....	20
Context-Sensitive Help for System Commands.....	21
Viewing Output With the More Prompt.....	22
Disabling the More Prompt.....	23
Configuring Using the ACLI.....	23
Line-by-Line Commands.....	23
Working with Configuration Elements.....	23
Creating configurations.....	24
Saving configurations with the done command .....	24
Viewing configurations with the show command.....	24
Navigating the configuration tree with the exit command.....	24
Choosing configurations with the select command.....	25
Deleting configurations with the no command.....	25
ACLI Configuration Summaries.....	26
Viewing Summaries.....	26
Data Entry.....	27
ACLI Field Formats.....	27
Boolean Format.....	27
Carrier Format.....	27
Date Format.....	27
Date and Time Format.....	27
Day of Week Format.....	27
Enumerated Format.....	28
Hostname (or FQDN) Format.....	28
IP Address Format.....	28
Name Format.....	28
Number Format.....	28
Text Format.....	29
Time of Day Format.....	29
Preset Values.....	29
Default Values.....	29
Error Messages.....	29

Special Entry Types Quotation Marks and Parentheses.....	30
Multiple Values for the Same Field.....	30
Multi-Word Text Values.....	30
An Additional Note on Using Parentheses.....	31
Option Configuration.....	31

## 2 ACLI Commands A-M..... 33

acquire-config.....	33
arp-add.....	34
arp-check.....	34
arp-delete.....	35
backup-config.....	36
check-space-remaining.....	36
check-stack.....	37
clear-alarm.....	37
clear-cache.....	38
clear-cache dns.....	38
clear-cache enum.....	38
clear-cache registration.....	39
clear-cache tls.....	39
clear-deny.....	39
clear-sess.....	40
clear-trusted.....	40
cli.....	41
configure terminal.....	42
delete realm-specifics.....	42
delete-backup-config.....	42
delete-config.....	43
delete-import.....	43
delete-status-file.....	44
display-alarms.....	44
display-backups.....	45
display-current-cfg-version.....	45
display-logfiles.....	46
display-running-cfg-version.....	46
enable.....	47
exit.....	47
format.....	48
generate-certificate-request.....	48
generate-key.....	48
import-certificate.....	49
kill.....	50
load image.....	50
log-level.....	51
management.....	51
monitor.....	52

## 3 ACLI Commands N-Z..... 53

packet-capture.....	53
packet-capture clear.....	54
packet-capture modify.....	54
packet-capture detail.....	54
packet-capture show.....	54
packet-trace.....	54

password-secure-mode.....	55
ping.....	56
prompt-enabled.....	56
realm-specifics.....	57
reboot.....	57
request audit.....	58
request collection.....	58
reset.....	59
restore-backup-config.....	60
save-config.....	61
secret.....	61
set-system-state.....	62
ssh-password.....	63
show.....	63
show acl.....	63
show accounting.....	64
show algd.....	64
show arp.....	65
show backup-config.....	66
show buffers.....	66
show built-in-sip-manipulations.....	66
show call-recording-server.....	66
show clock.....	67
show configuration.....	67
show directory.....	69
show dns.....	69
show dnalg rate.....	70
show enum.....	70
show ext-band-mgr.....	70
show ext-clf-svr.....	71
show features.....	71
show h323d.....	71
show health.....	72
show hosts.....	73
show imports.....	73
show interfaces.....	73
show ip.....	74
show logfile.....	74
show loglevel.....	75
show lrt.....	75
show mbed.....	75
show media.....	80
show memory.....	81
show mgcp.....	81
show monthly-minutes.....	82
show msrp statistics.....	82
show nat.....	82
show net-management-control.....	83
show nsep-stats.....	83
show ntp.....	83
show packet-trace.....	84
show policy-server.....	84
show power.....	84
show privilege.....	84
show processes.....	85
show prom-info.....	86

show qos.....	87
show radius.....	87
show ramdrv.....	88
show realm.....	88
show redundancy.....	88
show registration.....	89
show route-stats.....	90
show routes.....	90
show running-config.....	91
show sa.....	91
show security.....	92
show sessions.....	93
show sipd.....	93
show snmp-community-table.....	99
show spl.....	99
show support-info.....	99
show system-state.....	100
show tacacs.....	100
show temperature.....	100
show timezone.....	100
show trap-receiver.....	101
show uptime.....	101
show users.....	101
show version.....	101
show virtual-interfaces.....	102
show voltage.....	102
show wancom.....	102
ssh-pub-key.....	102
stack.....	103
start learned-allowed-elements.....	103
stop-task.....	104
stop learned-allowed-elements.....	104
switchover-redundancy-link.....	105
synchronize.....	105
system-set.....	105
tail-logfile-close.....	106
tail-logfile-open.....	106
tcb.....	107
test-audit-log.....	107
test-pattern-rule.....	108
test-policy.....	108
test-translation.....	109
timezone-set.....	110
verify-config.....	110
watchdog.....	111

## **4 Configuration Elements A-M..... 113**

access-control.....	113
account-config.....	115
account-config > account-servers.....	119
account-config > push-receiver.....	121
allowed-elements-profile.....	122
allowed-elements-profile > rule-sets.....	123
allowed-elements-profile > rule-sets > header-rules.....	123
auth-params.....	125

authentication.....	125
authentication > radius-servers.....	127
authentication > tacacs-servers.....	128
bootparam.....	129
call-recording-server.....	130
capture-receiver.....	131
certificate-record.....	131
cert-status-profile.....	133
class-profile.....	134
class-profile > policy.....	134
data-flow.....	135
dnssalg-constraints .....	136
dns-config.....	137
dns-config > server-dns-attributes.....	138
dns-config > server-dns-attributes > address-translation.....	139
dpd-params.....	139
enforcement-profile.....	140
enforcement-profile > subscribe-event.....	141
enum-config.....	141
ext-policy-server.....	143
h323.....	147
h323 > h323-stacks.....	149
h323 > h323-stacks > alarm-threshold.....	153
home-subscriber-server.....	154
host-route.....	155
ike-certificate-profile.....	155
ike-config.....	156
ike-interface.....	161
ike-sainfo.....	162
ims-aka-profile.....	163
ipsec.....	164
ipsec > ipsec-global-config.....	165
ipsec > security-association.....	165
ipsec > security-association > manual.....	166
ipsec > security-association > tunnel-mode.....	167
ipsec > security-policy.....	168
ipsec > security-policy > outbound-sa-fine-grained-mask.....	169
iwf-config.....	170
license.....	171
local-address-pool.....	171
local-address-pool > address-range.....	172
local-policy.....	173
local-policy > policy-attributes.....	174
local-response-map.....	176
local-response-map > entries.....	176
local-routing-config.....	177
media-manager-config.....	178
media-policy.....	183
media-policy > tos-settings.....	184
media-profile.....	184
media-security.....	186
media-security > sipura-profile.....	186
media-sec-policy.....	187
media-sec-policy > inbound.....	187
media-sec-policy > outbound.....	188
mgcp-config.....	188

mikey-profile.....	192
msrp-config.....	193

## 5 Configuration Elements N-Z..... 195

net-management-control.....	195
network-interface.....	197
network-interface > gw-heartbeat.....	199
network-parameters.....	200
ntp-sync.....	202
qos-constraints.....	202
password-policy.....	203
phy-interface.....	204
phy-interface > network-alarm-threshold.....	206
public-key.....	206
q850-sip-map.....	207
q850-sip-map > entries.....	207
realm-config.....	208
realm-group.....	215
redundancy.....	216
redundancy > peers.....	220
redundancy > peers > destinations.....	221
rph-policy.....	221
rph-profile.....	222
sdes-profile.....	223
security-config.....	224
session-agent.....	224
session-agent > auth-params.....	233
session-agent > rate-constraints.....	233
session-agent-group.....	234
session-constraints.....	236
session-constraints > rate-constraints.....	238
session-router-config.....	239
session-router > holidays.....	241
session-timer-profile.....	241
session-translation.....	242
sip-config.....	243
sip-feature.....	247
sip-interface.....	249
sip-interface > sip-ports.....	256
sip-isup-profile.....	257
sip-manipulation.....	257
sip-manipulation > header-rules.....	258
sip-manipulation > header-rules > element-rules.....	259
sip-manipulation > mime-isup-rules.....	261
sip-manipulation > mime-isup-rules > mime-header-rules.....	262
sip-manipulation > mime-isup-rules > isup-param-rules.....	263
sip-manipulation > mime-rules.....	264
sip-manipulation > mime-rules > mime-headers.....	265
sip-manipulation > mime-sdp-rules.....	266
sip-manipulation > mime-sdp-rules > sdp-session-rules > sdp-line-rules.....	267
sip-manipulation > mime-sdp-rules > sdp-session-rules > sdp-line-rules.....	268
sip-manipulation > mime-sdp-rules > sdp-media-rules.....	269
sip-nat.....	270
sip-profile.....	272
sip-q850-map.....	273



sip-q850-map > entries.....	273
sip-response-map.....	274
sip-response-map > entries.....	274
sipura-profile.....	275
snmp-community.....	276
snmp-user-entry.....	276
spl-config.....	277
spl-config > plugins.....	277
static-flow.....	277
steering-pool.....	279
surrogate-agent.....	280
system-access-list.....	282
system-config.....	282
system-config > alarm-threshold.....	287
system-config > collect.....	288
system-config > collect > push-receiver.....	289
system-config > collect > group-settings.....	290
system-config > syslog-servers.....	291
system-config > directory-cleanup.....	292
tcp-media-profile.....	292
tcp-media-profile > tcp-media-profile-entry.....	293
test-policy.....	294
test-translation.....	294
tls-global.....	295
tls-profile.....	295
translation-rules.....	297
trap-receiver.....	298
tunnel-orig-params.....	299
<b>Glossary.....</b>	<b>301</b>



# Preface

---

## About This Guide

The ACLI Reference Guide provides a comprehensive explanation of all commands and configuration parameters available to you in the Acme Command Line Interface (ACLI). This document does not explain configurations and the logic involved in their creation.

Release Version S-CX6.4.0 is supported on the Acme Packet 4500 and Acme Packet 3800 series platforms. Release S-CX6.3.0 is not supported by the legacy 4250 platform.

### Document Organization

- About this Guide—This chapter.
- How to Use the ACLI—Explains how to use the ACLI, the CLI-based environment for configuring the Net-Net family of products.
- Commands A-M—Lists commands starting with A-M, their syntax, and their usage.
- Commands N-Z—Lists commands starting with N-Z, their syntax, and their usage.
- Configuration Elements A-M—Lists configuration elements starting with A-M, their syntax, and their usage. Subelements are listed directly after the element where they are located.
- Configuration Elements N-Z—Lists configuration elements starting with N-Z, their syntax, and their usage. Subelements are listed directly after the element where they are located.

### Audience

This document is written for all users of the Oracle Communications Session Border Controller. Since the ACLI is one of the primary ways of configuring, monitoring, and maintaining your Oracle Communications Session Border Controller, this document lists the ACLI commands and their syntax.

### Conventions

This section explains the documentation conventions used in this guide. Each of the following fields is used in the Net-Net ACLI Reference Guide. The following are the fields associated with every command or configuration element in this guide. When no information is applicable, the field is omitted (this occurs mostly with the Notes field).

- Description—Describes each command, its purpose, and use.
  - Syntax—Describes the proper syntax needed to execute the command. Syntax also includes syntax-specific explanation of the command.
  - Arguments—Describes the argument place holders that are typed after a command. For commands only.
  - Parameters—Describes the parameters available in a configuration element. For configuration elements only.
-

- 
- **Default**—Default value that populates this parameter when the configuration element is created.
  - **Values**—Valid values to enter for this parameter.
  - **Notes**—Lists additional information not included in the above fields.
  - **Mode**—Indicates whether the command is executed from User or Superuser mode.
  - **Path**—Describes the ACLI path used to access the command.
  - **Release**—Gives the original release version and the release last modified version for the command.
  - **Example**—Gives an example of how the command should be entered using one of the command's valid arguments.

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

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

## Related Documentation

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

Document Name	Document Description
Acme Packet 4500 System Hardware Installation Guide (400-0101-00)	Contains information about the components and installation of the Acme Packet 4500 system.
Acme Packet 3800 Hardware Installation Guide (400-0118-00)	Contains information about the components and installation of the Acme Packet 3800 system.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the SBC.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about support for its Administrative Security license.

---

---

## Revision History

Date	Revision Number	Revision Description
October 19, 2012	Rev 1.00	Initial Release
November 26, 2012	Rev 1.10	<ul style="list-style-type: none"><li>• Adds conditions under which arp-check command does not issue request</li><li>• Corrects error in ping command related to applicable permission mode</li><li>• Corrects default values for sip-int and SA redirect-action</li><li>• Adds missing status parameter to show enum command</li><li>• Adds missing status parameter to show registration command, which applies only to the Net-Net 3800</li><li>• Removes listing for non-existent ppi-to-pai parameter from sip-interface element</li><li>• Corrects typo in force-report-trunk-info documentation</li><li>• Adds refer-src-routing command</li><li>• Removes deprecated packet-capture command</li><li>• Adds missing output rows to show sipd and show enum commands</li><li>• Specify 1023 as maximum number of characters in an ACLI command</li><li>• Correctly state ntp-sync command as RTC supported</li><li>• Added refer-src-routing as parameter to sip-config</li></ul>
Jan 31, 2013	Rev 1.11	<ul style="list-style-type: none"><li>• Adds system-config &gt; alarm-threshold configuration element</li></ul>
February 12, 2013	Rev 1.12	<ul style="list-style-type: none"><li>• Chapter 5, for SIP Manipulation parameters, added information regarding the use of capital letters in header and element rule names.</li></ul>
March 22, 2013	Rev 1.20	<ul style="list-style-type: none"><li>• Specifies sip-nat parameter ext-address as non-RTC</li><li>• Specifies network-parameter SCTP parameters as non-RTC</li></ul>
August 30, 2013	Rev 1.21	<ul style="list-style-type: none"><li>• Corrected maximum configurable value of max-incoming-conns</li></ul>

---

Date	Revision Number	Revision Description
		and per-src-ip-max-incoming-conns in sip-interface.
August 22, 2013	Rev 1.21	<ul style="list-style-type: none"> <li>• In Chapter 1, changed “Set the system’s watchdog timer” to “View the system’s watchdog timer” regarding User access.</li> <li>• In Chapter 3, adds a note that the Net-Net SBC no longer uses the “show backup-config” command.</li> <li>• In Chapter 3, removes the limitation that the show registrations statistics command applies to the Net-Net 3800 only.</li> <li>• In Chapter 3, adds information about POSIX to the timezone-set description.</li> <li>• In Chapter 5, adds the “timezone” element and parameters.</li> <li>• In Chapter 5, under “Session-Agent-Groups”, the “dest” parameter description was re-worded. It incorrectly stated that SAGs can be nested.</li> <li>• Corrected maximum configurable value of max-incoming-conns and per-src-ip-max-incoming-conns in sip-interface.</li> </ul>
October 1, 2013	Rev 1.22	<ul style="list-style-type: none"> <li>• Updated enable-snmp-syslog-notify</li> </ul>
November 22, 2013	Rev 1.23	<ul style="list-style-type: none"> <li>• Clarifies the effect of internal events on stop-sag-recurse.</li> <li>• Adds dynamic and static TLS transport options to session agent.</li> <li>• Corrects LeastBusy Session agent group explanation, removing reference indicating it is relative to max-outbound-sessions.</li> <li>• Clarifies interaction of tolerance window with invalid-signal-threshold.</li> </ul>
December 27, 2013	Rev 1.24	<ul style="list-style-type: none"> <li>• Adds auth-attribute sub-element.</li> </ul> <p>Adds IP family suffix to realm-config network interface configuration format</p>
January 31, 2014	Rev 1.25	<ul style="list-style-type: none"> <li>• Updates authentication &gt; tacacs-servers configuration element</li> </ul>

Date	Revision Number	Revision Description
		<p>description to indicate that the address must be reachable from a media interface and the realm-id parameter must be a realm configured on a media interface.</p> <ul style="list-style-type: none"> <li>• Updates alternate-name parameter in certificate-record configuration element with more detail.</li> </ul>
February 2014	Rev 1.26	<ul style="list-style-type: none"> <li>• Corrects the descriptions of the ext-policy-server's admission-control and bandwidth-mgmt settings.</li> <li>• Updates <b>restriction-mask</b> parameter with maximum value of 128</li> </ul>
December 2014	Rev 1.27	<ul style="list-style-type: none"> <li>• Update trust me configuration reference.</li> <li>• Updates <b>session-agent-group &gt; group-name</b> parameter's syntax.</li> <li>• Updates <b>session-agent &gt; ping-to-user-part</b> and <b>session-agent &gt; ping-from-user-part</b> parameter descriptions</li> </ul>
	Rev 1.28	<ul style="list-style-type: none"> <li>• Informs the user on valid values for the <b>volume</b> parameter within the <b>system-config</b> element.</li> </ul>
October 2015	Rev 1.29	<ul style="list-style-type: none"> <li>• Clarifies that you must include the pathname along with the filename for the <b>synchronize lrt</b> command.</li> <li>• Rewrites the first Note in the description of the password-policy parameter for clarity</li> </ul>
March 2016	Rev 1.30	<ul style="list-style-type: none"> <li>• Clarifies explanation of prevent-duplicate-attrs parameter.</li> <li>• Adds the -t option to show sipd agents command.</li> <li>• Corrects the description of the ext-policy-server parameter disconnect-on-timeout .</li> <li>• Corrects entry range for account-config max-files parameter.</li> </ul>





---

## How to use the ACLI

### The ACLI

---

The ACLI is an administrative interface that communicates with other components of the Oracle Communications Session Border Controller. The ACLI is a single DOS-like, line-by-line entry interface.

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

### Using the ACLI

---

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

### Privilege Levels

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

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

You know you are in User mode when your system prompt ends in the angle bracket (>).

- Superuser—At Superuser level, you are allowed access to all system commands and configuration privileges. You can use all of the commands set out in this guide, and you can perform all configuration tasks.

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

### Enabling Superuser Mode

To enable Superuser mode:

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

## How to use the ACLI

---

```
ACMEPACKET> enable
Password:
```

2. Enter your password and press <Enter>.

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

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

## System Access

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

### Local Console Access

Console access takes place via a serial connection to the console port directly on the Oracle Communications Session Border Controller chassis. When you are working with the Oracle Communications Session Border Controller at the console, the ACLI comes up automatically.

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

### Remote Telnet Access

Accessing the ACLI via Telnet gives you the flexibility to connect to your Oracle Communications Session Border Controller from a remote location. In addition, you can administer multiple Oracle Communications Session Border Controllers from a single location.



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

### Remote SSH Access

SSH provides strong authentication and secure communications over unsecured channels. Accessing the ACLI via an SSH connection gives you the flexibility to connect to your Oracle Communications Session Border Controller from a remote location over an insecure connection.

## ACLI Help and Display

The Oracle Communications Session Border Controller's ACLI offers several features that aid with navigation and allow you to customize the ACLI so that you can work more efficiently.

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

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

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

## Exiting the ACLI

Typing exit at any ACLI prompt moves you to the next “higher” level in the ACLI. After exiting out of the User mode, you are logged out of the system.

## Navigation Tips

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

## Hotkeys

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

Category	Hotkey	Description
General	<Ctrl-D>	Equivalent of the done command when used at the end of a command line. When used within a command line, this hotkey deletes the character at the cursor.
	<UParrow>	Scrolls forward through former commands.
	<DOWNarrow>	Scrolls backward through former commands.
	<Tab>	Completes a partial command or lists all options available if the characters entered match multiple commands. Executed at the beginning of the command line, this hotkey lists the available commands or configurable elements/parameters .
Context-Sensitive Help	?	Provides context-sensitive help. It functions both for ACLI commands and configuration elements and is displayed in alphabetical order.
Moving the Cursor	<Ctrl-B>	Moves the cursor back one character.
	<Esc-B>	Moves the cursor back one word.
	<Ctrl-F>	Moves the cursor forward one character.
	<Esc-F>	Moves the cursor forward one word.
	<Ctrl-A>	Moves the cursor to the beginning of the command line.
	<Ctrl-E>	Moves the cursor to the end of the command line.
	<Ctrl-L>	Redraws the screen.
Deleting Characters	<Delete>	Deletes the character at the cursor.
	<Backspace>	Deletes the characters behind the cursor.
	<Ctrl-D>	Deletes the character at the cursor when used from within the command line.
	<Ctrl-K>	Deletes all characters from the cursor to the end of the command line.

## How to use the ACLI

Category	Hotkey	Description
	<Ctrl-W>	Deletes the word before the cursor.
	<Esc-D>	Deletes the word after the cursor.
Displaying Previous Command Lines	<Ctrl-P>	Scrolls backward through the list of recently executed commands.

## Command Abbreviation and Completion

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

### Command Abbreviation

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

### Tab Completion

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

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

```
ACMEPACKET# generate-key
```

## Configuration Element and System Command Menus

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

```
ACMEPACKET(local-policy)# ?
from-address      from address list
to-address        to address list
source-realm      source realm list
description       local policy description
activate-time     policy activation date & time
deactivate-time   policy deactivation date & time
state            enable/disable local policy
policy-priority   priority for this local policy
policy-attributes list of policy attributes
select           select a local policy to edit
no               delete selected local policy
show             show selected local policy
done            write local policy information
exit            return to previous menu
```

## Context-Sensitive Help

In addition to the information that ACLI menus offer, context-sensitive help can assist you with navigation and configuration. Within this one-line entry, you have access to context-sensitive help that tells you what values are valid

for a given field and when you have completed an entry. When the <ENTER> no further known parameters line appears, the ACLI is informing you that there is no subsequent information to enter.

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

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

## Context-Sensitive Help for System Commands

The ACLI's context-sensitive help feature displays information you need to complete system commands and the body of subcommands available for each system command. In the following example, the show command menu appears. Typing a ? after a system command asks if the system requires further information to complete a specific command. The system responds with a list of available subcommands.

```
ACMEPACKET# show ?
about                credit information for acli
accounting            accounting statistics
acl                  show host access table
algd                 ALG MGCP status
arp                  ARP table
backup-config        show a backup configuration
balancer              show session load balancer information
bgfd                 BGFD status
buffers              show memory buffer statistics
built-in-sip-manipulations Displays all built-in sip-manipulations
call-recording-server Call Recording Server Statistics
clock                system clock
configuration         show current configuration
directory             show files in a directory
dns                  DNS information
enum                 ENUM information
ext-band-mgr          External Bandwidth Manager status
ext-clf-svr           External CLF Server status
features              currently enabled features
h248d                 H248D status
h323d                 H323D status
health               system health information
hosts                show host table
imports              show all files available for import
interfaces            show network interfaces
ip                   IP system information
logfile              Display a log file, 'enter' to display list
loglevel             loglevels of current processes
lrt                  LRT (local-routing) information
mbcd                 MBCD status
media                show media interface information
memory               memory statistics
mgcp                 ALG MGCP status
monthly-minutes       monthly minutes information for a specified realm
nat                  show NAT table
neighbor-table        ICMPv6 neighbor table
net-management-control Network Management Controls Statistics
nsep-stats            NS/EP RPH call statistics
ntp                  NTP status
packet-trace          displays the current packet trace addresses
policy-server         external policy server name
power                current state of each power supply
privilege             show current privilege level
processes             active process statistics
```

## How to use the ACLI

prom-info	show prom information
qos	show qos FPGA information
radius	radius accounting and authentication statistics
ramdrv	ramdrv space usage
realm	realm statistics
redundancy	redundancy status
registration	SIP Registration Cache status
route-stats	show routing statistics
routes	show routing table entries
running-config	current operating configuration
sa	security-associations information
security	security information
sessions	Session Statistics
show	
sipd	SIPD status
snmp-community-table	show snmp community table
snmp-info	show snmp
space	check the remaining space on the device specified
spl	SPL information
spl-options	display information on all SPL options
support-info	show all required support information
system-state	current system-state
tacacs	tacacs authorization, accounting and
authentication statistics	
temperature	current SD temperature readings
timezone	show timezone for the system (start and end time
in mmddHH format)	
trap-receiver	show snmp trap receivers
uptime	system uptime
users	currently logged in users
version	system version information
virtual-interfaces	show virtual interfaces
voltage	current SD voltages (SD-II only)
wancom	show wancom interfaces

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

```
ACMEPACKET# show about ?
<ENTER!> no further known parameters
ACMEPACKET# show about
```

## Viewing Output With the More Prompt

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

- <Space> —Display the next section of output
- <q>—Quits and returns to the system prompt
- <c>—Displays the rest of the output in its entirety

```
ACMEPACKET# show ?
about          credit information for acli
accounting     accounting statistics
acl            show host access table
algd           ALG MGCP status
arp            ARP table
backup-config  show a backup configuration
balancer       show session load balancer information
bgfd           BGFD status
buffers        show memory buffer statistics
built-in-sip-manipulations Displays all built-in sip-manipulations
call-recording-server Call Recording Server Statistics
clock          system clock
configuration  show current configuration
```

directory	show files in a directory
dns	DNS information
enum	ENUM information
ext-band-mgr	External Bandwidth Manager status
ext-clf-svr	External CLF Server status
features	currently enabled features
h248d	H248D status
h323d	H323D status
health	system health information
hosts	show host table
imports	show all files available for import
interfaces	show network interfaces
ip	IP system information
logfile	Display a log file, 'enter' to display list
('space' for next page; 'q' to quit; 'enter' for next line; 'c' to continue)	

## Disabling the More Prompt

If you don't want the Oracle Communications Session Border Controller to display the More prompt, you can disable it using the cli command.

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

## Configuring Using the ACLI

This section describes the two ACLI methods available for configuring the Oracle Communications Session Border Controller using line-by-line ACLI commands.

### Line-by-Line Commands

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

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

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

## Working with Configuration Elements

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

A common set of commands appear in all configuration elements, and are not applicable for user and superuser commands. These commands are:

- **select**—Used to select a configuration element to edit or view.
- **no**—Used to delete the current configuration element object.
- **show**—Used to view the current values of parameters in the selected configuration element.

- **done**—Used to save configuration changes.
- **exit**—Used to exit the current configuration element or path to the next higher level.

### Creating configurations

Creating configuration elements involves first traversing to the ACLI path to enter configurations. Once you are in the element you want to configure, enter a parameter name followed by a value.

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

### Saving configurations with the done command

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

- The **done** command, which is entered within a configuration element.
- The hotkey <Ctrl-D>, which is entered within a configuration element. This enters the done command in the command line and saves your information.

The Save Changes y/n ? # prompt appears when you **exit** a configuration element without saving your changes. This prompt only appears if you have changed old information and/or entered new information.

Every configuration element contains the **done** command.

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

```
ACMEPACKET(snmp-community) # done
      community-name          acme_community
      access-mode             READ-ONLY
      ip-addresses            10.0.0.2
      last-modified-by
      last-modified-date
ACMEPACKET(snmp-community) #
```

### Viewing configurations with the show command

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

To view configuration information, type show when you are finished with a line-by-line entry. The following example illustrates the use of the **show** command before executing the done command.

```
ACMEPACKET(host-route) # show
host-route
      dest-network            10.1.0.0
      netmask                 255.255.0.0
      gateway                 172.30.0.1
      description            Test host route
      last-modified-by       admin@console
      last-modified-date     2014-01-15 17:12:07
```

### Navigating the configuration tree with the exit command

The **exit** command moves you to the next-higher location in the configuration tree. In addition, when you use the **exit** command and have not already saved your changes, the ACLI produces the following message:

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



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

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

## Choosing configurations with the select command

Editing individual configurations in the ACLI involves finding the element or field you need to update, entering the new information, and then saving the element.

To select an existing configuration element:

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

```
ACMEPACKET (phy-interface) # select
<name>: <Enter>
1: phyTEST
2: phyTEST-RIGHT
3: mn1
selection:3
ACMEPACKET (phy-interface) #
```

4. Use the **show** command to display all configured values of the selected configuration element.

```
ACMEPACKET (phy-interface) #show
phy-interface
      name                mn1
  operation-type          Control
      port                0
      slot                0
  virtual-mac
  wancom-health-score     55
  overload-protection     disabled
  last-modified-by        admin@console
  last-modified-date      2012-11-12 11:02:09
```

5. Optionally make any changes you to parameters in the selected configuration element. You can also overwrite parameters by entering a new value after a previous value has been created.
6. Use the **done** command to save your updates.

## Deleting configurations with the no command

There are two methods of deleting configurations.

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

For either method, use the **no** command to clear configurations. Only Multiple Instance Elements can be deleted from the system. Single Instance Elements can not be deleted; they can only be edited.

### Deleting an existing configuration element example

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

To delete an existing element:

1. Enter the ACLI path to the element you wish to delete.

## How to use the ACLI

---

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

```
ACMEPACKET(media-profile)# no
<name>: <Enter>
1: PCMU
2: G723
3: G729
```

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

```
selection:3
```

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

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

## ACLI Configuration Summaries

---

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

### Viewing Summaries

The show command that appears for each ACLI configuration element allows you to view the configured information for a given element. The following example shows how to view media-profile configuration summaries.

To view the settings for the media-profile element:

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

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)# media-profile
ACMEPACKET(media-profile)#
```

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

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

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

```
selection: 1
```

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

```
ACMEPACKET(media-profile)# show
media-profile
  name                PCMU
  subname
  media-type          audio
  payload-type
  transport            RTP/AVP
  req-bandwidth        0
  frames-per-packet    0
  parameters
  average-rate-limit   0
```

peak-rate-limit	0
max-burst-size	0
sdp-rate-limit-headroom	0
sdp-bandwidth	disabled
police-rate	0
standard-pkt-rate	0
last-modified-by	
last-modified-date	

## Data Entry

To enter data using the ACLI, your entries must conform to required field formats. This section describes these formats, gives information about preset values, default values, and error messages.

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

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

## ACLI Field Formats

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

### Boolean Format

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

### Carrier Format

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

### Date Format

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

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

### Date and Time Format

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

### Day of Week Format

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

- U—Sunday
- M—Monday
- T—Tuesday
- W—Wednesday

- R—Thursday
- F—Friday
- S—Saturday
- H—Holiday

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

## Enumerated Format

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

## Hostname (or FQDN) Format

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

All hostname fields support IPv4 addresses as well as hostnames.

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

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

Note that each label is separated by a period.

The following describes hostname (FQDN) format label types:

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

## IP Address Format

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

## Name Format

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

## Number Format

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

## Text Format

Text entries (e.g., description fields) do not need to follow a particular format. Text fields can accommodate any combination of printable numerical and alphabetical characters, spaces, and most symbols. Noted exceptions are the ampersand (&), the apostrophe ('), and the less than symbol (<). Entries with spaces must be entered fully within quotation marks. For example, "This is the official Acme Packet Oracle Communications Session Border Controller configuration" is a valid text entry.

## Time of Day Format

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

## Preset Values

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

## Default Values

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

## Error Messages

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

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

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

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

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

Message	Description
error invalid data...	You have entered a value not permitted by the system. This error includes numeric values that exceed defined parameters and misspellings of specifically spelled values (such as "enabled" or "disabled").
% command not found	You entered a command that is not valid. The command may be misspelled, or it may not exist where you are working.
invalid selection...	You have selected an item that does not exist in the system.
invalid number of arguments	You either have entered too many arguments (or commands) on one line or you may not have quotation marks ("" ) around your multi-word entry.
error 500 saving ...	The system could not save the data you entered to the system database.

### Special Entry Types Quotation Marks and Parentheses

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


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

### Multiple Values for the Same Field

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

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

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

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

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

### Multi-Word Text Values

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

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

```
ACMEPACKET(session-router-config)# holidays
ACMEPACKET(session-router-holidays)# date 2008-01-01
ACMEPACKET(session-router-holidays)# description "new year's day"
ACMEPACKET(session-router-holidays)# done
    holiday
    date
    description
    2010-10-10
    sample day
```

## An Additional Note on Using Parentheses

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

## Option Configuration

The options parameter shows up in many configuration elements. This parameter is used for configuring the Oracle Communications Session Border Controller to behave with either non-standard or customer-specific behavior.

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

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

### Append Example

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

```
ACMEPACKET(h323) # options +noAliasInRCF
ACMEPACKET(h323) # show
h323-config
    state                enabled
    log-level            NOTICE
    response-tmo         4
    connect-tmo          32
    rfc2833-payload      101
    alternate-routing     proxy
    codec-fallback        disabled
    enum-sag-match       disabled
    remove-t38           disabled
    options              noAliasInRCF
    last-modified-by     admin@console
    last-modified-date   2014-01-14 20:17:42
```

### Delete Example

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

```
ACMEPACKET(h323) # options -forceH245
ACMEPACKET(h323) # show
h323-config
    state                enabled
    log-level            NOTICE
    response-tmo         4
    connect-tmo          32
    rfc2833-payload      101
    alternate-routing     proxy
    codec-fallback        disabled
    enum-sag-match       disabled
    remove-t38           disabled
    options              noAliasInRCF
    last-modified-by     admin@console
    last-modified-date   2014-01-14 20:19:43
```





---

## ACLI Commands A-M

### acquire-config

---

The acquire-config command retrieves the configuration from one Oracle Communications Session Border Controller for configuration checkpointing an HA node.

#### Syntax

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

Example:

#### Arguments

<IPAddress> Enter the IP address of the Oracle Communications Session Border Controller to acquire configuration from.

#### Mode

Superuser

#### Release

First appearance: 1.2.1 / Most recent update: 2.0

#### Notes

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

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

#### Example

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

## arp-add

---

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

### Syntax

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

### Arguments

<slot> Select the media interface slot

Values:

- 0—Left slot
- 1—Right slot

<port> Select the media interface port

Values:

- 0—Leftmost port
- 1—Second from left port
- 2—Third from left port (not applicable for GigE cards)
- 3—Rightmost port (not applicable for GigE cards)

<vlan ID> VLAN identifier

<ip-address> Enter the IP address

<mac-address> Enter the MAC address in hexadecimal notation

### Mode

Superuser

### Release

First appearance: 1.0 / Most recent update: 1.2.1

### Example

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

## arp-check

---

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

### Syntax

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

### Arguments

<slot> Select the media interface slot

Values

- 0—Left slot
- 1—Right slot

<port> Select the media interface port

Values

- 0—Leftmost port
- 1— Second from left port
- 2 —Third from left port (not applicable for GigE cards)
- 3 —Rightmost port (not applicable for GigE cards)

<vlan ID> Enter the VLAN identifier

<ip-address> Enter the IP address

### Mode

Superuser

### Release

First appearance: 1.0 / Most recent update: 1.2.1

### Example

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

## arp-delete

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

### Syntax

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

### Arguments

<slot> Select the media interface slot

Values:

- 0—Left slot
- 1—Right slot

<port> Select the media interface port

Values:

- 0—Leftmost port
- 1— Second from left port
- 2 —Third from left port (not applicable for GigE cards)
- 3 —Rightmost port (not applicable for GigE cards)

<vlan ID> Enter the VLAN identifier

<ip-address> Enter the IP address

### Mode

Superuser

### Release

First appearance: 1.0 / Most recent update: 1.2.1

### Example

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

## backup-config

---

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

### Syntax

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

### Arguments

**<name-of-backup>** Enter the name of the backup configuration file

**running-** Backup the configuration from the running configuration cache. This is an optional argument

**editing-** Backup the configuration from the editing configuration cache. This is an optional argument.

**standard-** Use standard XML as the file format

**non-standard-** Use non-standard, legacy XML for the file format

### Mode

Superuser

### Release

First appearance: 1.0 / Most recent update: 6.3

### Example

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



**Note:** If insufficient disk space is available, the Oracle Communications Session Border Controller will not complete the task.

## check-space-remaining

---

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

### Syntax

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

### Argument

**<device>** Select where to check the remaining space

Values:

- boot
- code
- ramdrv

**Mode**

Superuser

**Release**

First appearance: 1.1

**Example**

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



**Note:** The output of this command is in bytes.

## check-stack

---

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

**Syntax**

```
check-stack
```

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

**Mode**

Superuser

**Release**

First appearance: 1.1

**Example**

```
ACMEPACKET# check-stack
```



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

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

## clear-alarm

---

The clear-alarm command clears a specified alarm.

**Syntax**

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

### Arguments

<alarm\_id> Enter a unique 32-bit integer that contains a 16-bit category name or number and a unique 16-bit identifier for the error or failure within that category

<task\_id> Enter the task ID of the task that sent the alarm

### Release

First appearance: 1.0

### Example

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



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

---

## clear-cache

The clear-cache command allows you to clear a specified cache entry on the Oracle Communications Session Border Controller.

### clear-cache dns

#### Syntax

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

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

#### Arguments

- <realm id | all> Specify the realm whose DNS cache you want to clear or enter all if you want to clear the cache of all realms
- <cache entry key> Enter a specific cache entry key or enter all for all entries. A specified cache entry key should take one of the following forms.
  - NAPTR entries—NAPTR:test.com
  - SRV entries—SRV:\_sip\_udp.test.com
  - A entries—A:test.com

#### Example

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

### clear-cache enum

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

#### Syntax

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

#### Arguments

- <EnumConfig Name> Enter the name of the specific EnumConfig for which you want to clear the cache
- <cache entry key> Enter the cache key of the specific EnumConfig for which you want to clear the cache
- <all> Enter all to clear all caches. In order for this command to work the DNS cache needs to be cleared.

### Example

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

## clear-cache registration

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

### Syntax

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

### Arguments

- <sip> Clear the SIP registration cache. The following are the types of information for which you can clear:
  - all
  - by-ip <IPaddress>
  - by-user <phone number>
- <mgcp> Clear the MGCP registration cache. The following are the types of information for which you can clear:
  - all
  - by-endpoint <endpoint name>
- <h323> Clear the H.323 registration cache. The following are the types of information for which you can query:
  - all
  - by-alias <terminalAlias>

### Example

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

## clear-cache tls

This command allows you to clear the TLS cache.

### Syntax

```
clear-cache tls
```

### Example

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

### Mode

Superuser

### Release

First appearance: 5.0

## clear-deny

The clear-deny command deletes a denied ACL entry.

### Syntax

```
clear-deny [<index> | "all"]
```

### Arguments

- <index> Enter the index number of the ACL entry to delete
- <"all"> Delete all denied ACL entries

### Mode

Superuser

### Release

First appearance: 4.0

### Example

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



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

---

## clear-sess

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

### Syntax

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

### Arguments

- <all> Delete all sessions for the specified protocol
- <by-agent> Delete sessions for a specified session agent
- <by-callid> Delete sessions for a specified call identifier
- <by-ip> Delete sessions for a specified endpoint IP address (entered in quotation marks)
- <by-user> Delete sessions for a specified calling or called number

### Mode

Superuser

### Release

First appearance: 5.1

### Example

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



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

---

## clear-trusted

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



## Syntax

```
clear-trusted [<index> | "all"]
```

## Arguments

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

<"all"> Delete all trusted ACL entries

## Mode

Superuser

## Release

First appearance: 4.0

## Example

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



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

# cli

The `cli` command allows you to modify ACLI session terminal settings and “more” options on your Oracle Communications Session Border Controller.

## Syntax

```
cli ["more" | "terminal-height"]
```

## Arguments

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

- Values: enabled | disabled

**terminal-height** Enter the number of rows in the terminal

- Default: 24
- Values: Min: 0 / Max: 1000

## Mode

User

## Release

First appearance: 5.0

## Example

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

## configure terminal

---

The configure terminal command enters you into the system level where you can configure all operating and system elements on your Oracle Communications Session Border Controller.

### Syntax

```
configure terminal
```

### Arguments

configure terminal

### Mode

Superuser

### Release

First appearance: 1.0

### Example

```
ACMEPACKET# configure terminal
```

## delete realm-specifics

---

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

### Syntax

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

### Arguments

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

### Mode

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

### Release

First appearance: S-C6.1.0

### Example

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



**Note:** This command should be used with the utmost care.

## delete-backup-config

---

The delete-backup-config command deletes a saved configuration file from the Oracle Communications Session Border Controller flash memory.

### Syntax

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

### Arguments

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

### Mode

Superuser

### Release

First appearance: 1.2.1

### Example

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



**Note:** Use display-backups to list backup configurations to delete.

## delete-config

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

### Syntax

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

### Arguments

- [cached] Delete the cached configuration. This is an optional argument.

### Mode

Superuser

### Release

First appearance: 1.1 / Most recent update: 2.0

### Example

```
ACMEPACKET# delete-config
```



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

## delete-import

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

### Syntax

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

### Arguments

- <file name> - The name of the SIP manipulation rules file to delete

### Mode

Superuser

### Release

First appearance: S-C6.2.0

### Example

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



**Note:** Include the complete file name in the argument, including .gz.

## delete-status-file

---

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

### Syntax

```
delete-status-file
```

### Arguments

none

### Mode

Superuser

### Release

First appearance: 1.1 / Most recent update: 1.3

### Example

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



**Note:** This command deletes the /code/statsDump.dat file which retains all system data if the Oracle Communications Session Border Controller has to reboot. This command also removes the contents of the /code/taskCheckDump.dat file which contains system failure information.

## display-alarms

---

The display-alarms command displays details about the specific alarms on the Oracle Communications Session Border Controller.

### Syntax

```
display-alarms
```

### Arguments

none

### Mode

User

### Release

Release First appearance: 1.0

### Example

```
ACMEPACKET# display-alarms
```



**Note:** This command shows the current alarms on the Oracle Communications Session Border Controller. Each alarm entry lists alarm ID, task ID, alarm severity code, number of occurrences, when the alarm first and last occurred, the number of times it has occurred, and a description of the alarm.

## display-backups

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

### Syntax

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

### Arguments

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

### Mode

User

### Release

First appearance: 2.0

### Example

```
ACMEPACKET# display-backups
```

## display-current-cfg-version

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

### Syntax

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

### Arguments

none

### Mode

User

### Release

First appearance: 1.2.1

### Example

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



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

## display-logfiles

---

The display-logfiles command lists the current logfiles located in the /code/logs directory.

### Syntax

```
display-logfiles
```

### Arguments

none

### Mode

User

### Release

First appearance: 1.0

### Example

```
ACMEPACKET# display-logfiles
```

## display-running-cfg-version

---

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

### Syntax

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

### Arguments

none

### Mode

User

### Release

First appearance: 1.2.1

### Example

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



**Note:** This command displays the version number of the running configuration, an integer value that is incremented by one for each new configuration version.

## enable

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

### Syntax

```
enable
```

### Arguments

none

### Mode

User

### Release

First appearance: 1.0



**Note:** Observing the command prompt can tell you if the Oracle Communications Session Border Controller is in user or superuser mode. A ">" (close-angle-bracket) indicates User mode and a "#" (pound) sign indicates Superuser mode.

### Example

```
ACMEPACKET> enable
ACMEPACKET#
```

## exit

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

### Syntax

```
exit
```

### Arguments

none

### Mode

User

### Release

Release First appearance: 1.0

### Example

```
ACMEPACKET# exit
```

## format

---

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

### Syntax

```
format <device>
```

### Arguments

- <device> - Enter the name of a device

### Mode

Superuser

### Release

First appearance: 1.0

### Example

```
ACMEPACKET# format device1
```

## generate-certificate-request

---

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

### Syntax

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

### Arguments

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

### Mode

Superuser

### Release

First appearance: 4.1

### Example

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

## generate-key

---

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



## Syntax

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

## Arguments

- <type> - Select the type of key you want to generate. The following is a list of valid security keys.
- Values:
  - 3des— Generate a 3DES 192 bit, odd parity key
  - aes-128— Generate an AES 128 bit key
  - aes-256— Generate an AES 256 bit key
  - des— Generate a DES 64 bit, odd parity key
  - hmac-md5— Generate an HMAC MD5 secret
  - hmac-sha1— Generate an HMAC SHA1 secret

## Mode

Superuser

## Release

First appearance: 5.0

### Example

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

# import-certificate

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

## Syntax

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

## Arguments

- <type> - Enter the type of certificate you want to import.
- Values
  - pkcs7—Import using a password enhanced mail format
  - x509—Import using a password enhanced mail format
  - try-all—Try importing from both pkcs7 and x509

## Mode

Superuser

## Release

First appearance: 4.1

### Example

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

### kill

---

The kill command terminates a Telnet session on the Oracle Communications Session Border Controller.

#### Syntax

```
kill <id>
```

#### Arguments

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

#### Mode

Superuser

#### Release

Release First appearance: 2.0



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

#### Example

```
ACMEPACKET# kill 11
```

### load image

---

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

#### Syntax

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

#### Arguments

<IP address> Enter the IP address of the remote host

<filename> Enter the remote filename with path

<username> Enter the username for the remote host

#### Mode

Superuser

#### Release

Release First appearance: 5.1.1



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

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

#### Example

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

## log-level

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

### Syntax

```
log-level system <log-level> log-level <task-name | "all"> <log-level>
```

### Arguments

<log-level> Select the log level either by name or by number

- Values • emergency (1)
    - critical (2)
    - major (3)
    - minor (4)
    - warning (5)
    - notice (6)
    - info (7)
    - trace (8)
    - debug (9)
  - detail<task-name> Enter the task name for the log level being set<all> Change the log level for all Acme Packet SBC tasks
- Superuser

### Release

Release First appearance: 1.0 / Most recent update: 1.1



**Note:** The log setting changes made by the log-level command are not persistent after a reboot. Upon reboot, you need to change the log settings in the system configuration in order for them to be persistent. When entering multiple log types in the log-type-list argument, use a space for separation.

### Example

#### Example

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

## management

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

### Syntax

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

### Arguments

<state> Select the operating state of service

- Values:
    - enable—Enable the service set in the <service> argument from starting at boot time
    - disable—Disable the service set in the <service> argument from starting at boot time
- <service> Select the <service> that you are setting boot time status

- Values:
  - ftp—Enter the FTP service
  - telnet—Enter the Telnet service

### Mode

Superuser

### Release

First appearance: 2.0

### Example

```
ACMEPACKET# management enable ftp
```

---

## monitor

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

### Syntax

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

### Arguments

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

### Mode

User

### Release

First appearance: 1.0



**Note:** This command outputs real-time media and signaling statistics to the ACLI. Pressing a numerical digit (0-9) changes the refresh rate to that interval in seconds. By default, there is a 2 second refresh rate. Type "q" to exit the monitor display. Monitor session will display the equivalent of show sipd statistics, and monitor media will display the equivalent of show mbed statistics.

### Example

```
ACMEPACKET# monitor media
```

---

## ACLI Commands N-Z

### packet-capture

---

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

#### Syntax

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

#### Arguments

<state> - Select the state of packet capturing on the slot and port pair

- enabled — Enable packet capturing
- disabled — Disable packet capturing

<slot> - Select the media interface slot

- 0—Left slot
- 1—Right slot

<port> - Select the media interface port

- 0—Leftmost port
- 1—Second from left port
- 2—Third from left port (not applicable for GigE cards)
- 3—Rightmost port (not applicable for GigE cards)

#### Mode

Superuser

#### Release

First appearance: 1.0 / Most recent update: 1.2.1

#### Example

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

### packet-capture clear

Empty the packet buffer of captured packets

```
packet-capture clear
```

### packet-capture modify

#### Syntax

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

#### Arguments

<integer> - Enter the number of packets to show in the buffer

- Default: 100
- Values: Min: 0 / Max: 100

<y [es] | n [o]> - Signify whether the packet buffer wraps when full

- Default: n
- Values: yes | no

#### Example

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

### packet-capture detail

Display a specific packet on the screen.

#### Syntax

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

#### Arguments

<integer> - Identify the packet number to view

### packet-capture show

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

```
packet-capture show
```

## packet-trace

---

The packet-trace command starts or stops packet tracing on the Oracle Communications Session Border Controller. Once the trace is initiated, the Oracle Communications Session Border Controller duplicates all packets sent to and from the endpoint identified by the IP address that are sent or received on the specified Oracle Communications Session Border Controller network interface.

#### Syntax

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

#### Arguments

<start> - Start **packet-tracing** on the Oracle Communications Session Border Controller. Once the trace is initiated, the Oracle Communications Session Border Controller duplicates all packets sent to and from the endpoint identified

by the IP address that are sent or received on the specified Oracle Communications Session Border Controller network interface.

- **network-interface**—The name of the network interface on the Oracle Communications Session Border Controller from which you want to trace packets; this value can be entered as either a name alone or as a name and subport identifier value (name:subportid)
- **ip-address**—IP address of the endpoint to and from which the Oracle Communications Session Border Controller will mirror calls
- **local-port**—Layer 4 port number on which the Oracle Communications Session Border Controller receives and from which it sends. This is an optional parameter; if no port is specified or if it is set to 0, then all ports will be traced.
- **remote-port**—Layer 4 port to which the Oracle Communications Session Border Controller sends and from which it receives. This is an optional parameter; if no port is specified or if it is set to 0, then all ports are traced.

**<stop>** - Manually stop packet tracing on the Oracle Communications Session Border Controller. With this command you can either stop an individual packet trace or all packet traces that the Oracle Communications Session Border Controller is currently conducting.

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

## Mode

Superuser

## Release

First appearance: 5.0

## Example

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

# password-secure-mode

The password-secure-mode command allows you to enable and view the status of the password secure mode functionality on the Oracle Communications Session Border Controller

## Syntax

```
password-secure-mode ["enable" | "status"]
```

## Arguments

**enable** - Enable the password secure mode on the Oracle Communications Session Border Controller

**status** - Display the current status of the password secure mode functionality on the Oracle Communications Session Border Controller.

### Mode

Superuser

### Release

First appearance: 5.0

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

---

## ping

The ping command pings a remote IP address.

### Syntax

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

### Arguments

<ip-address> - Enter the IP address of host to ping

<vlan> - Enter the network interface or vlan to use. This is an optional argument.

<source-ip> - Enter the source IP address to use. This is an optional argument.

### Mode

Superuser

### Release

First appearance: 1.0



**Note:** This command sends ICMP echo messages, and displays:

- minimum round trip time (RTT)
- maximum RTT
- average RTT
- number of packets transmitted
- number of packets received
- percentage of packets lost

The default ping timeout is 64ms.

### Example

```
ACMEPACKET# ping 100.20.11.30
```

---

## prompt-enabled

The Oracle Communications Session Border Controller lets you know if a configuration has been changed and you've applied the done command, but have not saved and activated yet. When you issue the done command and return to Superuser mode, the ACLI prompt prefixes two asterisks (\*\*). When you have saved, but not yet activated, the ACLI prompt prefixes one asterisk (\*).



The prompt-enabled command allows you to decide whether or not you want the Oracle Communications Session Border Controller to give you this prompt. When this command is entered without an argument, the Oracle Communications Session Border Controller displays the current setting of the prompt.

### Syntax

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

### Arguments

**enabled** - Enable the prompt-enabled feature

**disabled** - Disable the prompt-enabled feature

### Mode

Superuser

### Release

First appearance: 5.0

### Example

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

## realm-specifics

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

### Syntax

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

### Arguments

<realm-ID> Enter the name of realm

### Mode

User

### Release

First appearance: 2.0

### Example

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



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

## reboot

The reboot command reboots the Oracle Communications Session Border Controller.

### Syntax

```
reboot <arguments>
```

### Arguments

<arguments> The following are arguments for this command:

- Values:
  - force—Reboot the Oracle Communications Session Border Controller system using the last running configuration. The confirmation prompt is bypassed when using this command.
  - activate—Reboot the Oracle Communications Session Border Controller system using the last-saved configuration. You are presented with a confirmation prompt when using this command.
  - no argument—Reboot the Oracle Communications Session Border Controller system using the last running configuration

### Mode

Superuser

### Release

First appearance: 1.0 / Most recent update: 1.2.1

### Example

```
ACMEPACKET# reboot activate
```

---

## request audit

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

### Syntax

```
request audit <registration>
```

### Arguments

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

### Mode

Superuser

### Release

First appearance: 5.0

### Example

```
ACMEPACKET# request audit SIP
```

---

## request collection

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

## Syntax

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

<start> Start data collection. If a collection object is not specified, collection is performed on all groups. <stop> Stop data collection. <restart> Restart data collection in general or for the collection object specified. <purge> Delete all data files resident on the Oracle Communications Session Border Controller for collection function. <collection-object> Enter the collection groups you can configure to collect data information from. This is an optional argument and when no group is specified, the Oracle Communications Session Border Controller collects information from all groups. The following is a list of collection groups:

- Values :
  - algd-ACL—Request collection on the ALGD ACL Operations group
  - algd-state—Request collection on the ALGD State group
  - fan—Request collection on the fan group
  - h323-stats—Request collection on the H323 Statistics group
  - interface—Request collection on the interface group
  - mgcp-ACL—Request collection on ALGD MGCP ACL Status group
  - mgcp-media-events—Request collection on the ALGD MGCP Media Events group
  - mgcp-trans—Request collection on the ALGD MGCP transactions group
  - session-agent—Request collection on the session agent group
  - session-realm—Request collection on the session realm group
  - sip-ACL-oper—Request collection on the SIP ACL Operations group
  - sip-ACL-status—Request collection on the SIP ACL Status group
  - sip-client—Request collection on the SIP Client Transaction group
  - sip-errors—Request collection on the SIP Errors/Events group
  - sip-policy—Request collection on the SIP Policy/Routing group
  - sip-server—Request collection on the SIP Server Transaction group
  - sip-sessions—Request collection on the SIP Session Status group
  - sip-status—Request collection on the SIP Status group
  - system—Request collection on the system group
  - temperature—Request collection on the temperature group
  - voltage—Request collection on the voltage group

## Mode

Superuser

## Release

First appearance: 5.0

## Example

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

## reset

The reset command resets statistic counters.

## Syntax

```
reset <statistic>
```

### Arguments

<statistic> The following is a list of specific statistics which you can tell the Oracle Communications Session Border Controller to reset:

- Values :
  - algd—Reset algd-related statistics shown in the show algd command
  - all—Reset the statistics shown in the following commands: show sipd, show mbcd, show algd, show mbcd redundancy, show algd redundancy, show sipd redundancy, show redundancy mbcd, show redundancy algd, show redundancy, show memory
  - application—Reset the application statistics shown in the show application command
  - ebmd—Reset EMBD statistics
  - h323d—Reset the h323-related signaling statistics
  - mbcd—Reset mbcd-related statistics shown in the show mbcd command (except statistics related to high availability)
  - nsep-stats—Reset counters for NSEP-related statistics; to reset counters for a specific r-value, add the specific r-value to the end of the command
  - redundancy—Reset the redundancy statistics shown in the show mbcd redundancy, show algd redundancy, show sipd redundancy, show redundancy mbcd, show redundancy algd, and show redundancy sipd commands
  - security-associations—Reset Security Association statistics
  - session-agent <hostname>—Reset statistics for a specified session agent
  - sipd—Reset sipd statistics in the show sipd command
  - snmp-community-table—Reset the counters on SNMP community table statistics
  - spl <filename>—reloads the supplied filename
  - trap-receiver—Reset the counters for trap receiver statistics
  - net-management-control—Reset Network Management Control statistics
  - lrt—Reset Local Routing statistics
  - enum—Reset ENUM statistics
  - dns—Reset DNS statistics



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

### Mode

Superuser

### Release

First appearance: 1.0.1 / Most recent update: 2.0.1

### Example

```
ACMEPACKET# reset h323d
```

---

## restore-backup-config

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

### Syntax

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

### Arguments


<config-name> Enter the name of backup configuration to restore<saved> Restore the configuration to the last saved configuration. This is an optional argument.<running> Restore the configuration to the last running configuration. This is an optional argument.

### Mode

Superuser

### Release

First appearance: 1.0

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

### Example

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

## save-config

The save-config command saves the current configuration to the Oracle Communications Session Border Controller's last-saved configuration, stored in flash memory.

### Syntax

```
save-config <type>
```

### Arguments

<type> Chooses the file format for the internal configuration file.

- Values:
  - standard—Use standard XML as the file format
  - non-standard—Use non-standard, legacy XML for the file format



**Note:** When this command is executed and resources are sufficient, the Oracle Communications Session Border Controller notifies you that the configuration has been saved successfully and the current configuration number will be incremented by one.

### Mode

Superuser

### Release

First appearance: 1.0 / Most recent update: 6.3

### Example

```
ACMEPACKET# save-config
```

## secret

The secret command sets the User and Superuser passwords.

### Syntax

```
secret <user level>
```

### Arguments

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

- Values:
  - login—Set the Oracle Communications Session Border Controller's user password
  - enable—Set the Oracle Communications Session Border Controller's superuser password
  - backup—Set the backup password
  - config—Set the configuration password

#### Superuser



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

We recommend that you do not change the default User and Superuser passwords on Oracle Communications Session Border Controllers in your lab and testing facilities.

### Mode

Superuser

### Release

First appearance: 1.0

### Example

```
ACMEPACKET# secret login
```

---

## set-system-state

The set-system-state command sets the Oracle Communications Session Border Controller as either online or offline.

### Syntax

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

### Arguments

<state> Select the system state

- Values :
  - online—Enable online system state
  - offline—Enable offline system state



**Note:** The offline setting puts the Oracle Communications Session Border Controller into a state where it is powered on and available for administrative purposes, but does not accept calls. Existing calls in progress are not affected.

### Mode

Superuser

## Release

First appearance: 2.0

## Example

```
ACMEPACKET# set-system-state online
```

# ssh-password

The ssh-password command creates SSH login accounts and passwords for secure access into a Oracle Communications Session Border Controller.

## Syntax

```
ssh-password <username> <password>
```

## Arguments

<username> — Enter the username of the new account or the username of the existing SSH account

<password> — Enter a password for the new account or a new password for the existing account

## Mode

Superuser

## Release

First appearance: 2.0



**Note:** Passwords must be 6-9 characters with at least one non-alphabetical character. To execute this command, you must type ssh-password and press <enter>. You will be prompted for the user name to create and the password for the account. You can change the password of a previously existing account by entering the existing username when prompted. You will be prompted a second time to re-enter the password for confirmation.

## Example

```
ACMEPACKET# ssh-password user1 acme
```

# show

The show command displays Oracle Communications Session Border Controller statistics, configurations, and other information. Many of the show commands display period and lifetime statistic counts.

## show acl

## Syntax

```
show acl <arguments>
```

## Arguments

denied—Display denied ACL entries

untrusted—Display untrusted ACL entries

trusted—Display trusted ACL entries

info—Display amount of space used in the CAM with regard to ACL entries. Number of entries, percent utilization, and maximum entries are displayed for each ACL type. The following are the ACL types displayed:

- Denied
- Trusted
- Media
- Untrusted
- Dynamic-trusted

reset—Reset the summary counts of all host ACL entries

summary—Display a summary of all host ACL entries

ip—Display the same output as show acl all, but takes an IP address as an argument to filter all ACL statistics for the given IP address

all—Display all ACL entries

### Example

```
ACMEPACKET# show acl untrusted
```

## show accounting

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

### Syntax

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

### Arguments

Entered without any arguments, the show account command displays the global Accounting Status Summary, returns the equivalent of the show accounting all command .

**<IP address:port>** — With the supplied IP address and port of a configured accounting server, the statistics for that object will be displayed on the screen.

**all** — Display the all accounting servers statistics

### Release

First appearance: S-C6.2.0

### Example

```
ACMEPACKET# show accounting 192.168.81.81:1813
```

## show algd

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

### Syntax

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

### Arguments

Entered without any arguments, the show algd command displays all ALG statistics.

statistics—Display MGCP statistics



errors—Display MGCP error statistics

acls—Display ACL statistics for MGCP

rsip—Display RSIP command statistics

rqnt—Display RQNT command statistics

ntfy—Display NTFY command statistics

crcx—Display CRCX command statistics

mdcx—Display MDCX command statistics

dlcx—Display DLCX command statistics

aupe—Display AUEP command statistics

aucx—Display AUCX command statistics

epcf—Display EPCF command statistics

other—Display other MGCP command statistics

redundancy—Display MGCP redundancy statistics

all—Display all ALG statistics



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

### Example

```
ACMEPACKET# show algd rsip
```

## show arp

### Syntax

```
show arp
```

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

The first section of the show arp command displays the Link Level ARP table including:

- destination address
- ARP gateway
- flags
- reference count
- use
- physical interface on the system.

The second section of the show arp command displays the following information that refers only to media interfaces:

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

The third section of the show arp command shows general ARP table information.

### Example

```
ACMEPACKET# show arp
```

### show backup-config

#### Syntax

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

#### Arguments

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

The show backup-config command displays a specified configuration file saved on the Oracle Communications Session Border Controller's standard backup file directory.

#### Example

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

### show buffers

#### Syntax

```
show buffers
```

This command shows memory buffer statistics divided into three sections.

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

#### Example

```
ACMEPACKET# show buffers
```

### show built-in-sip-manipulations

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

#### Syntax

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

#### Release

First appearance: S-C6.2.0

#### Example

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

### show call-recording-server

This command displays information regarding the IP call replication for call recording (IPRCR) feature configured on the Oracle Communications Session Border Controller. Entering this command without the optional IPRCR ID displays all IPRCR endpoints configured on the Oracle Communications Session Border Controller along with their state.

#### Syntax

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

## Arguments

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

## Example

```
ACMEPACKET# show call-recording-server crs1
```

## show clock

This command displays the current date and time for your Oracle Communications Session Border Controller.

## Syntax

```
show clock
```

## Example

```
ACMEPACKET# show clock
```

## show configuration

## Syntax

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

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

## Arguments

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

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

- Values
  - account-config— Show account-config configuration
  - access-control—Show access-control configuration
  - audit-logging—Show the audit logging configurations
  - auth-params—Show the auth-params configurations
  - authentication—Show the authentication configuration
  - cert-status-profile—Show certificate status profile
  - call-recording-server—Show call-recording-server configurations
  - certificate-record—Show the certificate record configuration
  - class policy—Show all ClassPolicy configuration
  - data-flow—Show the data-flow configurations
  - dns-config—Show all dns-config configurations
  - dpd-params—Show the dpd-params configurations
  - enum-config—Show the enum-config configuration
  - ext-policy-server—Show the external-policy-server configuration
  - h323-config—Show h323 configuration
  - h323-stack—Show all h323-stack configurations
  - ike-certificate-profile—Show the ike-certificate-profile configurations
  - ike-config—Show the ike-config configuration

- ike-interface—Show the ike-interface configurations
- ike-sainfo—Show the ike-sainfo configurations
- ims-aka-profile—Show the ims-aka-profile configurations
- ipsec-global-config—Show the ipsec-global-config configurations
- iwf-stack—Show iwf-stack configuration
- host-route—Show all host-route configurations
- local-address-pool—Show the local-address-pool configurations
- local-policy—Show all local-policy configurations
- local-response-map—Show sip-local-map configuration
- login-config—Show the login configurations
- media-profile—Show all media-profile configurations
- media-manager—Show media-manager configuration
- media-policy—Show all MediaPolicy configurations
- mgcp-config—Show mgcp-config configurations
- network-interface—Show all network-interface configurations
- network-parameters—Show all network-parameters configurations
- ntp-config—Show ntp-config configuration
- capture-receiver—Show capture-receiver configurations
- phy-interface—Show all phys-interface configurations
- public-key—Show the public-key configurations
- realm-config—Show all realm configurations
- q850-sip-map—Show q850-sip-map configurations
- qos-constraints—Show the qos-constraints configurations
- redundancy-config—Show redundancy-config configuration
- sip-response-map—Show all response map configurations
- rph-profile—Show rph-profile configurations
- rph-policy—Show rph-policy configurations
- session-agent—Show all session-agent configurations
- session-group—Show all session-group configurations
- session-translation—Show all session-translation configurations
- session-router—Show session-router configuration
- sip-config—Show all sip-config configurations
- sip-feature—Show all sip-feature configurations
- sip-interface—Show all sip-interface configurations
- sip-manipulation—Show all of the sip-manipulation configurations
- sip-nat—Show all sip-nat configurations
- sip-profile—Show the sip-profile configurations
- sip-isup-profile—Show the sip-isup-profile configurations
- enforcement-profile—Show enforcement-profile configurations
- sip-q850-map—Show sip-q850-map configuration
- snmp-community—Show all snmp-community configurations
- ssh-config—Show the SSH configurations
- static-flow—Show all static-flow configurations
- steering-pool—Show all steering-pool configurations
- realm-group—Show realm-group configurations
- surrogate-agent—Show all of the surrogate-agent configurations
- system-config—Show system-config configuration
- tls-profile—Show TLS profile configurations
- translation-rules—Show all translation-rules configurations
- trap-receiver—Show all TrapReceiver configurations

- codec-policy—Show all codec-policy configurations
- local-routing-config—Show all local-routing configurations
- net-management-control—Show all net-management-control configurations
- security-association—Show all security-association configurations
- security-policy—Show all security-policy configurations
- password-policy—Show password-policy configuration
- session-constraints—Show all session-constraint configurations
- system-access-list—Show all system-access-list configurations
- tls-global—Show all tls-global configurations
- inventory—Display an inventory of all configured elements on the Oracle Communications Session Border Controller

### Example

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

## show directory

This command displays a list of file directories on the storage expansion module. Disk space on the Storage Expansion Module appears as a local volume on the Oracle Communications Session Border Controller.

### Syntax

```
show directory <path>
```

### Arguments

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

### Mode

Superuser

### Release

First appearance: S-C6.2.0

### Example

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

## show dns

### Syntax

```
show dns <arguments>
```

### Arguments

<arguments> Each show dns argument is listed below:

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

Your entries must follow the following formats:

- NAPTR records—NAPTR:abc.com
- SRV records—SRV:\_sip.\_tcp.abc.com
- A records—A:abc.com

### Example

```
ACMEPACKET# show dns stats
```

## show dnsalg rate

show dnsalg rate command

Displays the transaction rate of DNS ALG bound and sourced messages.

## show enum

### Syntax

```
show enum <arguments>
```

Displays ENUM statistics for your Oracle Communications Session Border Controller.

### Arguments

Each valid enum argument is listed below:

- all—Shows stats summary of all ENUM Agents
- cache-entry—Look in the ENUM cache for a specific entry
- h323d —Shows stats summary of all h323d ENUM Agents
- lookup—Query an ENUM cache for a specific E.164 number
- sipd —Shows stats summary of all sipd ENUM Agents
- stats—Show the statistics for the ENUM configuration
- status—Show the state of configured ENUM agents
- rate—Displays the transaction rate of ENUM messages

The following information may be displayed for each output:

- Enum Agent—Name of enum agents
- Queries Total—Number of enum queries
- Successful Total—Number of successful enum queries
- Not Found Total—Number of enum queries returning not found
- Timeout Total—Number of enum query timeouts

### Example

```
ACMEPACKET# show enum lookup
```

## show ext-band-mgr

### Syntax

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

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

### Example

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

## show ext-clf-svr

### Syntax

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

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

### Example

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

## show features

### Syntax

```
show features
```

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

### Example

```
ACMEPACKET# show features
```

## show h323d

### Syntax

```
show h323d <arguments>
```

This command displays H.323 statistics for your Oracle Communications Session Border Controller.

### Arguments

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

- Incoming Calls—Number of incoming H.323 calls; displayed for period, lifetime, and active counts
- Outgoing Calls—Number of outgoing H.323 calls; displayed for period, lifetime, and active counts
- Connected Calls—Number of currently connected H.323 calls; displayed for period, lifetime, and active counts
- Incoming Channels—Number of established incoming channels; displayed for period, lifetime, and active counts
- Outgoing Channels—Number of established outgoing channels; displayed for period, lifetime, and active counts
- Contexts—Number of established H.323 contexts; displayed for period, lifetime, and active counts
- Queued Messages—Number of messages queued; displayed for current and lifetime durations
- TPKT Channels—Number of TPKT channels open(ed); displayed for current and lifetime durations
- UDP Channels—Number of UDP channels open(ed); displayed for current and lifetime durations

config—Display the H.323 configuration

stacklist—Display the configured H.323 stacks

stackconfig <stack name> —Display detailed H.323 stack information about the stack-name you specify.

agentlist—Display H323 session agents

grouplist—Display H.323 session agent groups

agentconfig—Display H.323 session agents configuration. This command shows detailed information about the session agent specified by its IP address in the <hostname> argument.

groupconfig—Display H.323 session agent group configuration

**agentstats**—Display H.323 session agent statistics. By typing `show h323d agentstats <agent>`, you can view activity for the H.323 session agent that you specify.

**groupstats**—Display session information for session agent groups

**h323stats**—Display H.323 stacks and statistics on the Oracle Communications Session Border Controller. The display identifies the H.323 stack by its name and then provides the data for each H.323 stack. Adding a stackname `h323d h323stats <stack-name>` displays detailed statistics for the H.323 stack that you specify. This information is displayed according to the following categories: H.225, H.245, and RAS.

**registrations**—Display H.323 registration endpoints information

**sessions all**—Display all H.323 sessions currently on the system

**sessions by-agent <agent name>**—Display H.323 sessions for the session agent specified; adding `iwf` to the end of the command shows sessions for the IWF; adding `detail` to the end of the command expands the displayed information

**sessions by-callid <call ID>**—Display H.323 sessions for the call ID specified; adding `iwf` to the end of the command shows sessions for the IWF; adding `detail` to the end of the command expands the displayed information

**sessions by-ip <endpoint IP address>**—Display H.323 sessions for the specified IP address for an endpoint; adding `iw` to the end of the command shows sessions for the IWF; adding `detail` to the end of the command expands the displayed information

**sessions by-user <calling or called number>**—Display H.323 sessions for the specified user; adding `iw` to the end of the command shows sessions for the IWF; adding `detail` to the end of the command expands the displayed information

**stack-alarms**—Display a list of H.323 stacks that raised an alarm

**stackCallstats**—Show a summary of H.323 call statistics for all stacks

**stackPvtstats**—Show a summary of H.323 stack's internal data structures

**stackDisconnectInstats**—Show a summary of H.323 pvt statistics for all stacks

**tackDisconnectOutstats**— Show Summary of H.323 pvt statistics for all stacks

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

### Example

```
ACMEPACKET# show h323d status
```

## show health

### Syntax

```
show health
```

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

- Health score
- Current Oracle Communications Session Border Controller HA state as active, standby, or out of service
- If media flow information is synchronized for all supported protocols: SIP, H.323, and MGCP (true/false). If media flow information is not available, Media Synchronized disabled will be displayed in the `show health` output.
- If SIP signaling information is synchronized (true/false). If SIP signaling is not available, SIP Synchronized disabled will be displayed in the `show health` output.
- If MGCP signaling information is synchronized (true/false). If MGCP signaling is not available, MGCP Synchronized disabled will be displayed in the `show health` output.
- If configuration information is synchronized (true/false). If configuration checkpointing is not available, Config Synchronized disabled will be displayed in the `show health` output.
- IP address of the current HA Oracle Communications Session Border Controller's active peer (no peer is denoted with an IP address of 0.0.0.0)



- Last message received from the HA Oracle Communications Session Border Controller peer
- A switchover log containing the last 20 switchover events

### Example

```
ACMEPACKET# show health
```

## show hosts

### Syntax

```
show hosts
```

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

### Examples

```
ACMEPACKET# show hosts
```

## show imports

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

### Syntax

```
show imports
```

### Mode

Superuser

### Release

First appearance: S-C6.2.0

### Example

```
ACMEPACKET# show imports
```

## show interfaces

### Syntax

```
show interfaces [brief]
```

The show interfaces command shows all information concerning the Oracle Communications Session Border Controller's rear interfaces:

- Flags (such as loopback, broadcast, promiscuous, ARP, running, and debug)
- Type
- Internet address
- VLAN ID (if applicable)
- Broadcast address (if applicable)
- Netmask
- Subnet mask (if applicable)
- Gateway (if applicable)
- Ethernet (MAC) address (if applicable)
- Route metric
- Maximum transfer unit size

- Number of octets sent and received on this interface (if applicable)
- Number of packets sent and received on this interface
- Number of non-unicast packets sent and received on this interface (if applicable)
- Number of unicast packets sent and received on this interface (if applicable)
- Number of multicast packets sent and received on this interface (if applicable)
- Number of input discards (if applicable)
- Number of input unknown protocols (if applicable)
- Number of input and output errors
- Number of collisions
- Number of drops

This command also displays information for loopback interfaces.

### Arguments

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

### Example

```
ACMEPACKET# show interfaces
```

## show ip

### Syntax

```
show ip <arguments>
```

Displays IP statistics for your Oracle Communications Session Border Controller.

### Arguments

The following is a list of valid show ip arguments:

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

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

### Example

```
ACMEPACKET# show ip connections
```

## show logfile

### Syntax

```
show logfile [filename]
```

Display log files saved onto the Oracle Communications Session Border Controller. Entering this command without specifying a filename displays a complete list of log files.

### Arguments

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

### Example

```
ACMEPACKET# show logfile
```

## show loglevel

### Syntax

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

This command displays loglevel statistics for your Oracle Communications Session Border Controller.

### Arguments

**<task>** Enter the name of the Oracle Communications Session Border Controller task for which you are requesting information. By typing all, you are given an abbreviated display of all running processes.

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

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

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

### Example

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

## show lrt

### Syntax

```
show lrt <route-entry> | "stats"
```

This command displays Local Routing Table (LRT) statistics on the Oracle Communications Session Border Controller.

### Arguments

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

**<stats>** Display all LRT statistics

### Example

```
ACMEPACKET# show lrt stats
```

## show mbcd

### Syntax

```
show mbcd <arguments>
```

The show mbcd command displays MBCD statistics for your Oracle Communications Session Border Controller.

### Arguments

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

The following counts are given for Period (high and total) and Lifetime (Total, period-max, High) windows. Currently Active counts are also displayed.

- Client Sessions—Number of media sessions established by application clients of the MBCD task. Clients of MBCD include all signaling protocol tasks (SIP, MGCP, and H.323).
- Client Trans—Number of MBCD transactions in the application clients to create, modify and remove flows
- Contexts—Number of Contexts in the MBCD task. A Context represents the MBCD Server side of a media session. It contains all flows for the media session.
- Flows—Number of unidirectional flows established in MBCD. This includes both static flows defined by the signaling configuration, and dynamic flows for media sessions.
- Flow-Port—Number of "anchor" ports established by MBCD. MBCD maintains a mapping of the RTP steering port allocated for a flow so it can recognize flows that hairpin or spiral through the Oracle Communications Session Border Controller. This statistic reflects the number of entries in that table.
- Flow-NAT—Number of entries in the MBCD table that maps CAM entry indexes to flows. An entry is added to this table when a NAT entry is added to the CAM for a flow.
- Flow-RTCP—Number of special NAT table entries for RTCP. For Hosted NAT Traversal (HNT), the RTP and RTCP flows must be treated separately because the source port of the RTCP cannot be predicted.
- Flow-Hairpin—Number of hairpined/spiraled flows recognized by MBCD. This occurs when the signaling originates in an access realm, goes into a backbone realm, and then back into the same access realm, or another access realm on the same network interface.
- Flow-Released—Number of hairpined/spiraled flows released back into the original realm (when mm-in-realm or mm-in-network is disabled)
- MSM-Release—Number of flows that have been released as part of the SIP distributed (multi-system) release feature
- NAT Entries—Number of NAT table entries in the CAM established by MBCD for its flows. The NAT table can be viewed with the show nat commands.
- Free Ports—Number of ports available from configured steering pools
- Used Ports—Number of ports allocated to flows
- Port Sorts—Number of times the free ports list had to be sorted because consecutive ports (for RTP & RTCP) could not be found
- MBC Trans—Number of MBC transactions currently in progress
- MBC Ignored—Number of requests ignored because it is in standby mode in an HA configuration
- ARP Trans—Number of ARP Transactions. In some cases, MBCD must obtain the MAC address of the destination of a flow before an entry can be added to the NAT table. This statistic shows the number of outstanding ARP requests for MBCD flows.
- Relatch NAT
- Relatch RTCP
- MSM-SRTP-Passthrough
- SRTP Sessions

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

- Adds—Number of times an entry was added to the NAT table
- Deletes—Number of times an entry was removed from the NAT table
- Updates—Number of times a NAT table entry was updated, including updates due to the "latching" event when the first packet for a flow is received
- Non-Starts—Number of initial flow guard timeouts (i.e. number of times a packet was never received for a NAT table entry)
- Stops—Number of subsequent flow guard timeouts (i.e. number of times that packets stopped for a NAT table entry)
- Timeouts—Number of total session limit timeouts (i.e. number of times the session limit for a flow was exceeded)

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

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

- Static Blocked
- Dynamic Trusted
- Dynamic Blocked

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

- Add Requests
- Added
- Removed
- Dropped

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

- Client statistics count errors and events encountered by applications that use the MBCD to set up and tear down media sessions:
- Client Errors—Number of errors in the client application related to MBC transactions that are otherwise uncategorized
- Client IPC Errors—Number of errors in the client application related to the Inter-Process Communication
- No Session (Open)—Number of MBC transactions creating or updating a media session that could not be sent to MBCD because the media session state information could not be located
- No Session (Drop)—Number of MBC transactions deleting a media session that could not be sent to MBCD because the media session state information could not be located
- Exp Flow Events—Number of flow timer expiration notifications received from the MBCD by all applications
- Exp Flow Not Found—Number of flow timer expiration notifications received from the MBCD by all applications for which no media session or flow information was present in the application
- Transaction Timeouts—Number of MBC transaction timeouts

Server statistics count errors and events encountered by MBCD:

- Server Errors—Number of uncategorized errors in the MBC server
- Server IPC Errors—Number of errors on the server related to the IPC
- Flow Add Failed—Number of errors encountered when attempting to add an entry to the NAT table
- Flow Delete Failed—Number of errors encountered when attempting to remove an entry from the NAT table
- Flow Update Failed—Number of errors encountered when attempting to update an entry in the NAT table upon receipt of the first packet for a media flow
- Flow Latch Failed—Number of errors when attempting to locate an entry in the NAT table upon receipt of the first packet for a media flow
- Pending Flow Expired—Number of flow timer expirations for pending flows that have not been added to the NAT table
- ARP Wait Errors—Number of errors and timeouts related to obtaining the Layer 2 addressing information necessary for sending media
- Exp CAM Not Found—Number that the NAT table entry for an expired flow could not find in the NAT table. This usually occurs due to a race condition between the removal of the NAT entry and the flow timer expiration notification being sent to MBCD.
- Drop Unknown Exp Flow—Number of flows deleted by the MBCD because of a negative response from the application to a flow timer expiration notification
- Unk Exp Flow Missing—Number of negative responses from the application to a flow timer expiration notification for which the designated flow could not be found in MBCD's tables
- Exp Notify Failed—Number of errors encountered when the MBCD attempted to send a flow timer expiration notification to the application
- Unacknowledged Notify—Number of flow expiration notification messages sent from MBCD to the application for which MBCD did not receive a response in a timely manner
- No Ports Available—Number of steering port allocation requests not be satisfied due to a lack of free steering ports in the realm
- Invalid Realm—Number of flow setup failures due to an unknown realm in the request from the application

- Insufficient Bandwidth—Number of flow setup failures due to insufficient bandwidth in the ingress or egress realm
- Open Streams Failed—Number of MBC transactions creating or updating a media session that could not be sent to the MBCD because the media session state information could not be located
- Drop Streams Failed—Number of MBC transactions deleting a media session that could not be sent to MBCD because the media session state information could not be located
- Drop/Exp Flow Missing—Number of negative responses from the application to a flow timer expiration notification for which the designated flow could not be found in MBCD's tables
- Stale Ports Reclaimed—For an HA node, this is the number of ports that were reclaimed when the standby had a stale flow that the active system replaced; when the flow is replaced, the steering ports are also reallocated properly (i.e., according to the active system)
- Stale Flows Replaced—For an HA node, this is the number of times that the standby system had entries in its flow tables that did not match those on the active system; the active system replaced the standby's stale flows with valid ones
- Pipe Alloc Errors—For communication between the Oracle Communications Session Border Controller's tasks (sipd, h323d, and algd) and middlebox control protocol tasks, this is the number of times that buffer allocation failed
- Pipe Write Errors—For communication between the Oracle Communications Session Border Controller's tasks (sipd, h323d, and algd) and middlebox control protocol tasks, this is the number of times that messages were not sent (possibly because of a pipe/buffer allocation error)

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

- Add incoming statistics when an add message is received by the Oracle Communications Session Border Controller
  - Incoming requests received—Number of mbc add commands received
  - Incoming replies sent—Number of responses sent in response to an mbc add
  - Incoming errors sent—Number of errors sent in response to an mbc add
- Add outgoing statistics when an mbc add message is sent by the Oracle Communications Session Border Controller:
- Outgoing requests sent—Number of MBCD add commands sent from the Oracle Communications Session Border Controller
  - Outgoing replies received—Number of responses received in response to a sent Add message
  - Outgoing errors received—Number of errors received in response to a sent Add message

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

- Add incoming statistics when a modify message is received by the Oracle Communications Session Border Controller:
  - Incoming requests received—Number of mbc modify commands received
  - Incoming replies sent—Number of responses sent in response to an mbc modify
  - Incoming errors sent—Number of errors sent in response to an mbc modify
- Add outgoing statistics when an mbc modify message is sent by the Oracle Communications Session Border Controller:
- Outgoing requests sent—Number of MBCD modify commands sent from the Oracle Communications Session Border Controller
  - Outgoing replies received—Number of responses received in response to a sent modify message
  - Outgoing errors received—Number of errors received in response to a sent modify message

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

- Add incoming statistics when a subtract message is received by the Oracle Communications Session Border Controller:

- Incoming requests received—Number of mbcd subtract commands received
- Incoming replies sent—Number of responses sent in response to an mbcd subtract
- Incoming errors sent—Number of errors sent in response to an mbcd subtract

Add outgoing statistics when an MBCD subtract message is sent by the Oracle Communications Session Border Controller:

- Outgoing requests sent—Number of MBCD subtract commands sent from the Oracle Communications Session Border Controller
- Outgoing replies received—Number of responses received in response to a sent subtract message
- Outgoing errors received—Number of errors received in response to a sent subtract message

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

- Add incoming statistics when a notify message is received by the Oracle Communications Session Border Controller:
- Incoming requests received—Number of mbcd notify commands received
- Incoming replies sent—Number of responses sent in response to an mbcd notify
- Incoming errors sent—Number of errors sent in response to an mbcd notify

Add outgoing statistics when an mbcd notify message is sent by the Oracle Communications Session Border Controller:

- Outgoing requests sent—Number of MBCD notify commands sent from the Oracle Communications Session Border Controller
- Outgoing replies received—Number of responses received in response to a sent notify message
- Outgoing errors received—Number of errors received in response to a sent notify message

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

- Add incoming statistics when a customer-specific message is received by the Oracle Communications Session Border Controller:
- Incoming requests received—Number of customer-specific mbcd commands received
- Incoming replies sent—Number of responses sent in response to a customer-specific mbcd command
- Incoming errors sent—Number of errors sent in response to a customer-specific mbcd command

Add outgoing statistics when a customer-specific mbcd message is sent by the Oracle Communications Session Border Controller:

- Outgoing requests sent—Number of MBCD notify commands sent from the Oracle Communications Session Border Controller
- Outgoing replies received—Number of responses received in response to a customer-specific message
- Outgoing errors received—Number of errors received in response to a sent customer-specific message

realms—Display steering ports and bandwidth usage for home, public, and private realms. The following is a list of statistics displayed when you enter this command:

- Used—Number of steering ports used
- Free—Number of free steering ports
- No Ports—Number of times that a steering port could not be allocated
- Flows—Number of established media flows
- Ingress—Amount of bandwidth being used for inbound flows
- Egress—Amount of bandwidth being used for outbound flows
- Total—Maximum bandwidth set for this realm
- Insuf BW—Number of times that a session was rejected due to insufficient bandwidth

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

- Ports Used—Number of ports used

- Free Ports—Number of free ports
- No Ports Avail—Number of times no steering ports were available
- Ingress Band—Amount of bandwidth used for inbound flows
- Egress Band—Amount of bandwidth used for outbound flows
- BW Allocations—Number of times that bandwidth was allocated
- Band Not Avail—Number of times a session was rejected due to insufficient bandwidth

redundancy —Display the equivalent of the show redundancy mbed command

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

- MBC status
- NAT entries
- MBC errors
- MBC messages including: add, modify, subtract, notify, and other

stun—Display STUN server statistics

- Servers—The number of STUN servers (the same as the number of realms configured with a STUN server).
- Server Ports—Number of ports per STUN server; there will be four ports per STUN server.
- Binding Requests—Number of STUN Binding Request messages received by all STUN servers.
- Binding Responses—Number of STUN Binding Response messages sent by all STUN servers.
- Binding Errors—Number of STUN Binding Error messages sent by all STUN servers.
- Messages Dropped—Number of messages dropped by all STUN servers.

### Example

```
ACMEPACKET# show mbed errors
```

## show media

### Syntax

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

### Arguments

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

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

<slot>— Select the media interface slot

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

<port> —Select the media interface port



- Values 0 (leftmost) | 1 | 2 | 3 (rightmost)

<vlan> Enter the VLAN ID if required

### Example

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

## show memory

### Syntax

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

This command displays statistics related to the memory of your Oracle Communications Session Border Controller.

### Arguments

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

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

### Example

```
ACMEPACKET# show memory application
```

## show mgcp

### Syntax

```
show mgcp <type>
```

This command displays MGCP statistics on the Oracle Communications Session Border Controller.

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

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

### Example

```
ACMEPACKET# show mgcp ntfy
```

### show monthly-minutes

#### Syntax

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

Display the monthly minutes for a specified realm.

#### Arguments

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

#### Example

```
ACMEPACKET# show monthly-minutes realm1
```

### show msrp statistics

show msrp statistics command.

Displays cumulative MSRP session counts.

### show nat

#### Syntax

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

Displays NAT statistics for a specified NAT time on the Oracle Communications Session Border Controller.

#### Arguments

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

**by-index** —Display a specified range of entries in the NAT table, with a maximum of 5024 entries. The default range is 1 through 200. The range corresponds to line numbers in the table, and not to the number of the entry itself. The syntax for using the show nat by-index command is:

```
show nat by-index <starting entry> <ending entry>
```

**in-tabular** —Display a specified range of entries in the NAT table display in table form, maximum of 5024 entries. The syntax is modeled on the show nat by-index command:

```
show nat in-tabular <starting entry> <ending entry>
```

**by-addr**—Display NAT table information matching source and destination addresses. You must specify source address (SA) and/or destination address (DA) values. If no addresses are entered, the Oracle Communications Session Border Controller shows all of the table entries. NAT entries can be matched according to SA or DA or both.

```
show nat by-addr <source IPv4 address> <destination IPv4 address>
```

**info**—Display general NAT table information. The output is used for quick viewing of a Oracle Communications Session Border Controller's overall NAT functions, including the maximum number of NAT table entries, the number of used NAT table entries, the length of the NAT table search key, the first searchable NAT table entry address, the length of the data entry, the first data entry address, and whether or not aging and policing are enabled in the NAT table.

**flow-info**—Display NAT table entry debug information. You must specify if you want to view NAT data for all entries or if you want to specify an address or a switch ID.

```
show nat flow-info [by-addr | srtp]
```

#### Example

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

## show net-management-control

### Syntax

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

This command displays network management control statistics on the Oracle Communications Session Border Controller.

### Arguments

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

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

### Example

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

## show nsep-stats

### Syntax

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

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

### Arguments

<all> Display information about inbound sessions and r-values for the Oracle Communications Session Border Controller's NSEP support feature. This is an optional argument.

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

### Mode

User, Superuser

### Release

First appearance: 5.1

## show ntp

### Syntax

```
show ntp <arguments>
```

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

### Arguments

servers—Display information about the quality of the time being used in terms of offset and delay measurement; maximum error bounds are also displayed.

status—Display information about configuration status, NTP daemon synchronization, NTP synchronizations in process, if NTP is down.

### Mode

User, Superuser

### Release

First appearance: 5.1

### Example

```
ACMEPACKET# show ntp servers
```

## show packet-trace

### Syntax

```
show packet-trace
```

The show packet-trace command allows you to check whether the Oracle Communications Session Border Controller's tracing status is currently enabled or disabled.

### Mode

Superuser

### Release

First appearance: 5.0

### Example

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

## show policy-server

The show policy server command allows you to view specific information about a supplied policy server object.

### Syntax

```
show policy-server [standby] <policy server name>
```

## show power

The show power command allows you to view Oracle Communications Session Border Controller power supply information including the state of the power supply and the installation position.

### Example

```
ACMEPACKET# show power
```

## show privilege

### Syntax

```
show privilege
```

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

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

## Example

```
ACMEPACKET# show privilege
```

## show processes

### Syntax

```
show processes <process>
```

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

### Arguments

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

- sysmand—Display sysmand process statistics related to the system's startup tasks
- acliSSH0—Show acliSSH0 process statistics
- acliSSH1—Show acliSSH1 process statistics
- acliSSH2—Show acliSSH2 process statistics
- acliSSH3—Show acliSSH3 process statistics
- acliSSH4—Show acliSSH4 process statistics
- acliTelnet0—Show acliTelnet0 process statistics
- acliTelnet1—Show acliTelnet1 process statistics
- acliTelnet2—Show acliTelnet2 process statistics
- acliTelnet3—Show acliTelnet3 process statistics
- acliTelnet4—Show acliTelnet4 process statistics
- ebmd—Show ebmd process statistics
- h323d—Show h323d process statistics
- lid—Show lid process statistics
- pusher—Show pusher process statistics
- snmpd—Show snmpd process statistics
- cliworker—Show CliWorker process statistics
- berpd—Display statistics for the border element redundancy protocol tasks; only accessible if your system is operating in an HA node
- lemd—Display lemd process statistics
- brokerd—Display brokerd process statistics
- mbcd—Display mbcd process statistics related to the middlebox control daemon
- radd—Display radd process statistics related to RADIUS; only accessible if your Oracle Communications Session Border Controller is using RADIUS
- algd—Display algd process statistics
- sipd—Display sipd process statistics
- acliConsole—Display acliConsole process statistics

current—Show the date and time that the current monitoring period began and statistics for the current application process events. The following fields explain the output of the show processes current command:

- Svcs—Number of times the process performs actions for different services (e.g., sockets, timeout queues, etc.)
- TOQ—Number of active timers (in the Timed Objects) placed in the timeout queue
- Ops—Number of times the process was prompted (or polled) to perform an action
- Rcvd—Number of messages received by the process
- Sent—Number of messages sent by the process
- Events—Number of times a TOQ entry timed out
- Alrm—Number of alarms the process sent

- Slog—Number of times the process wrote to the system log
- Plog—Number of times the process wrote to the process log
- CPU—Average CPU usage over the last minute
- Now—CPU usage for the last second

total —Display the total statistics for all of the application processes applicable to your Oracle Communications Session Border Controller. The following fields explain the output of the show processes total command:

- Svcs—Number of times the process performed actions for different services (e.g., sockets, timeout queues, etc.)
- Rcvd—Number of messages received by the process
- Sent—Number of messages sent by the process
- Events—Number of times a TOQ entry timed out
- Alarm—Number of alarms the process sent
- Slog—Number of times the process wrote to the system log
- Plog—Number of times the process wrote to the process log
- CPU—Average CPU usage since last reboot
- Max—Maximum percentage of CPU usage in a 60 second period

collect—Show collector process statistics

CPU —Display information about the CPU usage for your Oracle Communications Session Border Controller, categorized on a per task/process basis. The following fields explain the output of the show processes cpu command:

- Task Name—Name of the Oracle Communications Session Border Controller task or process
- Task Id—Identification number for the task or process
- Pri—Priority for the CPU usage
- Status—Status of the CPU usage
- Total CPU—Total CPU usage since last reboot in hours, minutes, and seconds
- Avg—Displays percentage of CPU usage since the Oracle Communications Session Border Controller was last rebooted
- Now—CPU usage in the last second

all — concatenate the show process command for all running procoesses

memory—Show memory process statistics

### Example

```
ACMEPACKET# show processes sysmand
```

## show prom-info

### Syntax

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

The show prom-info command displays hard-coded information about Oracle Communications Session Border Controller (PROM) information. Valid devices to query are dependent on the platform.

### Arguments

<devices> The following is a list of available prom-info devices to query:

- mainboard—Display mainboard PROM information
- CPU—Display CPU PROM information
- PHY—Display left physical interface card PROM information
- all—Show all above PROM information

### Example

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

## show qos

### Syntax

```
show qos <argument>
```

The show qos command displays information about the Oracle Communications Session Border Controller's QoS FPGA.

### Arguments

history— Display the QoS history for an FPGA entry

revision— Display the QoS FPGA hardware revision

usage— Display the current QoS FPGA usage

### Example

```
ACMEPACKET# show qos usage
```

## show radius

### Syntax

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

This command displays RADIUS statistics.

### Arguments

authentication—Show the authentication statistics

all—Show both accounting and authentication statistics

cdr—Display all CDR statistics

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

The command's output is divided into three sections:

1. Client Display—Display general accounting setup (as established in the account-config element); includes the following information:
  - state of the RADIUS client
  - accounting strategy
  - IP address and port on which the Oracle Communications Session Border Controllers server is listening
  - maximum message delay in seconds
  - number of configured accounting servers
2. Waiting Queue—Display the number of accounting (RADIUS) messages waiting to be sent that are queued on the client side
3. <IP Address:Port>—IP Address and port headings indicated will be per the referenced RADIUS server active on the IP Address and port shown; also includes information about the accounting server's state

### Example

```
ACMEPACKET# show radius authentication
```

### show ramdrv

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

#### Example

```
ACMEPACKET# show ramdrv
```

### show realm

#### Syntax

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

#### Arguments

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

#### Example

```
ACMEPACKET# show realm realm1
```

### show redundancy

#### Syntax

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

The show redundancy command displays HA statistics for a redundant Oracle Communications Session Border Controller.

#### Arguments

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

mbcd—Display the synchronization of media flows for the members of an HA Oracle Communications Session Border Controller pair

algd—Display the synchronization of MGCP signaling for the members of an HA Oracle Communications Session Border Controller pair

sipd—Display the synchronization of SIP signaling for the members of an HA Oracle Communications Session Border Controller pair

config—Display the synchronization of configuration information for the members of an HA Oracle Communications Session Border Controller pair

collect—Display the Collect redundancy statistics

link—Display the Link redundancy statistics

radius-cdr—Display the number of CDRs that have been synchronized from active to standby when the local CDR storage is enabled

iked—Display IKE redundancy statistics

manuald—Display manual redundancy statistics

rotated-cdr—Display statistics for rotated CDRs on the Oracle Communications Session Border Controller . The following HA statistics are shown for the Period and Lifetime monitoring spans.



- Queued entries—Number of transactions not yet sent to standby Oracle Communications Session Border Controller peer
- Red Records—Total number of HA transactions created
- Records Dropped—Number of HA transaction records lost because the standby Oracle Communications Session Border Controller fell behind in synchronization
- Server Trans—Number of HA transactions in which the Oracle Communications Session Border Controller acted as the server
- Client Trans—Number of HA transactions where the Oracle Communications Session Border Controller was the client

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

- Requests received—Number of HA requests received by the Oracle Communications Session Border Controller, acting as server
- Duplicate requests—Number of situations in which an HA request was received by the Oracle Communications Session Border Controller, and (acting as the server side in the client-server relationship) the Oracle Communications Session Border Controller responded to it, but the client system did not receive the response in time and retransmitted its original request
- Success responses—Number of HA requests that were received followed by a successful response to the client
- Error responses—Number of HA requests that were received followed by a error response to the client
- Request sent—Number of HA requests that were sent by the standby Oracle Communications Session Border Controller
- Retransmission sent—Number of times an HA request was retransmitted after no response
- Success received—Number of HA requests receiving a reply from the other Oracle Communications Session Border Controller in an HA pair
- Errors received—Number of errors received in response to HA requests
- Transaction timeouts—Number of HA transactions that timed out

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

### Example

```
ACMEPACKET# show redundancy sipd
```

## show registration

### Syntax

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

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

### Arguments

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

- sipd
- mgcp
- h323

by-user <user> — Show registration information for a specific IP address of an endpoint, or a wildcarded IP address value with an asterisk (\*) at the end.

by-realm <realm> — Display information for calls that have registered through a specified ingress realm whose registration cache information you want to view. The realm value can be wildcarded.

by-registrar <registrar> —Display information for calls that use a specific registrar. Add the IP address of the registrar whose registration cache information you want to view. This value can be wildcarded.

**by-route <IP address>** — Display information for calls by their Internet-routable IP address. This allows you to view the endpoints associated with public addresses. Enter the IP address whose registration cache information you want to view. This value can be wildcarded.

**by-endpoint <IP address>** — Show registration information for a specific phone number or username. Provide the IP address of an endpoint, or a wildcarded IP address value with an asterisk (\*) at the end. This command is only available if you configure the `reg-via-key` parameter in the SIP interface configuration prior to endpoint registration. The `reg-via-key` parameter keys all registered endpoints by IP address and username.

**Phone number or username**—Full phone number or username, or a wildcarded number/username with an asterisk (\*). The display shows statistics for the Period and Lifetime monitoring spans.

- **user Entries**—The number of unique SIP Addresses of Record in the cache
- **Local Contacts**—The number of contact entries in the cache
- **Free Map Ports**—The number of ports available in the free signaling port pool
- **Used Map Ports**—The number of signaling ports allocated for registration cache entries
- **Forwards**—Number of registration requests forwarded to the real registrar
- **Refreshes**—Number of registrations the Oracle Communications Session Border Controller answered without having to forward registrations to the real registrar
- **Rejects**—Number of unsuccessful registrations sent to real registrar
- **Timeouts**—Number of times a refresh from the HNT endpoint was not received before the timeout
- **Fwd Postponed**—The number of times sipd responded out of the cache instead of forwarding to the registrar due to the `max-register-forward` threshold
- **Fwd Rejected**—The number of REGISTER 503s done after checking for a cached entry
- **Refr Extension**—The number of times the `max-register-refresh` threshold was exceeded. The "Active" and "High" show the number of seconds added to the expiration
- **Refresh Extended**—The number of times the expire time in a REGISTER response was extended due to the `max-register-refresh` threshold
- **Surrogate Regs**— The total number of surrogate registers
- **Surrogate Sent**— The total number of surrogate registers sent
- **Surrogate Reject**—The total number of surrogate register rejects
- **Surrogate Timeout**— The total number of surrogate register timeouts

**statistics**— Display a table of counters showing the total and periodic number of registrations, by protocol. This argument applies to the Acme Packet 3800 only.

### Example

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

## show route-stats

### Syntax

```
show route-stats
```

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

### Example

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

## show routes

### Syntax

```
show routes
```

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

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

### Example

```
ACMEPACKET# show routes
```

## show running-config

### Syntax

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

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

### Arguments

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

<configuration-element> — Specify the configuration element you want to view. This is an optional argument. If you do not specify a configuration element, the Oracle Communications Session Border Controller displays the entire configuration.

### Example

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

## show sa

### Syntax

```
show sa
```

or

```
show sa stats
```

This command displays the security associations information for IMS-AKA. The srtp option is not available for the ETC NIU.

### Example

```
ACMEPACKET# show sa stats
```

## show security

### Syntax

```
show security <argument>
```

This command displays configured security information on the Oracle Communications Session Border Controller

### Arguments

**certificates <argument>** — Show certificate information on the Oracle Communications Session Border Controller.

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

**ike <arguments>** — Displays statistics for IKE transactions

- **data-flow**—Display data-flow information for IKE2
- **local-address-pool <pool ID | brief>** —Display local address pool information for IKE2
  - **pool ID**—Display a specific local address pool in detail
  - **brief**—Display all local address pools briefly

**ipsec <arguments>** — Show IPSEC related information on the Oracle Communications Session Border Controller. You can specify the name of the network interface whose IPSEC information you want to view.

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

**srtp <arguments>** — Show SRTP related information.

- **sad**—security-association database entries (Only the brief option is valid for ETC NIU)
- **sessions**—number of active SRTP sessions (not valid for ETC NIU)
- **spd**—security-policy database entries
- **statistics**—interface and SA entry statistics (not valid for ETC NIU)
- **status**—display interface IPSEC status (not valid for ETC NIU)
- **check-mini-cert <sipuraProfileName>**—reads the XML file corresponding to the given sipura profile from /code/sipura/ directory of the SBC, then parses and checks the validity of the Sipura mini-certificate present in the file by verifying the signature and the expiration date of the certificate. It outputs if the mini-certificate is verified successfully or not
- **display-mini-cert <sipuraProfileName>**—reads the file corresponding to the given sipura profile from /code/sipura directory of the SBC, then parses the file and decodes the base-64 encoded information. It outputs the information present in the mini-certificate in text format. This includes the user name, user ID, expiration date, public key and the signature.
- **update-mini-cert <sipuraProfileName>**—If a user wishes to change the content of a certificate file (thus the minicertificate and keys) and would like the SBC to use this updated certificate and keys during call setup, then the user can accomplish this by first changing the content of the file and then executing this ACLI command specifying the Sipura profile that uses this file. This command when executed will attempt to read the file that is configured in the given Sipura profile and then will parse the file and update the minicertificate and keys that is used for this sipura profile. This command assumes that the file is present in /code/sipura directory and the user has not changed the file name configured in the Sipura profile.

**ssm-accelerator** — Display the SSM status on the Oracle Communications Session Border Controller

**tls <argument>** Display TLS related information

- **session-cache**—Display TLS session cache information

ssh-pub-key <arguments> — Displays public key record information including login name, fingerprint, fingerprint raw, comment (detailed view only), and public key (detailed view only).

- brief—View a brief display
- detail—View a detailed displayfips Displays FIPS status. This command is only available with an appropriate license.

### Example

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

## show sessions

### Syntax

```
show sessions
```

Displays session capacity for license and session use.

The following statistics are available in a table for Period and Lifetime monitoring spans:

- Total Sessions—The aggregation of all current active subscriber sessions (H.323 call/SIP session/MGCP connection) and is the total session count against the capacity license.
- SIP Sessions—The total current active SIP sessions
- H.323 Calls—The total current active H.323 calls
- MGCP Connections—The total current active MGCP connections

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

- H.323 to SIP Calls—The calls that come in H.323 and go out SIP. These calls are included in “H.323 Calls” in the Session Statistics.
- SIP to H.323 Calls—The calls that come in SIP and go out H.323. These calls are included in “SIP Sessions” in the Session Statistics.

Total session capacity of the system list listed from this command.

### Example

```
ACMEPACKET# show sessions
```

## show sipd

### Syntax

```
show sipd <arguments>
```

The show sipd command displays SIP statistics on your Oracle Communications Session Border Controller.

### Arguments

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

- Dialogs—Number of end-to-end SIP signaling connections
- CallID Map—Total number of successful session header Call ID mappings
- Sessions—Number of sessions established by an INVITE
- Subscriptions—Number of sessions established by SUBSCRIPTION
- Rejections—Number of rejected INVITEs
- ReINVITEs—Number of ReINVITEs

- Media Sessions—Number of successful media sessions
- Media Pending—Number of media sessions waiting to be established
- Client Trans—Number of client transactions
- Server Trans—Number of server transactions that have taken place on the Oracle Communications Session Border Controller
- Resp Contexts—Number of current response contexts
- Saved Contexts—Total number of saved contexts
- Sockets—Number of active SIP sockets
- Req Dropped—Number of requests dropped
- DNS Trans—Number of DNS transactions
- DNS Sockets—Number of DNS Sockets
- DNS Results—Number of dns results
- Session Rate—The rate, per second, of SIP invites allowed to or from the Oracle Communications Session Border Controller during the sliding window period. The rate is computed every 10 seconds
- Load Rate—Average Central Processing Unit (CPU) utilization of the Oracle Communications Session Border Controller during the current window. The average is computed every 10 seconds unless the load-limit is configured in the SIPConfig record, in which case it is 5 seconds

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

- SDP Offer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Offer in the Offer/Answer model (RFC 3264)
- SDP Answer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Answer in the Offer/Answer model (RFC 3264)
- Drop Media Errors—Number of errors encountered in tearing down the media for a dialog or session that is being terminated due to: a) non-successful response to an INVITE transaction; or b) a BYE transaction received from one of the participants in a dialog/session; or c) a BYE initiated by the Acme Packet SBC due to a timeout notification from MBCD
- Transaction Errors—Number of errors in continuing the processing of the SIP client transaction associated with setting up or tearing down of the media session
- Missing Dialog—Number of requests received by the SIP application for which a matching dialog count not be found
- Application Errors—Number of miscellaneous errors in the SIP application that are otherwise uncategorized
- Media Exp Events—Flow timer expiration notifications received from MBCD
- Early Media Exps—Flow timer expiration notifications received for media sessions that have not been completely set up due to an incomplete or pending INVITE transaction
- Exp Media Drops—Number of flow timer expiration notifications from the MBCD that resulted in the termination of the dialog/session by the SIP application
- Multiple OK Drops—Number of dialogs terminated upon reception of a 200 OK response from multiple UASs for a given INVITE transaction that was forked by a downstream proxy
- Multiple OK Terms—Number of dialogs terminated upon reception of a 200 OK response that conflicts with an existing established dialog on the Oracle Communications Session Border Controller
- Media Failure Drops—Number of dialogs terminated due to a failure in establishing the media session
- Non-ACK 2xx Drops— Number of sessions terminated because an ACK was not received for a 2xx response
- Invalid Requests— Number of invalid requests; an unsupported header for example
- Invalid Responses—Number of invalid responses; no Via header for example
- Invalid Messages—Number of messages dropped due to parse failure
- CAC Session Drop—Number of call admission control session setup failures due to user session count exceeded
- Expired Sessions—Number of sessions terminated due to the session timer expiring
- CAC BW Drop—Number of call admission control session setup failures due to insufficient bandwidth

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

- Recent—Number of errors occurring in the number of seconds listed after the time stamp
- Total—Number of errors occurring since last reboot
- PerMax—Identifies the highest individual Period Total over the lifetime of the monitoring

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

- Local Policy Lookups— Number of Local policy lookups
- Local Policy Hits— Number of successful local policy lookups
- Local Policy Misses— Number of local policy lookup failures
- Local Policy Drops— Number of local policy lookups where the next hop session agent group is H323
- Agent Group Hits— Number of successful local policy lookups for session agent groups
- Agent Group Misses— Number of successful local policy lookups where no session agent was available for session agent group
- No Routes Found— Number of successful local policy lookups but temporarily unable to route; session agent out of service for instance
- Missing Dialog— Number of local policy lookups where the dialog not found, for a request addressed to the Oracle Communications Session Border Controller with a To tag or for a NOTIFY-SUBSCRIBE sip request
- Inb SA Constraints— Number of successful local policy lookups where inbound session agent exceeded constraints
- Outb SA Constraints— Number of successful outbound local policy lookups where session agent exceeded constraints
- Inb Reg SA Constraints— Number of successful inbound local policy lookups where registrar exceeded constraints
- Out Reg SA Constraints— Number of successful outbound local policy lookups where registrar exceeded constraints
- Requests Challenged— Number of requests challenged
- Challenge Found— Number of challenges found
- Challenge Not Found— Number of challenges not found
- Challenge Dropped— Number of challenges dropped

server—Display statistics for SIP server events when the Oracle Communications Session Border Controller is acting as a SIP server in its B2BUA role. Period and Lifetime monitoring spans for SIP server transactions are given.

- All States—Number of all server transactions
- Initial—Number of times the “initial” state was entered after a request was received
- Queued—Number of times the “queued” state is entered because resources are temporarily unavailable
- Trying—Number of times the “trying” state was entered due to the receipt of a request
- Proceeding—Number of times a server transaction has been constructed for a request
- Cancelled—Number of INVITE transactions that received a CANCEL
- Established—Number of times the server sent a 2xx response to an INVITE
- Completed—Number of times the server received a 300 to 699 status code and entered the “completed” state
- Confirmed—Number of times that an ACK was received while the server was in “completed” state and transitioned to “confirmed” state
- Terminated—Number of times that the server received a 2xx response or never received an ACK in the “completed” state, and transitioned to the “terminated” state

client —Display statistics for SIP client events when the Oracle Communications Session Border Controller is acting as a SIP client in its B2BUA role. Period and Lifetime monitoring spans are displayed.

- All States—Number of all client transactions
- Initial—State when initial server transaction is created before a request is sent
- Trying—Number of times the “trying” state was entered due to the sending of a request
- Calling—Number of times that the “calling” state was entered due to the receipt of an INVITE request
- Proceeding—Number of times that the “proceeding” state was entered due to the receipt of a provisional response while in the “calling” state

- Early Media—Number of times that the “proceeding” state was entered due to the receipt of a provisional response that contained SDP while in the “calling” state
- Completed—Number of times that the “completed” state was entered due to the receipt of a status code in the range of 300-699 when either in the “calling” or “proceeding” state
- SetMedia—Number of transactions in which the Oracle Communications Session Border Controller is setting up NAT and steering ports
- Established—Number of situations when client receives a 2xx response to an INVITE, but cannot forward it because it NAT and steering port information is missing
- Terminated—Number of times the “terminated” state was entered after a 2xx message

acls—Display ACL information for Period and Lifetime monitoring spans

- Total entries—Total ACL Entries, including both trusted and blocked
- Trusted—Number of trusted ACL entries
- Blocked—Number of blocked ACL entries

Lifetime monitoring span is displayed for SIP ACL Operations.

- ACL Requests—Number of ACL requests
- Bad Messages —Number of bad messages
- Promotions—Number of ACL entry promotions
- Demotions—Number of ACL entry demotions
- Trust->Untrust—Number of ACL entries demoted from trusted to untrusted
- Untrust->Deny—Number of acl entries demoted from untrusted to deny

sessions—Display the number of sessions and dialogs in various states for the Period and Lifetime monitoring spans, in addition to the current Active count:

- Sessions—Identical to the identically named statistic on the show sipd status command
- Initial—Displays sessions for which an INVITE or SUBSCRIBE is being forwarded
- Early—Displays sessions for which the first provisional response (1xx other than 100) is received
- Established—Displays sessions for which a success (2xx) response is received
- Terminated—Displays sessions for which the session is ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or “Early” session. The session will remain in the “Terminated” state until all the resources for the session are freed.
- Dialogs—Identical to the identically named statistic on the show sipd status command
- Early—Displays dialogs that were created by a provisional response
- Confirmed—Displays dialogs that were created by a success response. An “Early” dialog will transition to “Confirmed” when a success response is received
- Terminated—Displays dialogs that were ended by receiving/sending a BYE for an “Established” session or receiving/sending error response “Early” dialog. The dialog will remain in the “Terminated” state until all the resources for the session are freed.

sessions all—Display all SIP sessions currently on the system

sessions by-agent <agent name>—Display SIP sessions for the session agent specified; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-ip <endpoint IP address>—Display SIP sessions for the specified IP address for an endpoint; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-user <calling or called number>—Display SIP sessions for the specified user; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-callid <call ID>—Display SIP sessions for the specified call ID; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

redundancy— Display sipd redundancy statistics. Executing the show sipd redundancy command is the equivalent to the show redundancy sipd command.



**agents [hostname][method][-t]** —Display statistics related to defined SIP session agents. Entering this command without any arguments list all SIP session agents. By adding the IP address or hostname of a session agent as well as a specified method at the end of the command, you can display statistics for that specific session agent and method. For a specific session agent, identified by IP address, the **show sipd agents** command lists:

- session agent state
  - D—disabled
  - I—in-service
  - O—out-of-service
  - S—transitioning from out-of-service to in-service
- inbound and outbound statistics
- average and maximum latency for each session agent
- maximum burst rate for each session agent as total number of session invitations sent to or received from the session agent within the amount of time configured in the burst-rate-window field

Inbound Statistics:

- Active—Number of active sessions sent to each session agent listed
- Rate—Average rate of session invitations (per second) sent to each session agent listed
- ConEx—Number of times the constraints have been exceeded

Outbound Statistics:

- Active—Number of active sessions sent from each session agent
- Rate—Average rate of session invitations (per second) sent from each session agent listed
- ConEx—Number of times the constraints have been exceeded

Latency:

- Avg—Average latency for packets traveling to and from each session agent
- Max—Maximum latency for packets traveling to and from each session agent listed

**-t**— Append to the end of the command to specify the current time period for the max-burst value.

**interface [interface-id][method]**—Display SIP interface statistics. By adding the optional interface-id and method arguments you can narrow the display to view just the interface and method you want to view.

**ip-cac <IP address>**—Display CAC parameters for an IP address

**publish**—Display statistics related to incoming SIP PUBLISH messages

**agent <agent>** —Display activity for the session agent that you specify

- Inbound Sessions:
  - Rate Exceeded—Number of times session or burst rate was exceeded for inbound sessions
- Num Exceeded—Number of times time constraints were exceeded for inbound sessions

Outbound Sessions:

- Rate Exceeded—Number of times session or burst rate was exceeded for outbound sessions
- Num Exceeded—Number of times time constraints were exceeded for inbound sessions
- Burst—Number of times burst rate was exceeded for this session agent
- Out of Service—Number of times this session agent went out of service
- Trans Timeout—Number of transactions timed out for this session agent
- Requests Sent—Number of requests sent via this session agent
- Requests Complete—Number of requests that have been completed for this session agent
- Messages Received—Number of messages received by this session agent

**realm**—Display realm statistics related to SIP processing

**routers**—Display status of Oracle Communications Session Border Controllerconnections for session router functionality

directors—Display the status of Oracle Communications Session Border Controller connections for session director functionality

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

- INVITE—Display the number of SIP transactions including an INVITE method
- REGISTER—Display the number of SIP transactions including a REGISTER method
- OPTIONS—Display the number of SIP transactions including an OPTIONS method
- CANCEL—Display the number of SIP transactions including a CANCEL method
- BYE—Display the number of SIP transactions including a BYE method
- ACK—Display the number of SIP transactions including an ACK method
- INFO—Display the number of SIP transactions including an INFO method
- PRACK—Display the number of SIP transactions including a PRACK method
- SUBSCRIBE—Display the number of SIP transactions including a SUBSCRIBE method
- NOTIFY—Display the number of SIP transactions including a NOTIFY method
- REFER—Display the number of SIP transactions including a REFER method
- UPDATE—Display the number of SIP transactions including an UPDATE method
- other—Display the number of SIP transactions including non-compliant methods and protocols used by specific customers

The following lists information displayed for each individual SIP message statistic. Some or all of the following messages/events may appear in the output from a show sipd command.

- INVITE Requests—Number of times method has been received or sent
- Retransmissions—Information regarding sipd message command requests received by the Oracle Communications Session Border Controller
- 100 Trying—Number of times some unspecified action is being taken on behalf of a call (e.g., a database is being consulted), but user has not been located
- 180 Ringing—Number of times called UA identified a location where user has registered recently and is trying to alert the user
- 200 OK—Number of times request has succeeded
- 408 Request Timeout—Number of times server could not produce a response before timeout
- 481 Does Not Exist—Number of times UAS received a request not matching existing dialog or transaction
- 486 Busy Here—Number of times callee's end system was contacted successfully but callee not willing to take additional calls
- 487 Terminated—Number of times request was cancelled by a BYE or CANCEL request
- 4xx Client Error—Number of times the 4xx class of status code appeared for cases where the client seems to have erred
- 503 Service Unavail—Number of times server was unable to handle the request due to a temporary overloading or maintenance of the server
- 5xx Server Error—Number of times the 5xx class of status code appeared
- Response Retrsns—Number of response retransmissions sent and received
- Transaction Timeouts— Number of times a transaction timed out. The timer related to this transaction is Timer B, as defined in RFC 3261
- Locally Throttled—Number of locally throttled invites. Does not apply to a server.

show sipd <message> output is divided in two sections: Server and Client, with information for recent, total, and period maximum time frames. This command also displays information about the average and maximum latency. For each type of SIP message, only those transactions for which there are statistics are shown. If there is no data available for a certain SIP message, the system displays the fact that there is none and specifies the message about which you inquired.

groups—Display cumulative information for all session agent groups on the Oracle Communications Session Border Controller. This information is compiled by totaling the session agent statistics for all of the session agents that make up a particular session agent group. While the show sipd groups command accesses the subcommands that are

described in this section, the main `show sipd groups` command (when executed with no arguments) displays a list of all session agent groups.

`groups -v` —Display statistics for the session agents that make up the session agent groups that are being reported. The `-v` (meaning “verbose”) executed with this command must be included to provide verbose detail.

`groups <specific group name>`— Display statistics for the specified session agent group

`endpoint-ip <phone number>` —Displays registration information for a designation endpoint entered in the `<phone number>` argument; also show IMS-AKA data

`all`—Display all the show sipd statistics listed above

`sip-endpoint-ip`—See show sipd endpoint-ip

`sa-nsep-burst`—Display NSEP burst rate for all SIP session agents

`subscriptions-by-user`—Display data for SIP per user subscribe dialog limit

`rate`—Displays the transaction rate of SIP messages

### Example

```
ACMEPACKET# show sipd errors
```

## show snmp-community-table

### Syntax

```
show snmp-community-table
```

The `show snmp-community-table` command displays all information for configured SNMP communities including request and responses for each community.

### Example

```
ACMEPACKET# show snmp-community-table
```

## show spl

The `show spl` command displays the version of the SPL engine, The filenames and version of the SPL plugins currently loaded on the Oracle Communications Session Border Controller, The signature state of each plugin , The system tasks that each loaded plugin interacts with, enclosed in brackets.

`show spl <task>` — command displays SPL file information including the signature state.

## show support-info

### Syntax

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

This command allows you to gather a set of information commonly requested by the Acme Packet TAC when troubleshooting customers.

### Arguments

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

`standard` — Display information for all commands the `show support-info` command encompasses.

`media` — Display and write out only the show media commands to the log file.

`signaling` — Display and write out all commands and exclude the show media commands to the log file.

config — Optionally add the show running-config output to the output of the standard arguments.

### Example

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

## show system-state

### Syntax

```
show system-state
```

Displays the system state based on the latest setting of the set-system-state command.

### Example

```
ACMEPACKET# show system-state
```

## show tacacs

### Syntax

```
show tacacs stats
```

Displays statistics related to communications between the Oracle Communications Session Border Controller and configured TACACS servers, including:

- number of ACLI commands sent for TACACS+ accounting
- number of successful TACACS+ authentications
- number of failed TACACS+ authentications
- number of successful TACACS+ authorizations
- number of failed TACACS+ authentications
- the IP address of the TACACS+ daemon used for the last transaction

## show temperature

### Syntax

```
show temperature
```

Displays the temperature in Celsius for all given components with temperature sensors.

### Example

```
ACMEPACKET# show temperature
```

## show timezone

### Syntax

```
show timezone
```

Displays the information set with the timezone-zet command including the name of the timezone, its minutes from UTC, and the start and stop date and hours for daylight saving time.

### Example

```
ACMEPACKET# show timezone
```

## show trap-receiver

### Syntax

```
show trap-receiver
```

The show trap-receiver command displays trap receiver information for each configured SNMP community.

### Example

```
ACMEPACKET# show trap-receiver
```

## show uptime

### Syntax

```
show uptime
```

The show uptime command displays information about the length of time the system has been running in days, hours, minutes, and seconds, as well as the current date and time information.

### Example

```
ACMEPACKET# show uptime
```

## show users

### Syntax

```
show users
```

The show users command displays all users currently logged into the Oracle Communications Session Border Controller by index number. Other display information includes:

- Task-ID
- remote IP address—Only displayed for telnet or SSH connections
- IdNumber
- Duration of connection
- Connection Type
- State—\* Denotes the current connection

### Example

```
ACMEPACKET# show users
```

## show version

### Syntax

```
show version
```

The show version command shows the OS version information including: the OS version number, the date that the current copy of the OS was made, and other information.

### Example

```
ACMEPACKET# show version
```

### show virtual-interfaces

#### Syntax

```
show virtual-interface
```

The show virtual-interface command shows the virtual interfaces for Oracle Communications Session Border Controller signaling services; for example, SIP-NAT external address, H.323 interface (stack) IP interface, and MGCP IP interface.

#### Example

```
ACMEPACKET# show virtual-interfaces
```

### show voltage

#### Syntax

```
show voltage
```

Displays current operating voltages for components in the Oracle Communications Session Border Controller.

#### Mode

User and Superuser

#### Example

```
ACMEPACKET# show voltage
```

### show wancom

#### Syntax

```
show wancom
```

Displays negotiated duplex mode and speed for all Oracle Communications Session Border Controller system control interfaces.

#### Mode

User and Superuser

#### Example

```
ACMEPACKET# show wancom
```

### ssh-pub-key

---

The ssh-pub-key command allows you to display, import, and delete public key records on the Oracle Communications Session Border Controller.

#### Syntax

```
ssh-pub-key [delete | export | generate | import] <login name>
```

#### Arguments

**delete** <key name> — Delete an SSH public key associated with a specific name.

**export** <key name>— Displays a public key in RFC 4716 (SECSH) format, by object name, on the screen.

**generate** <key name> — Generate an SSH key pair for an existing key.

**import** — Import an SSH public key.

- **authorized-key** <key name> — Import a key you will paste into the ACLI with the supplied object name.
- **known-host** <key name> — Import a host key you will paste into the ACLI with the supplied object name.

## Mode

Superuser

## Release

First appearance: 5.1.1

## Example

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

# stack

The stack command shows the function call stack trace for a specified stack.

## Syntax

```
stack <task>
```

## Arguments

<task> Enter a task name or task ID

## Mode

Superuser

## Release

First appearance: 1.0

## Example

```
ACMEPACKET# stack sipd
```



**Note:** This command displays a list of nested routine calls for the specified stack. Each routine call and its parameters are shown.

# start learned-allowed-elements

The start learned-allowed-elements command begins the Oracle Communications Session Border Controller to analyze traffic and create an allowed-elements-profile configuration element to match and pass that traffic.

## Syntax

```
start learned-allowed-elements [method] [msg-type] [params]
```

### Arguments

Entered without any arguments, the system captures and parses all messages sent through to create an allowed-elements-profile, based on headers only.

method—Adding this argument writes out rule set information that includes message method criteria.

msg-type—Adding this argument writes out rule set information that includes message type criteria, including any, request, or response.

params—Adding this argument writes out rule set information that includes header parameter criteria, that appears in the header-rules subelement.

### Mode

Superuser

### Release

First appearance: 6.3.0

---

## stop-task

The stop-task command shuts down a specified task.

### Syntax

```
stop-task <task>
```

### Arguments

<task> Enter a task name or task ID



**Note:** Use this command with caution as there is no direct way to restart a task without rebooting the Oracle Communications Session Border Controller.

### Mode

Superuser

### Release

First appearance: 1.0

### Example

```
ACMEPACKET# stop-task sipd
```

---

## stop learned-allowed-elements

The stop learned-allowed-elements command stops the Oracle Communications Session Border Controller from analyzing traffic and closes all created configuration elements. You must then perform a save and activate for created elements to be saved to the running config

### Syntax

```
stop learned-allowed-elements <configuration name>
```



**Arguments**

<configuration-name>—Enter a name that will become the allowed-elements-profile configuration name that reflects passing the traffic captured during the start learned-allowed-elements task.

**Mode**

Superuser

**Release**

First appearance: 6.3.0

---

**switchover-redundancy-link**

---

The switchover-redundancy-link command allows you to switchover the physical interface to standby in a redundant link configuration.

**arguments**

<slot> Select the slot number to switchover the link from active to standby.

- Values 1 | 2

**Mode**

Superuser

**Release**

First appearance: 5.0

**Example**

```
ACMEPACKET# switchover-redundancy-link 2
```

---

**synchronize**

---

The synchronize command is used to synchronize files across HA nodes.

**arguments**

spl <filename>—Synchronizes SPL plugins from the /code/spl directory.

lrt <path><filename>—Synchronize Local Routing Tables (LRT) files between active and standby (e.g. synchronize lrt /code/lrt/filename.xml).

**Mode**

Superuser

**Release**

First appearance: 6.3

---

**systemtime-set**

---

The systemtime-set command sets the system clock.

### Syntax

```
sysitime-set
```



**Note:** The sysitime-set command prompts the user for the date and time and updates the system clock. The command will not set the system time if an invalid year, month, or day is entered. Attempting to change the date and time on the Oracle Communications Session Border Controller displays a warning message as use of this command could be service affecting.

### Mode

Superuser

### Release

First appearance: 1.0 / Most recent update: 1.2.1

### Example

```
ACMEPACKET# sysitime-set
```

---

## tail-logfile-close

The tail-logfile-close command ends the echoing of a process's logfile to the screen as initiated by the tail-logfile-open command.

### Syntax

```
tail-logfile-close <process> [<logfile>]
```

### Arguments

<process> — Enter the name of the process that is writing to the specified logfile.

<logfile> — Enter the logfile's name that you want to stop being echoed to the screen. This argument is optional.



**Note:** Must be a valid logfile that is currently being written to.

### Mode

Superuser

### Release

First appearance: 4.0

### Example

```
ACMEPACKET# tail-logfile-close sipd
```

---

## tail-logfile-open

The tail-logfile-open command displays all messages on the console that are normally written to a specified logfile. As a message is written to the logfile, it is also displayed on the screen. The specified logfile will continue to be updated on the Oracle Communications Session Border Controller's filesystem.

## Syntax

tail-logfile-open <process> [<logfile>]

## Arguments

<process> — Enter the name of the process that is writing to the specified logfile

<logfile> Enter an alternate logfile's name for which you want new entries echoed to the console screen. Not entering the logfile argument forces the default log for the named process to be displayed on the screen. This argument is optional.

## Release

First appearance: 4.0

## Mode

Superuser



**Note:** Must be a valid logfile that is currently being written to. The level of detail displayed on the screen is related to the loglevel of the process.

## Example

```
ACMEPACKET# tail-logfile-open sipd
```

# tcb

The tcb command displays task control block (TCB) information for a particular task.

## Syntax

```
tcb <task>
```

## Arguments

<task> — Enter a task name or task ID

## Mode

Superuser

## Release

First appearance: 1.1



**Note:** This command returns a pointer to the TCB for a specified task. Although all task state information is contained in the TCB, you must not modify it directly. This command is used only for debugging purposes.

## Example

```
ACMEPACKET# tcb sipd
```

# test-audit-log

The test-audit-log command allows the user to test audit log functionality.

### Arguments

<log-msg> Enter the audit log string to be written into the audit file

### Syntax

```
test-audit-log <log-msg>
```

### Mode

Superuser

### Release

First appearance: S-C6.2.0

### Example

```
ACMEPACKET# test-audit-log log1
```

## test-pattern-rule

---

The test-pattern-rule command allows you to test header manipulation pattern rules for expression validation.

### Arguments

<expression> Enter the regular expression that you want to test. The Oracle Communications Session Border Controller informs you whether or not there is a match. <string> Enter the string against which you want to compare the regular expression <show> View the test pattern you entered, whether there was a match, and if so, the number of matches <exit> End the test User

### Mode

User

### Release

First appearance: 5.0

### Example

```
ACMEPACKET# test-pattern-rule expression '.*;tgid=(.+).*'
```



**Note:** This command exists both as a command and as a configuration element.

## test-policy

---

The test-policy element tests and displays local policy routes from the ACLI.

### Parameters

**source-realm** Enter the name set in the source-realm field of a configured local policy. Entering an “\*” in this field matches for any source realm. Leaving the field empty indicates that only the “global” realm will be tested.

**from-address** Enter the “from” address of the local policy to look up/test. From addresses should be entered as SIP-URLs in the form of sip:19785551212@netnetsystems.com.

<b>to-address</b>	Enter the “to” address of the local policy to look up/test. To addresses should be entered as SIP-URLs in the form of sip:19785551212@netnetsystems.com.
<b>time-of-day</b>	Enable or disable use of the time of day value set in the start-time and end-time fields you set in configured local-policy elements <ul style="list-style-type: none"> <li>• Values: enabled   disabled</li> </ul>
<b>carriers</b>	Enter the names of permitted carriers set in the carriers fields set in configured local-policy elements. This field is formatted as a list of comma separated text strings enclosed in quotation marks.
<b>media-profile</b>	Enter a list of media profiles
<b>show</b>	Show the next hop and the associated carrier information for all routes matching the “from” and “to” addresses entered

## Path

test-policy is available under the session-router path.

## Release

First appearance: 1.0 / Most recent update: 1.2.1

## RTC Status

Supported

## Notes

Type the show command to perform the actual test lookup after parameters have been entered.

The test-policy element can also be configured in Superuser mode as a command.

# test-translation

The test-translation command is used to test translation rules configured for the address translation feature. This command is also found in the session-router path. Details on its use are found in the Configuration Elements N-Z chapter.

## Syntax

```
test-translation <argument>
```

## Arguments

<argument> The following is a list of test-translation arguments:

- Values :
  - called-address—Enter the address on which the called rules are be applied. This entry is required.
  - calling-address—Enter the address on which the calling rules will be applied. This entry is required.
  - show—Show results of translation
  - translation-id—Enter translation rules to test
  - exit—Exit the test translationUser

## Mode

User

### Release

First appearance: 1.3

### Example

```
ACMEPACKET# test-translation show
```

## timezone-set

---

The `timezone-set` command sets the time zone and daylight savings time on the Oracle Communications Session Border Controller.

### Syntax

```
timezone-set
```

### Mode

Superuser

### Release

First appearance: 1.0.



**Note:** The `timezone-set` command prompts the user for time zone, UTC offset, and daylight saving time information. If daylight savings time for your time zone changes start and stop dates yearly, this command must be set yearly.

### Example

```
ACMEPACKET# timezone-set
```

If you need to exit the `timezone-set` command before completing it, use the key sequence **Ctrl-D**.

## verify-config

---

The `verify-config` command verifies the Oracle Communications Session Border Controller's current configuration. The `verify-config` command checks the consistency of configuration elements that make up the current configuration and should be carried out prior to activating a configuration on the Oracle Communications Session Border Controller.

### Syntax

```
verify-config
```

### Mode

Superuser

### Release

First appearance: 1.3; Most recent update: S-C6.1.0

## Notes

The verify-config command, entered either directly or via the save-config command, checks for address duplication for a given network-interface within a configuration. Addresses are checked for duplication based on the following criteria:

- Every address entered is checked against the Primary and Secondary Utility addresses
- All UDP, TCP, and TFTP addresses are checked against other UDP, TCP, and TFTP addresses respectively within the same port range



**Note:** For detailed information, refer to the Maintenance and Troubleshooting Guide.

## Example

```
ACMEPACKET# verify-config
```

# watchdog

The watchdog command sets or queries the state of the watchdog timer. If the system becomes unstable causing the watchdog timer to not reset, the system reboots.

## Syntax

```
watchdog <arguments>
```

## Arguments

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

- Values:
  - enable—Enable the watchdog timer
  - disable—Disable the watchdog timer
  - fetch—Display the watchdog timer configuration



**Note:** The fetch argument can be accessed from user mode.

## Mode

User

## Release

First appearance: 2.0.1

## Example

```
ACMEPACKET# watchdog enable
```





---


## Configuration Elements A-M

### access-control

---

The access-control configuration element is used to manually create ACLs for the host path in the Oracle Communications Session Border Controller.

#### Parameters

<b>realm-id</b>	Enter the ingress realm of traffic destined to host to apply this ACL
<b>description</b>	Provide a brief description of the access-control configuration element
<b>destination-address</b>	<p>Enter the destination address, net mask, port number, and port mask to specify traffic matching for this ACL. Not specifying a port mask implies an exact source port. Not specifying an address mask implies an exact IP address. This parameter is entered in the following format: &lt;ip-address&gt;[/&lt;num-bits&gt;] [:&lt;port&gt;][/&lt;port-bits&gt;]</p> <ul style="list-style-type: none"> <li>• Default: 0.0.0.0</li> </ul> <p>An IPV6 address is valid for this parameter.</p>
<b>source-address</b>	<p>Enter the source address, net mask, port number, and port mask to specify traffic matching for this ACL. Not specifying a port mask implies an exact source port. Not specifying an address mask implies an exact IP address. This parameter is entered in the following format: &lt;ip-address&gt;[/&lt;num-bits&gt;] [:&lt;port&gt;][/&lt;port-bits&gt;]</p> <ul style="list-style-type: none"> <li>• Default: 0.0.0.0</li> </ul> <p>An IPV6 address is valid for this parameter.</p>
<b>application-protocol</b>	<p>Select the application-layer protocol configured for this ACL entry</p> <ul style="list-style-type: none"> <li>• Values: SIP   H.323   MGCP   NONE</li> </ul> <p> <b>Note:</b> If application-protocol is set to none, the destination-address and port will be used. Ensure that your destination-address is set to a non-default value (0.0.0.0.)</p>
<b>transport-protocol</b>	<p>Select the transport-layer protocol configured for this ACL entry</p> <ul style="list-style-type: none"> <li>• Default: ALL</li> <li>• Values: ALL   TCP   UDP</li> </ul>
<b>access</b>	Select the access control type for this entry

	<ul style="list-style-type: none"><li>• Default: permit</li><li>• Values:<ul style="list-style-type: none"><li>• permit—Puts the entry in trusted or untrusted list depending on the trust-level parameter. This gets promoted and demoted according to the trust level configured for the host.</li><li>• deny—Puts this entry in the deny list.</li></ul></li></ul>
<b>average-rate-limit</b>	<p>Enter the allowed sustained rate in bytes per second for host path traffic from a trusted source within the realm. A value of 0 disables the policing.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>trust-level</b>	<p>Select the trust level for the host</p> <ul style="list-style-type: none"><li>• Default: None</li><li>• Values:<ul style="list-style-type: none"><li>• none—Hosts will always remain untrusted. Will never be promoted to trusted list or will never get demoted to deny list</li><li>• low—Hosts can be promoted to trusted-list or can get demoted to deny-list</li><li>• medium—Hosts can get promoted to trusted, but can only get demoted to untrusted. Hosts will never be put in deny-list.</li><li>• high—Hosts always remain trusted</li></ul></li></ul>
<b>minimum-reserved-bandwidth</b>	<p>Enter the minimum reserved bandwidth in bytes per second that you want for the session agent, which will trigger the creation of a separate pipe for it. This parameter is only valid when the trust-level parameter is set to high. Only a non-zero value will allow the feature to work properly.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 4294967295</li></ul>
<b>invalid-signal-threshold</b>	<p>Enter the rate of signaling messages per second to be exceeded within the tolerance-window that causes a demotion event. This parameter is only valid when trusted-level is configured as low or medium. A value of 0 means no threshold.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>maximum-signal-threshold</b>	<p>Enter the maximum number of signaling messages per second that one host can send within the tolerance-window. The host will be demoted if the Oracle Communications Session Border Controller receives messages more than the configured number. This parameter is only valid when trusted-level is configured low or medium. A value of 0 means no threshold.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>untrusted-signal-threshold</b>	<p>Enter the maximum number of signaling messages from untrusted sources allowed within the tolerance window.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>deny-period</b>	<p>Enter the time period in seconds a deny-listed or deny entry is blocked by this ACL. The host is taken out of deny-list after this time period elapses.</p> <ul style="list-style-type: none"><li>• Default: 30</li><li>• Values: Min: 0 / Max: 999999999</li></ul>

<b>nat-trust-threshold</b>	<p>Enter maximum number of denied endpoints that set the NAT device they are behind to denied. 0 means dynamic demotion of NAT devices is disabled.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 65535</li> </ul>
<b>cac-failure-threshold</b>	<p>Enter the number of CAC failures for any single endpoint that will demote it from the trusted queue to the untrusted queue.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 4294967295</li> </ul>
<b>untrust-cac-failure-threshold</b>	<p>Enter the number of CAC failures for any single endpoint that will demote it from the untrusted queue to the denied queue.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 4294967295</li> </ul>

## Path


**access-control** is an element of the session-router path. The full path from the topmost CLI prompt is: **configure terminal > session-router > access-control**.

## Release

First appearance: 2.0 / Most recent update: S-C6.2.0

## RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

# account-config

The account-config configuration element allows you to set the location where accounting messages are sent.

## Parameters

<b>hostname</b>	<p>Enter the hostname of this Oracle Communications Session Border Controller; must be set to “localhost” or the accounting configuration will not work properly. Entries are in FQDN format.</p> <ul style="list-style-type: none"> <li>• Default: Localhost name</li> </ul>
<b>port</b>	<p>Enter the UDP port number from which RADIUS messages are sent</p> <ul style="list-style-type: none"> <li>• Default: 1813</li> <li>• Values: Min: 1025 / Max: 65535</li> </ul>
<b>strategy</b>	<p>Select the strategy used to select the current accounting server</p> <ul style="list-style-type: none"> <li>• Default: Hunt</li> <li>• Values: <ul style="list-style-type: none"> <li>• hunt—Selects accounting servers in the order in which they are listed</li> <li>• failover—Uses first and subsequent servers in accounting server list until a failure is received from that server</li> </ul> </li> </ul>

	<ul style="list-style-type: none"><li>• roundrobin—Selects accounting server in order, distributing the selection of each accounting server evenly over time</li><li>• fastestrtt—Selects accounting server with the fastest RTT observed during transactions with the servers</li><li>• fewestpending—Selects accounting server with the fewest number of unacknowledged accounting messages</li></ul>
<b>protocol</b>	<p>Set the type of message protocol type for accounting CDRs.</p> <ul style="list-style-type: none"><li>• Default: radius</li><li>• Values: radius   diameter</li></ul>
<b>state</b>	<p>Enable or disable the accounting system</p> <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>max-msg-delay</b>	<p>Enter the time in seconds the Oracle Communications Session Border Controller continues to send each accounting message</p> <ul style="list-style-type: none"><li>• Default: 60</li><li>• Values: Min: 0 / Max: 4294967295</li></ul>
<b>max-wait-failover</b>	<p>Enter the number of accounting messages held in message waiting queue before a failover situation status is enacted</p> <ul style="list-style-type: none"><li>• Default: 100</li><li>• Values: Min: 1/ Max: 4096</li></ul>
<b>trans-at-close</b>	<p>Enable the Oracle Communications Session Border Controller to transmit accounting message information at the close of a session only. Setting this parameter to disabled tells the Oracle Communications Session Border Controller to transmit accounting information at the start of a session (Start), during the session (Interim), and at the close of a session (Stop).</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>generate-start</b>	<p>Select the type of SIP event that triggers the Oracle Communications Session Border Controller to transmit a RADIUS Start message</p> <ul style="list-style-type: none"><li>• Default: ok</li><li>• Values:<ul style="list-style-type: none"><li>• none—RADIUS Start message is not generated</li><li>• invite—RADIUS Start message is generated once a SIP session INVITE is received</li><li>• ok—RADIUS Start message is generated an OK message in response to an INVITE is received</li></ul></li></ul>
<b>generate-interim</b>	<p>SBC to transmit a RADIUS Interim message</p> <ul style="list-style-type: none"><li>• Default: reinvite-response</li><li>• Values:<ul style="list-style-type: none"><li>• ok—RADIUS Start message is generated when an OK message is received in response to an INVITE</li><li>• reinvite—RADIUS Interim message is generated when a SIP session reINVITE message is received</li><li>• reinvite-response—RADIUS Interim message is generated when a SIP session reINVITE is received and the system responds to it</li></ul></li></ul>

	<ul style="list-style-type: none"> <li>• <b>reinvite-cancel</b>—RADIUS Interim message is generated when a SIP session reINVITE is received, and the Reinvite is cancelled before the Oracle Communications Session Border Controller responds to it</li> <li>• <b>unsuccessful-attempt</b>—RADIUS Interim message is generated when a session set-up attempt from a preference-ordered list of next-hop destinations is unsuccessful. This can happen when a local policy lookup, LRT lookup, ENUM query response, or SIP redirect returns a preference-ordered list of next-hop destinations. The interim message contains: the destination IP address, the disconnect reason, a timestamp for the failure, and the number that was called</li> </ul>
<b>generate-event</b>	<p>Enter one or more valid events that prompt creation of an Event record. Current valid values are register and local-register. Multiple values are entered enclosed in parenthesis and separated by spaces.</p> <ul style="list-style-type: none"> <li>• Default:</li> <li>• Values: register   local-register</li> </ul>
<b>file-output</b>	<p>Enable or disable the output of comma-delimited CDRs</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>file-path</b>	<p>Enter the path in which to save the comma-delimited CDR file. Most common settings for this parameter are /ramdrv or /ramdrv/logs directories. You cannot set this parameter to the /code or /boot directories.</p>
<b>max-file-size</b>	<p>Set the maximum file size in bytes for each CDR file</p> <ul style="list-style-type: none"> <li>• Default: 1000000</li> <li>• Values: Min: 1000000 / Max: 100000000</li> </ul>
<b>max-files</b>	<p>Set the maximum number of files to store on the Oracle Communications Session Border Controller. The parameter's value range is from 0 to unlimited. The user should consider the <b>max-file-size</b> setting and available space to specify this value.</p> <ul style="list-style-type: none"> <li>• Default: 5</li> </ul>
<b>file-compression</b>	<p>Enable or disable compression of CDR files; when enabled, comma-delimited CDR files are zipped on the backup device to maximize storage space</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>file-rotate-time</b>	<p>Set the time in minutes that the Oracle Communications Session Border Controller rotates the CDR files; the Oracle Communications Session Border Controller will overwrite the oldest file first</p> <ul style="list-style-type: none"> <li>• Default: 60</li> <li>• Values: Min: 2 / Max: 2147483647</li> </ul>
<b>file-delete-alarm</b>	<p>Enable or disable the raising of an alarm when CDR files are deleted due to lack of space.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>ftp-push</b>	<p>Enable or disable the FTP push feature</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>ftp-address</b>	<p>Enter the IP address for the FTP server used with the FTP push feature</p>

<b>ftp-port</b>	<p>Set the TCP port on the FTP server to use with the FTP push feature</p> <ul style="list-style-type: none"><li>• Default: 21</li><li>• Values: Min: 1 / Max: 65535</li></ul>
<b>ftp-user</b>	<p>Enter the username the Oracle Communications Session Border Controller will use to log in to the FTP server</p>
<b>ftp-password</b>	<p>Enter the password the Oracle Communications Session Border Controller will use to log in to the FTP server</p>
<b>ftp-remote-path</b>	<p>Enter the file path the Oracle Communications Session Border Controller will use to work in on the FTP server</p>
<b>ftp-strategy</b>	<p>Set the strategy for the Oracle Communications Session Border Controller to use when selecting from multiple push receivers</p> <ul style="list-style-type: none"><li>• Default: hunt</li><li>• Values:<ul style="list-style-type: none"><li>• hunt—The Oracle Communications Session Border Controller selects the push receiver from the available list according to the priority level</li><li>• failover—The Oracle Communications Session Border Controller selects the push receiver based on priority level and continues to use that same push receiver until it fails over</li><li>• roundrobin—The Oracle Communications Session Border Controller selects push receivers systematically one after another, balancing the load among all responsive push receivers</li><li>• fastesttrtt—The Oracle Communications Session Border Controller selects the push receiver based on best average throughput. For this situation, throughput is the number of bytes transferred divided by the response time. The system uses a running average of the five most recent throughput values to accommodate for network load fluctuations</li></ul></li></ul>
<b>intermediate-period</b>	<p>Set the time interval used to generate periodic interim records during a session</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>account-servers</b>	<p>Access the account-server subelement</p>
<b>cdr-output-redundancy</b>	<p>Enable or disable the redundant storage of comma-delimited CDR files</p> <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>ftp-max-wait-failover</b>	<p>Enable or disable the prevention of duplicate accounting attributes</p> <ul style="list-style-type: none"><li>• Default: 60</li><li>• Values: Min: 1 / Max: 4096</li></ul>
<b>prevent-duplicate-attrs</b>	<p>Enable this parameter to prevent the Oracle Communications Session Border Controller from duplicating attributes in the accounting records it generates. This duplication can be caused, for example, by multiple media sessions within the context of a call. Retaining the default (disabled) allows the Oracle Communications Session Border Controller to include duplicate attributes in RADIUS, Diameter and Local accounting records. This can result in attribute placement and counts that are less consistent.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>


<b>vsa-id-range</b>	Enter the range of accounting attributes to include in CDRs. A blank field means this feature is turned off and all attributes are included.
<b>cdr-output-inclusive</b>	<p>Enable or disable the guarantees placement of attributes in CSV files used for local CDR storage and FTP pus</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>push-receiver</b>	Access the push-receiver subelement.
<b>watchdog-ka-timer</b>	<p>Sets the value in seconds that the Oracle Communications Session Border Controller waits between sending DWRs.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: 0,6-65535</li> </ul>
<b>msg-queue-size</b>	<p>Sets the message queue sizefor both RADIUS and Diameter accounting interfaces.</p> <ul style="list-style-type: none"> <li>• Default: 5000</li> <li>• Values: 5000-15000</li> </ul>
<b>diam-srv-ctx-ext</b>	Value to substitute in the extension portion of the Service-Context-ID AVP value. This value can be any string.
<b>diam-srv-ctx-mnc-mcc</b>	Value to substitute in the MNC.MCC portion of the Service-Context-ID AVP value. This value must follow the NUM1.NUM2 format.
<b>diam-srv-ctx-rel</b>	Value to substitute in the release portion of the Service-Context-ID AVP value. This value can be any number $\geq 1$ .
<b>diam-acme-attr-id-range</b>	The range of Acme-specific AVP's to include in ACR messages.
<b>max-acr-retries</b>	<p>The maximum number of times that the SBC can resend an ACR for a session.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: 0 - 4</li> </ul>
<b>acr-retry-interval</b>	<p>The time in seconds for the SBC to wait before resending an ACR for a session.</p> <ul style="list-style-type: none"> <li>• Default: 10</li> <li>• Values: 5 - 20</li> </ul>

## Path

**account-config** is an element of the session-router path. The full path from the topmost CLI prompt is. **configure terminal > session-router > account-config**.

## Release

First appearance: 1.0 / Most recent update: S-CZ7.1.2

 **Note:** This is a single instance configuration element.

## account-config > account-servers

The account-server configuration subelement stores the accounting server information for the account-config.

### Parameters

<b>hostname</b>	Enter the hostname of the accounting server. Entries are in FQDN or IP Address Format
<b>port</b>	Enter the UDP port number associated with the accounting server is configured here <ul style="list-style-type: none"><li>• Default: 1813</li><li>• Values: Min: 1025 / Max: 65535</li></ul>
<b>state</b>	Enable or disable this account-server <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>min-round-trip</b>	Enter the time in milliseconds of the minimum RTT for an accounting message for use with the fastest RTT strategy method <ul style="list-style-type: none"><li>• Default: 250</li><li>• Values: Min: 10 / Max: 5000</li></ul>
<b>max-inactivity</b>	Enter the maximum time in seconds the Oracle Communications Session Border Controller waits when accounting messages are pending without a response before this account server is set as inactive for its failover scheme <ul style="list-style-type: none"><li>• Default: 60</li><li>• Values: Min: 1 / Max: 300</li></ul>
<b>restart-delay</b>	Enter the time in seconds the Oracle Communications Session Border Controller waits after declaring an accounting server inactive before resending an accounting message to that same accounting server <ul style="list-style-type: none"><li>• Default: 30</li><li>• Values: Min: 1 / Max: 300</li></ul>
<b>bundle-vsa</b>	Enable or disable the bundling of the VSAs within RADIUS accounting on the account-server <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>secret</b>	Enter the secret passed from the account-server to the client server; entries in this field must follow the Text Format
<b>NAS-ID</b>	Enter the value the account-server uses to identify the Oracle Communications Session Border Controller so messages can be transmitted; entries in this field must follow the Text Format
<b>priority</b>	Enter the number corresponding to the priority for this account server to have in relation to the other account servers to which you send traffic. The default is 0, meaning there is no set priority. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0</li></ul>

### Path

**account-server** is a subelement of the account-config element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > account-config > account-servers**.

### Release

First appearance: 1.0



**RTC Status**

Unsupported



**Note:** This list can contain as many accounting servers as necessary. By default, this list remains empty. RADIUS will not work unless an account server is configured. This is a multiple instance configuration element.

## account-config > push-receiver

You can configure multiple CDR push receivers for use with the FTP push feature.

**Parameters**

- server** Send the IP address of the FTP/SFTP server to which you want the Oracle Communications Session Border Controller to push CDR files
- Default: 0.0.0.0
- port** Enter the port number on the FTP/SFTP server to which the Oracle Communications Session Border Controller will send CDR files.
- Default: 21
  - Values: Min: 1 / Max: 65535
- admin-state** Set the state of an FTP/SFTP push receiver to enabled for the Oracle Communications Session Border Controller to send CDR files to it
- Default: enabled
  - Values: enabled | disable
- remote-path** Enter the pathname on which the CDR files are sent to the push receiver. CDR files are placed in this location on the FTP/SFTP server.
- Default: non
  - Values: <string> remote pathname
- filename-prefix** Enter the filename prefix to prepend to the CDR files the Oracle Communications Session Border Controller sends to the push receiver. The Oracle Communications Session Border Controller does not rename local files.
- Default: none
  - Values: <string> prefix for filenames
- priority** Enter a number 0 through 4 to set the priority of this push receiver in relation to the others you configure on the system. The highest priority—and the push receiver the system uses first—is 0. The lowest priority—and the push receiver the system uses last—is 4.
- Default: 4
  - Values: Min: 0 (highest) / Max: 4 (lowest)
- protocol** Select the transport protocol to be used for this push receiver. If this is an STFTP push receiver, enter the public-key information in the appropriate parameter in this configuration subelement.
- Default: ftp
  - Values: ftp | sftp

**username** Enter the username the Oracle Communications Session Border Controller uses to connect to push receiver.

**password** Enter the password corresponding to the username of this push receiver.

**public-key** Enter the public key profile to use for authentication when the server is defined for SFTP push receiver. If you define this as an SFTP push receiver but do not set a public-key value, the Oracle Communications Session Border Controller will use password authentication.

### Path

**push-receiver** is a subelement under the account-config element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > account-config > push-receiver**.

### Release

First appearance: S-C6.2.0

### RTC Status

Supported

## allowed-elements-profile

---

This configuration element is used to configure SIP whitelists which controls the passage of unknown headers and parameters in request and response traffic.

### Parameters

**name** A unique identifier of this allowed-elements-profile

**description** A textual description for the allowed-elements-profile

**allow-any** Enter list of headers that are allowed (with any parameter). When header-rules are added to a rule-set, they are automatically removed from this list. A header list is entered separated by commas, but without the “:” part of the header name. This parameter is initially populated with many allowed headers.

- Default: Accept, Accept-Resource-Priority, Alert-Info, Allow, Allow-Events, Authentication-Info, Authorization, Call-ID, Contac, Content-Disposition, Content-Encoding, Content-Length, Content-Type, CSeq, Diversion, Event, Expires, From, History-Info, Join, Max-Forwards, Min-Expires, Min-SE, P-Access-Network-Info, P-Asserted-Identity, P-Associated-URI, P-Called-Party-ID, P-Charging-Function-Addresses, P-Charging-Vector, P-DCS-LAES, P-DCS-Redirect, P-Preferred-Identity, P-Visited-Network-ID, Path, Privacy, Proxy-Authenticate, Proxy-Authorization, Proxy-Require, RAck, Reason, Record-Route, Refer-To, Replaces, request-uri, Require, Resource-Priority, Retry-After, Route, RSeq, Security-Client, Security-Server, Security-Verify, Service-Route, Session-Expires, Session-ID, Subscription-State, Supported, To, Via, WWW-Authenticate

**rule-sets** See the rule-sets subelement that follows.

### Path

**allowed-elements-profile** is an element under the session router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > allowed-elements-profile**

### Release

First appearance: S-C6.3.0

**RTC Status**

Supported

**allowed-elements-profile > rule-sets**

This configuration subelement is used to configure SIP whitelists which controls the passage of unknown headers and parameters in request and response traffic.

**Parameters**

<b>name</b>	A unique identifier of this rule set.
<b>unmatched-action</b>	Identifies the action that the Oracle Communications Session Border Controller performs when it encounters a non-whitelisted header. <ul style="list-style-type: none"> <li>• Default: Reject</li> <li>• Values: reject   delete</li> </ul>
<b>msg-type</b>	Specifies the message type to which the rule applies <ul style="list-style-type: none"> <li>• Default: any</li> <li>• Values: any   request   response</li> </ul>
<b>methods</b>	Specifies list of methods to which the rule applies. This applies to all methods when none are specified. Enter this as a comma separated list.
<b>logging</b>	Enables logging when an unmatched element is intercepted. <ul style="list-style-type: none"> <li>• Default: disabled</li> </ul>

**Path**

**rule-sets** is a subelement under the **allowed-elements-profile** element under the session router path. The full path from the topmost CLI prompt is: **configure terminal > session-router > allowed-elements-profile > rule-sets**.

**Release**

First appearance: S-C6.3.0

**RTC Status**

Supported

**allowed-elements-profile > rule-sets > header-rules**

This configuration subelement is used to configure SIP whitelists which controls the passage of unknown headers and parameters in request and response traffic.

**Parameters**

<b>header-name</b>	the name of the header in the whitelist that the Oracle Communications Session Border Controller allows from incoming messages. It is case-insensitive and supports abbreviated forms of header names. For example, "Via", "via", or "v" all match against the same header. A header name of "request-uri" refers to the request URI of requests, while a header name of "*" applies to any header-type not matched by any other header-rule. The default value is "*". This default value provides the ability to have header-rules for commonly known headers that remove unknown parameters, but leave unknown headers alone.
--------------------	--

<b>unmatched-action</b>	<p>the action for the Oracle Communications Session Border Controller to perform when an incoming header's parameters do not match the relevant allowed parameters specified for this header-name. This parameter applies to non-matching header names only (not non-matching URI parameters).</p> <ul style="list-style-type: none"><li>• Default: reject</li><li>• Values:<ul style="list-style-type: none"><li>• reject—Rejects all incoming messages that have header parameters that do not match the parameters specified in this header-name.</li><li>• delete — Deletes the non-matching elements from incoming messages with header parameters that do not match those specified in this header-name.</li></ul></li></ul>
<b>allow-header-param</b>	<p>The header parameter that the Oracle Communications Session Border Controller allows from the headers in incoming messages. You can enter up to 255 characters, including a comma (,), semi-colon (;), equal sign (=), question mark (?), at-symbol (@), backslash (\), or plus sign (+). The default value is "*", which allows all header parameters to pass through. If you leave this field empty, no header parameters are allowed.</p> <ul style="list-style-type: none"><li>• Default: *</li></ul>
<b>allow-uri-param</b>	<p>the URI parameter that the Oracle Communications Session Border Controller allows from the headers in incoming messages. You can enter up to 255 characters, including a comma (,), semi-colon (;), equal sign (=), question mark (?), at-symbol (@), backslash (\), or plus sign (+). The default value is "*", which allows all URI parameters to pass through. If you leave this field empty, no URI parameters are allowed.</p> <ul style="list-style-type: none"><li>• Default: *</li></ul>
<b>allow-uri-user-param</b>	<p>the URI user parameter that the Oracle Communications Session Border Controller allows from the headers in incoming messages. You can enter up to 255 characters, including a comma (,), semi-colon (;), equal sign (=), question mark (?), at-symbol (@), backslash (\), or plus sign (+). The default value is "*", which allows all URI user parameters to pass through. If you leave this field empty, no URI user parameters are allowed.</p> <ul style="list-style-type: none"><li>• Default: *</li></ul>
<b>allow-uri-header-name</b>	<p>the URI header name that the Oracle Communications Session Border Controller allows from the headers in incoming messages. You can enter up to 255 characters, including a comma (,), semi-colon (;), equal sign (=), question mark (?), at-symbol (@), backslash (\), or plus sign (+). The default value is "*", which allows all URI header name parameters to pass through. If you leave this field empty, no URI header name parameters are allowed.</p> <ul style="list-style-type: none"><li>• Default: *</li></ul>

### Path

**header-rules**header-rules is a subelement under rule-sets under the allowed-elements-profile element under the session router path. The full path from the topmost CLI prompt is: **configure terminal >terminal > session-router > allowed-elements-profile rule-sets header-rules**

### Release

First appearance: S-C6.3.0


### RTC Status

Status: Supported

# auth-params

The auth-params element provides a list of RADIUS servers used for authentication, along with protocol and operation details that define RADIUS access.

## Parameters

- name** Enter the name of this instance of the auth-params configuration element.
- protocol** Enter the protocol to use for obtaining authentication data from a RADIUS server.
- Default: eap
  - Values: eap
-  **Note:** The current software version only supports EAP.
- strategy** Enter the management strategy used to distribute authentication requests. This parameter is only relevant if multiple RADIUS servers have been identified by the servers parameter.
- Default: hunt
  - Values: round-robin | hunt
- server** Enter a RADIUS server by IP address.

## Path

**auth-params** is an element under the security path. The full path from the topmost ACLI prompt is: **configure terminal > security > auth-params**.

## Release

First appearance: S-C6.2.0

## RTC Status

Supported

# authentication

The authentication configuration element is used for configuring an authentication profile.

## Parameters

- source-port** Enter the port number on the Oracle Communications Session Border Controller to send messages to the RADIUS server
- Default: 1812
  - Values: 1645 | 1812
- type** Enter the type of user authentication
- Default: local
  - Values: local | radius| tacacs
- protocol** Select the protocol type to use with your RADIUS server(s)
- Default: pap

	<ul style="list-style-type: none"><li>• Values: pap   chap   mschapv2   ascii</li></ul>
<b>tacacs-authorization</b>	Enable or disable command-based authorization of admin users for TACACS. <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>tacacs-accounting</b>	Enable or disable accounting of admin CLI operations. <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>server-assigned-privilege</b>	Enables a proprietary TACACS+ variant that, after successful user authentication, adds an additional TACACS+ request/reply exchange. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>allow-local-authorization</b>	Enable this parameter if you want the Oracle Communications Session Border Controller to authorize users to enter Super (administrative) mode locally even when your RADIUS server does not return the ACME_USER_CLASS VSA or the Cisco-AVPair VSA. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>login-as-admin</b>	Enable this parameter if you want users to be logged automatically in Superuser (administrative) mode. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>management-strategy</b>	Enter the management strategy used to distribute authentication requests. <ul style="list-style-type: none"><li>• Default: hunt</li><li>• Values: round-robin   hunt</li></ul>
<b>ike-radius-params-name</b>	Enter the auth-params instance to be assigned to this element. <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: Name of an existing auth-params configuration element</li></ul>
<b>management-servers</b>	Enter a list of servers used for management requests
<b>radius-servers</b>	Enter the radius-servers subelement
<b>tacacs-server</b>	Enter the tacacs-servers subelement

### Path

**authentication** is an element under the security path. The full path from the topmost prompt is: **configure terminal > security > authentication**.

### Release

First appearance: 4.0

### RTC Status

Supported

## authentication > radius-servers

The radius-servers subelement defines and configures the RADIUS servers that the Oracle Communications Session Border Controller communicates with.

### Parameters

<b>address</b>	Enter the IP address for the RADIUS server
<b>port</b>	Enter the port number on the remote IP address for the RADIUS server <ul style="list-style-type: none"> <li>• Default: 1812</li> <li>• Values: 1645   1812</li> </ul>
<b>state</b>	Enable or disable this configured RADIUS server <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>secret</b>	Enter the password the RADIUS server and the Oracle Communications Session Border Controller share. This password is not transmitted between the two when the request for authentication is initiated.
<b>nas-id</b>	Enter the NAS ID for the RADIUS server
<b>realm-id</b>	Enter the RADIUS server realm ID.
<b>retry-limit</b>	Set the number of times the Oracle Communications Session Border Controller retries to authenticate with this RADIUS server <ul style="list-style-type: none"> <li>• Default: 3</li> <li>• Values: Min: 1 / Max: 5</li> </ul>
<b>retry-time</b>	Enter the time in seconds the Oracle Communications Session Border Controller waits before retrying to authenticate with this RADIUS server <ul style="list-style-type: none"> <li>• Default: 5</li> <li>• Values: Min: 5 / Max: 10</li> </ul>
<b>maximum-sessions</b>	Enter the maximum number of sessions to maintain with this RADIUS server <ul style="list-style-type: none"> <li>• Default: 255</li> <li>• Values: Min: 1 / Max: 255</li> </ul>
<b>class</b>	Select the class of this RADIUS server as either primary or secondary. A connection to the primary server is tried before a connection to the secondary server is tried. <ul style="list-style-type: none"> <li>• Default: primary</li> <li>• Values: primary   secondary</li> </ul>
<b>dead-time</b>	Set the time in seconds before the Oracle Communications Session Border Controller retries a RADIUS server that it has designated as dead <ul style="list-style-type: none"> <li>• Default: 10</li> <li>• Values: Min: 10 / Max: 10000</li> </ul>
<b>authentication-methods</b>	Select the authentication method the Oracle Communications Session Border Controller uses when communicating with the RADIUS server <ul style="list-style-type: none"> <li>• Default: pap</li> <li>• Values: all   pap   chap   mschapv2</li> </ul>

### Path

**radius-servers** is a subelement under the **authentication** configuration element under the security path. The full path from the topmost prompt is: **configure terminal > security > authentication > radius-servers**.

### Release

First appearance: 4.0 / Most recent update: S-C6.2.0

### RTC Status

Supported

## authentication > tacacs-servers

---

The **tacacs-servers** subelement defines and configures the TACACS+ servers that the Oracle Communications Session Border Controller communicates with.

### Parameters

<b>address</b>	Enter the IP address for the TACACS server. This address must be reachable over the system's media interfaces.
<b>port</b>	Enter the port number on the remote IP address for the TACACS server <ul style="list-style-type: none"><li>• Default: 49</li><li>• Values: 1645   1812</li></ul>
<b>state</b>	Enable or disable this configured TACACS server <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>secret</b>	Enter the password the TACACS server and the Oracle Communications Session Border Controller share. This password is not transmitted between the two when the request for authentication is initiated.
<b>realm-id</b>	Enter the TACACS server realm ID. This realm must be reachable from the system's media interfaces.
<b>dead-time</b>	Set the time in seconds before the Oracle Communications Session Border Controller retries a TACACS server that it has designated as dead <ul style="list-style-type: none"><li>• Default: 10</li><li>• Values: Min: 10 / Max: 10000</li></ul>
<b>authentication-methods</b>	Select the authentication method the Oracle Communications Session Border Controller uses when communicating with the TACACS server <ul style="list-style-type: none"><li>• Default: pap</li><li>• Values: all   pap   chap   ascii</li></ul>

### Path

**tacacs-servers** is a subelement under the **authentication** configuration element under the security path. The full path from the topmost prompt is: **configure terminal > security > authentication > tacacs-servers**.

### Release

First appearance: S-C6.3.0 / Most recent update: S-C6.3.0



**RTC Status**

Supported

**bootparam**

The bootparam command establishes the parameters that a Oracle Communications Session Border Controller uses when it boots.



**Note:** In the physical interface and the network interface configuration elements, you can set values that may override the values set within the boot configuration parameters. If you are configuring these elements and enter information that matches information in the boot configuration parameters, the system will warn you that your actions may change the boot configuration parameters.

The bootparam command presents you with the parameters to enter on a line-by-line basis. You can press <Enter> to accept a given default parameter and move to the next parameter.

**Parameter**

- |                          |   |
|--------------------------|---|
| <b>boot device</b>       | Enter the name and port number of the device from which an image is downloaded (e.g., wancom0). This parameter is only required if you are booting from an external device; if you are doing so, the name must be wancom followed by the port number  |
| <b>processor number</b>  | Enter the processor number on the backplane   |
| <b>host name</b>         | Enter the name of the boot host used when booting from an external device   |
| <b>file name</b>         | Enter the name of the file containing the image to be booted. If you are booting off the system flash memory, this filename must always match the filename that you designate when you FTP the image from the source to the Oracle Communications Session Border Controller. When booting off the system flash memory, this filename must always start with: /tffs0/.   |
| <b>inet on ethernet</b>  | Enter the internet address of the Oracle Communications Session Border Controller's Ethernet interface. An optional subnet mask in the form inet_adrs:subnet_mask is available. If DHCP is used to obtain the configuration parameters, lease timing information may also be included. The information takes the form of lease duration:lease_origin and is appended to the end of the field. The subnet mask for this parameter is given in hex. |
| <b>inet on backplane</b> | Not used  |
| <b>host inet</b>         | Enter the internet address of the boot host, used when booting from an external device  |
| <b>gateway inet</b>      | Enter the IP gateway for the management interface's subnet  |
| <b>user</b>              | Enter the FTP username on the boot host   |
| <b>ftp password</b>      | Enter the FTP password for the FTP user on the boot host  |
- flags** Set the Oracle Communications Session Border Controller to know from where to boot. Also sets how to use the files in the booting process.
- Values • 0x08—Quickboot. The system bypasses the 7 second countdown prior to booting.
  - 0x10008—This flag does the same as 0x08. In addition, it connects to usr/acme on the boot host defined in the boot parameters. Connecting externally to usr/acme is useful for copying data off the Oracle Communications Session Border Controller to the external host over NFS.
  - 0x70008—This flag does all of the above. In addition, it stores the configuration in usr/acme on the boot host defined in the boot parameters rather than in /code in the system flash memory file system.

- 0x80008—Source based routing.

**target name** Enter the name of this Oracle Communications Session Border Controller. This field also sets the name of the Oracle Communications Session Border Controller as it appears in the system prompt (e.g., ACMEPACKET> or ACMEPACKET#).

- Values 0-38 Characters in length.startup script—Internal use onlyother—Internal use only

**startup script** Internal use only

**other** Internal use only

### Path

**bootparam** is in the configuration path. The full path from the topmost prompt is: **configure terminal > bootparam**.

### Release

First appearance: 1.0

### RTC Status

Unsupported

## call-recording-server

---

The call-recording-server configuration element allows you to forward both signaling and media packets to and from a realm to a specified destination.

### Parameters


<b>name</b>	Enter the name of the IPRCR you are configuring
<b>primary-realm</b>	Enter the primary realm to which you want this IPRCR to be associated. This must be an existing realm or the IPRCR will be considered invalid and this server will be ignored.
<b>primary-signaling-addr</b>	Enter the primary address you want to use as a destination for forwarding signaling packets
<b>primary-media-addr</b>	Enter the primary address you want to use as a destination for forwarding media packets. If both the signaling and media primary addresses are the same, this parameter can be left blank
<b>secondary-realm</b>	Enter the secondary realm you want this IPRCR to be associated with if the primary-network becomes unreachable. This must be an existing realm or the IPRCR will be considered invalid and this server will be ignored.
<b>secondary-signaling-addr</b>	Enter the address you want to use as a destination for forwarding signaling packets if the address you entered in the primary-signaling-addr parameter becomes unreachable.
<b>secondary-media-addr</b>	Enter the address you want to use as a destination for forwarding media packets if the address you entered in the primary-media-addr parameter becomes unreachable
<b>ping-method</b>	Enter the SIP method you want to be used for ping messages send to the IPRCR
<b>ping-interval</b>	Enter the time in seconds to allow between the transmission of ping requests in an HA configuration. A value of 0 means this parameter is disabled. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0; 2 / Max: 9999999</li></ul>
<b>crs-tls-decryption</b>	Enables decryptions of TLS/SRTP packets.

**Path**

**call-recording-server** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > call-recording-server**

**Release**

First appearance: 6.0

 **Note:** This is a multiple instance element.

**RTC Status**

Supported

---

**capture-receiver**

The capture-receiver configuration element allows you to configure packet tracing functionality on your Oracle Communications Session Border Controller.

**Parameters**

<b>state</b>	Enable or disable the Oracle Communications Session Border Controller’s TRACE capability <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>address</b>	Enter the TRACE server IP address
<b>network-interface</b>	Enter the TRACE server outbound interface <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>

**Path**

**capture-receiver** is an element of the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > capture-receiver**.

**Release**

First appearance: 5.0

**RTC Status**

Supported

---

**certificate-record**

This configuration element configures certificate records for TLS support.

**Parameter**

<b>name</b>	The name of this certificate record object.
<b>country</b>	Enter the name of the locality for the state

	<ul style="list-style-type: none"><li>• Default: US</li></ul>
<b>state</b>	Enter the name of the locality for the state <ul style="list-style-type: none"><li>• Default: MA</li></ul>
<b>locality</b>	Enter the name of the organization holding the certificate <ul style="list-style-type: none"><li>• Default: Burlington</li></ul>
<b>organization</b>	Enter the name of the organization holding the certificate <ul style="list-style-type: none"><li>• Default: Engineering</li></ul>
<b>unit</b>	Enter the name of the unit for holding the certificate within the organization.
<b>common-name</b>	Enter the common name for the certificate record.
<b>key-size</b>	Set the size of the key for the certificate. <ul style="list-style-type: none"><li>• Default: 1024</li><li>• Values: 512   1024   2048</li></ul>
<b>alternate-name</b>	The alternate name of the certificate holder which can be expressed as an IP address, DNS host, or email address. Configure this parameter using the following syntax to express each of these 3 forms. <ul style="list-style-type: none"><li>• <b>IP:</b>&lt;IP address&gt;</li><li>• <b>DNS:</b>&lt;DNS IP address/domain&gt;</li><li>• <b>email:</b>&lt;email address&gt;</li></ul>
<b>trusted</b>	Enable or disable trust of this certificate <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>key-usage-list</b>	Enter the usage extensions to use with this certificate record; can be configured with multiple values. <ul style="list-style-type: none"><li>• Default: digitalSignature and keyEncipherment</li></ul>
<b>extended-key-usage-list</b>	Enter the extended key usage extensions you want to use with this certificate record. <ul style="list-style-type: none"><li>• Default: serverAuth</li></ul>

### Path

**certificate-record** is an element under the security path. The full path from the topmost prompt is: **configure terminal > security > certificate-record**.

### Release

First appearance: 4.1


### RTC Status

Supported

## cert-status-profile

The cert-status-profile configuration element identifies an OCSP responder, the transport protocol used to access the responder, and the certificates used to sign the OCSP request and to validate the OCSP response.

### Parameters

<b>name</b>	Enter the name of this cert-status-profile instance, thus allowing the configuration of multiple configuration elements of this type. This parameter is required. <ul style="list-style-type: none"> <li>Default: None</li> <li>Values: Any valid object name — the name must be unique within the cert-status-profile namespace</li> </ul>
<b>ip-address</b>	Enter the IPv4 address of the destination OCSP responder. This parameter is required. <ul style="list-style-type: none"> <li>Default: None</li> <li>Values: Any valid IPv4 address</li> </ul>
<b>hostname</b>	hostname of the OCSR. If this parameter and the ip-address parameter are both configured, the Oracle Communications Session Border Controller uses the IP address.
<b>port</b>	Enter the destination port number. This parameter is optional. <ul style="list-style-type: none"> <li>Default: 80</li> <li>Values: Any valid port number</li> </ul>
<b>type</b>	Enter the protocol type used for certificate checking. This parameter is optional. <ul style="list-style-type: none"> <li>Default: ocsdp</li> <li>Values: ocsdp</li> </ul> <div>  <b>Note:</b> The current software version only supports ocsdp. </div>
<b>trans-protocol</b>	Enter the protocol used to transmit the OCSP request; the single currently supported value is http. This parameter is optional. <ul style="list-style-type: none"> <li>Default: http</li> <li>Values: http</li> </ul>
<b>requester-cert</b>	Enter the name of the certificate configuration element used to sign the outgoing OCSP request; this parameter is required only if the OCSP responder mandates a signed request. <ul style="list-style-type: none"> <li>Default: None</li> <li>Values: An existing certificate configuration element name</li> </ul>
<b>responder-cert</b>	Enter the name of the certificate configuration element used to validate the incoming OCSP response. <ul style="list-style-type: none"> <li>Default: None</li> <li>Values: An existing certificate configuration element name</li> </ul>
<b>realm-id</b>	Enter the name of the realm used for transmitting OCSP requests. This parameter is optional. <ul style="list-style-type: none"> <li>Default: wancom</li> <li>Values: Any valid realm name</li> </ul>
<b>retry-count</b>	Enter the maximum number of times to retry an OCSP responder in the event of connection failure. <ul style="list-style-type: none"> <li>Default: 1</li> </ul>

- Values: Min: 0/Max: 10

**dead-time** Enter the interval (in seconds) between the trigger of the retry-count(er) and the next attempt to access the unavailable OCSP responder. This parameter is optional.

- Default: 0 (seconds)
- Values: Min: 0/Max: 3600

### Path

**cert-status-profile** is a subelement under the security configuration element. The full path from the topmost ACLI prompt is: **configure-terminal > security > cert-status-profile**.

### Release

First appearance: S-C6.2.0

### RTC Status

Supported



**Note:** This is a multiple instance configuration.

## class-profile

---

The class-profile configuration element lets you access the class-policy configuration element for creating classification policies for ToS marking for SIP or H.323.

### Parameters

**policy** Enter the class-policy subelement

### Path

**class-profile** is an element under the session-router path. The full path from the topmost prompt is: **configure terminal > session-router > class-profile**.

### Release

First appearance: 1.3 / Most recent update: 2.0

### RTC Status

Supported

## class-profile > policy

---

The class-policy configuration subelement lets you create classification policies that are used to create a ToS marking on incoming traffic based upon a matching media-policy and destination address.

### Parameters

**profile-name** Enter the classification profile name

**to-address** Enter a list of addresses to match for when determining when to apply this class-policy. Addresses can take the forms:

- Values:
  - +<number>—E164 address
  - <number>—Default address type
  - [<host>].domain—Host and/or domain address

**media-policy** Enter the media-policy used for this class-policy

## Path

**class-policy** is a subelement under the session-router path. The full path from the topmost prompt is: **configure terminal > session-router > class-profile > policy**.

## Release

First appearance: 1.3 / Most recent update: 2.0

## RTC Status

Unavailable

# data-flow

The data-flow configuration element specifies pass-through data-traffic processing when using IKE.

## Parameters

**name** Specify the name of this instance of the data-flow configuration element.

**realm-id** Specify the realm that supports the upstream (core side) data-flow.

**group-size** Specify the maximum number of user elements grouped together by this data-flow instance. For maximum efficiency, this value should be set to a power of 2.

- Default: 128
- Values: 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256



### Note:

The optional group-size parameter specifies the divisor used by this data-flow instance to segment the total address pool into smaller, individually-policed segments.

**upstream-rate** Specify the allocated upstream bandwidth.

- Default: 0 (allocates all available bandwidth)
- Values: Min: 0 / Max: 4294967295

**downstream-rate** Specify the allocated downstream (access side) bandwidth.

- Default: 0 (unlimited, no bandwidth restrictions)
- Values: Min: 0 / Max: 4294967295

## Path

Data-flow is a subelement under the ike element. The full path from the topmost ACLI prompt is: **configure terminal > security > ike > data-flow**.

### First appearance

S-C6.2.0

### RTC Status

Supported



**Note:** This is a multiple instance configuration element.

## dnsgalg-constraints

---

The dnsgalg-constraints configuration element is used to provision various traffic constraints upon existing dns-config configurations.

### Parameters

<b>name</b>	name of the dnsgalg constraint configuration element this value is applied in a dns-config configuration element.
<b>state</b>	State of this dnsgalg-constraint. <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>max-burst-rate</b>	Maximum number of messages that can pass through the system in the burst rate window before setting the element to Constraints Exceeded.
<b>max-inbound-burst-rate</b>	maximum number of inbound messages received by the referencing element within the burst rate window before setting the element to Constraint Exceeded. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: 0-999999</li></ul>
<b>max-outbound-burst-rate</b>	maximum number of outbound messages forwarded from the referencing element within the burst rate window before setting the element to Constraints Exceeded. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: 0-999999</li></ul>
<b>burst-rate-window</b>	Number of seconds during which to count messages toward a maximum burst rate. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: 0-999999</li></ul>
<b>max-sustain-rate</b>	maximum number of messages that can pass through the system in the sustained rate window before setting the element to Constraints Exceeded. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: 0-999999</li></ul>
<b>max-inbound-sustain-rate</b>	maximum number of inbound messages received by the referencing element within the sustained rate before setting the element to Constraints Exceeded. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: 0-999999</li></ul>
<b>max-outbound-sustain-rate</b>	maximum number of outbound messages forwarded from the referencing element within the sustained rate window before setting the element to Constraints Exceeded.



	<ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: 0-999999</li> </ul>
<b>sustain-rate-window</b>	<p>number of seconds during which to count messages toward a maximum sustained rate. a maximum sustained rate.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: 0-999999</li> </ul>
<b>max-latency</b>	<p>The maximum time in seconds a reply to a DNS request can take before considering that DNS server as out of service.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: 0-999999</li> </ul>
<b>time-to-resume</b>	<p>number of seconds that the referencing element stays in Constraints Exceeded state and rejects messages before it returns to service.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: 0-999999</li> </ul>

### Path

Path: **dnsalg-constraints** is a configuration element under the **media-manager** path. The full path from the topmost ACLI prompt is: full path from the topmost ACLI prompt is: **configure terminal > media-manager > dnsalg-constraints**.

### Release

First appearance: S-CX6.4.0

---

## dns-config

---

The dns-config configuration element configures the DNS-ALG on a per-client realm basis.

### Parameters

<b>client-realm</b>	Enter the realm from which DNS queries are received. This value is the name of a configured realm.
<b>description</b>	Describe the dns-alg configuration element
<b>extra-dnsalg-stats</b>	<p>Enables tracking of extra DNS ALG statistics.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• enabled   disabled</li> </ul>
<b>server-dns-attributes</b>	Enter the server-dns-attributes subelement .
<b>constraint-name</b>	Name of the <b>dnsalg-constraints</b> configuration element to apply to this <b>dns-config</b> .
<b>client-address-list</b>	Enter the IP client realm address(es) from which the Oracle Communications Session Border Controller can receive DNS queries. This field is required.

### Path


**dns-config** is a subelement under the media-manager path. The full path from the topmost CLI prompt is: **configure terminal > media-manager > dns-config**.

### Release

First appearance: 1.3

### RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

## dns-config > server-dns-attributes

---

The server-dns-attributes subelement configures DNS servers.

### Parameters

<b>server-realm</b>	Enter the realm from which DNS responses are sent. This value must be the name of a configured realm. This value is required.
<b>domain-suffix</b>	Enter the domain suffixes for which this DNS server attribute list is used. This field is required, and can start with an asterisk or a period.
<b>server-address-list</b>	Enter a list of DNS server IP addresses used for the specified domains. This field is required, and can include multiple entries.
<b>source-address</b>	Enter the source IP address from which the ALG sends queries to the DNS server (i.e., a layer 3/layer 4 source address). This field is required.
<b>source-port</b>	Enter the UDP port number from which the ALG sends queries to the DNS server (i.e., layer 3/layer 4 source address). This value is required. <ul style="list-style-type: none"><li>• Default: 53</li><li>• Values: 1025-65535</li></ul>
<b>transaction-timeout</b>	Enter the number of seconds that the ALG maintains information to map a DNS server response to the appropriate client request. This value is required. <ul style="list-style-type: none"><li>• Default: 10 seconds</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>address-translation</b>	Access the address-translation subelement

### Path

**server-dns-attributes** is a subelement under the dns-config element. The full path from the topmost CLI prompt is: **configure terminal > media-manager > dns-config > server-dns-attributes**.

### Release

First appearance: 1.3

### RTC Status

Supported



**Note:** This is a multiple instance configuration element.

## dns-config > server-dns-attributes > address-translation

The address-translation subelement sets the list of IP address translations and determines how the NAT function for this feature occurs. Multiple entries in this field allow one DNS-ALG network entity to service multiple Oracle Communications Session Border Controllers or multiple sets of addresses.

### Parameters

- server-prefix** Enter the address/prefix returned by the DNS server. The server-prefix is an IP address and number of bits in slash notation.
- client-prefix** Enter the address/prefix to which a response is returned. The client-prefix is an IP address and number of bits in slash notation.

### Path

**address-translation** is a sub-subelement of the media-manager element. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > dns-config > server-dns-attributes > address-translation**.

### Release

First appearance: 1.3

### RTC Status

Supported




**Note:** Values specified for the number of bits dictates how much of the IP address will be matched. If the number of bits remains unspecified, then the Oracle Communications Session Border Controller will use all 32 bits for matching. Setting the bits portion after the slash to 0 is the same as omitting it. This is a multiple instance configuration element.

## dpd-params

The dpd-params configuration element enables creation of one or more sets of DPD Protocol parameters.

### Parameters

- name** Enter a unique identifier for this instance of the dpd-params configuration element.
- Default: None
  - Values: Valid configuration element name that is unique within the dpd-params namespace
- max-loop** Set the maximum number of endpoints examined every dpd-time-interval.
- Default: 100
  - Values:
-  **Note:** If CPU workload surpasses the threshold set by max-cpu-limit, the max-loop value is over-ridden by load-max-loop.
- max-endpoints** Set the maximum number of simultaneous DPD Protocol negotiations supported when the CPU is not under load (as specified by the max-cpu-limit property).
- Default: 25

- Values: An integer value, should be greater than load-max-endpoints



**Note:** If CPU workload surpasses the threshold set by max-cpu-limit, the max-endpoints value is over-ridden by load-max-endpoints.

**max-cpu-limit** Set a threshold value (expressed as a percentage of CPU capacity) at which DPD protocol operations are minimized to conserve CPU resources.

- Default: 60 percent
- Values: An integer value, 0 (effectively disabling DPD) through 100

**load-max-loop** Set the maximum number of endpoints examined every dpdtime-interval when the CPU is under load, as specified by the max-cpu-limit parameter.

- Default: 40
- Values: an integer value, should be less than max-loop

**load-max-endpoints** Set the maximum number of simultaneous DPD Protocol negotiations supported when the CPU is under load, as specified by the max-cpulimit property.

- Default: 5
- Values: An integer value, should be less than max-endpoints

### Path

dpd-params is a subelement under the ike element. The full-path from the topmost ACLI prompt is: **configure-terminal > security > ike > dpd-params**.

### Release

First appearance: S-C6.2.0

### RTC Status

Supported



**Note:** This is a multiple instance configuration element.

## enforcement-profile

---

The enforcement-profile sets groups of SIP methods to apply in the global SIP configuration, a SIP interface, a SIP session agent, or a realm.

### Parameters

<b>name</b>	Enter the name of the ENUM configuration
<b>allowed-methods</b>	Select a list of SIP methods that you want to allow in this set. <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: INVITE, REGISTER, PRACK, OPTIONS, INFO, SUBSCRIBE, NOTIFY, REFER, UPDATE, MESSAGE, PUBLISH</li></ul>
<b>sdp-address-check</b>	Enable or disable SDP address checking on the Oracle Communications Session Border Controller. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>

<b>add-certificate-info</b>	list of one or more certificate attribute names to enable TLS certificate information caching and insertion of cached certificate information into a customized SIP INVITES. This list is entered enclosed in quotes with attributes separated by spaces.
<b>certificate-ruri-check</b>	<p>Sets Oracle Communications Session Border Controller to cache TLS certificate information and use it to validate Request-URIs.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>

## Path

**enforcement-profile** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > enforcement-profile**.

## Release

First appearance: 5.1, Last updated: S-C6.2.0

## RTC Status

Supported

---

## enforcement-profile > subscribe-event

---

The subscribe-event subelement defines subscription event limits for SIP per-user dialogs.

## Parameters

<b>name</b>	Enter a name for this enforcement profile.
<b>event-type</b>	Enter the SIP subscription event type for which to set up limits. You can wildcard this value (meaning that this limit is applied to all event types except the others specifically configured in this enforcement profile). To use the wildcard, enter an asterisk (*) for the parameter value.
<b>max-subscriptions</b>	<p>Enter the maximum number of subscriptions allowed</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 65535</li> </ul>

## Path

**subscribe-event** is a subelement under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > enforcement-profile > subscribe-event**.

## Release

First appearance: S-C6.1.0

## RTC Status

Supported

---

## enum-config

---

The enum-config is used to configure ENUM functionality on your Oracle Communications Session Border Controller.

### Parameters

<b>name</b>	Enter the name of the ENUM configuration
<b>top-level-domain</b>	Enter the domain extension used to query the ENUM servers for this configuration. The query name is a concatenation of the number and the domain.
<b>realm-id</b>	Enter the realm-id is used to determine on which network interface to issue an ENUM query.
<b>enum-servers</b>	Enter the name of an ENUM server and its corresponding redundant servers to be queried. In a query, separate each server address with a space and enclose list within parentheses.
<b>service-type</b>	<p>Enter the ENUM service types you want supported in this ENUM configuration. Possible entries are E2U+sip and sip+E2U (the default), and the types outlines in RFCs 2916 and 3721. If you add to the pre-existing E2U+sip and sip+E2U list and want those values to remain, you must enter them with your new values.</p> <ul style="list-style-type: none"><li>• Default: E2U+sip,sip+E2U</li></ul>
<b>query-method</b>	<p>Enter the ENUM query distribution strategy</p> <ul style="list-style-type: none"><li>• Default: hunt</li><li>• Values: hunt   round-robin</li></ul>
<b>timeout</b>	<p>Enter the total time, in seconds, that should elapse before a query sent to a server (and its retransmissions) will timeout. If the first query times out, the next server is queried and the same timeout is applied. This process continues until all the servers in the list have timed out or one of the servers responds. The retransmission of ENUM queries is controlled by three timers:</p> <ul style="list-style-type: none"><li>• Values:<ul style="list-style-type: none"><li>• Init-timer—The initial retransmission interval. The minimum value allowed for this timer is 250 milliseconds.</li><li>• Max-timer—The maximum retransmission interval. The interval is doubled after every retransmission. If the resulting retransmission interval is greater than the value of max-timer, it is set to the max-timer value.</li><li>• Expire-timer—The query expiration timer. If a response is not received for a query and its retransmissions within this interval, the server will be considered non-responsive and the next server in the list will be tried.</li></ul></li></ul>
<b>cache-inactivity-timer</b>	<p>Enter the time interval, in seconds, after which you want cache entries created by ENUM requests deleted, if inactive for this interval. If the cache entry gets a hit, the timer restarts and the algorithm is continued until the cache entry reaches its actual time to live.</p> <ul style="list-style-type: none"><li>• Default: 3600</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>lookup-length</b>	<p>Specify the length of the ENUM query, starting from the most significant bit</p> <ul style="list-style-type: none"><li>• Values: Min: 0 / Max: 255</li></ul>
<b>max-response-size</b>	<p>Set the maximum size in bytes for UDP datagram responses.</p> <ul style="list-style-type: none"><li>• Default: 512</li></ul>
<b>health-query-number</b>	Enter the phone number for the ENUM server health query; when this parameter is blank the feature is disabled.
<b>health-query-interval</b>	<p>Enter the interval in seconds at which you want to query ENUM server health.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 65535</li></ul>
<b>failover-to</b>	Enter the name of the enum-config to which you want to failover.

<b>cache-addl-records</b>	<p>Set this parameter to enabled to add additional records received in an ENUM query to the local DNS cache.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>include-source-info</b>	<p>Set this parameter to enabled to send source URI information to the ENUM server with any ENUM queries.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>recursive-query</b>	<p>Enables the Oracle Communications Session Border Controller to query a DNS server for a hostname returned in an ENUM result.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>retarget-requests</b>	<p>When set to enabled, the Oracle Communications Session Border Controller replaces the Request-URI in the outgoing request. When set to disabled, the Oracle Communications Session Border Controller routes the request by looking to the Route header to determine where to send the message.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>

### Path

**enum-config** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > enum-config**.

### Release

First appearance: 2.1.1/ Most recent update: S-C6.3.0

### RTC Status

Supported

---

## ext-policy-server

The ext-policy-server is used for configuring PDP/RACF or CLF functionality on the Oracle Communications Session Border Controller.

### Parameters

<b>name</b>	Enter the name of this external policy server configuration
<b>state</b>	<p>Enable or disable the operational state of this external policy server configuration</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>operation-type</b>	<p>Select the function this external policy server performs</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values:</li> </ul>

	<ul style="list-style-type: none"><li>• disabled</li><li>• admission-control—Oracle Communications Session Border Controller communicates with a CLF to obtain location string</li><li>• bandwidth-mgmt— Oracle Communications Session Border Controller acts as a PEP in a PDP/RACF deployment</li></ul>
<b>protocol</b>	<p>Select the external policy server communication protocol</p> <ul style="list-style-type: none"><li>• Default: C-SOAP</li><li>• Values:<ul style="list-style-type: none"><li>• COPS—Standard COPS implementation. COPS client type is 0x7929 for CLF, and 0x7926 for PDP/RACF usage as defined in the operation-type parameter.</li><li>• A-COPS—Vendor specific protocol. COPS client type is 0x4AC0 for admission-control operation-type.</li><li>• SOAP—Not used</li><li>• C-SOAP—Not used</li><li>• DIAMETER—Connects the Oracle Communications Session Border Controller to the policy-server</li></ul></li></ul>
<b>address</b>	<p>Enter the IP address of external policy server</p>
<b>port</b>	<p>Enter the port on the external policy server to connect to for COPS messages. The standard port for COPS is 3288.</p> <ul style="list-style-type: none"><li>• Default: 80</li><li>• Values: Valid Range: 0-65535</li></ul>
<b>realm</b>	<p>Enter the realm where the external policy server exists</p>
<b>num-connections</b>	<p>Enter the number of TCP connections to external policy server</p> <ul style="list-style-type: none"><li>• Default: 1</li><li>• Values: Min: 0 / Max: 65535</li></ul>
<b>reserve-incomplete</b>	<p>Enable or disable admission requests being made before all of the details of the call are known</p> <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values:<ul style="list-style-type: none"><li>• Enabled—Supports the usual behavior when the AAR is sent upon SDP offer as well as SDP answer. This mode ensures backwards compatibility with releases prior to Release S-C6.1.0.</li><li>• Orig-realm-only—Allows calls originating from a realm with a policy server associated with it to send the AAR upon SDP offer; calls terminating at a realm with a policy server associated with it send the AAR post SDP exchange.</li><li>• Disabled—Allows no bandwidth reservation for incomplete flows.</li></ul></li></ul>
<b>permit-conn-down</b>	<p>Enable or disable the Oracle Communications Session Border Controller's ability to permit calls if there is no connection to the external policy server.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>permit-on-reject</b>	<p>Change this parameter to enabled if you want the Oracle Communications Session Border Controller to forward the session on at a "best-effort". Leave this parameter set to disabled (Default), if you want the Oracle Communications Session Border Controller to deny the session on attempts to revert to the previously-requested bandwidth</p> <ul style="list-style-type: none"><li>• Default: disabled</li></ul>



	<ul style="list-style-type: none"> <li>Values: enabled   disabled</li> </ul>
<b>permit-on-reject</b>	<p>Change this parameter to enabled if you want the Oracle Communications Session Border Controller to forward the session on at a “best-effort”. Leave this parameter set to disabled (default), if you want the Oracle Communications Session Border Controller to deny the session on attempts to revert to the previously-requested bandwidth.</p> <ul style="list-style-type: none"> <li>Default: disabled</li> <li>Values: enabled   disabled</li> </ul>
<b>disconnect-on-timeout</b>	<p>Disable this parameter to prevent timeouts triggered by Gate-Set or Gate-Delete message sequences between the Oracle Communications Session Border Controller and a policy server from tearing down their connection. Retaining the default (enabled) allows all timeouts to tear down and re-establish the TCP connection.</p> <ul style="list-style-type: none"> <li>Default: enabled</li> <li>Values: enabled   disabled</li> </ul>
<b>product-name</b>	Enter the vendor product name
<b>application-mode</b>	<p>Select the mode in which the policy server interface is operating</p> <ul style="list-style-type: none"> <li>Default: none</li> <li>Values: Rq   Rx   Gq   e2   pktmm3</li> </ul>
<b>application-id</b>	<p>Enter the application mode of this interface</p> <ul style="list-style-type: none"> <li>Default: 0</li> <li>Values: Min: 0 / Max: 999999999</li> </ul>
<b>framed-ip-addr-encoding</b>	<p>Set the format of the Frame-IP-Address (AVP 8) value in Diameter messages.</p> <ul style="list-style-type: none"> <li>Default: octet-string</li> <li>Values: octet-string (i.e., 0xC0A80A01)   ascii-string (i.e., 192.168.10.1)</li> </ul>
<b>dest-realm-format</b>	<p>Set the format for the Destination-Realm AVP.</p> <ul style="list-style-type: none"> <li>Default: user_with_realm</li> <li>Values: user_with_realm   user_only   realm_only</li> </ul>
<b>ingress-realm-location</b>	<p>Set this parameter to configure the child realm or its parent for the Address-Realm in the Globally-Unique-Address AVL in DIAMETER UDR messages that the Oracle Communications Session Border Controller sends to the policy server.</p> <ul style="list-style-type: none"> <li>Default: realm-in</li> <li>Values: <ul style="list-style-type: none"> <li>realm-in—This setting means that the Oracle Communications Session Border Controller will use the same realm on which the REGISTRATION request arrived.</li> <li>sip-interface—This setting means that the Oracle Communications Session Border Controller will use the realm associated with the SIP interface on which the REGISTRATION request arrived.</li> <li>diam-address-realm - For the e2 interface, this value enables configurable Address-Realm AVPs. This setting points the Oracle Communications Session Border Controller to the associated realm from which it will learn Address-Realm AVP information.</li> </ul> </li> </ul>
<b>user-name-mode</b>	<p>Determines how the User-Name AVP is constructed. Used primarily with e2 based CLF functionality.</p> <ul style="list-style-type: none"> <li>Default: none</li> </ul>

	<ul style="list-style-type: none"><li>• Values:<ul style="list-style-type: none"><li>• none—Net-Net SBC does not include the User-Name AVP in any UDRs</li><li>• endpoint-ip—IP address of the registering endpoint is sent as the payload for the User-Name AVP</li><li>• public-id—SIP-URI portion of the TO header from the register message is sent as the payload for the User-Name AVP</li><li>• auth-user—Username attribute of the Authorization header from the register is sent as the payload for the User-Name AVP; if there is no authorization header, the Net-Net SBC will not consult the CLF and will forward the registration message.</li></ul></li></ul>
<b>domain-name-suffix</b>	<p>Sets the suffix for Origin-Realm and Origin-Host AVPs that have a payload string constructed as a domain name. If your entry does not include the dot, the system prepends one.</p> <ul style="list-style-type: none"><li>• Default: .com</li></ul>
<b>gate-spec-mask</b>	<p>With this parameter, you can configure the Oracle Communications Session Border Controller to use a mask comprised entirely of zeros (0). The default value is 255. This parameter sets the value to use for the COPs pkt-mm-3 interface. This interface maintains a persistent TCP connection to the external policy server, even without responses to requests for bandwidth. This permits calls to traverse the Oracle Communications Session Border Controller even though the external policy server either fails to respond, or rejects the session.</p> <ul style="list-style-type: none"><li>• Default: 255</li><li>• Values: Min: 0 / Max: 255</li></ul>
<b>allow-srv-proxy</b>	<p>Enable this parameter if you want to include the proxy bit in the header. The presense of the proxy bit allows the Oracle Communications Session Border Controller to tell the external policy server whether it wants the main server to handle the Diameter message, or if it is okay to proxy it to another server on the network (disabled)</p> <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>wildcard-trans-protocol</b>	<p>Set this parameter from enabled if you want to use transport protocol wildcarding for Rx/Rq Flow-Description AVP (507) generation. Enabled sends a flow description of “ip”. Set this parameter to disabled if you want to use the specific media stream transport protocol.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>watchdog-ka-timer</b>	<p>Enter the number of seconds to define the interval for watchdog/keep-alive messages; this is the time in which the Oracle Communications Session Border Controller must receive a COPS-KA message from the policy server to ensure collection is still valid.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>include-rtcp-in-request</b>	<p>Change this parameter from disabled (default), to enabled so the Oracle Communications Session Border Controller will include RTCP information in AARs.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>provision-signaling-flow</b>	<p>Enables the Oracle Communications Session Border Controller to send AARs to PCRFs after registration that includes the grouped Media-Component-Description AVP as described in 3GPP TS 29.213 section B1b [1], and the procedures specified in TS 29.214 section 4.4.5a.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>

<b>max-timeouts</b>	max number of request timeouts before the Oracle Communications Session Border Controller sets this external policy server to inactive. <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 200</li> </ul>
<b>max-connections</b>	Number of external policy servers to be monitored as a server cluster <ul style="list-style-type: none"> <li>• Default: 1</li> </ul>
<b>srv-selection-strategy</b>	Strategy used to select an external policy server from the cluster. <ul style="list-style-type: none"> <li>• Default: Failover</li> </ul>
<b>optimize-aar</b>	Reduces the number of ARRs sent to the PCRF. <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>options</b>	Enter any customer-specific features and/or parameters for this external policy server. This parameter is optional.

### Path

**ext-policy-server** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > ext-policy-server**.

### Release

First appearance 4.0 / Last updated: S-CX6.4.0

### RTC Status

Supported

## h323

---

The h323 configuration element is the top level of the H.323 configuration, and it contains h323 parameters that apply globally.

### Parameters

<b>state</b>	Enable or disable H.323 functionality. <ul style="list-style-type: none"> <li>• Default: INFO</li> <li>• Values: EMERGENCY   CRITICAL   MAJOR   MINOR   WARNING   NOTICE   INFO   TRACE   DEBUG</li> </ul>
<b>log-level</b>	Select the log level for monitoring H.323 functionality. This parameter overrides the process-log level field value set in the system-config element only for H.323 functionality. If the state parameter in this element is set to disabled, this parameter still overrides the process-log-level field from the system-config element for H.323. <ul style="list-style-type: none"> <li>• Default: INFO</li> <li>• Values: EMERGENCY   CRITICAL   MAJOR   MINOR   WARNING   NOTICE   INFO   TRACE   DEBUG</li> </ul>
<b>response-tmo</b>	Set the number of seconds Oracle Communications Session Border Controller waits between sending a SETUP message and receiving no response before the call is torn down

	<ul style="list-style-type: none"><li>• Default: 4</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>connect-tmo</b>	Set the number of seconds Oracle Communications Session Border Controller waits between sending out a SETUP message and failing to receive a CONNECT message before the call is torn down. If the Oracle Communications Session Border Controller receives a PROCEEDING or ALERT message from the endpoint, it will tear down the session after this timer elapses if a CONNECT message is not received. <ul style="list-style-type: none"><li>• Default: 32</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>options</b>	Enter customer-specific features and/or parameters that affect H.323 behavior globally. This parameter sets a comma-separated list of “feature=value” or “feature” parameters.
<b>h323-stacks</b>	Enter the h323-stacks subelement.
<b>rfc2833-payload</b>	Enter the payload type used by the H.323 stack in preferred rfc2833-mode <ul style="list-style-type: none"><li>• Default: 101</li><li>• Values: Valid Range: 96-127</li></ul>
<b>alternate-routing</b>	Choose between pre-4.1 or 4.1 behavior: <ul style="list-style-type: none"><li>• Pre-4.0 behavior—Alternate routing is disabled, and the Oracle Communications Session Border Controller sends a release complete message back to the caller, proxy</li><li>• 4.1 behavior—The Oracle Communications Session Border Controller performs alternate routing, recur<ul style="list-style-type: none"><li>• Default: proxy</li><li>• Values: proxy   recur</li></ul></li></ul>
<b>codec-fallback</b>	Enable or disable slow start to fast start codec negotiation. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>enum-sag-match</b>	Enable or disable matching against the hostnames in ENUM/LRT lookup responses and session agent groups <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>remove-t38</b>	Enable or disable the removal of t38 fax capabilities received in a SIP call’s SDP, from the TCS of the outgoing IWF call. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>

### Path

**h323** is an element under the session-router path. The full path from the topmost CLI prompt is: **configure terminal** > **session-router** > **h323**.

### Release

First appearance: 1.2.1 / Most recent update:S-C6.1

### RTC Status

Supported









**Note:** Unlike other single-instance configuration elements, the h323 element does not have to be selected before it can be viewed. The options field does not appear in the output for the show command within the h323 element or for running-config subcommand unless it contains configured values. This is a single instance configuration element.

## h323 > h323-stacks


The h323-stack subelement supports the SFIWF, FSIWF, H.323<—>SIP traffic, and general H.323 functionality.

### Parameters


<b>name</b>	Enter the name of H.323 stack. This value is required and must be unique. The value you enter in this parameter for your H.323 interface (stack) configuration cannot start with a number; it must start with a letter. The Oracle Communications Session Border Controller considers names that start with numbers to be invalid.
<b>description</b>	Provide a brief description of the h323-config configuration element
<b>state</b>	<p>Enable or disable this h323-stack</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>isgateway</b>	<p>Enable or disable H.323 stack functionality as a Gateway. When this field is set to enabled, the H.323 stack runs as a Gateway. When this field is set to disabled, the H.323 stack runs as a Gatekeeper proxy.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>realm-id</b>	<p>Enter the realm served by this H.323 stack. This value must be a valid identifier for a realm configuration.</p> <p> <b>Note:</b> This parameter is not RTC supported</p>
<b>assoc-stack</b>	<p>Enter the name of associated outbound H.323 stack for this h323-stack instance. If not configured, the Oracle Communications Session Border Controller will use policy-based stack selection based on a local policy (configured in a local-policy element). If you wish to use static stack selection, then each configured h323-stack subelement must have an associated outbound stack. This parameter must correspond to a valid name field value in another instance of the h323-stack subelement.</p> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>local-ip</b>	<p>Enter the IP address H.323 stack uses when opening sockets. This field value is the default H.323 stack address.</p> <ul style="list-style-type: none"> <li>• Default: 0.0.0.0</li> </ul> <p> <b>Note:</b> This command is not RTC supported</p>
<b>max-calls</b>	Enter the maximum number of calls allowed for the network associated with this H.323 stack

- Default: 200
  - Values: Min: 0 / Max: 4294967295
-  **Note:** This command is not RTC supported.


**max-channels** Enter the maximum number of concurrent channels (or pathways used between nodes) allowed for each call associated with this H.323 stack

- Default: 6
  - Values: Min: 0 / Max: 4294967295
-  **Note:** This command is not RTC supported.


**registration-ttl** Enter the TTL in seconds before a registration becomes invalid. During the initial registration process, after a registration is confirmed, the TTL value set by the Gatekeeper in the RCF message will override this field value. This field is only applicable when the h323-stack:isgateway field is set to enabled.

- Default: 120
  - Values: Min: 0 / Max: 4294967295
-  **Note:** This command is not RTC supported.


**terminal-alias** Enter a list of alias addresses that identify the H.323 stack terminal. This field value must be entered as a space-separated type=value string (e.g., h323-ID=acme01). This field is only applicable when the isgateway field is set to enabled.

- Values: h323-ID | e164 | url | email | ipAddress
-  **Note:** This command is not RTC supported.

**ras-port** Select a listening port number for RAS requests. When this field value is 0, H.323 stack uses port assigned by the operating system and not the well-known port 1719.

- Default: 1719
  - Values: Min: 0, Max: 65535
-  **Note:** This command is not RTC supported.







**auto-gk-discovery** Enable or disable Automatic Gatekeeper discovery feature upon start-up. This field is applicable only when h323-stack:isgateway field is enabled.




- Default: disabled
  - Values: enabled | disabled
-  **Note:** This parameter is not RTC supported.

**multicast** Enter the multicast address and port of the RAS Multicast IP Group used for automatic gatekeeper discovery. In order to clear this field, you must enter an empty string by typing a space. 224.0.1.41:1718 is the well known value used to discover the Gatekeeper.


- Default: 0.0.0.0:0
-  **Note:** This parameter is not RTC supported.

**gatekeeper** Enter the IP address and RAS port of the Gatekeeper. In order to clear this field, you must enter an empty string.

	<ul style="list-style-type: none"> <li>• Default: 0.0.0.0:0</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>gk-identifier</b>	<p>Enter the gatekeeper identifier with which the H.323 stack registers</p> <ul style="list-style-type: none"> <li>• Values: 1 to 128 characters</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>q931-port</b>	<p>Enter the Q.931 call signaling port. This is the port for the h323-stack: local-ip address set above.</p> <ul style="list-style-type: none"> <li>• Default: 1720</li> <li>• Values: Min: 0 / Max: 65535</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>alternate-transport</b>	<p>Enter the alternate transport addresses and ports (i.e., the Annex E address(es) and port(s)). If this field is left empty, the H.323 stack will not listen for incoming Annex E requests.</p> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>q931-max-calls</b>	<p>Set the maximum number of concurrent, active calls allowed on the Oracle Communications Session Border Controller. If this field value is exceeded, the H.323 stack returns a state of “busy.”</p> <ul style="list-style-type: none"> <li>• Default: 200</li> <li>• Values: Min: 0 / Max: 65535</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>h245-tunneling</b>	<p>Enable or disable H.245 tunneling supported by this H.323 stack</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>fs-in-first-msg</b>	<p>Enable or disable Fast Start fields sent in the first message in response to a SETUP message that contains Fast Start fields</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>call-start-fast</b>	<p>Enable or disable conversion of an incoming Slow Start call into a Fast Start call. This H.323 stack must be the outgoing stack for conversion to work. If this field is set to disabled, the outgoing call will be set up with the same starting mode as the incoming call. This parameter must take the opposite value as the call-start-slow parameter.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>call-start-slow</b>	<p>Enable or disable conversion of an incoming Fast Start call into a Slow Start call. This H.323 stack must be the outgoing stack for this conversion to work. If this field is set to disabled, the outgoing call will be set up to have the same starting mode as the incoming call. This parameter must take the opposite value as the call-start-slow parameter.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> </ul>

	<ul style="list-style-type: none"><li>• Values: enabled   disabled</li></ul>
<b>media-profiles</b>	Enter a list of media profile names used for the logical channels of the outgoing call. These names are configured in the media-profile element. The media-profiles field value must correspond to a valid name field entry in a media-profile element that has already been configured.
<b>prefixes</b>	<p>Enter a list of supported prefixes for this particular H.323 stack</p> <ul style="list-style-type: none"><li>• Values: e164   url   h323-ID   ipAddress</li></ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>process-registration</b>	<p>Enable or disable registration request processing for this H.323 stack . Oracle Communications Session Border Controller will process any RRQs that arrive on this H.323 stack if enabled. Oracle Communications Session Border Controller will not acknowledge any requests and drop all RRQ if disabled.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>allow-anonymous</b>	<p>Enter the admission control of anonymous connections accepted and processed by this H.323 stack</p> <ul style="list-style-type: none"><li>• Default: all</li><li>• Values:<ul style="list-style-type: none"><li>• all—allow all anonymous connections</li><li>• agents-only—only requests from session agents allowed</li><li>• realm-prefix—session agents and address matching realm prefix</li></ul></li></ul>
<b>options</b>	<p>Enter customer-specific features and/or parameters on a per-stack basis. This parameter sets a comma-separated list of “feature=value” or “feature” parameters. This options field affects H.323 behavior for this particular h323 stack whereas the options field in the main h323 element affects H.323 behavior globally.</p> <p> <b>Note:</b> This command is not RTC supported.</p>
<b>proxy-mode</b>	<p>Select the proxy functionality for signaling only operation</p> <ul style="list-style-type: none"><li>• Values: H225   H245</li></ul> <p> <b>Note:</b> This command is not RTC supported.</p>
<b>h245-stage</b>	<p>Select the H.245 stage at which the Oracle Communications Session Border Controller allows either of the following:</p> <ul style="list-style-type: none"><li>• Transfer of the H.245 address to remote side of the call</li><li>• Acting on the H.245 address sent by the remote side</li><li>• Default: connect</li><li>• Values: setup   proceeding   alerting   connect   early   facility   noh245   dynamic</li></ul>
<b>q931-start-port</b>	<p>Set the starting port number for Q.931 port range used for Q.931 call signalling</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: 0   1024   2048   4096   8192   16384   32768</li></ul>
<b>q931-number-ports</b>	<p>Set the number of ports in Q.931 port range used for the H.323 registration proxy feature</p>



	<ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: 0   1024   2048   4096   8192   16384   32768</li> </ul>
<b>dynamic-start-port</b>	<p>Set the starting port number for Q.931 port range used for the H.323 registration proxy feature</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: 0   1024   2048   4096   8192   16384   32768</li> </ul>
<b>dynamic-number-ports</b>	<p>Enter the number of ports in port range used for dynamic TCP connections the H.323 registration proxy feature</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: 0   1024   2048   4096   8192   16384   32768</li> </ul>
<b>filename</b>	<p>Enter the name of the configuration file used to override the default configuration. H.323 stack configuration is read from the file specified by this field value. The configuration file does not override manually configured values; the configuration uses the values you have configured plus the information that resides in the file. This file resides in &lt;default-dir&gt;/H323CfgFile, where &lt;defaultdir&gt; is usually /ramdrv.</p> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>tcp-keepalive</b>	<p>Enable or disable TCP keepalive processing on call-signaling port</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>rfc2833-mode</b>	<p>Select whether 2833/UII negotiation will be transparent to the Oracle Communications Session Border Controller (pre-4.1 behavior), or use 2833 for DTMF and signal it in its TCS</p> <ul style="list-style-type: none"> <li>• Default: transparent</li> <li>• Values: transparent   preferred</li> </ul>
<b>alarm-threshold</b>	Access the alarm-threshold subelement.

## Path


**h323-stacks** is a subelement under the h323 element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > h323 > h323-stacks**.

## Release

First appearance: 1.2 / Most recent update: S-C6.2.0

## RTC Status

Supported

 **Note:** This is a multiple instance configuration subelement.

## h323 > h323-stacks > alarm-threshold

The alarm-threshold subelement allows you to set a threshold for sending an alarm when the Oracle Communications Session Border Controller approaches the max-calls limit.

### Parameters

- severity** Enter the level of alarm to be configured per port.
- Default: minor
  - Values: minor | major | critical
- value** Set the percentage of the value defined in the max-calls parameter to determine when the Oracle Communications Session Border Controller issues an alarm
- Default: 0
  - Values: Min: 0 | Max: 100

### Path

**alarm-threshold** is a subelement under the h323-stacks subelement. The full path from the topmost ACLI prompt is: **configure terminal > session-router > h323 > h323-stacks > alarm-threshold.**

### Release

First appearance: S-C6.2.0

### RTC Status

Supported

## home-subscriber-server

---

The **home-subscriber-server** element allows you to configure an HSS configuration element with which to exchange information over the Diameter Cx interface.

### Parameters

- name** Name of this home-subscriber-server configuration element.
- state** Running state of this home-subscriber-server configuration element.
- address** IP address of this HSS.
- port** Port to connect to on this HSS.
- Default: 3868
- realm** Realm name in which this HSS exists.
- watchdog-ka-timer** Period of time in seconds that DWRs are sent to this HSS.
- Default: 0 (disabled)
  - Values: Min: 0 / Max: 65535
- add-lookup-parameter** Inserts a P-Acme-Serving header into a message sent into the network. The sender of this message must have been verified by this HSS.
- value** Set the percentage of the value defined in the max-calls parameter to determine when the SBC issues an alarm.

### Path

**home-subscriber-server** is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > home-subscriber-server.**


**Release**

First appearance: S-CX6.4.0

**host-route**

The host-route configuration element establishes routing exceptions on the Oracle Communications Session Border Controller for management traffic.

**Parameters**

- dest-network** Enter the IP address of the destination network for this host route. No two host-route elements can have the same dest-network field value.  
An IPV6 address is valid for this parameter.
- netmask** Enter the destination network subnet mask. The network-interface element will not function properly unless this field value is valid.  
An IPV6 address is valid for this parameter.
- gateway** Enter the gateway used to leave the local network. The gateway field identifies the next hop to use when forwarding a packet out of the originator's LAN.  
 **Note:** The gateway entered must already be defined as a gateway for an existing network interface.  
An IPV6 address is valid for this parameter.
- description** Provide a brief description of this host-route configuration.

**Path**


**host-route** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** > **system** > **host-route**.

**Release**

First appearance: 1.0.1

**RTC Status**

Supported

 **Note:** This is a multiple instance configuration element.

**ike-certificate-profile**

The ike-certificate-profile subelement references a public certificate that authenticates a specific IKEv2 identity, as well as one of more CA certificates used to validate a certificate offered by a remote peer.

**Parameters**

- identity** Enter the local IKEv2 entity that using the authentication and validation credentials provided by this ike-certificate-profile instance.
- Default: None
  - Values: An IP address or fully-qualified domain name (FQDN) that uniquely identifies the user of resources provided by this ike-certificate-profile instance

<b>end-entity-certificate</b>	<p>Enter the unique name of a certificate-record configuration element referencing the identification credential (specifically, an X509.v3 certificate) offered by a local IKEv2 entity in support of its asserted identity.</p> <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: Name of an existing certificate-record configuration element</li></ul>
<b>trusted-ca-certificates</b>	<p>Enter the unique names of one or more certificate-record configuration elements referencing Certification Authority (CA) certificates used to authenticate a remote IKEv2 peer.</p> <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: A comma separated list of existing CA certificate-record configuration elements.</li></ul>
<b>verify-depth</b>	<p>Enter the maximum number of chained certificates that will be processed while authenticating the IKEv2 peer.</p> <ul style="list-style-type: none"><li>• Default: 10</li><li>• Values: Min: 1   Max: 10</li></ul>

### Path

**ike-certificate-profile** is a subelement under the **ike** element. The full path from the topmost ACLI prompt is: **configure-terminal > security > ike > ike-certificate-profile**.

### Release

First appearance: S-C6.2.0

### RTC Status

Supported



**Note:** This is a multiple instance configuration element.





## ike-config

---

The **ike-config** subelement defines a single, global Internet Key Exchange (IKE) configuration object.

### Parameters

<b>state</b>	<p>Enter the state (enabled or disabled) of the <b>ike-config</b> configuration element.</p> <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: disabled   disabled</li></ul>
<b>ike-version</b>	<p>Enter an integer value that specifies IKE version. Select 1 for IKEV1 protocol implementation. Select 2 for IKEV2 protocol implementation.</p> <ul style="list-style-type: none"><li>• Default: 2</li><li>• Values: 1   2</li></ul>
<b>log-level</b>	<p>Enter the IKE log level; events of this level and other events deemed more critical are written to the system log.</p> <ul style="list-style-type: none"><li>• Default: info</li><li>• Values: emergency   critical   major   minor   warning   notice   info   trace   debug   detail</li></ul>

<b>udp-port</b>	<p>Enter the UDP port used for IKEv1 protocol traffic.</p> <ul style="list-style-type: none"> <li>• Default: 500</li> <li>• Values: Min: 1025 / Max: 65535</li> </ul>
<b>negotiation-timeout</b>	<p>Enter the maximum interval between Diffie-Hellman message exchanges.</p> <ul style="list-style-type: none"> <li>• Default: 15 (seconds)</li> <li>• Values: Min: 1 / Max:4294967295 (seconds)</li> </ul> <p> <b>Note:</b> In the event of timer expiration, the IKE initiator must restart the Diffie-Hellman exchange.</p>
<b>event-timeout</b>	<p>Enter the maximum time allowed for the duration of an IKEv1 event, defined as the successful establishment of an IKE or IPsec Security Association (SA).</p> <ul style="list-style-type: none"> <li>• Default: 60 (seconds)</li> <li>• Values: Min: 1 / Max:4294967295 (seconds)</li> </ul> <p> <b>Note:</b> In the event of timer expiration, the IKE initiator must restart the Phase 1 (IKE SA) or Phase 2 (IPsec SA) process.</p>
<b>phase1-mode</b>	<p>Enter the IKE phase 1 exchange mode: aggressive or main.</p> <ul style="list-style-type: none"> <li>• Default: main</li> <li>• Values: <ul style="list-style-type: none"> <li>• aggressive—is less verbose (requiring only three messages), but less secure in providing no identity protection, and less flexible in IKE SA negotiation</li> <li>• main—is more verbose, but provides greater security in that it does not reveal the identity of the IKE peers. Main mode requires six messages (3 requests and corresponding responses) to (1) negotiate the IKE SA, (2) perform a Diffie-Hellman exchange of cryptographic material, and (3) authenticate the remote peer</li> </ul> </li> </ul>
<b>phase1-dh-mode</b>	<p>Enter the Diffie-Hellman group used during IKE phase 1 negotiation.</p> <ul style="list-style-type: none"> <li>• Default: first-supported</li> <li>• Values: <ul style="list-style-type: none"> <li>• dh-group1 — as initiator, propose Diffie-Hellman group 1 (768-bit primes, less secure )</li> <li>• dh-group2 — as initiator, propose Diffie-Hellman group 2 (1024-bit primes, more secure)</li> <li>• first-supported — as responder, use the first supported Diffie-Hellman group proposed by initiator</li> </ul> </li> </ul> <p> <b>Note:</b> Diffie-Hellman groups determine the lengths of the prime numbers exchanged during the symmetric key generation process.</p>
<b>v2-ike-life-secs</b>	<p>Enter the default IKEv2 SA lifetime in seconds.</p> <ul style="list-style-type: none"> <li>• Default: 86400 (24 hours)</li> <li>• Values: Min: 1 / Max: 4294967295 (seconds)</li> </ul> <p> <b>Note:</b> This global default can be over-ridden at the IKEv2 interface level.</p>
<b>v2-ipsec-life-secs</b>	<p>Enter the default IPsec SA lifetime in seconds.</p> <ul style="list-style-type: none"> <li>• Default: 28800 (8 hours)</li> <li>• Values: Min: 1 / Max:4294967295 (seconds)</li> </ul>



**Note:** This global default can be over-ridden at the IKEv2 interface level.

**phase1-life-seconds** Set the time (in seconds) proposed for IKE SA expiration during IKE Phase 1 negotiations.

- Default: 3600 (1 hour)
- Values: Min: 1 / Max: 4294967295 (seconds)



**Note:** Relevant only when the Oracle Communications Session Border Controller is acting in the IKE initiator role.

**phase2-life-seconds** relevant only when the Oracle Communications Session Border Controller is acting in the IKE initiator role, contains the time proposed (in seconds) for IPsec SA expiration during IKE Phase 2 negotiations.

- Default: 28800 (8 hours)
- Values: Min: 1 / Max: 4294967295 (seconds)



**Note:** During IKE Phase 2, the IKE initiator and responder establish the IPsec SA.

**phase2-life-seconds-max** Set the maximum time (in seconds) accepted for IPsec SA expiration during IKE Phase 2 negotiations.

- Default: 86400 (24 hours)
- Values: Min: 1 / Max: 4294967295 (seconds)



**Note:** Relevant only when the Oracle Communications Session Border Controller is acting in the IKE responder role.

**phase2-exchange-mode** Enter the Diffie-Hellman group used during IKE Phase 2 negotiation.

- Default: phase1-group
- Values:
  - dh-group1 — use Diffie-Hellman group 1 (768-bit primes, less secure)
  - dh-group2 — use Diffie-Hellman group 2 (1024-bit primes, more secure)
  - no-forward-secrecy — use the same key as used during Phase 1 negotiation



**Note:** During IKE Phase 2, the IKE initiator and responder establish the IPsec SA.

Diffie-Hellman groups determine the lengths of the prime numbers exchanged during the symmetric key generation process.

**shared-password** Enter the default PSK used during IKE SA authentication.  
This global default can be over-ridden at the IKE interface level.

- Default: None
- Values: A string of ACSII-printable characters no longer than 255 characters (not displayed by the ACLI)

**eap-protocol** Enter the EAP protocol used with IKEv2.

- Default: eap-radius-passthru
- Values: eap-radius-passthru



**Note:** The current software performs EAP operations by a designated RADIUS server or server group; retain the default value.

**addr-assignment** Set the method used to assign addresses in response to an IKEv2 Configuration Payload request.

- Default: local
- Values:
  - local — use local address pool
  - radius-only — obtain local address from RADIUS server
  - radius-local — try RADIUS server first, then local address pool



**Note:** This parameter specifies the source of the returned IP address, and can be over-ridden at the IKE interface level.

<b>eap-bypass-identity</b>	<p>Contains a value specifying whether or not to bypass the EAP (Extensible Authentication Protocol) identity phase</p> <p>EAP, defined in RFC 3748, provides an authentication framework widely used in wireless networks.</p> <p>An Identity exchange is optional within the EAP protocol exchange. Therefore, it is possible to omit the Identity exchange entirely, or to use a method-specific identity exchange once a protected channel has been established.</p> <ul style="list-style-type: none"> <li>• Default: disabled (requires an identity exchange)</li> <li>• Values: disabled   enabled</li> </ul>
<b>red-port</b>	<p>Enter the port number monitored for IKEv2 synchronization messages; used in high-availability environments.</p> <p>The default value (0) effectively disables redundant high-availability configurations. Select a port value other than 0 (for example, 1995) to enable high-availability operations.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 1024 / Max: 65535</li> </ul>
<b>red-max-trans</b>	<p>For HA nodes, set the maximum number of retained IKEv2 synchronization message.</p> <ul style="list-style-type: none"> <li>• Default: 10000 (messages)</li> <li>• Values: Min: 1 / Max: 4294967295 (messages)</li> </ul>
<b>red-sync-start-time</b>	<p>For HA nodes, set the timer value for transitioning from standby to active role — the amount of time (in milliseconds) that a standby device waits for a heartbeat signal from the active device before transitioning to the active role.</p> <ul style="list-style-type: none"> <li>• Default: 5000 (milliseconds)</li> <li>• Values: Min: 1 / Max: 4294967295 (milliseconds)</li> </ul>
<b>red-sync-comp-time</b>	<p>For HA nodes, set the interval between synchronization attempts after the completion of an IKEv2 redundancy check.</p> <ul style="list-style-type: none"> <li>• Default: 1000 (milliseconds)</li> <li>• Values: Min: 1 / Max: 4294967295 (milliseconds)</li> </ul>
<b>dpd-time-interval</b>	<p>Set the maximum period of inactivity (in seconds) before the Dead Peer Detection (DPD) protocol is initiated on a specific endpoint.</p> <p>The default value, 0, disables the DPD protocol; setting this parameter to a non-zero value globally enables the protocol and sets the inactivity timer.</p> <ul style="list-style-type: none"> <li>• Default: 0 (DPD disabled)</li> <li>• Values: Min: 1 / Max: 4294967295 (seconds)</li> </ul>
<b>overload-threshold</b>	<p>Set the percentage of CPU usage that triggers an overload state.</p> <ul style="list-style-type: none"> <li>• Default: 100 (disabling overload processing)</li> </ul>

	<ul style="list-style-type: none"><li>• Values: An integer from 1 to 100, and less than the value of overload-critical-threshold</li></ul>
<b>overload-interval</b>	<p>Set the interval (in seconds) between CPU load measurements while in the overload state.</p> <ul style="list-style-type: none"><li>• Default: 1</li><li>• Values: Min: 0 / Max: 60</li></ul>
<b>overload-action</b>	<p>Select the action to take when the Oracle Communications Session Border Controller (as a Acme Packet SG) CPU enters an overload state. The overload state is reached when CPU usage exceeds the percentage threshold specified by the overload-threshold</p> <ul style="list-style-type: none"><li>• Default: none</li><li>• Values: • drop-new-connection—use to implement call rejection</li><li>• none—use to retain default behavior (no action)</li></ul>
<b>overload-critical-threshold</b>	<p>Set the percentage of CPU usage that triggers a critical overload state. This value must be greater than the value of overload-threshold.</p> <ul style="list-style-type: none"><li>• Default: 100 (disabling overload processing)</li><li>• Values: Min: 0 / Max: 100</li></ul>
<b>overload-critical-interval</b>	<p>Set the interval (in seconds) between CPU load measurements while in the critical overload state.</p> <ul style="list-style-type: none"><li>• Default: shared-password</li><li>• Values: Min: 0 / Max: 60</li></ul>
<b>sd-authentication-method</b>	<p>Select the method used to authenticate the IKEv2 SA. Two authentication methods are supported.</p> <p>This global default can be over-ridden at the IKEv2 interface level.</p> <ul style="list-style-type: none"><li>• Default: shared-password</li><li>• Values:<ul style="list-style-type: none"><li>• certificate—uses an X.509 certificate to digitally sign a block of data</li><li>• shared-password—uses a PSK that is used to calculate a hash over a block of data</li></ul></li></ul>
<b>certificate-profile-id</b>	<p>When sd-authentication-method is certificate , identifies the default ike-certificate-profile configuration element that contains identification and validation credentials required for certificate-based IKEv2 authentication.</p> <ul style="list-style-type: none"><li>• This parameter can be over-ridden at the IKEv2 interface level.</li><li>• Default: None</li><li>• Values: Name of an existing ike-certificate-profile configuration element.</li></ul>

### Path

**ike-config** is a subelement under the ike element. The full path from the topmost ACLI prompt is: **configure-terminal > security > ike > ike-config**.

### Release

First appearance: S-C6.2.0

### RTC Status

Supported








**Note:** This is a single instance configuration element.

## ike-interface

The ike-interface configuration element enables creation of multiple IKE-enabled interfaces.

### Syntax

<b>address</b>	Enter the IPv4 address of a specified IKEv1 interface. <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: Any valid IPv4 address</li> </ul>
<b>realm-id</b>	Enter the name of the realm that contains the IP address assigned to this IKEv1 interface. <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: Name of an existing realm configuration element.</li> </ul>
<b>ike-mode</b>	Select the IKE operational mode. <ul style="list-style-type: none"> <li>• Default: responder</li> <li>• Values: initiator   responder</li> </ul>
<b>local-address-pool</b>	Select a list local address pool from a list of configured local-address-pools.
<b>dpd-params-name</b>	Enter the specific set of DPD operational parameters assigned to this IKEv1 interface (relevant only if the Dead Peer Detection (DPD) Protocol is enabled). <ul style="list-style-type: none"> <li>• Default: None</li> <li>• Values: Name of an existing dpd-params configuration element.</li> </ul>
<b>v2-ike-life-secs</b>	Enter the default IKEv2 SA lifetime in seconds <ul style="list-style-type: none"> <li>• Default: 86400 (24hours)</li> <li>• Values: Min: 1 / Max: 4294967295 (seconds)</li> </ul> <div>  <b>Note:</b> The global default can be over-ridden at the IKEv2 interface level. </div>
<b>v2-ipsec-life-secs</b>	Enter the default IPsec SA lifetime in seconds. <ul style="list-style-type: none"> <li>• Default: 28800 (8 hours)</li> <li>• Values: Min:1 / Max: 2 thirty two -1 (seconds)</li> </ul> <div>  <b>Note:</b> This global default can be over-ridden at the IKEv2 interface level. </div>
<b>shared-password</b>	Enter the interface-specific PSK used during IKE SA authentication. This IKEv1-specific value over-rides the global default value set at the IKE configuration level. <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: a string of ACSII printable characters no longer than 255 characters (not displayed by the ACLI).</li> </ul>
<b>eap-protocol</b>	Enter the EAP protocol used with IKEv2. <ul style="list-style-type: none"> <li>• Default: eap-radius-pssthru</li> <li>• Values: eap-radius-pssthru</li> </ul> <div>  <b>Note:</b> The current software performs EAP operations by a designated RADIUS server or server group; retain the default value. </div>

<b>addr-method</b>	<ul style="list-style-type: none"><li>• Values: radius-only-Use the radius server for the local address   radius-local -Use the radius server first and then try the local address pool   local -Use the local address pool to assign the local address</li></ul>
<b>sd-authentication-method</b>	<p>Enter the allowed Oracle Communications Session Border Controller authentication methods</p> <ul style="list-style-type: none"><li>• Default: none</li><li>• Values: none-Use the authentication method defined in ike-config for this interface   shared-password - Endpoints authenticate the Oracle Communications Session Border Controller using a shared password   certificate-Endpoints authenticate the Oracle Communications Session Border Controller using a certificate</li></ul>
<b>certificate-profile-id-list</b>	Select an IKE certificate profile from a list of configured <b>ike-certificate-profiles</b> .

### Path


**ike-interface** is a subelement under the **ike** element. The full path from the topmost CLI prompt is: **configure terminal > security > ike > ike-interface**.

### Release

First appearance: S-C6.2.0

### RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

## ike-sainfo

---

The ike-sainfo configuration element enables negotiation and establishment of IPsec tunnels.

### Parameters

<b>name</b>	<p>Enter the unique name of this instance of the ike-sainfo configuration element.</p> <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: A valid configuration element name, that is unique within the ike-sainfo namespace</li></ul>
<b>security-protocol</b>	<p>Enter the IPsec security (authentication and encryption) protocols supported by this SA.</p> <ul style="list-style-type: none"><li>• Default: ah</li><li>• Values:<ul style="list-style-type: none"><li>• ah—RFC 4302 authentication services</li><li>• esp—RFC 4303 encryption services</li><li>• esp-auth—RFC 4303 encryption and authentication services</li><li>• esp-null—RFC 4303 encapsulation, lacks encryption — not for production environments</li><li>• auth-algo — Set the authentication algorithms supported by this SA.</li></ul></li></ul>
<b>auth-algo</b>	<p>Set the authentication algorithms supported by this SA.</p> <ul style="list-style-type: none"><li>• Default: any</li></ul>

- Values:
  - ah-Chose any
  - md5-Message Digest algorithm 5
  - sha1-Secure Hash Algorithm

**ipsec-mode** Select the IPsec operational mode. Transport mode provides a secure end-to-end connection between two IP hosts. Tunnel mode provides VPN service where entire IP packets are encapsulated within an outer IP envelope and delivered from source (an IP host) to destination (generally a secure gateway) across an untrusted internet.

- Default: transport
- Values: transport | tunnel

**tunnel-local-addr** Enter the IP address of the local IP interface that terminates the IPsec tunnel (relevant only if the ipsec-mode is tunnel, and otherwise is ignored).

- Default: None
- Values: Any valid local IP address

**tunnel-remote-addr** Enter the IP address of the remote peer or host (relevant only if the ipsec-mode is tunnel, and is otherwise ignored).

- Default: \* (matches all IP addresses)
- Values: Any valid IP address

## Path

**ike-sainfo** is a subelement under the **ike** element. The full path from the topmost ACLI prompt is: **configure terminal > security > ike > ike-sainfo**.

## Release

First appearance: S-C6.2.0

## RTC Status

Supported



**Note:** This is a multiple instance configuration element.

Configures an **ike-sainfo** instance named star.

Default values for auth-algo (any) and encryption-algo (any) provide support for MD5 and SHA1 authentication and AES/3DES encryption. The default value for tunnel-remote-address (\*) matches all IPv4 addresses.

Non-default values specify IPsec tunnel mode running ESP, and identify the local tunnel endpoint.

## ims-aka-profile

The **ims-aka-profile** configuration element establishes supports IP Media Subsystem-Authentication and Key Agreement, defined in 3GPP7 (specifications in TS 33.203 and call flows in TS 24.228).

## Parameters

- |                              |   |
|------------------------------|---|
| <b>name</b>                  | Enter the name for this IMS-AKA profile   |
| <b>protected-server-port</b> | Enter the port number on which the Oracle Communications Session Border Controller receives protected messages; 0 disables the function |

	<ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 1025   Max: 65535</li></ul>
<b>protected-client-port</b>	Enter the port number on which the Oracle Communications Session Border Controller sends out protected messages <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 1025   Max: 65535</li></ul>
<b>encr-alg-list</b>	Enter the list of encryption algorithms <ul style="list-style-type: none"><li>• Values: aes-cbc   des-ede3-cbc   null</li></ul>
<b>auth-alg-list</b>	Enter the list of authentication algorithms <ul style="list-style-type: none"><li>• Default: hmac-sha-1-96</li></ul>

### Path

**ims-aka-profile** is an element under the security path. The full path from the topmost ACLI prompt is: **configure terminal > security > ims-aka-profile**.

### Release

First appearance: S-C6.1.0

### RTC Status

Supported



**Note:** This is a multiple instance configuration element.

## ipsec

---

The ipsec configuration element allows you to configure security policies and security associations on your Oracle Communications Session Border Controller.

### Parameters

<b>security-policy</b>	Enter the security-policy configuration element.
<b>security-association</b>	Enter the security-association configuration element.
<b>ipsec-global-config</b>	Access the ipsec-global-config subelement.

### Path

ipsec is an element of the security path. The full path from the topmost ACLI prompt is: **configure terminal > security > ipsec**.

### Release

First appearance: 5.0

### RTC Status

Supported

## ipsec > ipsec-global-config

The ipsec-global-config subelement allows you to configure establish the parameters governing system-wide IPSec functions and behavior, including IPSec redundancy.

### Parameters

<b>red-ipsec-port</b>	Enter the port on which the Oracle Communications Session Border Controller should listen for redundancy IPSec synchronization messages <ul style="list-style-type: none"> <li>• Default: 1994</li> <li>• Values: Min: 1025 / Max: 65535</li> </ul>
<b>red-max-trans</b>	Enter the maximum number of redundancy transactions to retain on the active <ul style="list-style-type: none"> <li>• Default: 10000</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>red-sync-start-time</b>	Enter the time in milliseconds before the system starts to send redundancy synchronization requests <ul style="list-style-type: none"> <li>• Default: 5000</li> <li>• Min: 0   Max: 999999999</li> </ul>
<b>red-sync-comp-time</b>	Enter the time in milliseconds to define the timeout for subsequent synchronization requests once redundancy synchronization has completed <ul style="list-style-type: none"> <li>• Default: 1000</li> <li>• Min: 0   Max: 999999999</li> </ul>
<b>options</b>	Enter the appropriate option name for the behavior you want to configure

### Path

**security-association** is a subelement of the ipsec path. The full path from the topmost ACLI prompt is: configure terminal > security> ipsec>security-association.

### Release

First appearance S-C6.1.0

### RTC Status



**Note:** This is a single instance configuration element.

## ipsec > security-association

The security-association subelement allows you to configure a security association (SA), the set of rules that define the association between two endpoints or entities that create the secured communication.

### Parameters

<b>manual</b>	Enter the manual subelement where you can manually configure a security association
---------------	---

### Path

security-association is a subelement of the ipsec path. The full path from the topmost ACLI prompt is: **configure terminal > security > ipsec > security-association**.

### Release

First appearance: 5.0

### RTC Status

Supported

## ipsec > security-association > manual

---

The manual subelement is where you manually configure a security association on the Oracle Communications Session Border Controller.

### Parameters

<b>name</b>	Enter the name for this security policy
<b>spi</b>	Set the security parameter index <ul style="list-style-type: none"><li>• Default: 256</li><li>• Values: Min: 256   Max: 2302</li></ul>
<b>network-interface</b>	Enter the network interface and VLAN where this security association applies in the form of: interface_name:VLAN
<b>local-ip-address</b>	Enter the local IP address to match for traffic selectors for this SA
<b>remote-ip-addr</b>	Enter the remote IP address to match for traffic selectors for this SA
<b>local-port</b>	Enter the local port to match for traffic selectors for this SA
<b>remote-port</b>	Enter the remote port to match for traffic selectors for this SA <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 (disabled)   Max: 65535</li></ul>
<b>trans-protocol</b>	Select the transport protocol to match for traffic selectors for this SA <ul style="list-style-type: none"><li>• Default: ALL</li><li>• Values: UDP   TCP   ALL   ICMP</li></ul>
<b>ipsec-protocol</b>	Select the IPsec protocol used for this SA <ul style="list-style-type: none"><li>• Default: esp</li><li>• Values: esp   ah</li></ul>
<b>direction</b>	Set the direction of traffic this security association can apply to <ul style="list-style-type: none"><li>• Default: both</li><li>• Values: in   out   both</li></ul>
<b>ipsec-mode</b>	Select the IPsec mode of this SA <ul style="list-style-type: none"><li>• Default: transport</li><li>• Values: tunnel   transport</li></ul>
<b>auth-algo</b>	Select the IPsec authentication algorithm for this SA

	<ul style="list-style-type: none"> <li>• Default: null</li> <li>• Values: hmac-md5   hmac-sha-1   null</li> </ul>
<b>enrc-algo</b>	Enter the IPsec encryption algorithm for this SA <ul style="list-style-type: none"> <li>• Default: null</li> <li>• Values: des   3des   aes-128-cbc   aes-256-cbc   aes-128-ctr   aes-256-ctr   null</li> </ul>
<b>auth-key</b>	Enter the authentication key for the previously chosen authentication algorithm for this SA
<b>encr-key</b>	Enter the encryption key for the previously chosen encryption algorithm for this SA
<b>aes-ctr-nonce</b>	Enter the AES nonce. This only applies if aes-128-ctr or aes-256-ctr are chosen as your encryption algorithm. <ul style="list-style-type: none"> <li>• Default: 0</li> </ul>
<b>tunnel-mode</b>	Enter the tunnel-mode subelement

### Path

**security-association** is a subelement under the ipsec element. The full path from the topmost CLI prompt is: **configure-terminal > security > ipsec > security-association**

### Release

First appearance: 5.0

### RTC Status

Supported

## ipsec > security-association > tunnel-mode

This configuration element allows you to configure the addresses in the security-association. These addresses represent the external, public addresses of the termination points for the IPSEC tunnel.

### Parameters

<b>local-ip-addr</b>	Enter the local IP address of this tunnel mode profile
<b>remote-ip-addr</b>	Enter the remote IP address of this tunnel mode profile

### Path

**tunnel-mode** is a subelement under the **ipsec>security-association**. The full path from the topmost CLI prompt is: **configure-terminal > security > ipsec > security-association>tunnel-mode**. **configure-terminal > security > ipsec > security-association>tunnel-mode**.

### Release

First appearance: 5.0

### RTC Status



Supported

## ipsec > security-policy


---

This configuration element defines multiple policy instances with each policy defining match criteria and an operational action performed on matching traffic flows.

### Parameters

<b>name</b>	<p>Enter a unique identifier for this security-policy instance.</p> <ul style="list-style-type: none"><li>• Default: none</li><li>• Value: A valid configuration element name that is unique within the security-policy namespace.</li></ul>
<b>network-interface</b>	<p>Enter the unique name of the network-interface supported by this security-policy instance.</p> <p>Identify the network interface by providing the interface name and VLAN ID separated by a colon; for example access:10.</p> <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: Name and VLAN ID of an existing network-interface configuration element.</li></ul>
<b>priority</b>	<p>Set the priority of this security-policy instance, where 0 is the highest priority</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 126</li></ul>
<b>local-ip-addr-match</b>	<p>Enter an IPv4 address; in conjunction with local-ip-mask and local-port-match, this parameter specifies address-based matching criteria for inbound traffic.</p> <p> <b>Note:</b> Specifically, local-ip-addr-match works with local-ip-mask to define a range of inbound IP address subject t this security-policy instance. Using default values for both properties, the security-policy instance matches all IPv4 addresses.</p> <ul style="list-style-type: none"><li>• Default: 0.0.0.0</li><li>• Values: A valid IPv4 address; the special address value, 0.0.0.0 matches all IPv4 addresses.</li></ul>
<b>remote-ip-addr-match</b>	<p>Enter an IPv4 address; in conjunction with remote-ip-mask and remote-port-match specifies address-based matching criteria for outbound traffic.</p> <p> <b>Note:</b> Specifically, remote-ip-addr-match works with remote-ip-mask to define a range of outbound IP addresses subject to this security-policy instance. Using default values for both properties, the security-policy instance matches all IPv4 addresses.</p> <ul style="list-style-type: none"><li>• Default: 0.0.0.0</li><li>• Values: A valid IPV4 address; the special address value, 0.0.0.0 matches all IPv4 addresses.</li></ul>
<b>local-port-match</b>	<p>Enter a port number, or the special value 0; in conjunction with local-ip-addr-match and local-ip-mask, the parameter specifies address-based matching criteria for inbound traffic.</p> <p>The default value disables port-based matching, meaning port numbers are ignored in the default state.</p> <ul style="list-style-type: none"><li>• Default: 0 (disables port-based matching)</li><li>• Values: Min: 0 / Max: 65535</li></ul>
<b>remote-port-match</b>	<p>Enter a port number, or the special value 0; in conjunction with remote-ip-addr-match and remote-ip-mask, this parameter specifies address-based matching criteria for outbound traffic.</p> <p>The default value disables port-based matching, meaning port numbers are ignored in the default state.</p>



	<ul style="list-style-type: none"> <li>• Default: 0 (disables port-based matching)</li> <li>• Values: Min: 0 / Max: 65535</li> </ul>
<b>trans-protocol-match</b>	<p>Select a specified protocol or the special value all that specifies transport-protocol-based matching criteria for inbound and outbound traffic.</p> <p>The default value all matches all supported transport layer protocols</p> <ul style="list-style-type: none"> <li>• Default: all</li> <li>• Values: all   ICMP   SCTP   TCP   UDP</li> </ul>
<b>direction</b>	<p>Select an indicator of the directionality of this security-policy instance.</p> <ul style="list-style-type: none"> <li>• Default: both</li> <li>• Values: both - the policy applies to all traffic.   in - the policy applies only to inbound traffic.   out - the policy applies only to outbound traffic.</li> </ul>
<b>local-ip-mask</b>	<p>Enter an IPv4 address; in conjunction with local-ipaddr-match and local-port-match, this parameter specifies address-based matching criteria for inbound traffic.</p> <p>Specifically, local-ip-addr-match works with local-ip-mask to define a range of inbound IP addresses subject to this security-policy instance matches all IPv4 addresses.</p> <ul style="list-style-type: none"> <li>• Default: 255.255.255.255</li> <li>• Values: A dotted decimal IP address mask.</li> </ul>
<b>remote-ip-mask</b>	<p>Enter an IPv4 address; in conjunction with remote-ip-addr-match and remote-port-match, this parameter specifies address-based matching criteria for outbound traffic.</p> <p>Specifically, remote-ipaddr-match works with remote-ip-mask to define a range of out IP addresses subject to this security-policy instance matches all IPv4 addresses.</p> <ul style="list-style-type: none"> <li>• Default: 255.255.255.255</li> <li>• Values: A valid IPv4 address mask</li> </ul>
<b>action</b>	<p>Select the process of trafficking that conforms to the match criteria specified by this security-policy instance.</p> <ul style="list-style-type: none"> <li>• Default: ipsec</li> <li>• Values: allow-forwards matching traffic but performs no security processing.   discard-discards matching traffic   ipsec-processes matching traffic per configured IPsec properties.</li> </ul>
<b>outbound-sa-fine-grained-mask</b>	<p>not used for IKE operation.</p>
<b>ike-sainfo-name</b>	<p>Enter the name of the <b>ike-sainfo</b> configuration element assigned to this security-policy instance.</p> <ul style="list-style-type: none"> <li>• Default: None</li> <li>• Values: A valid configuration element name that is unique within the ike-sainfo namespace.</li> </ul> <p> <b>Note:</b> The <b>ike-sainfo</b> configuration element identifies the algorithms and protocols available for the establishment of IPsec Security Associations (SA).</p>

## ipsec > security-policy > outbound-sa-fine-grained-mask

This configuration element allows you to configure a fine grained security policy.

### Parameters

<b>local-ip-mask</b>	Enter the local IP address mask <ul style="list-style-type: none"><li>• Default: 255.255.255.255</li></ul>
<b>remote-ip-mask</b>	Enter the remote IP address mask. <ul style="list-style-type: none"><li>• Default: 255.255.255.255</li></ul>
<b>local-port-mask</b>	Enter the local port mask for this security policy. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 65535</li></ul>
<b>remote-port-mask</b>	Enter the remote port mask for this security policy. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 65535</li></ul>
<b>trans-protocol-mask</b>	Enter the transport protocol mask for this security policy <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 255</li></ul>
<b>vlan-mask</b>	Enter the VLAN ID mask <ul style="list-style-type: none"><li>• Default: 0x000</li><li>• Values: 0x000 (disabled)-0xFF</li></ul>

### Path

**outbound-sa-fine-grained-mask** is a subelement under the `ipsec>security-policy` element. The full path from the topmost ACLI prompt is: **configure-terminal > security > ipsec > security-policy > outbound-sa-fine-grained-mask**.

### Release

First appearance: 5.0

### RTC Status

Supported

## iwf-config

---

The `iwf-config` element enables the H.323—SIP interworking (IWF) and provides a list of media profiles to use when IWF translations occur.

### Parameters

<b>state</b>	Enable or disable the Oracle Communications Session Border Controller's IWF <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>media-profiles</b>	Set the default media SDP profiles that Oracle Communications Session Border Controller uses for Slow Start IWF calls. This field does not have a relationship with the <code>media-profiles</code> field found in the <code>h323-stack</code> subelement, as the values configured there affect calls that take place entirely in H.323. This list must be populated with the SDP codec names.

- Values: • PCMU | PCMA | G722 | G723 | G726-32 | G728 | G729 | H261 | H263

**logging** Enable or disable IWF-related SIP messages logging

- Default: disabled
- Values: enabled | disabled

**add-reason-hdr** Enable or disable adding the Reason header to IWF calls

- Default: disabled
- Values: enabled | disabled

## Path

**iwf-config** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > iwf-config**.

## Release

First appearance: 1.2.1

## RTC Status

Supported



**Note:** This is a single instance configuration element.

# license

The license configuration element is used for configuring Oracle Communications Session Border Controller licenses.

## Parameters

**add** Add a license by entering a key obtained from your service representative.

**no** Delete licenses by feature. You are prompted to choose a license for deletion based on license features.

## Path

**licenses** is an element under the system-config path. The full path from the topmost ACLI prompt is: **configure terminal > system > license**.

## Release

First appearance: 2.0

## RTC Status

Supported

# local-address-pool

The local-address-pool configuration element enables creation of local address pools, which can be used to provide a local (internal) address in response to remote requests for IP addresses.

### Parameters

<b>name</b>	Enter a unique identifier for this local-address-pool instance. <ul style="list-style-type: none"><li>• Default None</li><li>• Values A valid configuration element name that is unique within the local-address-pool namespace.</li></ul>
<b>address-range</b>	Access the address-range subelement.
<b>dns-realm-id</b>	Enter a DNS realm that supports this local-address-pool instance. <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: Name of an existing dns-realm configuration element.</li></ul>
<b>data-flow-list</b>	Enter a data-flow configuration element assigned to this local-address-pool instance. This parameter specifies bandwidth available to the pool of addresses specified by this local-address-pool instance. <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: Name of an existing data-flow configuration element local-address-pool is a subelement under the ike element. The full path from the topmost ACLI prompt is: <b>configure&gt;terminal&gt;security&gt;ike&gt;local-address-pool.</b></li></ul>

### Path


**local-address-pool** is a subelement under the ike element. The full path from the topmost ACLI prompt is: **configure terminal > security > ike > local-address-pool**

### Release

First appearance: S-C6.2.0

### RTC Status

S-C6.2.0

 **Note:** This is a multiple instance configuration element.

---

## local-address-pool > address-range

---

The address-range configuration element specifies a single range of contiguous IPv4 addresses that are available to fulfill remote requests for a local address.

### Parameters

<b>network-address</b>	In conjunction with this parameter defines a range of IPv4 addresses available for dynamic assignment. <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: A valid IPv4 network address.</li></ul>
<b>subnet-mask</b>	In conjunction with network-address, the parameter defines a range of IPv4 addresses available for dynamic assignment. <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: A valid IPv4 subnet mask</li></ul>

**Path**

**local-address-pool** > **address-range** is a subelement under the **ike** element. The full path from the topmost ACLI prompt: **configure-terminal** > **security** > **ike** > **local-address-pool** > **address-range**.

**Release**

First appearance: S-C6.2.0

**RTC Status**

Supported



**Note:** This is a multiple instance configuration.

## local-policy

---

The local-policy configuration element determines where session signaling messages are routed and/or forwarded.

**Parameters**

- |                        |   |
|------------------------|---|
| <b>from-address</b>    | Enter the source IP address, POTS number, E.164 number, or hostname for the local-policy element. At least one address must be set within this list, but it can include as many addresses as necessary. This parameter may be wildcarded, or entered with a DS: prefix (dialed string).<br>An IPv6 address is valid for this parameter.                                     |
| <b>to-address</b>      | Enter the destination IP address, POTS number, E.164 number, or hostname for the local-policy element. At least one address must be set within this list, but it can include as many addresses as necessary. This parameter may be wildcarded.<br>An IPv6 address is valid for this parameter.  |
| <b>source-realm</b>    | Enter the realms used to determine how to route traffic. This list identifies incoming traffic on a realm and is used for routing by ingress realm via the local policy element. Source-realm entries must be a valid realm.<br><ul style="list-style-type: none"><li>• Default: *</li></ul>  |
| <b>description</b>     | Provide a brief description of the local-policy configuration element   |
| <b>activate-time</b>   | Set the time when selected local-policy becomes valid<br>activate-time yyyy-mm-dd hh:mm:ss.zzz<br>y=year; m=month; d=day h=hour (24-hour clock) m=minute; s=second; z=millisecond   |
| <b>deactivate-time</b> | Set the time when selected local-policy becomes invalid<br>deactivate-time yyyy-mm-dd hh:mm:ss.zzz<br>y=year; m=month; d=day h=hour (24-hour clock) m=minute; s=second; z=millisecond   |
| <b>state</b>           | Enable or disable the local-policy element<br><ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>   |
| <b>policy-priority</b> | Set the policy priority parameter for this local policy. It is used to facilitate emergency sessions from unregistered endpoints. This value is compared against a policy priority parameter in a SIP interface configuration element.<br><ul style="list-style-type: none"><li>• Default: none</li><li>• Values: none   normal   non-urgent   urgent   emergency</li></ul> |

### Path


**local-policy** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > local-policy**.

### Release

First appearance: 1.0 / Most recent update: 1.2.1

### RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

## local-policy > policy-attributes

---

The policy-attributes subelement in conjunction with local-policy make routing decisions for the session based on the next-hop field value.

### Parameters

<b>next-hop</b>	<p>Enter the next signaling host IP address, SAG, hostname, or ENUM config; ENUM is also an accepted value. You can use the following as next-hops:</p> <ul style="list-style-type: none"><li>• IPv4 address or IPv6 address of a specific endpoint</li><li>• Hostname or IPv4 address or IPv6 address of a configured session agent</li><li>• Group name of a configured session agent group</li></ul> <p>The group name of a configured session agent group must be prefixed with SAG: For example:</p> <ul style="list-style-type: none"><li>• policy-attribute: next-hop SAG:appserver</li><li>• policy-attribute: next-hop lrt:routetable</li><li>• policy-attribute: next-hop enum:lrg</li></ul>
<b>realm</b>	<p>Enter the egress realm, or the realm of the next hop. If traffic is routed using the local policy, and the selected route entry identifies an egress realm, then this realm field value will take precedence. This value must be a valid entry in a realm configuration.</p>
<b>action</b>	<p>Set this parameter to redirect if you want to send a redirect next-hop message back to the calling party with the information in the Contact. The calling party then needs to send an INVITE using that information.</p> <ul style="list-style-type: none"><li>• Default: none</li><li>• Values:<ul style="list-style-type: none"><li>• none—No specific action requested</li><li>• replace-uri—To replace the Request-URI with the next hop</li><li>• redirect—To send a redirect response with this next hop as contact</li></ul></li></ul>
<b>carrier</b>	<p>Enter the carrier for this local-policy. Carrier names are arbitrary names used to affect the routing of SIP signaling messages based on their being specified in the local-policy, session-agent, and the sip-config. These carrier names are global in scope, especially if they are exchanged in TRIP.</p>
<b>start-time</b>	<p>Set the time of day these policy attributes considered for preference determination</p> <ul style="list-style-type: none"><li>• Default: 0000</li><li>• Values: Min: 0000   Max: 2400</li></ul>

<b>end-time</b>	<p>Set the time of day these policy attributes cease to be considered for preference determination</p> <ul style="list-style-type: none"> <li>• Default: 2400</li> <li>• Values: Min: 0000   Max: 2400</li> </ul>
<b>days-of-week</b>	<p>Enter the combination of days of the week plus holidays that policy attributes can be considered for preference determination. A holiday entry coincides with a configured holiday. At least one day or holiday must be specified in this field.</p> <ul style="list-style-type: none"> <li>• Default: U-S</li> <li>• Values: <ul style="list-style-type: none"> <li>• U—Sunday</li> <li>• M—Monday</li> <li>• T—Tuesday</li> <li>• W—Wednesday</li> <li>• R—Thursday</li> <li>• F—Friday</li> <li>• S—Saturday</li> <li>• H—Holiday</li> </ul> </li> </ul>
<b>cost</b>	<p>Enter the cost configured for local policy to rank policy attributes. This field represents the cost of a route relative to other routes reaching the same destination address.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>state</b>	<p>Enable or disable these policy attributes as part of the local-policy element</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>app-protocol</b>	<p>Select the signaling protocol used when sending messages to the configured next-hop. When the Oracle Communications Session Border Controller receives an ingress signaling message and uses local policy to determine the message's destination, it will interwork the signaling between protocols (H.323&lt;—&gt;SIP or SIP&lt;—&gt;H.323) if the signaling type does not match the value configured in the app-protocol field.</p> <ul style="list-style-type: none"> <li>• Values: H323   SIP</li> </ul>
<b>media-profiles</b>	<p>Enter the names of media-profile elements related to the policy attribute. Media profiles define a set of media formats that the Oracle Communications Session Border Controller can recognize in SDP. This list does not have to be configured. However, if this list is configured, there can be as many entries within it as necessary.</p>
<b>terminate-recursion</b>	<p>Terminate route recursion with this next hop</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>methods</b>	<p>Enter the SIP methods you want to use for matching this set of policy attributes</p>
<b>lookup</b>	<p>Enable multistage local policy routing, or leave the parameter at the default single for single stage local policy routing.</p> <ul style="list-style-type: none"> <li>• Default: single</li> <li>• Values: single   multi</li> </ul>
<b>next-key</b>	<p>Select the key to use for the next stage of local policy look-up.</p> <ul style="list-style-type: none"> <li>• Values: \$TO   \$FROM   \$PAI</li> </ul>

- eloc-str-lookup** Set this parameter to enabled for the Oracle Communications Session Border Controller to parse the emergency location string, as received in a CLF Line Identifier AVP, for emergency LRT lookup.
- Default: enabled
  - Values: enabled | disabled
- eloc-str-match** Set this parameter to the attribute name found in the location-string whose value will be used as a lookup key in the LRT named in the next-hop parameter.
- Values: <string> string used as key for emergency LRT lookup

### Path

**policy-attributes** is a subelement under the local-policy element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > local-policy > policy-attributes**.

### Release

First appearance: 1.0 / Most recent update: S-C6.1.0

### RTC Status

Supported



**Note:** You must select a local-policy element to which you want to add policy attributes before you enter those elements. If you do not select a local-policy element prior to entering configurations for the policy attributes, your information will be lost. This is a multiple instance configuration element.

## local-response-map

---

The local-response-map configuration element is used for RFC3326 support.

### Parameters

- entries** Enter the entries configuration subelement.
- delete** Remove the specified response map entry type.
- edit** Select a pre- configured RFC 3326 response map for media not allocated

### Path

**local-response-map** is an element under the session router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > local-response-map**.

## local-response-map > entries

---

The entries subelement is used to add a local response map entry for RFC3326 support.

### Parameters

- sip-status** Enter the SIP response code to use for this error
- Values: Min: 100 / Max: 699
- q850-cause** Enter the Q.850 cause code



<b>sip-reason</b>	Enter the SIP response code description
<b>q850-reason</b>	Enter the Q850 cause code description
<b>method</b>	Enter the name of the locally generated SIP failure response message you want to map to a 200 OK. When this parameter is left blank, the SIP registration response mapping feature is turned off.
<b>register-response-expires</b>	Enter the time, in seconds, you want to use for the expires time when mapping the SIP method you identified in the method parameter. <ul style="list-style-type: none"> <li>Values: Min: 0   Max: 999999999</li> </ul>

## Path

**local-response-map-entries** is a subelement under the local-response-map configuration element. The full path from the topmost CLI prompt is: **configure terminal > session-router > local-response-map > local-response-map-entries**.

## Release

First appearance: 4.0

## RTC Status

Supported

# local-routing-config

The local-routing-config element allows you to configure local route tables, giving the Oracle Communications Session Border Controller the ability to determine next hops and map E.164 to SIP URIs locally, providing extensive flexibility for routing.

Note: Entering XML comments on the same line as LRT XML data is not currently supported.

## Parameters

<b>name</b>	Enter a unique identifier for the local route table. This is the name you use to refer to this local route table when you configure policy attributes. This is a required parameter.
<b>filename</b>	Enter the name for the file from which the database corresponding to this local route table is created. You should use the <b>.gz</b> format, and the file should be placed in the <b>/code/lrt/</b> directory. This is a required parameter.
<b>prefix-length</b>	Enter the number of significant digits/bits to be used for lookup and cache storage. <ul style="list-style-type: none"> <li>Default: 0</li> <li>Value: Min:0   Max 999999999</li> </ul>
<b>string-lookup</b>	Sets the Oracle Communications Session Border Controller to perform LRT lookups on table keys of a string data type. Leave this parameter to its default as disabled to continue using E.164 type lookups. <ul style="list-style-type: none"> <li>Default disabled</li> </ul>
<b>retarget-requests</b>	When set to enabled, the Oracle Communications Session Border Controller replaces the Request-URI in the outgoing request. When set to disabled, the Oracle Communications Session Border Controller routes the request by looking to the Route header to determine where to send the message. <ul style="list-style-type: none"> <li>Default: enabled</li> </ul>

<b>match-mode</b>	Determines how the Oracle Communications Session Border Controller makes amongst LRT entries. <ul style="list-style-type: none"><li>• Default: exact</li><li>• Values:<ul style="list-style-type: none"><li>• exact-When searching the applicable LRT, the search and table keys must be an exact match.</li><li>• best-The longest matching table key in the LRT is the chosen match.</li><li>• all-The all mode makes partial matches where the table's key value is a prefix of the lookup key. For example, a lookup in the following table with a key of 123456 returns entries 1, 2, and 4. The 'all' mode incurs a performance penalty because it performs multiple searches of the tables with continually shortened lookup keys to find all matching entries. This mode also returns any exact matches too.</li></ul></li></ul>
-------------------	--

### Path

**local-routing-config** is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > local-routing-config**.

### Release

First appearance: 4.1.1

### RTC Status

Supported

## media-manager-config





---


This media-manager-config element defines parameters used in the media steering functions performed by the Oracle Communications Session Border Controller including the flow timers.


### Parameters

<b>state</b>	Enable or disable media management functionality <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>latching</b>	Enable or disable the Oracle Communications Session Border Controller obtaining the source of the first packet received for a dynamic flow. This parameter is only applicable to dynamic flows. If packet source is unresolved, but Oracle Communications Session Border Controller expects a packet, it will use newly arrived packet's source address if latching is enabled. All subsequent packets for the dynamic flow must come from the "latched" source address; otherwise, the packets are dropped. <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>flow-time-limit</b>	Enter the total time limit in seconds for the flow. The Oracle Communications Session Border Controller notifies the signaling application when this time limit is exceeded. This field is only applicable to dynamic flows. A value of 0 seconds disables this function and allows the flow to continue indefinitely. <ul style="list-style-type: none"><li>• Default: 86400</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>initial-guard-timer</b>	Enter the time in seconds allowed to elapse before first packet of a flow arrives. If first packet does not arrive within this time limit, Oracle Communications Session Border Controller notifies

	<p>the signaling application. This field is only applicable to dynamic flows. A value of 0 seconds indicates that no flow guard processing is required for the flow and disables this function.</p> <ul style="list-style-type: none"> <li>• Default: 300</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>subsq-guard-timer</b>	<p>Enter the maximum time in seconds allowed to elapse between packets in a flow. The Oracle Communications Session Border Controller notifies the signaling application if this timer is exceeded. This field is only applicable to dynamic flows. A field value of zero seconds means that no flow guard processing is required for the flow and disables this function.</p> <ul style="list-style-type: none"> <li>• Default: 300</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>tcp-flow-time-limit</b>	<p>Enter the maximum time in seconds that a media-over-TCP flow can last</p> <ul style="list-style-type: none"> <li>• Default: 86400</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>tcp-initial-guard-timer</b>	<p>Enter the maximum time in seconds allowed to elapse between the initial SYN packet and the next packet in a media-over-TCP flow</p> <ul style="list-style-type: none"> <li>• Default: 300</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>tcp-subsq-guard-timer</b>	<p>Enter the maximum time in seconds allowed to elapse between all subsequent sequential media-over-TCP packets</p> <ul style="list-style-type: none"> <li>• Default: 300</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>tcp-number-of-ports-per-flow</b>	<p>Enter the number of ports, inclusive of the server port, to use for media over TCP. The total number of supported flows is this value minus one.</p> <ul style="list-style-type: none"> <li>• Default: 2</li> <li>• Values: Min: 2 / Max: 5</li> </ul>
<b>hnt-rtcp</b>	<p>Enable or disable support of RTCP when the Oracle Communications Session Border Controller performs HNT. If disabled, the Oracle Communications Session Border Controller will only do RTP for endpoints behind a NAT. If enabled, the Oracle Communications Session Border Controller will add a separate CAM entry for the RTCP flow so that it can send the RTCP back to the endpoint behind the NAT.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>algd-log-level</b>	<p>Select the log level for the MGCP process</p> <ul style="list-style-type: none"> <li>• Default: notice</li> <li>• Values: <ul style="list-style-type: none"> <li>• emergency</li> <li>• critical</li> <li>• major</li> <li>• minor</li> <li>• warning</li> <li>• notice</li> <li>• info</li> <li>• trace</li> </ul> </li> </ul>

	<ul style="list-style-type: none"><li>• debug</li><li>• detail</li></ul>
<b>mbcd-log-level</b>	<p>Select the log level for the MBCD process</p> <ul style="list-style-type: none"><li>• Default: notice</li><li>• Values:<ul style="list-style-type: none"><li>• notice</li><li>• emergency</li><li>• critical</li><li>• major</li><li>• minor</li><li>• warning</li><li>• notice</li><li>• info</li><li>• trace</li><li>• debug</li><li>• detail</li></ul></li></ul>
<b>red-flow-port</b>	<p>Enter the number of the port for checkpointing media flows associated with the HA interface. Setting the red-flow-port value to 0 disables media flow HA.</p> <ul style="list-style-type: none"><li>• Default: 1985</li><li>• Values: Min: 1025 / Max: 65535</li></ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>red-mgcp-port</b>	<p>Enter the number of the port for checkpointing MGCP signaling associated with the HA interface. Setting the red-mgcp-port value to 0 disables MGCP HA.</p> <ul style="list-style-type: none"><li>• Default: 1986</li><li>• Values: Min: 1025 / Max: 65535</li></ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>red-max-trans</b>	<p>Set the size of media flow and MGCP signaling transaction lists (i.e., Number of media flow or MGCP signaling transactions to store in memory at a time)</p> <ul style="list-style-type: none"><li>• Default: 10000</li><li>• Values: Min: 0 / Max: 999999999</li></ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>red-sync-start-time</b>	<p>Enter the time in milliseconds before this HA Oracle Communications Session Border Controller should start media flow or MGCP signaling state checkpointing. This timer begins immediately upon entering the Active state. After the timer expires, the HA Oracle Communications Session Border Controller checks to see if it is still active. If this Oracle Communications Session Border Controller is no longer active and becomes standby, it needs to checkpoint with its HA Oracle Communications Session Border Controller peer, now the active Oracle Communications Session Border Controller peer.</p> <ul style="list-style-type: none"><li>• Default: 5000</li><li>• Values: Min: 0 / Max: 999999999</li></ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>

<b>red-sync-comp-time</b>	<p>Enter the time in milliseconds that this standby Oracle Communications Session Border Controller waits before checkpointing again with the active Oracle Communications Session Border Controller to obtain the latest media flow and/or MGCP signaling transaction information once the initial checkpointing process is complete</p> <ul style="list-style-type: none"> <li>• Default: 1000</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>media-policing</b>	<p>Enable or disable the media policing feature</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>max-signaling-bandwidth</b>	<p>Enter the maximum signaling bandwidth allowed to the host-path in bytes per second</p> <ul style="list-style-type: none"> <li>• Default: 1000000</li> <li>• Values: Min: 71000 / Max: 10000000</li> </ul>
<b>app-signaling-bandwidth</b>	<p>Select the percentage of the untrusted bandwidth reserved for specific application messages. Currently the only supported application message is RSIP for MGCP and NCS.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 1 / Max: 100</li> </ul>
<b>tolerance-window</b>	<p>Enter the tolerance window size in seconds used to measure host access limits</p> <ul style="list-style-type: none"> <li>• Default: 30</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>trap-on-demote-to-deny</b>	<p>Enable or disable the Oracle Communications Session Border Controller to send a trap in the event of an endpoint demotion.</p> <ul style="list-style-type: none"> <li>• Default disabled</li> <li>• Values enabled   disabled</li> </ul>
<b>syslog-on-demote-to-deny</b>	<p>Enable or disable the Oracle Communications Session Border Controller to send a message to the syslog in the event of an endpoint demotion.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>trap-on-demote-to-untrusted</b>	<p>Enable for the Oracle Communications Session Border Controller to send a trap in the event of an endpoint demotion from trusted to untrusted.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>rtcp-rate-limit</b>	<p>Enter the maximum speed in bytes per second for RTCP traffic</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 125000000</li> </ul>
<b>syslog-on-call-reject</b>	<p>Enables generation of a syslog message in response to the rejection of a SIP call.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>anonymous-sdp</b>	<p>Enable or disable username and session name fields anonymous in SDP</p>

	<ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>arp-msg-bandwidth</b>	<p>Enter the maximum bandwidth that can be used by an ARP message</p> <ul style="list-style-type: none"><li>• Default: 32000</li><li>• Values: Min: 2000   Max: 200000</li></ul>
<b>fragment-msg-bandwidth</b>	<p>Enter the maximum bandwidth that can be used by IP fragment messages</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 (fragment packets are treated as untrusted bandwidth); 2000   Max: 10000000</li></ul>
<b>rfc2833-timestamp</b>	<p>Enable or disable use of a timestamp value calculated using the actual time elapsed since the last RTP packet for H.245 to 2833 DTMF interworking</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>default-2833-duration</b>	<p>Enter the time in milliseconds for the Net-Net SBC to use when receiving an alphanumeric UII or SIP INFO with no specified duration.</p> <ul style="list-style-type: none"><li>• Default: 100</li><li>• Values: Min: 50   Max: 5000</li></ul>
<b>rfc2833-end-pkts-only-for-non-sig</b>	<p>Enable this parameter if you want only the last three end 2833 packets used for non-signaled digit events. Disable this parameter if you want the entire start-interim-end RFC 2833 packet sequence for non-signaled digit events.</p> <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>translate-non-rfc2833-event</b>	<p>Enable or disable the Oracle Communications Session Border Controller's ability to translate non-rfc2833 events.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>media-supervision-traps</b>	<p>The Oracle Communications Session Border Controller will send the following trap when the media supervision timer has expired:</p> <pre>apSysMgmtMediaSupervisionTimerExpTrap NOTIFICATION-TYPE OBJECTS { apSysMgmtCallId } STATUS current</pre> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>active-arp</b>	<p>When enabled, this option causes all ARP entries to get refreshed every 20 minutes.</p> <p> <b>Note:</b> As a security measure, in order to mitigate the effect of the ARP table reaching its capacity, configuring active-arp is advised.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>dnssalg-server-failover</b>	<p>Enable or disable allowing DNS queries to be sent to the next configured server, even when contacting the Oracle Communications Session Border Controller's DNS ALG on a single IP address; uses the transaction timeout value set in the dns-server-attributes configuration (part of the dns-config).</p> <ul style="list-style-type: none"><li>• Default: disabled</li></ul>

- Values: enabled | disabled

**Path**


Path: **media-manager-config** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > media-manager**.

**Release**

First appearance: 1.0 / Most recent update: S-CX6.4.0

**RTC Status**

state, latching, flow-time-limit, initial-guard-timer, and subsq-guard-timer are supported. The remaining parameters are not supported.

 **Note:** This is a single instance configuration element.

**Option**

**unique-sdp-id** Enables or disables codec negotiation by updating the SDP session ID and version number. When enabled, the Oracle Communications Session Border Controller will hash the session ID and IP address of the incoming SDP with the current date/time of the Oracle Communications Session Border Controller in order to generate a unique session ID.

**media-policy**

The media-policy element sets the TOS/DiffServ values that define an individual type or class of service.

**Parameters**

<b>name</b>	Name of this media policy
<b>tos-settings</b>	Enter into the tos-values subelement

**Path**


**media-policy** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > media-policy**.

**Release First appearance**

1.2.1

**RTC Status**

Supported

 **Note:** This configuration element sets the Packet Marking for Media features and defines an individual type or class of service for the Oracle Communications Session Border Controller. Media policies can be chosen on a per-realm basis.  
This is a multiple instance configuration element.

## media-policy > tos-settings

---

The tos-settings configuration subelement bases media classification on type and subtype to create any media type combination allowed by IANA standards.

### Parameters

<b>media-type</b>	Enter the type of media to use for this set of TOS settings <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: Any IANA-defined media type, such as: audio, image, model</li></ul>
<b>media-sub-type</b>	Enter the media sub-type to use for the specified media type <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: Any of the media sub-types IANA defines for the selected media type</li></ul>
<b>media-attribute</b>	Enter a list of one or more media attributes that will match in the SDP <ul style="list-style-type: none"><li>• Default: None</li></ul>
<b>tos-values</b>	Enter the TOS value to apply to matching traffic <ul style="list-style-type: none"><li>• Default: None (must be a decimal or hexadecimal value)</li><li>• Values: Range from 0x00 to 0xFF</li></ul>

### Path

**tos-settings** is a subelement under the media-policy element. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > media-policy>tos-settings**.

### Release First appearance

1.2.1

### RTC Status

Supported



**Note:** This configuration element sets the Packet Marking for Media features and defines an individual type or class of service for the Oracle Communications Session Border Controller. Media policies can be chosen on a per-realm basis.

This is a multiple instance configuration element.

## media-profile

---

### Parameters

<b>name</b>	Enter the encoding name used in the SDP rtpmap attribute. This is a required field. No two media-profile elements can have the same name field value.
<b>media-type</b>	Select the type of media used in SDP m lines <ul style="list-style-type: none"><li>• Values:<ul style="list-style-type: none"><li>• audio</li><li>• video</li></ul></li></ul>



	<ul style="list-style-type: none"> <li>• application</li> <li>• data</li> <li>• image</li> <li>• text</li> </ul>
<b>payload-type</b>	Enter the format in SDP m lines. No payload type number is assigned for newer, dynamic codecs. For RTP/AVP media-profile elements, this field should only be configured when there is a standard payload type number that corresponds to the encoding name. Otherwise, this field should be left blank. This field is used by the system to determine the encoding type when the SDP included with a session identifies the standard payload type on the m line, but does not include an a-rtpmap entry.
<b>transport</b>	Select the type of transport protocol used in the SDP rtpmap attribute <ul style="list-style-type: none"> <li>• Default: RTP/AVP</li> <li>• Values: " UDP   RTP/AVP</li> </ul>
<b>req-bandwidth</b>	Enter the total bandwidth in kilobits that the media requires <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 4294967295</li> </ul>
<b>frames-per-packet</b>	Enter the number of frames per RTP packet. This field is used to specify a media profile to facilitate Slow Start translations to Fast Start. A value of 0 means that this field is not being used. <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 256</li> </ul>
<b>average-rate-limit</b>	Enter the maximum speed in bytes per second for a flow that this media profile applies to <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 125000000</li> </ul>
<b>peak-rate-limit</b>	Enter the flowspec parameter r (bucket rate) / p (peak rate) value to insert into COPS message for RACF/PDP configuration <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 125000000</li> </ul>
<b>max-burst-size</b>	Enter the flowspec parameter b ( bucket depth) / m (minimum policed unit) / M (maximum datagram size ) value to insert into COPS message for RACF/PDP configuration <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 125000000</li> </ul>
<b>sdp-rate-limit-headroom</b>	Specify the percentage of headroom to be added while using the AS bandwidth parameter while calculating the average-rate-limit (rate limit for the RTP flow) <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 100</li> </ul>
<b>sdp-bandwidth</b>	Enable or disable the use of the AS modifier in the SDP if the req-bandwidth and sdp-rate-limit-headroom parameters are not set to valid values in the corresponding media profile <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>police-rate</b>	Enter the rate at which the Oracle Communications Session Border Controller polices media for external bandwidth

- Default: 0
- Values: Min: 0 | Max: 999999999

### standard-pkt-rate

Whenptime isn't available in received SDP for this codec, this is a user-configured default packetization rate baseline that the Oracle Communications Session Border Controller uses to make bandwidth allocations when communicating with an external policy server.

- Default: 0

### Path

**media-profile** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > media-profile**.

### Release First appearance

1.0 / Most recent update: 4.0

### RTC Status

Supported



**Note:** This element supports new SDP formats when they are defined. This element is used to associate bandwidth requirements with SDP requirements from information passed during the establishment of sessions. The names established in the media-profile elements are used to populate the corresponding fields in other elements.

This is a multiple instance configuration element.

## media-security

---

The media-security element lets you access configuration elements concerning media security configuration.

### Parameters

<b>media-sec-policy</b>	Access the media-sec-policy configuration element.
<b>sdes-profile</b>	Access the sdes-profile configuration element.
<b>mikey-profile</b>	Access the mikey-profile configuration element.

### Path

**media-security** is a element under the security path. The full path from the topmost ACLI prompt is: **configure terminal > security > media-security**.

## media-security > sipura-profile

---

The sipura-profile element is analogous to existing sdes-profiles, mikey-profiles, or IKE security associations in that all these objects specify materials (certificates, protocol suites, etc.) available in support of cryptographic operations.

### Parameters

<b>name</b>	A unique name for this sipura profile.
<b>crypto-list</b>	Cryptographic algorithm for this profile. <ul style="list-style-type: none"><li>• Default: AES_CM_128_HMAC_MD5</li></ul>

- Values: AES\_CM\_128\_HMAC\_MD5

**certificate-file-name** Required parameter to specify the file name of the minicertificate presented by the SBC in support of Linksys/sipura operations. This file must have been previously installed in the /code/sipura directory. When identifying the file, use the complete file name, to include the file extension, but omit the directory path.

**Path**

**sipura-profile** is an element of the media-security path. The full path from the topmost ACLI prompt is: **configure terminal > security > media-security > sipura-profile**

**Release**

First appearance: S-CX6.4.0

**media-sec-policy**

The media-sec-policy configuration element lets you access configuration elements concerning media security configuration.

**Parameters**

- name** Name of this media-sec-policy object.
- pass-through** Enable or disable pass-through mode. When enabled, the User Agent (UA) endpoints negotiate security parameters between each other; consequently, the Oracle Communications Session Border Controller simply passes SRTP traffic between the two endpoints.
- With pass-thru mode disabled (the default state), the Oracle Communications Session Border Controller disallows end-to-end negotiation — rather the Oracle Communications Session Border Controller initiates and terminates SRTP tunnels with both endpoints.
- Default: disabled
  - Values: enabled | disabled
- options** Options configured on this media security policy
- outbound** Enter this subelement to configure the policy parameters when this policy applies to outbound traffic.
- inbound** Enter this subelement to configure the policy parameters when this policy applies to inbound traffic.

**Path**

**media-sec-policy** is a configuration element under the security > media-security path. The full path from the topmost ACLI prompt is: **configure terminal > security > media-security > media-sec-policy**.

**media-sec-policy > inbound**

The media-sec-policy > inbound configuration element lets you configure the inbound media security policy.

**Parameters**

- profile** Indicates the name of the corresponding security profile that's active on the call leg that this policy direction specifies.

**mode** Selects the real time transport protocol.

- Default: rtp
- Values: rtp | srtp

**protocol** This sets the key exchange protocol

- Default: none
- Values: none | mikey | sdes

### Path

**inbound** is a subelement in the media-sec-policy configuration element under the security > media-security path. The full path from the topmost ACLI prompt is: **configure terminal > security > media-security > media-sec-policy > inbound**.

## media-sec-policy > outbound

---

The media-sec-policy > inbound configuration element lets you configure the outbound media security policy.

### Parameters

**profile** Indicates the name of the corresponding security profile that's active on the call leg that this policy direction specifies.

**mode** Selects the real time transport protocol.

- Default: rtp
- Values: rtp | srtp

**protocol** This sets the key exchange protocol

- Default: none
- Values: none | mikey | sdes

### Path

**outbound** is a subelement in the media-sec-policy configuration element under the security > media-security path. The full path from the topmost ACLI prompt is: **configure terminal > security > media-security > media-sec-policy > outbound**.

## mgcp-config

---

The mgcp-config element provides ALG functionality for MGCP messages between media gateways and media gateway controllers.

### Parameters

**private-realm** Enter the private realm (location of the media gateways). This is a required field. This private-realm field value must correspond to a valid identifier field entry in a realm-config.

**private-address** Enter the IP address on the media interface in the private realm that the media gateways use as their call agent or softswitch IP address. This is a required field.

**private-port** Enter the port of IP address on the media interface in the private realm that call agent or softswitch use

	<ul style="list-style-type: none"> <li>• Default: 2727</li> <li>• Values: Min: 1025 / Max: 65535</li> </ul>
<b>public-realm</b>	Enter the public realm of the call agent or softswitch. This is a required field. This public-realm field value corresponds to a valid identifier field entry in a realm-config that has already been configured.
<b>public-ca-host</b>	Enter the hostname for the public CA
<b>public-ca-address</b>	Enter the public IP address of call agent or softswitch. This is a required field. Entries in this field must follow the IP Address format.
<b>public-ca-port</b>	Enter the public UDP Port of call agent or softswitch <ul style="list-style-type: none"> <li>• Default: 2727</li> <li>• Values: Min: 1025 / Max: 65535</li> </ul>
<b>public-gw-host</b>	Enter the FQDN to use in the endpoint MGCP messages on the public side of the Oracle Communications Session Border Controller. If this field is left empty, the host part of the endpoint name will be the public gateway IP address (i.e., the public-gw-address field value).
<b>public-gw-address</b>	Enter the IP address on the media interface in the public realm. This field value is the media gateway address that the Oracle Communications Session Border Controller uses to communicate with the call agent or softswitch. This is a required parameter. If this parameter is entered with a subnet mask in slash notation, 1:1 gateway mapping is enabled. <ul style="list-style-type: none"> <li>• Default: 0.0.0.0</li> </ul>
<b>public-gw-port</b>	Enter the port on media interface in the public realm. This field value is the media gateway port that the Oracle Communications Session Border Controller uses to communicate with the call agent or softswitch. <ul style="list-style-type: none"> <li>• Default: 2427</li> <li>• Values: Min: 1025 / Max: 65535</li> </ul>
<b>second-public-gw-port</b>	Enter the second UDP port on public-gw-address where Oracle Communications Session Border Controller receives packets from the call agent or softswitch. Oracle Communications Session Border Controller can receive messages from the call agent or softswitch on either the public-gw-port or the second-public-gw-port. <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 1025 / Max: 65535</li> </ul>
<b>alg-port</b>	Enter the port used to send a packet from the network processor to the host processor. Each mgcp-config must have a unique ALG port so the ALG function can distinguish which mgcp-config element applies to packets sent up from the network processor. <ul style="list-style-type: none"> <li>• Default: 2427</li> <li>• Values: Min: 1025 /Max; 65535</li> </ul>
<b>mode</b>	Set the MGCP-NAT mode. This field defines how endpoint names are translated as MGCP flows traverse the Oracle Communications Session Border Controller. This is a required field. <ul style="list-style-type: none"> <li>• Default: LineUnit</li> <li>• Values:               <ul style="list-style-type: none"> <li>• Host—A “unit” term is added to endpoint name on public side to uniquely identify the gateway/host on the private side. The left-most part of the private FQDN is used as the unit term (or unit name).</li> </ul> </li> </ul>

- **LinePrefix**—Divisor field value is used to compute a number to insert into the localname part of the endpoint name. The number to be inserted is the IP address modulo the divisor. This mode inserts this number before the channel number. Example: aaln/1 becomes aaln/1231. The IP address part is replaced by the public-gw-address.
- **LineUnit**—Divisor field value is used to compute a number to insert into localname part of endpoint name. The number inserted is the IP address modulo the divisor. This mode adds the unit-number term defined in the conventions section of <ftp://ftp.rfc-editor.org/in-notes/rfc3435.txt> (e.g., aaln/2 becomes aaln/123/2). The IP address part is replaced by the public-gw-address (also defined in this element).
- **FQDN**—Dots are removed from the host portion of the private endpoint. Example: the address aaln/2@abc.xyz.com on the private (i.e., gateway) side would become aaln/abcxyzcom/2@sd.com on the public (i.e., call agent) side.
- **FQDN2**—Dots are retained in the host portion of the private endpoint. Example: the address aaln/2@abc.xyz.com on the private (i.e., gateway) side would become aaln/abc.xyz.com/2@sd.com on the public (i.e., call agent) side.
- **OnlyHost**—Endpoint name is not translated.
- **None**—Endpoint name is not translated.

<b>divisor</b>	<p>Enter the unit for computing name of an endpoint. This field is used to determine the number for the LinePrefix or LineUnit. The remainder of the private IP address divided by this number becomes the prefix/unit number. If FQDNs are used for network addressing, the divisor field is not used.</p> <ul style="list-style-type: none"><li>• Default 256</li><li>• Values 256   65535   16777216   4294967296</li></ul>
<b>unit-prefix</b>	<p>Enter the prefix for the unit term of the endpoint name. For modes that add a unit term to the user part of the endpoint name, this field value is placed in front of the unit number or name when creating a public endpoint name.</p>
<b>audit-interval</b>	<p>Enter the number of seconds between AUEP commands that the Oracle Communications Session Border Controller sends to the endpoint (gateway/IAD). No AUEPs are sent by default.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>nat-traversal</b>	<p>Enable or disable whether or not MGCP ALG assumes that all (gateway) endpoints are behind a NAT</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>dns-authentication</b>	<p>Enable or disable MGCP DNS authentication functionality on the Oracle Communications Session Border Controller</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>dns-translation</b>	<p>Enter the translation rule to use, i.e., what characters in the address will be added, replaced, or deleted. If you enable the MGCP DNS authentication feature, then this field is required. The value of this field must be a configured session translation.</p>
<b>ca-redundancy</b>	<p>Enable or disable the call agent redundancy feature</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>

<b>ca-ping-method</b>	Enter the ping method used for call agent redundancy. This parameter is the prototype of a ping method sent to a call agent to determine its state.
<b>ca-ping-interval</b>	Enter the amount of time in seconds between pings sent to the call agent to check for health <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>rsip-failures</b>	Enter the range of 5xx return codes that trigger MGCP endpoint removal or that will fail to create an MGCP session. To empty the default, enter a <Space> enclosed in quotation marks. <ul style="list-style-type: none"> <li>• Default: 500-509,511-519,522-599</li> <li>• Values: 5xx return codes per RFC 3435</li> </ul>
<b>ca-failover-ip-addresses</b>	Enter the IP addresses for call agent redundancy support. You must enter the list of IP addresses enclosed in parentheses and separate each IP address with a <Space>. You can enter one or more entries.
<b>options</b>	Enter the MGCP options. Used to place 911 calls for MGCP by use of the Via parameter. This parameter is set by entering #options x-via= <endpoint   both> in the ACLI <ul style="list-style-type: none"> <li>• Values: <ul style="list-style-type: none"> <li>• endpoint—Endpoint is either a router or a phone</li> <li>• both—There are two addresses, the phone number of the endpoint and the IP address of the Oracle Communications Session Border Controller</li> </ul> </li> </ul> <p>Also used to communicate with send-only devices by typing #options drain-sendonly.</p>
<b>port-map-start</b>	Enter the port number marking the beginning of the range of ports you want to use for MGCP port mapping. <ul style="list-style-type: none"> <li>• Default: 0 (disabled)</li> <li>• Values: Min: 0; 1025/ Max: 65535</li> </ul>
<b>port-map-end</b>	Enter the port number marking the end of the range of ports you want to use for MGCP port mapping. When MGCP port mapping is enabled, this value must be greater than the port-map-start value. <ul style="list-style-type: none"> <li>• Default: 0 (disabled)</li> <li>• Values: Min: 0; 1025 / Max: 65535</li> </ul>

## Path

**mgcp-config** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > mgcp-config**.

## Release First appearance

1.0 / Most recent update: 4.1

## RTC Status

Supported



**Note:** The combination of entries in the private-realm field and the private-address field must be unique. No two mgcp-config elements can have the same entries in the private-realm field and the private-address entries. This is a multiple instance configuration element.

## mikey-profile

---

The mikey-profile configuration element lets you configure the parameter values offered as a MIKEY initiator or accepted as a MIKEY responder.

### Parameters

<b>name</b>	Sets the name of this object.
<b>key-exchange-method</b>	<p>Sets the key exchange method that is offered when acting in the initiator role, or accepted when acting in the responder role.</p> <ul style="list-style-type: none"> <li>• Default: pre-shared</li> <li>• Values: pre-shared</li> </ul>
<b>encr-algorithm</b>	<p>Selects the encryption algorithm that is offered when acting in the initiator role, or accepted when acting in the responder role.</p> <p>Any indicates that the Oracle Communications Session Border Controller accepts the encryption algorithm specified in the MIKEY_I MESSAGE, as long as it is within the valid range. When NULL is used RTP and RTCP packets are not encrypted.</p> <p>For the outgoing direction, the selection of the encryption algorithm for any is as follows:</p> <ul style="list-style-type: none"> <li>• If MIKEY is used in the incoming direction the same encryption algorithm is used for the outgoing direction</li> <li>• If the incoming direction does not have SRTP, then AES-CM is used as the encryption algorithm.</li> <li>• Default: any</li> <li>• Values: NULL   AES-CM   any</li> </ul>
<b>auth-algorithm</b>	<p>Selects the encryption algorithm that is offered when acting in the initiator role, or accepted when acting in the responder role.</p> <ul style="list-style-type: none"> <li>• Default: any</li> <li>• Values: NULL   HMAC-SHA1-32   HMAC-SHA1-80   any</li> </ul>
<b>shared-secret</b>	This parameter contains the shared secret. A shared secret is not required as MIKEY messages are not protected in this implementation.
<b>mki</b>	<p>This parameter enables or disables the inclusion of the MKI:length field in the SDP crypto attribute.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: <ul style="list-style-type: none"> <li>• enabled – an MKI field is sent within the crypto attribute (16 bytes maximum)</li> <li>• disabled – no MKI field is sent</li> </ul> </li> </ul>
<b>egress-offer-format</b>	<p>Sets any manipulation on SDP offer.</p> <ul style="list-style-type: none"> <li>• Default: same-as-ingress</li> <li>• Values: <ul style="list-style-type: none"> <li>• same-as-ingress - the Oracle Communications Session Border Controller leaves the profile of the media lines unchanged.</li> <li>• simultaneous-best-effort - the Oracle Communications Session Border Controller Adds an RTP/SAVP media line for any media profile that has only the RTP/AVP media profile, and Adds an RTP/AVP media line for any media profile that has only the RTP/SAVP media profile</li> </ul> </li> </ul>



- use-ingress-session-params** Enter the list of values for which the Oracle Communications Session Border Controller will accept and (where applicable) mirror the UA's proposed cryptographic session parameters:
- **srtp-auth**—Decides whether or not authentication is performed in SRTP
  - **srtp-encrypt**—Decides whether or not encryption is performed in SRTP
  - **srtcp-encrypt**—Decides whether or not encryption is performed in SRTCP

```
ACMEPACKET(sdes-profile) # use-ingress-session-params "srtp-auth
srtp-encrypt
srtcp-encrypt"
```

### Path

**mikey-profile** is a configuration element under the `security > media-security` path. The full path from the topmost CLI prompt is: **configure terminal > security > media-security > mikey-profile**.

## msrp-config

The **msrp-config** element is used to configure global MSRP functionality.

### Parameters

- state** Enables MSRP operations.
- Default: enabled
  - enabled | disabled
- uri-translation** Enables or disables NAT of URIs found in the From-Path and To- Path headers of MSRP requests and responses, and in a=path attributes found in SDP offers.
- Default: enabled
  - enabled | disabled
- session-inactivity-timer** This parameter is configured in connection with the `sipconfig > msrp-delayed-bye-timer` parameter to implement the delayed transmission of SIP BYE requests. The `session-inactivity-timer` parameter specifies the maximum inactivity interval (defined as the absence of transmitted data) tolerated before the MSRP connection is terminated.
- Default: 5
  - Min: 5 / Max: 10

### Path

**msrp-config** is an element of the `media-manager` path. The full path from the topmost CLI prompt is: **configure terminal > media-manager > msrp-config**.

### Release

First appearance: S-CX6.4.0



---

## Configuration Elements N-Z

### net-management-control

---

The net-management-control configuration element allows you to control multimedia traffic, specifically for static call gapping and 911 exception handling. These controls limit the volume or rate of traffic for a specific set of dialed numbers or dialed-number prefixes.

#### Parameters

<b>name</b>	Enter the name of this network management control rule.
<b>state</b>	Select the state of this network management control rule. <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>type</b>	Enter the control type you want to use. <ul style="list-style-type: none"> <li>• Values: GAP-RATE   GAP-PERCENT   PRIORITY</li> </ul>
<b>value</b>	Enter the control value of the net management control. This parameter applies only when you set the control type to either GAP-RATE or GAP-PERCENT. <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: GAP-RATE: 0-2147483647   GAP-PERCENTAGE: 0-100</li> </ul>
<b>Treatment</b>	Enter the treatment method you want to use or leave this parameter set to <b>NONE</b> <ul style="list-style-type: none"> <li>• Values: REJECT   DIVERT</li> </ul>
<b>next-hop</b>	Enter the next hop for the Oracle Communications Session Border Controller to use when the treatment method is DIVERT. This value should contain one of the following: <ul style="list-style-type: none"> <li>• hostname(:port) or IPv4 address or IPv6 address of a configured session agent.</li> <li>• IPv4 address (:port) or IPv6 address (:port) of a specific endpoint</li> </ul> Group name of a configured session agent group. The group name of a configured session agent group must be prefixed with SAG: For example: <ul style="list-style-type: none"> <li>• policy-attribute: next-hop SAG:appserver</li> <li>• policy-attribute: next-hop lrt:routetable</li> </ul>

	<ul style="list-style-type: none"><li>• policy-attribute: next-hop enum: lerg</li></ul>
<b>realm-next-hop</b>	Enter the realm identifier to designate the realm of the next hop when the treatment type is DIVERT
<b>protocol-next-hop</b>	Enter the signaling protocol for the next hop when the treatment type is DIVERT
<b>status-code</b>	Enter the SIP response code that you want the Oracle Communications Session Border Controller to use when the treatment method is REJECT <ul style="list-style-type: none"><li>• Default: 503</li><li>• Values: Min: 1 / Max: 699</li></ul>
<b>cause-code</b>	Enter the Q.850 cause code that you want the Oracle Communications Session Border Controller to use when the treatment method is REJECT <ul style="list-style-type: none"><li>• Default: 63</li><li>• Values: Min: 1 / Max: 999999999</li></ul>
<b>gap-rate-max-count</b>	Enter the maximum token counter value for gapping rate <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>gap-rate-window-size</b>	Enter the window size (in seconds) for gapping rate calculation <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>destination-identifier</b>	<p>Enter the classification key. This parameter specifies information about the destination, which can be an IP address, an FQDN, and destination (called) number, or destination prefix. You can wildcard characters in the classification key using the caret symbol (^).</p> <p>This parameter can accommodate a list of entries so that, if necessary, you can specify multiple classification keys.</p>
<b>add-destination-identifier</b>	Add a destination identifier
<b>remove-destination-identifier</b>	Remove a destination identifier
<b>rph-feature</b>	Set the state of NSEP support for this NMC rule <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>rph-profile</b>	Enter the name of the RPH profile to apply to this NMC rule <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: Name of an rph-profile</li></ul>
<b>rph-policy</b>	Enter the name of the RPH policy to apply to this NMC rule <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: Name of an rph-policy</li></ul>
:	

**Path**

**net-management-control** is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > net-management-control**

**Release**

First appearance: 4.1.1

**RTC Status**

Supported

## network-interface

---

The network-interface element creates and configures a logical network interface.

**Parameters**

<b>name</b>	Enter the name of the physical interface with which this network-interface element is linked. Network-interface elements that correspond to phy-interface elements with an operation type of Control or Maintenance must start with “wancom.”
<b>sub-port-id</b>	Enter the identification of a specific virtual interface in a physical interface (e.g., a VLAN tag). A value of 0 indicates that this element is not using a virtual interface. The sub-port-id field value is only required if the operation type is Media. <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 4095</li> </ul>
<b>description</b>	Enter a brief description of this network interface
<b>hostname</b>	Enter the hostname of this network interface. This is an optional entry that must follow FQDN Format or IP Address Format. An IPV6 address is valid for this parameter.
<b>ip-address</b>	Enter the IP address of this network interface. This is a required entry that must follow the IP Address Format. An IPV6 address is valid for this parameter.
<b>pri-utility-addr</b>	Enter the utility IP address for the primary HA peer in an HA architecture An IPV6 address is valid for this parameter.
<b>sec-utility-addr</b>	Enter the utility IP address for the secondary Oracle Communications Session Border Controller peer in an HA architecture An IPV6 address is valid for this parameter.
<b>netmask</b>	Enter the netmask portion of the IP address for this network interface entered in IP address format. The network-interface element will not function properly unless this field value is valid. An IPV6 address is valid for this parameter.
<b>gateway</b>	Enter the gateway this network interface uses to forward packets. Entries in this field must follow the IP Address Format. No packets are forwarded if this value is 0.0.0.0. An IPV6 address is valid for this parameter.
<b>sec-gateway</b>	Enter the gateway to use on the secondary Oracle Communications Session Border Controller in an HA pair. Entries in this field must follow the IP address format. An IPV6 address is valid for this parameter.

<b>gw-heartbeat</b>	Access the gateway-heartbeat subelement
<b>dns-ip-primary</b>	Enter the IP address of the primary DNS to be used for this interface An IPV6 address is valid for this parameter.
<b>dns-ip-backup1</b>	Enter the IP address of the first backup DNS to be used for this interface An IPV6 address is valid for this parameter.
<b>dns-ip-backup2</b>	Enter the IP address of the second backup DNS to be used for this interface An IPV6 address is valid for this parameter.
<b>dns-domain</b>	Set the default domain name used to populate incomplete hostnames that do not include a domain. Entries must follow the Name Format.
<b>dns-timeout</b>	Enter the total time in seconds you want to elapse before a query (and its retransmissions) sent to a DNS server timeout <ul style="list-style-type: none"><li>• Default: 11</li><li>• Values: Min: 1/ Max: 999999999</li></ul>
<b>add-hip-ip</b>	Enter a list of IP addresses allowed to access signaling and maintenance protocol stacks via this front interface using the HIP feature An IPV6 address is valid for this parameter.
<b>remove-hip-ip</b>	Remove an IP address added using the add-hip-ip parameter
<b>add-ftp-ip</b>	Enter a list of IP addresses from which FTP traffic can be received and acted upon by a front media interface
<b>remove-ftp-ip</b>	Remove an IP address added using the add-ftp-ip parameter An IPV6 address is valid for this parameter.
<b>add-icmp-ip</b>	Enter a list of IP addresses from which ICMP traffic can be received and acted upon by a front media interface An IPV6 address is valid for this parameter.
<b>remove-icmp-ip</b>	Remove an IP address added using the add-icmp-ip parameter An IPV6 address is valid for this parameter.
<b>add-snmp-ip</b>	Enter a list of IP addresses from which SNMP traffic can be received and acted upon by a front media interface
<b>remove-snmp-ip</b>	Remove an IP address added using the add-snmp-ip parameter
<b>add-telnet-ip</b>	Enter a list of IP addresses from which telnet traffic can be received and acted upon by a front media interface
<b>remove-telnet-ip</b>	Remove an IP address added using the add-telnet-ip field
<b>add-ssh-ip</b>	Enter a list of IP addresses from which SSH traffic can be received and acted upon by a front media interface. <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: A valid IPv4 network address</li></ul>
<b>signaling-mtu</b>	MTU size for packets leaving this interface. <ul style="list-style-type: none"><li>• Default: inherits system wide MTU</li><li>• Values:<ul style="list-style-type: none"><li>• IPv4: &lt;0, 576-4096&gt;</li><li>• IPv6: &lt;0, 1280-4096</li></ul></li></ul>

**Path**


The full path from the topmost ACLI prompt is: **configure terminal > system > network-interface**

**Release**

First appearance: 1.0 / Most recent update: 4.1.

**RTC Status**

Supported

 **Note:** This is a multiple instance configuration subelement.

## network-interface > gw-heartbeat

The gw-heartbeat subelement supports the front interface link failure detection and polling feature.

**Parameters**

<b>state</b>	<p>Enable or disable front interface link detection and polling functionality on the Oracle Communications Session Border Controller for this network-interface element</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>heartbeat</b>	<p>Enter the time interval in seconds between heartbeats for the front interface gateway</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 65535</li> </ul>
<b>retry-count</b>	<p>Enter the number of front interface gateway heartbeat retries before a gateway is considered unreachable</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 65535</li> </ul>
<b>retry-timeout</b>	<p>Enter the heartbeat retry timeout value in seconds</p> <ul style="list-style-type: none"> <li>• Default: 1</li> <li>• Values: Min: 1   Max: 65535</li> </ul>
<b>health-score</b>	<p>Enter the amount to subtract from the health score if the front interface gateway heartbeat fails (i.e., expires). The health score will be decremented by the amount set in this field if the timeout value set in the gw-heartbeat: retry-timeout field is exceeded without the front interface gateway sending a response.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 100</li> </ul>

**Path**

**gw-heartbeat** is a subelement of the network-interface element. The full path from the topmost ACLI prompt is: **configure terminal > system > network-interface > gw-heartbeat**

**Release**

First appearance: 1.2.1

### RTC Status

Supported



**Note:** The values configured in the fields of a gw-heartbeat subelement apply to the Oracle Communications Session Border Controller on a per-network-interface basis, and can override the values configured in the redundancy element's corresponding front interface link detection and polling fields. This is a single instance configuration subelement.

## network-parameters

---

The network-parameters element enables and configures the TCP keepalive feature used for keeping H.323 connections open. This is also used for global SCTP configuration.

### Parameters

<b>tcp-keepalive-count</b>	Enter the number of outstanding keepalives before connection is torn down <ul style="list-style-type: none"><li>• Default: 8</li><li>• Values: Min: 0   Max: 4294967295</li></ul>
<b>tcp-keepalive-idle-timer</b>	Enter the idle time in seconds before triggering keepalive processing. If you have upgraded the release you are running and a value outside of the acceptable range was configured in an earlier release, the default value is used and a log message is generated. <ul style="list-style-type: none"><li>• Default: 7200</li><li>• Values: Min: 30   Max: 7200</li></ul>
<b>tcp-keepalive-mode</b>	Enter the TCP keepalive mode <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values:<ul style="list-style-type: none"><li>• 0—The sequence number is sent un-incremented</li><li>• 1—The sequence number is sent incremented</li><li>• 2—No packets are sent</li></ul></li></ul>
<b>tcp-keepinit-timer</b>	Enter the TCP connection timeout period if a TCP connection cannot be established. If you have upgraded the release you are running and a value outside of the acceptable range was configured in an earlier release, the default value is used and a log message is generated. <ul style="list-style-type: none"><li>• Default: 75</li><li>• Values: 0-999999999</li></ul>
<b>tcp-keepalive-interval-timer</b>	Enter the TCP retransmission time if a TCP connection probe has been idle for some amount of time <ul style="list-style-type: none"><li>• Default: 75</li><li>• Values: Min: 15 / Max: 75</li></ul>
<b>sctp-send-mode</b>	Leave this parameter set to its default (unordered) so data delivery can occur without regard to stream sequence numbering. If data delivery must follow stream sequence number, change this parameter to ordered. <ul style="list-style-type: none"><li>• Default: unordered</li><li>• Values: ordered   unordered</li></ul>
<b>sctp-rto-initial</b>	Sets the initial value of the SCTP retransmit timeout (RTO). <ul style="list-style-type: none"><li>• Default: 3000 msec (value recommended by RFC 4960)</li></ul>



	<ul style="list-style-type: none"> <li>• Values: 0-4294967295</li> </ul>
<b>sctp-rto-max</b>	Sets the maximum value of the SCTP retransmit timeout (RTO). <ul style="list-style-type: none"> <li>• Default: 60000 msec (value recommended by RFC 4960)</li> <li>• Values: 0-4294967295</li> </ul>
<b>sctp-rto-min</b>	Sets the maximum value of the SCTP retransmit timeout (RTO). <ul style="list-style-type: none"> <li>• Default: 1000 msec (value recommended by RFC 4960)</li> <li>• Values: 0-4294967295</li> </ul>
<b>sctp-hb-interval</b>	Sets the initial value of the SCTP Heartbeat Interval timer. <ul style="list-style-type: none"> <li>• Default: 30000 msec (value recommended by RFC 4960)</li> <li>• Values: 0-4294967295</li> </ul>
<b>sctp-max-burst</b>	Sets the maximum number of DATA chunks contained in a single SCTP packet. <ul style="list-style-type: none"> <li>• Default: 4 DATA chunks (value recommended by RFC 4960)</li> <li>• Values: 0-4294967295</li> </ul>
<b>sctp-sack-timeout</b>	Sets the initial value of the SACK (Selective Acknowledgement) Delay timer. <ul style="list-style-type: none"> <li>• Default: 200 msec (value recommended by RFC 4960)</li> <li>• Values: 0-500</li> </ul>
<b>sctp-assoc-max-retrans</b>	Specifies the maximum number of consecutive unacknowledged retransmissions to a specific SCTP endpoint. Should this value be exceeded, the endpoint is considered to be unreachable, and the SCTP association is placed in the CLOSED state. <ul style="list-style-type: none"> <li>• Default: 10 retries (value recommended by RFC 4960)</li> <li>• Values: 0-4294967295</li> </ul>
<b>sctp-path-max-retrans</b>	Specifies the maximum number of RTO expirations/unacknowledged HEARTBEATS to a specific SCTP transport address. Should this value be exceeded, the endpoint is considered to be inactive, and an alternate transport address, if available, will be used for subsequent transmissions. <ul style="list-style-type: none"> <li>• Default: 5</li> <li>• Values: 0-4294967295</li> </ul>
<b>options</b>	Enter any optional features or parameters

## Path

**network-parameters** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > network-parameters**

## Release

First appearance: 2.0; Last updated: S-C6.3.0

## RTC Status

Not supported

 **Note:** This is a single instance configuration subelement.

### ntp-sync

---

The ntp-sync element sets the ntp server IP address for correct and accurate time synchronization.

#### Parameters

- add-server** Add IP address of NTP server; entries must follow the IP Address Format
- del-server** Remove a previously entered NTP server. Entries must follow the IP Address Format.

#### Path

**ntp-sync** is a top-level element. The full path from the topmost CLI prompt is: **configure terminal > ntp-sync**.

#### Release

First appearance: 1.0 / Most recent update: 1.1

#### RTC Status

Supported



**Note:** In order for any changes to the NTP synchronization functionality to take effect, a save-config must be performed followed by a system reboot.

### qos-constraints

---

The qos-constraints configuration element allows you to enable QoS based routing, which uses the R-Factor on a per-realm basis to cut back on the traffic allowed by a specific realm. Oracle Communications Session Border Controller QoS reporting is a measurement tool that collects statistics on Voice over IP (VoIP) call flows for SIP and H.323. To provide information, the Oracle Communications Session Border Controller writes additional parameters to the Remote Authentication Dial-in User Service (RADIUS) call record and Historical Data Recording (HDR) records.

#### Parameters

- name** Enter the name of a QoS constraints configuration
- state** Enable or disable a set of QoS constraints
- Default: enabled
  - Values: enabled | disabled
- major-factor** Enter a numeric value set the threshold that determines when the Oracle Communications Session Border Controller applies the call reduction rate; must be less than the critical-rfactor
- Default: 0
  - Values: Min: 0 | Max: 9321 0
- critical-rfactor** Enter a numeric value to set the threshold that determines when the Oracle Communications Session Border Controller rejects all inbound calls for the realm, and rejects outbound calls when there is no alternate route
- Default: 0
  - Values: Min: 0 | Max: 9321
- call-load-reduction** Enter the percentage by which the Oracle Communications Session Border Controller will reduce calls to the realm if the major-rfactor is exceeded; a value of 0 means the call load will not be reduced

- Default: 0
- Values: Min: 0 | Max: 100

### Path

**qos-constraints** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > qos-constraints**.

### Release

First appearance: S-C6.1.0



### RTC Status

Supported

## password-policy

The **password-policy** element configures password rules for password secure mode.

### Parameters

<b>min-secure-pwd-len</b>	<p>Enter the minimum password length to use when system is in secure password mode. The maximum allowable length for any password is 64 characters.</p> <ul style="list-style-type: none"> <li>• Default: 9</li> <li>• Values: 6-64</li> </ul> <p> <b>Note:</b> The password using this minimum length value must contain at least one punctuation mark and two out of these three requirements: upper case letter, lower case letter, number. No special characters are allowed, for example: #, &amp;, @.</p> <p> <b>Note:</b> This parameter is ignored when the <b>password-policy-strength</b> parameter is used (the Admin Security and/or Admin Security ACP license is active).</p>
<b>expiry-interval</b>	<p>Specifies the maximum password lifetime in days.</p> <ul style="list-style-type: none"> <li>• Default: 90</li> <li>• Min: 1 / Max: 65535</li> </ul>
<b>password-change-interval</b>	<p>Specifies the minimum password lifetime.</p> <ul style="list-style-type: none"> <li>• Default: 24 hours</li> <li>• Min: 1 hour / Max: 24 hours</li> </ul>
<b>expiry-notify-period</b>	<p>Specifies the number of days prior to expiration that users begin to receive password expiration notifications.</p> <ul style="list-style-type: none"> <li>• Default: 30 days</li> <li>• Min: 1 day / Max: 90 days</li> </ul>
<b>grace-period</b>	<p>Time after password expiration user has until forced to change password.</p> <ul style="list-style-type: none"> <li>• Default: 30 days</li> <li>• Min: 1 day / Max: 90 days</li> </ul>
<b>grace-logins</b>	<p>Number of logins after password expiration the user has until forced to change password.</p> <ul style="list-style-type: none"> <li>• Default: 3</li> </ul>

- Min: 1 / Max: 10

**password-history-count** Specifies the number of previously used passwords retained in encrypted format in the password history cache.

- Default: 3
- Min: 1 / Max: 10

**password-policy-strength** Enables the enhanced password strength requirements provided by the Admin Security and/or Admin Security ACP license.

- Default: disabled
- enabled | disabled

### Path

**password-policy** is an element under the security path. The full path from the topmost CLI prompt is: **configure terminal > security > password-policy**.

### Release

First appearance: 5.1 / Most recent update: S-CX6.4.0

### RTC Status

Supported

## phy-interface

---

The phy-interface element is used to configure physical interfaces.

### Parameters

**name** Enter the name for this physical interface. Physical interfaces with an operation-type of Control or Maintenance must begin with “wancom.” This is a required field. Entries in this field must follow the Name Format. Name values for the phy-interface must be unique.

**operation-type** Select the type of physical interface connection

- Default: Control
- Values:
  - Media—Front-panel interfaces only. Port: 0-3 Slot: 0 or 1
  - Control—Rear-panel interfaces only. Port 0, 1, or 2 Slot: 0
  - Maintenance —Rear-panel interfaces only. Port 0, 1, or 2 Slot: 0

**port** Select the physical port number on an interface of the phy-interface being configured

- Default: 0
- Values:
  - 0-2 for rear-panel interfaces
  - 0-1 for two possible GigE ports on front of Oracle Communications Session Border Controller chassis
  - 0-3 for four possible FastE ports on front of Oracle Communications Session Border Controller chassis

**slot** Select the physical slot number on the Oracle Communications Session Border Controller chassis

	<ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: <ul style="list-style-type: none"> <li>• 0 is the motherboard (rear-panel interface) if the name begins with “wancom”</li> <li>• 0 is the left Phy media slot on front of Oracle Communications Session Border Controller chassis</li> <li>• 1 is the right Phy media slot on front of Oracle Communications Session Border Controller chassis</li> </ul> </li> </ul>
<b>virtual-mac</b>	Enter the MAC address identifying a front-panel interface when the Oracle Communications Session Border Controller is in the Active state. This field value should be generated from the unused MAC addresses assigned to a Oracle Communications Session Border Controller. The virtual-mac field is only applicable for front interfaces.
<b>admin-state</b>	<p>Enable or disable the Oracle Communications Session Border Controller to allow incoming and outgoing traffic to be processed using the front physical interface cards</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>auto-negotiation</b>	<p>Enable or disable auto negotiation on front Phy card interfaces taking place before either end begins sending packets over the Ethernet link. The auto-negotiation field is only applicable for front interfaces. The value configured in this field does not change the Oracle Communications Session Border Controller status at runtime.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>duplex-mode</b>	<p>Set whether the 10/100 Phy card interfaces located on the front panel of Oracle Communications Session Border Controller operate in full-duplex mode or half-duplex mode</p> <ul style="list-style-type: none"> <li>• Default: full</li> <li>• Values: full   half</li> </ul>
<b>speed</b>	<p>Set the speed in Mbps of the front-panel 10/100 Phy interfaces; this field is only used if the auto-negotiation field is set to disabled for 10/100 Phy cards</p> <ul style="list-style-type: none"> <li>• Default: 100</li> <li>• Values: 10   100</li> </ul>
<b>wancom-health-score</b>	<p>Enter the amount to subtract from the Oracle Communications Session Border Controller’s health score if a rear interface link goes down</p> <ul style="list-style-type: none"> <li>• Default: 50</li> <li>• Values: Min: 0   Max: 100</li> </ul>
<b>network-alarm-threshold</b>	Access the network-alarm-threshold subelement.
<b>overload-protection</b>	<p>Enable this parameter to turn graceful call control on. Disable (default) if you do not want to use this feature.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>overload-protection</b>	<p>Enable this parameter to turn graceful call control on. Disable (default) if you do not want to use this feature.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>

This parameter is not RTC supported

### Path

**phy-interface** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > phy-interface**.

### Release

First appearance: 1.0 / Most recent update: S-C6.2.0

### RTC Status

Supported



**Note:** Certain fields are visible based on the setting of the operation-type parameter. This is a multiple instance configuration subelement.

## phy-interface > network-alarm-threshold

---

The network-alarm-threshold subelement enables the Oracle Communications Session Border Controller to monitor network utilization of its media interfaces and send alarms when configured thresholds are exceeded.

### Parameters

**severity** Enter the level of alarm to be configured per port.

- Default: minor
- Values: minor | major | critical

**value** Set the threshold percentage of network utilization that triggers an SNMP trap and alarm for each severity value.

### Path

**network-alarm-threshold** is a subelement under the **system** path. The full path from the topmost ACLI prompt is: **configure terminal > system > phy-interface**.

### Release

First appearance: S-C6.2.0

### RTC Status

Supported

## public-key

---

The public-key configuration element is used to generate an SSH public key to authenticate SSH sessions.

### Parameters

**name** Enter the name of the public key

**type** Select the type of key you want to create.

- Default: rsa

- Values: rsa | dsa

**size** Enter the size of the key you are creating.

- Default: 1024
- Values: 512 | 1024 | 2048

### Path

**public-key** is an element under the security path. The full path from the topmost ACLI prompt is: **configure terminal > security > public-key**

### Release

First appearance: S-C6.2.0

### RTC Status

Supported



**Note:** This is a multiple instance configuration element.

---

## q850-sip-map

The q850-sip-map configuration element is used to map q850 cause codes to SIP response codes.

### Parameters

**entries** Enter the entries configuration subelement

**delete** Delete a q850 to SIP mapping. Enter the q850 code.

**edit** Edit a response map by number

### Path

**q850-sip-map** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > q850-sip-map**.

### Release

First appearance: 4.0

### RTC Status

Supported

---

## q850-sip-map > entries

The entries subelement is used to create the mapping of q850 cause to SIP reason code.

### Parameters

**q850-cause** Enter the q850 cause code to map to a SIP reason code

**sip-status** Enter the SIP response code that maps to this q850 cause code

- Values: Min: 100 | Max: 699

**sip-reason** Describe the mapped SIP response code

### Path

**entries** is a subelement under the **q850-sip-map** configuration element, which is located under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > q850-sip-map > entries**.

### Release

First appearance: 4.0

### RTC Status


Supported

## realm-config


---

The realm-config element is used to configure realms.

### Parameters

<b>identifier</b>	Enter the name of the realm associated with this Oracle Communications Session Border Controller. This is a required field. The identifier field value must be unique.
<b>description</b>	Provide a brief description of the realm-config configuration element
<b>addr-prefix</b>	<p>Enter the IP address prefix used to determine if an IP address is associated with the realm. This field is entered as an IP address and number of bits in the network portion of the address in standard slash notation.</p> <ul style="list-style-type: none"><li>• Default: 0.0.0.0</li></ul> <p>An IPV6 address is valid for this parameter.</p>
<b>network-interface</b>	<p>Enter the network interface through which this realm can be reached. Entries in this parameter take the form: <b>&lt;network-interface-ID&gt;:&lt;subport&gt;.&lt;ip_version&gt;</b>.</p> <p> <b>Note:</b> Only one network interface can be assigned to a single realm-config object.</p>
<b>mm-in-realm</b>	<p>Enable or disable media being steered through the Oracle Communications Session Border Controller when the communicating endpoints are located in the same realm</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>mm-in-network</b>	<p>Enable or disable media being steered through the Oracle Communications Session Border Controller when the communicating endpoints are located in different realms within the same network (on the same network-interface). If this field is set to enabled, the Oracle Communications Session Border Controller will steer all media traveling between two endpoints located in different realms, but within the same network. If this field is set to disabled, then each endpoint will send its media directly to the other endpoint located in a different realm, but within the same network.</p> <ul style="list-style-type: none"><li>• Default: enabled</li></ul>



	<ul style="list-style-type: none"> <li>Values: enabled   disabled</li> </ul>
<b>mm-same-ip</b>	<p>Enable the media to go through this Oracle Communications Session Border Controller if the mm-in-realm . When not enabled, the media will not go through the Oracle Communications Session Border Controller for endpoints that are behind the same IP.</p> <ul style="list-style-type: none"> <li>Default: enabled</li> <li>Values: enabled   disabled</li> </ul>
<b>mm-in-system</b>	<p>Set this parameter to enabled to manage/latch/steer media in the Oracle Communications Session Border Controller. Set this parameter to disabled to release media in the Oracle Communications Session Border Controller.</p> <p> <b>Note:</b> Setting this parameter to disabled will cause the Oracle Communications Session Border Controller to NOT steer media through the system (no media flowing through this Oracle Communications Session Border Controller).</p> <ul style="list-style-type: none"> <li>Default: enabled</li> <li>Values: enabled   disabled</li> </ul>
<b>bw-cac-non-mm</b>	<p>Set this parameter to enabled to turn on bandwidth CAC for media release</p> <ul style="list-style-type: none"> <li>Default: disabled</li> <li>Values: enabled   disabled</li> </ul>
<b>msm-release</b>	<p>Enable or disable the inclusion of multi-system (multiple Oracle Communications Session Border Controllers) media release information in the SIP signaling request sent into the realm identified by this realm-config element. If this field is set to enabled, another Oracle Communications Session Border Controller is allowed to decode the encoded SIP signaling request message data sent from a SIP endpoint to another SIP endpoint in the same network to restore the original SDP and subsequently allow the media to flow directly between those two SIP endpoints in the same network serviced by multiple Oracle Communications Session Border Controllers. If this field is set to disabled, the media and signaling will pass through both Oracle Communications Session Border Controllers. If this field is set to enabled, the media is directed directly between the endpoints of a call.</p> <ul style="list-style-type: none"> <li>Default: disabled</li> <li>Values: enabled   disabled</li> </ul>
<b>qos-enable</b>	<p>Enable or disable the use of QoS in this realm</p> <ul style="list-style-type: none"> <li>Default: disabled</li> <li>Values: enabled   disabled</li> </ul>
<b>generate-udp-checksum</b>	<p>Enable or disable the realm to generate a UDP checksum for RTP/RTCP packets.</p> <ul style="list-style-type: none"> <li>Default: disabled</li> <li>Values: enabled   disabled</li> </ul>
<b>max-bandwidth</b>	<p>Enter the total bandwidth budget in kilobits per second for all flows to/from the realm defined in this element. A max-bandwidth field value of 0 indicates unlimited bandwidth.</p> <ul style="list-style-type: none"> <li>Default: 0</li> <li>Values: Min: 0 / Max: 4294967295</li> </ul>
<b>fallback-bandwidth</b>	<p>Enter the amount of bandwidth available once the Oracle Communications Session Border Controller has determined that the target (of ICMP pings) is unreachable.</p> <ul style="list-style-type: none"> <li>Default: 0</li> <li>Values: Min: 0</li> </ul>

<b>max-priority-bandwidth</b>	<p>Enter the amount of bandwidth amount of bandwidth you want to want to use for priority (emergency) calls; the system first checks the max-bandwidth parameter, and allows the call if the value you set for priority calls is sufficient.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 999999999</li></ul>
<b>max-latency</b>	<p>Enter the maximum latency in milliseconds allowed for flows within this realm. If this parameter is set to 0, then no alarm condition is set and no requests to/from the realm are rejected. Reserved for future use.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 4294967295</li></ul>
<b>max-jitter</b>	<p>Enter the maximum jitter in milliseconds allowed for flows within this realm. If this field is set to 0, then no alarm condition is set and no requests to/from the realm are rejected. Reserved for future use.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 4294967295</li></ul>
<b>max-packet-loss</b>	<p>Enter the maximum packet loss percentage in hundredths of a percent allowed for flows within this realm. If this parameter is set to 0, then no alarm condition is set and no requests to/from the realm are rejected. Reserved for future use.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 4294967295</li></ul>
<b>observ-window-size</b>	<p>Enter the minimum time in milliseconds a threshold (latency, jitter, and packet loss) must be exceeded before triggering an alarm. Reserved for future use.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 4294967295</li></ul>
<b>parent-realm</b>	<p>Enter the parent realm for this particular realm. This must reference an existing realm identifier.</p>
<b>dns-realm</b>	<p>Enter the realm whose network interface's DNS server should be used to resolve FQDNs for requests sent into the realm. If this field value is left empty, the Oracle Communications Session Border Controller will use the DNS of the realm's network interface.</p>
<b>media-policy</b>	<p>Select a media-policy on a per-realm basis (via an association between the name field value configured in this field). When the Oracle Communications Session Border Controller first sets up a SIP or H.323 media session, it identifies the egress realm of each flow and then determines the media-policy element to apply to the flow. This parameter must correspond to a valid name entry in a media policy element.</p>
<b>media-sec-policy</b>	<p>Name of default media security policy.</p>
<b>srtplib-msm-passthrough</b>	<p>Enables multi system selective SRTP pass through in this realm.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>class-profile</b>	<p>Enter the name of class-profile to use for this realm for ToS marking</p>
<b>in-translationid</b>	<p>Enter the identifier/name of a session-translation element. The Oracle Communications Session Border Controller applies this group of rules to the incoming addresses for this realm. There can be only one entry in this parameter.</p>

<b>out-translationid</b>	Enter the identifier/name of a session-translation element. The Oracle Communications Session Border Controller applies this group of rules to the outgoing addresses for this realm. There can be only one entry in this parameter.
<b>in-manipulationid</b>	Enter the inbound SIP manipulation rule name
<b>out-manipulationid</b>	Enter the outbound SIP manipulation rule name
<b>average-rate-limit</b>	Enter the average data rate in bits per second for host path traffic from a trusted source <ul style="list-style-type: none"> <li>• Default: 0 (disabled)</li> <li>• Values: Min: 0   Max: 4294967295</li> </ul>
<b>access-control-trust-level</b>	Select a trust level for the host within the realm <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: <ul style="list-style-type: none"> <li>• high—Hosts always remains trusted</li> <li>• medium—Hosts belonging to this realm can get promoted to trusted, but can only get demoted to untrusted. Hosts will never be put in black-list.</li> <li>• low—Hosts can be promoted to trusted list or can get demoted to untrusted list</li> <li>• none—Hosts will always remain untrusted. Will never be promoted to trusted list or will never get demoted to untrusted list</li> </ul> </li> </ul>
<b>invalid-signal-threshold</b>	Enter the acceptable invalid signaling message rate falling within a tolerance window <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 4294967295</li> </ul>
<b>maximum-signal-threshold</b>	Enter the maximum number of signaling messages allowed within the tolerance window <ul style="list-style-type: none"> <li>• Default: 0 (disabled)</li> <li>• Values: Min: 0   Max: 4294967295</li> </ul>
<b>untrusted-signal-threshold</b>	Enter the allowed maximum signaling messages within a tolerance window. <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 4294967295</li> </ul>
<b>nat-trust-threshold</b>	Enter maximum number of denied endpoints that set the NAT device they are behind to denied. 0 means dynamic demotion of NAT devices is disabled. <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 65535</li> </ul>
<b>deny-period</b>	Enter the length of time an entry is posted in the deny list <ul style="list-style-type: none"> <li>• Default: 30</li> <li>• Values: Min: 0 / Max: 4294967295</li> </ul>
<b>cac-failure-threshold</b>	Enter the number of CAC failures for any single endpoint that will demote it from the trusted queue to the untrusted queue for this realm. <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 141842</li> </ul>
<b>untrust-cac-failure-threshold</b>	Enter the number of CAC failures for any single endpoint that will demote it from the untrusted queue to the denied queue for this realm. <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 4294967295</li> </ul>

<b>ext-pol-server</b>	Name of external policy server.
<b>diam-e2-address-realm</b>	The value inserted into a Diameter e2 Address-Realm AVP when a message is received on this realm.
<b>symmetric-latching</b>	Enable or disable symmetric latching between endpoints for RTP traffic
<b>pai-strip</b>	<p>Enable or disable P-Asserted-Identity headers being stripped from SIP messages as they exit the Oracle Communications Session Border Controller. The PAI header stripping function is dependent on this parameter and the trust-me parameter.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>trunk-context</b>	Enter the default trunk context for this realm
<b>early-media-allow</b>	<p>Select the early media suppression for the realm</p> <ul style="list-style-type: none"><li>• Values:<ul style="list-style-type: none"><li>• none: No early media is allowed in either direction</li><li>• both: Early media is allowed in both directions</li><li>• reverse: Early media received by Oracle Communications Session Border Controller in the reverse direction is allowed</li></ul></li></ul>
<b>enforcement-profile</b>	Enter the name of the enforcement profile (SIP allowed methods).
<b>additional-prefixes</b>	Enter one or more additional address prefixes. Not specifying the number of bits to use implies all 32 bits of the address are used to match.
<b>add-additional-prefixes</b>	Add one or more additional address prefixes. Not specifying the number of bits to use implies all 32 bits of the address are used to match.
<b>remove-additional-prefixes</b>	Remove one or more additional address prefixes. Not specifying the number of bits to use implies all 32 bits of the address are used to match.
<b>restricted-latching</b>	<p>Set the restricted latching mode</p> <ul style="list-style-type: none"><li>• Default: None</li><li>• Values:<ul style="list-style-type: none"><li>• none: No restricted latching</li><li>• sdp: Use the IP address specified in the SDP for latching purpose</li><li>• peer-ip: Use the peer-ip (Layer 3 address) for the latching purpose</li></ul></li></ul>
<b>restriction-mask</b>	<p>Set the restricted latching mask value</p> <ul style="list-style-type: none"><li>• Default: 32</li><li>• Values: Min: 1   Max: 128</li></ul>
<b>user-cac-mode</b>	<p>Set this parameter to the per user CAC mode that you want to use</p> <ul style="list-style-type: none"><li>• Default: none</li><li>• Values:<ul style="list-style-type: none"><li>• none—No user CAC for users in this realm</li><li>• AOR—User CAC per AOR</li><li>• IP—User CAC per IP</li></ul></li></ul>
<b>user-cac-bandwidth</b>	Enter the maximum bandwidth per user for dynamic flows to and from the user. By leaving this parameter set to 0 (default), there is unlimited bandwidth and the per user CAC feature is disabled for constraint of bandwidth.

<b>user-cac-sessions</b>	<p>Enter the maximum number of sessions per user for dynamic flows to and from the user. Leaving this parameter set to 0 (default), there is unlimited sessions and the CAC feature is disabled for constraint on sessions</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>icmp-detect-multiplier</b>	<p>Enter the multiplier to use when determining how long to send ICMP pings before considering a target unreachable. This number multiplied by the time set for the icmp-advertisement-interval determines the length of time</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0</li> </ul>
<b>icmp-advertisement-interval</b>	<p>Enter the time in seconds between ICMP pings the Oracle Communications Session Border Controller sends to the target.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0</li> </ul>
<b>icmp-target-ip</b>	<p>Enter the IP address to which the Oracle Communications Session Border Controller should send the ICMP pings so that it can detect when they fail and it needs to switch to the fallback bandwidth for the realm.</p> <ul style="list-style-type: none"> <li>• Default: (empty)</li> </ul>
<b>monthly-minutes</b>	<p>Enter the monthly minutes allowed</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: Min: 0 / Max: 71582788</li> </ul>
<b>options</b>	<p>Enter any optional features or parameters</p>
<b>accounting-enable</b>	<p>Select whether you want accounting enabled within the realm</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>net-management-control</b>	<p>Enable or disable network management controls for this realm</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>delay-media-update</b>	<p>Enable or disable media update delay</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>refer-call-transfer</b>	<p>REFER call transfer</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled   dynamic</li> </ul>
<b>refer-notify-provisional</b>	<p>Provisional mode for sending NOTIFY message</p> <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: <ul style="list-style-type: none"> <li>• none: no intermediate NOTIFY's are to be sent</li> <li>• initial: immediate 100 Trying NOTIFY has to be sent</li> <li>• all: immediate 100 Trying NOTIFY plus a NOTIFY for each non-100 provisional received by the SD are to be sent</li> </ul> </li> </ul>

<b>dyn-refer-term</b>	<p>Enable or disable the Oracle Communications Session Border Controller to terminate a SIP REFER and issue a new INVITE. If the dyn-refer-term value is disabled (the default), proxy the REFER to the next hop to complete REFER processing. If the dyn-refer-termvalue is enabled, terminate the REFER and issue an new INVITE to the referred party to complete REFER processing.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>constraint-name</b>	<p>Enter the name of the constraint you want to use for this realm</p>
<b>call-recording-server-id</b>	<p>Enter the name of the call recording server associated with this realm</p>
<b>xnq-state</b>	<p>set XNQ removal status within this realm</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>hairpin-id</b>	<p>hairpin id.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: 1-65535   0= disabled</li></ul>
<b>manipulation-string</b>	<p>Enter a string to be used in header manipulation rules for this realm.</p>
<b>manipulation-pattern</b>	<p>Enter the regular expression to be used in header manipulation rules for this realm.</p>
<b>stun-enable</b>	<p>Enable or disable the STUN server support for this realm</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>stun-server-ip</b>	<p>Enter the IP address for the primary STUN server port</p> <ul style="list-style-type: none"><li>• Default: 0.0.0.0</li></ul>
<b>stun-server-ip</b>	<p>Enter the IP address for the primary STUN server port</p> <ul style="list-style-type: none"><li>• Default: 0.0.0.0</li></ul>
<b>stun-server-port</b>	<p>Enter the port to use with the stun-server-ip for primary STUN server port</p> <ul style="list-style-type: none"><li>• Default: 3478</li><li>• Values: Min. 1025   Max. 65535</li></ul>
<b>stun-changed-ip</b>	<p>Enter the IP address for the CHANGED-ADDRESS attribute in Binding Requests received on the primary STUN server port; must be different from than the one defined for the stun-server-ip</p> <ul style="list-style-type: none"><li>• Default: 0.0.0.0</li></ul>
<b>stun-changed-port</b>	<p>Enter the port combination to define the CHANGED-ADDRESS attribute in Binding Requests received on the primary STUN server port</p> <ul style="list-style-type: none"><li>• Default: 3479</li><li>• Values: Min. 1025   Max. 65535</li></ul>
<b>sip-profile</b>	<p>Enter the name of the sip-profile to apply to this realm.</p>
<b>sip-isup-profile</b>	<p>Enter the name of the sip-isup-profile to apply to this realm.</p>

<b>match-media-profiles</b>	Enter the media profiles you would like applied to this realm in the form <name>::<subname>. See the Oracle Communications Session Border Controller Configuration Guide for information about wildcard values.
<b>qos-constraints</b>	Enter the name value from the QoS constraints configuration you want to apply to this realm
<b>block-rtcp</b>	Block RTCP from entering or leaving this realm. <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>hide-egress-media-update</b>	Hide changes to ingress RTP egressing into this realm <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>subscription-id-type</b>	Sets the supported Subscription ID Types and the subsequent values inserted into the Subscription-Id-Data AVP's in an AAR message for Rx transactions. <ul style="list-style-type: none"> <li>• END_USER_NONE   END_USER_E164   END_USER_SIP_URI   END_USER_IMSI</li> </ul>
<b>tcp-media-profile</b>	A configured tcp-media-profile name to use within this realm. Used for MSRP.
<b>stun-server-port</b>	Enter the port to use with the stun-server-ip for primary STUN server port <ul style="list-style-type: none"> <li>• Default: 3478</li> <li>• Values: Min. 1025   Max. 65535</li> </ul>
<b>tcp-media-profile</b>	A configured tcp-media-profile name to use within this realm. Used for MSRP.
<b>monitoring-filters</b>	Comma-separated list of monitoring filters used for SIP monitor and trace.
<b>node-functionality</b>	Sets the value inserted into the node-functionality AVP in Rf messages going into this realm. <ul style="list-style-type: none"> <li>• P-CSCF</li> <li>• BGCF</li> <li>• IBCF</li> <li>• E-CSCF</li> <li>• "" - This indicates that this realm should revert to the global node-functionality value.</li> </ul>

## Path

**realm-config** is an element under the **media-manager** path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > realm-config**.

## Release

First appearance: 1.0 / Most recent update: S-C6.1.0

## RTC Status

Supported



**Note:** This is a multiple instance configuration subelement.

## realm-group

The realm-group configuration element allows you to configure realm groups. Realm groups are sets of source and destination realms that allow early media to flow in the direction you configure.

### Parameters

<b>name</b>	Enter the name of this realm group
<b>source-realm</b>	Enter the list of one or more global/SIP realms that you want to designate as source realms for the purpose of blocking early media; this is the realm identifier value for the realms you want on the list. To enter more than one realm in this list, list all items separated by a comma and enclose the entire entry in quotation marks.
<b>destination-realm</b>	Enter the list of one or more global/SIP realms that you want to designate as destination realms for the purpose of blocking early media; this is the realm identifier value for the realms you want on the list. To enter more than one realm in the list, list all items separated by a comma and enclose the entire entry in quotation marks
<b>early-media-allow-direction</b>	<div>Set the direction for which early media is allowed for this realm group.</div> <ul style="list-style-type: none"><li>• Default: both</li><li>• Values:</li><li>• none—Turns off the feature for this realm group by blocking early media</li><li>• reverse - Allows early media to flow from called to caller.</li><li>• both - Allows early media to flow to/from called and caller</li></ul>
<b>state</b>	<div>Enable or disable this realm group</div> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>

### Path

**realm-group** is an element of the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > realm-group**.

### Release

First appearance: 4.1.4

### RTC Status


Supported

## redundancy


---




The redundancy element establishes HA parameters for a Oracle Communications Session Border Controller that participates in an HA architecture.

### Parameters

<b>state</b>	<div>Enable or disable HA for the Oracle Communications Session Border Controller</div> <ul style="list-style-type: none"><li>• Default enabled</li><li>• Values enabled   disabled</li></ul> <div> <b>Note:</b> This parameter is not RTC supported.</div>
<b>log-level</b>	<div>Select the starting log level for the HA process. This value supersedes the value configured in the process-log-level field in the system-config element for the HA process</div> <ul style="list-style-type: none"><li>• Default: info</li></ul>



	<ul style="list-style-type: none"> <li>• Values: <ul style="list-style-type: none"> <li>• emergency</li> <li>• critical</li> <li>• major</li> <li>• minor</li> <li>• warning</li> <li>• notice</li> <li>• info</li> <li>• trace</li> <li>• debug</li> <li>• detail</li> </ul> </li> </ul>
<b>health-threshold</b>	<p>Enter the health score at which standby Oracle Communications Session Border Controller switches over to the Active state and takes control of all system functionality as the active Oracle Communications Session Border Controller</p> <ul style="list-style-type: none"> <li>• Default: 75</li> <li>• Values: Min: 1   Max: 100</li> </ul>
<b>emergency-threshold</b>	<p>Enter the low health score value that triggers the initializing standby Oracle Communications Session Border Controller to become the active Oracle Communications Session Border Controller immediately. In addition, the active but unhealthy Oracle Communications Session Border Controller, regardless of its health, will not relinquish its Active state if the HA Oracle Communications Session Border Controller peer poised to become active upon switchover also has a health score below this emergency-threshold value.</p> <ul style="list-style-type: none"> <li>• Default: 50</li> <li>• Values: Min: 1   Max: 100</li> </ul>
<b>port</b>	<p>Enter the port number on which the border element redundancy protocol is listening</p> <ul style="list-style-type: none"> <li>• Default: 9090</li> <li>• Values: Min: 1025   Max: 65535</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>advertisement-time</b>	<p>Enter the time in milliseconds the Oracle Communications Session Border Controller continually sends its health score to its HA Oracle Communications Session Border Controller peer(s)</p> <ul style="list-style-type: none"> <li>• Default: 500</li> <li>• Values: Min: 50   Max: 999999999</li> </ul>
<b>percent-drift</b>	<p>Set the percentage of an HA Oracle Communications Session Border Controller peer's advertisement time for this HA Oracle Communications Session Border Controller to wait before considering its peer to be out of service</p> <ul style="list-style-type: none"> <li>• Default: 210</li> <li>• Values: Min: 100   Max: 65535</li> </ul>
<b>initial-time</b>	<p>Enter the number of milliseconds to set the longest amount of time the Oracle Communications Session Border Controller will wait at boot time to change its state from initial to either becoming active or becoming standby. This field is independent of the advertisement-time and percent-drift parameters; it is a timer used to decide the state transition.</p> <ul style="list-style-type: none"> <li>• Default: 1250</li> <li>• Values: Min: 5 / Max: 999999999</li> </ul>

<b>becoming-standby-time</b>	<p>Enter the time in milliseconds to wait before transitioning to the Standby state. This field allows the HA Oracle Communications Session Border Controller enough time to synchronize with its HA Oracle Communications Session Border Controller peer. If the HA Oracle Communications Session Border Controller has not become fully synchronized within the time frame established in this field, it will be declared out of service. We recommend setting this parameter to no less than 180000 if configuration checkpointing is used.</p> <ul style="list-style-type: none"><li>• Default: 45000</li><li>• Values: Min: 5 / Max: 999999999</li></ul>
<b>becoming-active-time</b>	<p>Enter the time in milliseconds a previously standby Oracle Communications Session Border Controller takes to become active. This field applies to the following scenarios:</p> <ul style="list-style-type: none"><li>• When the health of an active Oracle Communications Session Border Controller has failed</li><li>• When the standby Oracle Communications Session Border Controller is healthier than the active Oracle Communications Session Border Controller</li></ul>
<b>becoming-active-time</b>	<p>Enter the time in milliseconds a previously standby Oracle Communications Session Border Controller takes to become active. This field applies to the following scenarios:</p> <ul style="list-style-type: none"><li>• When the health of an active Oracle Communications Session Border Controller has failed</li><li>• When the standby Oracle Communications Session Border Controller is healthier than the active Oracle Communications Session Border Controller</li></ul> <p>This is a transitional state.</p> <ul style="list-style-type: none"><li>• Default: 100</li><li>• Values: Min: 5 / Max: 999999999</li></ul>
<b>cfg-port</b>	<p>Enter the port number from which HA checkpoint messages are sent and received. This field supports Configuration Checkpointing. Setting the cfg-port field value to 0 disables configuration checkpointing.</p> <ul style="list-style-type: none"><li>• Default: 1987</li><li>• Values: Min: 1025 / Max: 65535; 0</li></ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>cfg-max-trans</b>	<p>Enter the size of the HA checkpoint transaction list to store in memory at a time</p> <ul style="list-style-type: none"><li>• Default: 10000</li><li>• Values: Min: 0 / Max: 4294967295</li></ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>cfg-sync-start-time</b>	<p>Enter the time in milliseconds before HA Oracle Communications Session Border Controller begins sending HA configuration checkpointing requests. This timer begins immediately upon entering the Active state. As long as the active peer is healthy and active, it remains in a constant cycle of (re)setting this parameter's timer and checking to see if it has become standby.</p> <ul style="list-style-type: none"><li>• Default: 5000</li><li>• Values: Min: 0 / Max: 4294967295</li></ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>cfg-sync-comp-time</b>	<p>Enter the time in milliseconds the standby Oracle Communications Session Border Controller waits before checkpointing with the active Oracle Communications Session Border Controller</p>

to obtain the latest configuration transaction information once the initial checkpointing process is complete.

- Default: 1000
- Values: Min: 0 / Max: 4294967295



**Note:** This parameter is not RTC supported.

**gateway-  
heartbeat-interval**

Enter the time in seconds between heartbeats on the front interface gateway. This parameter is applicable until a front interface gateway failure occurs. This parameter applies globally to Oracle Communications Session Border Controllers operating in an HA node, but can be overridden on a network interface-by-network interface basis by the value configured in the gw-heartbeat: heartbeat field of the gw-heartbeat subelement in the network-interface element.

- Default: 0
- Values: Min: 0 / Max: 65535



**Note:** This parameter is not RTC supported.

**gateway-  
heartbeat-retry**

Enter the number of front interface gateway heartbeat retries after a front interface gateway failure occurs. The value configured in this field applies globally to Oracle Communications Session Border Controllers operating in HA pair architectures, but can be overridden on a per network interface basis by the value configured in the gw-heartbeat: retry-count field.

- Default: 0
- Values: Min: 0 / Max: 65535



**Note:** This parameter is not RTC supported.

**gateway-  
heartbeat-timeout**

Enter the heartbeat retry timeout value in seconds between subsequent ARP requests to establish front interface gateway communication after a front interface gateway failure occurs. The value configured in this field applies globally to Oracle Communications Session Border Controllers operating in HA pair architectures, but can be overridden on a network interface basis by the value configured in the gw-heartbeat: retry-timeout field.

- Default: 1
- Values: Min: 0 / Max: 65535



**Note:** This parameter is not RTC supported.

**gateway-  
heartbeat-health**

Enter the health score amount to subtract if the timeout value set in the gateway-heartbeat-timeout field has been exceeded without receiving a response from the front interface gateway. The value configured in this field applies globally to Oracle Communications Session Border Controllers operating in HA nodes, but can be overridden on a network interface basis by the value configured in the gw-heartbeat > health-score field of the gw-heartbeat. A field value of 0 means that the health score is not affected.

- Default: 0
- Values: Min: 0 / Max: 100



**Note:** This parameter is not RTC supported.

**media-if-  
peercheck-time**

Enter the amount of time in milliseconds for the standby system in an HA node to receive responses to its ARP requests via the front interface before it takes over the active role from its counterpart. A value of 0 turns the HA front interface keepalive off

- Default: 0

- Values: Min: 0 / Max: 500

**peers** Access the peers subelement

### Path

**redundancy** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > redundancy**.

### Release

First appearance: 1.1 / Most recent update: 1.2.1

### RTC Status

This element has both supported and unsupported parameters. Unsupported parameters are marked with a note.



**Note:** This is a single instance configuration element.

## redundancy > peers

---

The peers subelement establishes the name and state of an HA node.

### Parameters

**state** Enable or disable HA

- Default: enabled
- Values: enabled | disabled

**type** Select the HA peer type and which utility address to use

- Default: unknown
- Values:
  - primary—HA peer set as the primary Oracle Communications Session Border Controller. It is associated with the utility address configured in the pri-utility-addr field of each network-interface element.
  - secondary—HA peer set as the secondary Oracle Communications Session Border Controller. It is associated with the utility address configured in the sec-utility-addr field of each network-interface element.
  - unknown—Not assigned HA peer type with associated utility address unknown. This type field option is not valid for configuration checkpointing. Although unknown is the default value, Primary or Secondary field option must be set in order for configuration checkpointing to function properly.

**destinations** Access the destinations subelement

### Path

**peers** is a subelement under the redundancy element. The full path from the topmost ACLI prompt is: **configure terminal > system > redundancy > peers**.

### Release

First appearance: 1.0.1 / Most recent update: 1.2.1

**RTC Status**

Unsupported

**Note:** This is a multiple instance configuration subelement.**redundancy > peers > destinations**

The destinations subelement establishes locations where health and state information is sent and received.

**Parameters**

<b>address</b>	Enter the IP address and port on the interface of the HA Oracle Communications Session Border Controller peer where this HA Oracle Communications Session Border Controller peer sends HA messages. The parameter format is an IP address and port combination (IP address:port). This IP address must match the interface identified in its HA Oracle Communications Session Border Controller peer's corresponding rdncy-peer-dest > network-interface field. The port portion of this parameter must match the port identified in its HA Oracle Communications Session Border Controller peer's corresponding port field.
<b>network-interface</b>	Enter the name and subport ID of the interface where the HA Oracle Communications Session Border Controller receives HA messages (e.g., wancom1:0). Valid interface names are wancom1 and wancom2 only.

**Path**

**destinations** is a subelement under the peers subelement. The full path from the topmost ACLI prompt is: **configure terminal > system > redundancy > peers > destinations**

**Release**

First appearance: 1.0.1

**RTC Status**

Unsupported

**Note:** The destinations prompt is displayed as: rdncy-peer-dest. This is a multiple instance configuration element.**rph-policy**

The rph-policy element defines an override resource value and an insert resource value for ETS/WPS namespaces. These are applied to NMC rules.

**Parameters**

<b>name</b>	Enter the name of this RPH policy; this is the value used when applying this RPH policy to an NMC rule. <ul style="list-style-type: none"> <li>Default: None</li> </ul>
<b>override-r-value</b>	Set the value the Oracle Communications Session Border Controller uses to override the r-values in the original RPH. <ul style="list-style-type: none"> <li>Default: None</li> </ul>

**insert-r-value** Set the value the Oracle Communications Session Border Controller inserts into the RPH.

### Path

**rph-policy** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > rph-policy**.

### Release

First appearance: 5. 1

### RTC Status

Supported

## rph-profile

---

The rph-profile contains information about how the Oracle Communications Session Border Controller should act on the namespace(s) present in Resource-Priority headers.

### Parameters

- |                       |   |
|-----------------------|---|
| <b>name</b>           | Enter the name of this RPH profile; this is the value used when applying this RPH profile to an NMC rule. <ul style="list-style-type: none"><li>• Default: none</li></ul>                                   |
| <b>r-value</b>        | Enter a list of one or more r-values used for matching; WPS values must be entered before ETS values. <ul style="list-style-type: none"><li>• Default: none</li></ul>                                       |
| <b>media-policy</b>   | Enter the name of this RPH profile; this is the value used when applying this RPH profile to an NMC rule. <ul style="list-style-type: none"><li>• Default: none</li></ul>                                   |
| <b>call-treatment</b> | Select the call treatment method for a non-ETS call that contains RPH matching this profile. <ul style="list-style-type: none"><li>• Default: accept</li><li>• Values: accept   reject   priority</li></ul> |

### Path

**rph-profile** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > rph-profile**.

### Release

First appearance: 5. 1

### RTC Status

Supported

## sdes-profile

The sdes-profile configuration element lets you configure the parameter values offered or accepted during SDES negotiation.

### Parameters

<b>name</b>	Sets the name of this object.
<b>crypto-list</b>	<p>Sets the the encryption and authentication algorithms accepted or offered by this sdes-profile</p> <ul style="list-style-type: none"> <li>• Default: AES_CM_128_HMAC_SHA1_80</li> <li>• Values: AES_CM_128_HMAC_SHA1_80   AES_CM_128_HMAC_SHA1_32</li> </ul>
<b>srtp-auth</b>	<p>UNUSED</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>srtp-encrypt</b>	<p>This parameter enables or disables the encryption of RTP packets. With encryption enabled, the default condition, the Oracle Communications Session Border Controller offers RTP encryption, and rejects an answer that contains an UNENCRYPTED_SRTP session parameter in the crypto attribute.</p> <p>With encryption disabled, the Oracle Communications Session Border Controller does not offer RTP encryption and includes an UNENCRYPTED_SRTP session parameter in the SDP crypto attribute; it accepts an answer that contains an UNENCRYPTED_SRTP session parameter.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>srtcp-encrypt</b>	<p>This parameter enables or disables the encryption of RTCP packets. With encryption enabled, the default condition, the Oracle Communications Session Border Controller offers RTCP encryption, and rejects an answer that contains an UNENCRYPTED_SRTCP session parameter in the crypto attribute.</p> <p>With encryption disabled, the Oracle Communications Session Border Controller does not offer RTCP encryption and includes an UNENCRYPTED_SRTCP session parameter in the SDP crypto attribute; it accepts an answer that contains an UNENCRYPTED_SRTCP session parameter.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>mki</b>	<p>This parameter enables or disables the inclusion of the MKI:length field in the SDP crypto attribute.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: <ul style="list-style-type: none"> <li>• enabled – an MKI field is sent within the crypto attribute (16 bytes maximum)</li> <li>• disabled – no MKI field is sent</li> </ul> </li> </ul>
<b>egress-offer-format</b>	<p>Sets any manipulation on SDP offer.</p> <ul style="list-style-type: none"> <li>• Default: same-as-ingress</li> <li>• Values: <ul style="list-style-type: none"> <li>• same-as-ingress - the Oracle Communications Session Border Controller leaves the profile of the media lines unchanged.</li> <li>• simultaneous-best-effort - the Oracle Communications Session Border Controller Adds an RTP/SAVP media line for any media profile that has only the RTP/AVP media profile, and Adds an RTP/AVP media line for any media profile that has only the RTP/SAVP media profile</li> </ul> </li> </ul>

- use-ingress-session-params** Enter the list of values for which the Oracle Communications Session Border Controller will accept and (where applicable) mirror the UA's proposed cryptographic session parameters:
- **srtplib-auth**—Decides whether or not authentication is performed in SRTP
  - **srtplib-encrypt**—Decides whether or not encryption is performed in SRTP
  - **srtplib-encrypt**—Decides whether or not encryption is performed in SRTCP

```
ACMEPACKET(sdes-profile) # use-ingress-session-params "srtplib-auth srtplib-encrypt
srtplib-encrypt"
```

### Path

**sdes-profile** is a configuration element under the `security > media-security` path. The full path from the topmost CLI prompt is: **configure terminal > security > media-security > sdes-profile**.

## security-config

---

The `security-config` configuration element allows you to configure global TLS parameters.

### Parameters

- |                                   |   |
|-----------------------------------|---|
| <b>ocsr-monitoring-traps</b>      | Enable ocsr monitoring traps <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>  |
| <b>srtplib-msm-password</b>       | The shared secret used to derive the key for encrypting SDES or MIKEY keying material that is placed in the media attribute of an SDP media description.  |
| <b>srtplib-msm-attr-name</b>      | Specifies the name of the media attribute used to convey SDES or MIKEY keying information within a SDP media description. <ul style="list-style-type: none"><li>• Default: X-acme-srtplib-msm</li></ul> |
| <b>image-integrity-value</b>      | Sets the known SHA-256 HMAC value that is computed for the boot image.  |
| <b>local-cert-exp-trap-int</b>    | The local certificate expiration trap interval. <ul style="list-style-type: none"><li>• Default: 0 (disabled)</li></ul>   |
| <b>local-cert-exp-warn-period</b> | The local certificate expiration warning period. <ul style="list-style-type: none"><li>• Default: 0 (disabled)</li></ul>  |

Path: **security-config** is an element of the `security` path. The full path from the topmost CLI prompt is: **configure terminal > security > security-config**.

### Release

First appearance: 6.3

## session-agent

---


The `session-agent` element defines a signaling endpoint that can be configured to apply traffic shaping attributes and information regarding next hops or previous hops.



**Parameters**


<b>hostname</b>	Enter the hostname of this session agent. This is a required entry that must follow the Hostname (or FQDN) Format or the IP Address Format. Hostname values must be unique. An IPV6 address is valid for this parameter.
<b>ip-address</b>	Enter the IP address of session agent if hostname value is an FQDN An IPV6 address is valid for this parameter.
<b>port</b>	Enter the port number for this session agent. <ul style="list-style-type: none"> <li>• Default: 5060</li> <li>• Values: Min: 0; 1025   Max: 65535</li> </ul>
<b>state</b>	Enable or disable the session agent <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>app-protocol</b>	Select the signaling protocol used to signal with the session agent <ul style="list-style-type: none"> <li>• Default: SIP</li> <li>• Values: H323   SIP</li> </ul>
<b>app-type</b>	Set the H.323 session agent type as a gateway or a gatekeeper. This field is mandatory if the app-protocol parameter is set to H323. If the app-protocol parameter is set to SIP, then this field must be left blank. <ul style="list-style-type: none"> <li>• Values: H323-GW   H323-GK</li> </ul>
<b>transport-method</b>	Select the IP protocol used for communicating with this session agent <ul style="list-style-type: none"> <li>• Default: UDP</li> <li>• Values: <ul style="list-style-type: none"> <li>• UDP—UDP used as the transport method</li> <li>• UDP+TCP—Initial transport method of UDP, followed by a subsequent transport method of TCP if and when a failure or timeout occurs in response to a UDP INVITE. If this transport method is selected, then INVITEs are always sent via UDP as long as a response is received.</li> <li>• DynamicTCP—Dynamic TCP connections are the transport method for this session agent. A new connection must be established for each session originating from the session agent. This connection is torn down at the end of a session.</li> <li>• StaticTCP—Static TCP connections are the transport method for this session agent. Once a connection is established, it will remain and not be torn down.</li> <li>• SCTP—SCTP is used as the transport method.</li> <li>• *—support all transport methods</li> </ul> </li> </ul>
<b>realm-id</b>	Enter the realm for sessions coming from or going to this session agent. Entries in this field must follow the Name Format. This field must correspond to a valid identifier field entry in a realm-config.
<b>egress-realm-id</b>	Enter the name of the realm you want defined as the default egress realm used for ping messages. The Oracle Communications Session Border Controller will also use this realm when it cannot determine the egress realm for normal routing.
<b>description</b>	Describe the session-agent element. Entries in this field must follow the Text Format.
<b>carriers</b>	Enter the carrier names associated with this session agent. If this list is empty, any carrier is allowed. If it is not empty, only local policies that reference one or more of the carriers in

	this list will be applied to requests coming from this session agent. This list can contain as many entries within it as necessary. Entries in this field must follow the Carrier Format.
<b>allow-next-hop-lp</b>	<p>Enable or disable the session agent as the next hop in a local policy</p> <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>constraints</b>	<p>Enable or disable the constraints established in this element in the fields that follow (maximum numbers of sessions allowed, maximum session rates, and timeout values) that are applied to the sessions sent to the session agent</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>max-sessions</b>	<p>Enter the maximum number of sessions allowed by the session agent; 0 means there is no constraint</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 4294967295</li></ul>
<b>max-inbound-sessions</b>	<p>Enter the maximum number of inbound sessions allowed from this session agent</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>max-outbound-sessions</b>	<p>Enter the maximum number of simultaneous outbound sessions that are allowed to the session agent; 0 means there is no constraint</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 4294967295</li></ul>
<b>max-burst-rate</b>	<p>Enter the number of session invitations per second allowed to be sent to or received from the session agent. A session is rejected if the calculated per-second rate exceeds this value.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 4294967295</li></ul>
<b>max-inbound-burst-rate</b>	<p>Enter the maximum inbound burst rate in INVITEs per second from this session agent</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>max-outbound-burst-rate</b>	<p>Enter the maximum outbound burst rate in INVITEs per second</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>max-sustain-rate</b>	<p>Enter the maximum rate of session invitations per second allowed to or from the session agent within the current window. The period of time over which the rate is calculated is always between one and two window sizes. A session is rejected only if the calculated per-second rate exceeds the max-sustain-rate value. The value set for the max-sustain-rate field must be larger than the value set for the max-burst-rate field.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 4294967295</li></ul>
<b>max-inbound-sustain-rate</b>	<p>Enter the maximum inbound sustain rate in INVITEs per second</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>

<b>max-outbound-sustain-rate</b>	<p>Enter the maximum outbound sustain rate in INVITEs per second</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>min-seizures</b>	<p>Enter the minimum number of seizures that, when exceeded, cause the session agent to be marked as having exceeded its constraints. Calls will not be routed to the session agent until the time-to-resume has elapsed.</p> <ul style="list-style-type: none"> <li>• Default: 5</li> <li>• Values: Min: 1   Max: 999999999</li> </ul>
<b>min-asr</b>	<p>Enter the minimum percentage, that if the session agent's ASR for the current window falls below this percentage, the session agent is marked as having exceeded its constraints and calls will not be routed to it until the time-to-resume has elapsed</p> <ul style="list-style-type: none"> <li>• Default: 0%</li> <li>• Values: Min: 0% /Max: 100%</li> </ul>
<b>cac-trap-threshold</b>	<p>The CAC (session or burst-rate) utilization threshold expressed as a percent that when exceeded generates a trap</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 100</li> </ul>
<b>time-to-resume</b>	<p>Enter the number of seconds after which the SA (Session Agent) is put back in service (after the SA is taken out-of-service because it exceeded some constraint).</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 4294967295</li> </ul>
<b>ttr-no-response</b>	<p>Enter the time delay in seconds to wait before the SA (Session Agent) is put back in service (after the SA is taken out-of-service because it did not respond to the Oracle Communications Session Border Controller).</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 4294967295</li> </ul>
<b>in-service-period</b>	<p>Enter the time in seconds the session-agent must be operational (once communication is re-established) before the session agent is declared to be in-service. This value gives the session agent adequate time to initialize.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 4294967295</li> </ul>
<b>burst-rate-window</b>	<p>Enter the burst window period in seconds used to measure the burst rate. The term "window" refers to the period of time over which the burst rate is computed.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 4294967295</li> </ul>
<b>sustain-rate-window</b>	<p>Enter the sustained window period in seconds used to measure the sustained rate. The term "window" refers to the period of time over which the sustained rate is computed.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 10   Max: 4294967295</li> </ul> <p>The value you set here must be higher than or equal to the value you set for the burst rate window.</p> <p> <b>Note:</b> If you are going to use this parameter, you must set it to a minimum value of 10.</p>

<b>req-uri-carrier-mode</b>	<p>Select how a carrier determined by the local policy element should be added to the outgoing message</p> <ul style="list-style-type: none"><li>• Default: None</li><li>• Values:<ul style="list-style-type: none"><li>• None—Carrier information will not be added to the outgoing message</li><li>• uri-param—Adds a parameter to the Request-URI (e.g., cic-XXX)</li><li>• prefix—Adds the carrier code as a prefix to the telephone number in the Request-URI (in the same manner as is done in the PSTN)</li></ul></li></ul>
<b>proxy-mode</b>	<p>Select how SIP proxy forwards requests coming from the session agent. If this parameter is empty, its value is set to the value of the proxy-mode parameter in the sip-interface element by default. If the proxy-mode field in the element is also empty, the default is proxy.</p> <ul style="list-style-type: none"><li>• Values<ul style="list-style-type: none"><li>• proxy—If the Oracle Communications Session Border Controller is an SR, the system will proxy the request coming from the session agent and maintain the session and dialog state. If the Oracle Communications Session Border Controller is a Oracle Communications Session Border Controller, system will behave as a B2BUA when forwarding the request.</li><li>• redirect—System will send a SIP 3xx reDIRECT response with contacts (found in the local-policy) to the previous hop</li><li>• record-route—The Oracle Communications Session Border Controller forwards requests with a record-route</li></ul></li></ul>
<b>redirect-action</b>	<p>Select the action the SIP proxy takes when it receives a Redirect (3xx) response from the session agent. If the response comes from a session agent and this field is empty, the system uses the redirect action value defined in the sip-interface.</p> <ul style="list-style-type: none"><li>• Values:<ul style="list-style-type: none"><li>• proxy—SIP proxy passes the response back to the previous hop. The response will be sent based on the proxy-mode of the original request.</li><li>• recurse—SIP proxy sends the original request to the list of contacts in the Contact header of the response, serially (in the order in which the contacts are listed in the response)</li><li>• Recurse-305-only—recurse on the contacts in the 305 response</li></ul></li></ul>
<b>loose-routing</b>	<p>Enable or disable loose routing</p> <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>send-media-session</b>	<p>Enable or disable the inclusion of a media session description in the INVITE sent by the Oracle Communications Session Border Controller. The only instance in which this field should be set to disabled is for a session agent that always redirects requests, meaning that it returns an error or 3xx response instead of forwarding an INVITE message. Setting this field to disabled prevents the Oracle Communications Session Border Controller from establishing flows for that INVITE message until it recurses the 3xx response.</p> <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>response-map</b>	<p>Enter the name of the sip-response-map element set in the session router element to use for translating inbound final response values</p>
<b>ping-method</b>	<p>Enter the SIP message/method to use to “ping” a session agent</p>
<b>ping-interval</b>	<p>Set how often to ping a session agent in seconds</p>

	<ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>ping-send-mode</b>	<p>Set the mode with which you want to send ping messages to session agents</p> <ul style="list-style-type: none"> <li>• Default: keep-alive</li> <li>• Values: keep-alive   continuous</li> </ul>
<b>ping-all-addresses</b>	<p>Enable pinging each IP address dynamically resolved via DNS. If disabled (default), the Oracle Communications Session Border Controller only pings the first available resolved IP address.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>options</b>	<p>Establish customer-specific features and/or parameters. This value can be a comma separated list of "feature=&lt;value&gt;" or "feature" parameters.</p>
<b>media-profiles</b>	<p>Start up an outgoing call as a Fast Start call with the information in the media profile used for the logical channels when the incoming call is slow start for an H.323 operation. This list is used to determine if a source and/or destination of a call is a session agent on that list. If a media profiles list is configured in the matching session-agent element, then the frame and codec information in the corresponding media profile will be used for the outgoing call. If the media-profiles list in the session-agent element is empty, the h323-stack &gt; media-profiles list will be consulted. This field should reference the codec that you expect the gatekeeper/gateway to use. This media-profiles entry must correspond to at least one valid name field entry in a media profile element that has already been configured.</p>
<b>in-translationid</b>	<p>Enter the identifier/name of the configured session translation to apply. The Oracle Communications Session Border ControllerC applies this group of rules to the incoming leg of the call for this session agent. There can be only one entry in this field.</p>
<b>out-translationid</b>	<p>Enter the identifier/name of the configured session translation to apply. The Oracle Communications Session Border Controller applies this group of rules to the outgoing leg of the call for this session agent. There can be only one entry in this field.</p>
<b>trust-me</b>	<p>Enable or disable the trust of this session agent; used for privacy features</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>request-uri-headers</b>	<p>Enter a list of embedded headers extracted from the Contact header that will be inserted in the re INVITE message</p>
<b>stop-recurse</b>	<p>Enter a list of returned response codes that this session agent will watch for in order to stop recursion on the target's or contact's messages</p>
<b>local-response-map</b>	<p>Enter the name of local response map to use for this session agent. This value should be the name of a sip-response-map configuration element.</p>
<b>ping-to-user-part</b>	<p>The user portions of the Request-URI and To: headers that define the destination of a session agent ping message.</p>
<b>ping-from-user-part</b>	<p>The user portion of the From: header that defines the source of a session agent ping message.</p>
<b>li-trust-me</b>	<p>Set this parameter to enabled to designate this session agent as trusted for P-DCS-LAES use</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>in-manipulationid</b>	<p>Enter the name of the SIP header manipulations configuration to apply to the traffic entering the Oracle Communications Session Border Controller via this session agent</p>

<b>out-manipulationid</b>	Enter the name of the SIP header manipulations configuration to apply to the traffic exiting the Oracle Communications Session Border Controller via this session agent
<b>p-asserted-id</b>	Set the configurable P-Asserted-Identity header for this session agent. This value should be a valid SIP URI.
<b>trunk-group</b>	<p>Enter trunk group names and trunk group contexts to match in either IPTEL or custom format; one session agent can accommodate 500 trunk groups. If left blank, the Oracle Communications Session Border Controller uses the trunk group in the realm for this session agent. Multiple entries are surrounded in parentheses and separated from each other with spaces. You can add and delete single entries from the list using plus (+) and minus (-) signs without having to overwrite the whole list.</p> <p>Entries for this list must one of the following formats: tgrp:context or tgrp.context.</p>
<b>max-register-sustain-rate</b>	<p>Specify the registrations per second for this session agent. The constraints parameter must be enabled for this parameter to function.</p> <ul style="list-style-type: none"><li>• Default: 0 (disabled)</li><li>• Values: Min: 0   Max: 4294967295</li></ul>
<b>early-media-allow</b>	<p>Select the early media suppression for the session agent</p> <ul style="list-style-type: none"><li>• Values:<ul style="list-style-type: none"><li>• none—No early media allowed</li><li>• reverse—Allow early media in the direction of calling endpoint</li><li>• both—Allow early media in both directions</li></ul></li></ul>
<b>invalidate-registrations</b>	<p>Enable or disable the invalidation of all the registrations going to this SA when its state transitions to “out of service”</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values enabled   disabled</li></ul>
<b>rfc2833-mode</b>	<p>Select whether 2833/UII negotiation will be transparent to the Oracle Communications Session Border Controller (pre-4.1 behavior), or use 2833 for DTMF</p> <ul style="list-style-type: none"><li>• Default: none</li><li>• Values:<ul style="list-style-type: none"><li>• none—The 2833-UII interworking will be decided based on the h323-stack configuration.</li><li>• transparent—The session-agent will behave exactly the same way as before and the 2833 or UII negotiation will be transparent to the Oracle Communications Session Border Controller. This overrides any configuration in the h323-stack even if the stack is configured for “preferred” mode.</li><li>• preferred—The session-agent prefers to use 2833 for DTMF transfer and would signal that in its TCS. However, the final decision depends on the remote H323EP.</li></ul></li></ul>
<b>rfc2833-payload</b>	<p>Enter the payload type used by the SA in preferred rfc2833-mode</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Valid Range: 0, 96-127</li></ul> <p> <b>Note:</b> When this value is zero, the global “rfc2833-payload” configured in the H323 configuration element will be used instead. For SIP SA, the payload defined in the SIP Interface will be used, if the SIP-I is configured with rfc2833-mode as “preferred”.</p> <ul style="list-style-type: none"><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>codec-policy</b>	Enter the codec policy you want to apply to this session agent

<b>enforcement-profile</b>	<p>Enter the enforcement policy set of allowed SIP methods you want to use for this session agent</p> <ul style="list-style-type: none"> <li>• Default: None</li> <li>• Values: Name of a valid enforcement-profile element</li> </ul>
<b>refer-call-transfer</b>	<p>Enable or disable the refer call transfer feature for this session agent</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>refer-notify-provisional</b>	<p>Sends NOTIFY message after provisional messages are received in a REFER scenario.</p> <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: <ul style="list-style-type: none"> <li>• none—The system does not send any NOTIFY messages after receiving provisional messages.</li> <li>• initial—The system sends a NOTIFY, including 100 Trying, immediately after accepting the REFER.</li> <li>• all— The system sends an immediate 100 Trying NOTIFY and a NOTIFY for each non-100 provisional received.</li> </ul> </li> </ul>
<b>reuse-connections</b>	<p>Enter the SIP TCP connection reuse mode. The presence of “reuse-connections” in the options field of the sip-interface will cause the Oracle Communications Session Border Controller to reuse all inbound TCP connections for sending requests to the connected UA.</p> <ul style="list-style-type: none"> <li>• Default: tcp</li> <li>• Values: tcp   sctp   none</li> </ul>
<b>tcp-keepalive</b>	<p>Enable or disable standard keepalive probes to determine whether or not connectivity with a remote peer is lost.</p> <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: none   enabled   disabled</li> </ul>
<b>tcp-reconn-interval</b>	<p>Set the amount of time in seconds before retrying a TCP connection.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: 0, 2-300</li> </ul>
<b>max-register-burst-rate</b>	<p>Enter the maximum number of new registrations you want this session agent to accept within the registration burst rate window. When this threshold is exceeded, the Oracle Communications Session Border Controller responds to new registration requests with 503 Service Unavailable messages.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>register-burst-window</b>	<p>Enter the window size in seconds for the maximum number of allowable SIP registrations.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>rate-constraints</b>	<p>Access the rate-constraints subelement</p>
<b>ping-in-service-response-codes</b>	<p>Enter the response codes that keep a session agent in service when they appear in its response to the Oracle Communications Session Border Controller’s ping</p> <ul style="list-style-type: none"> <li>• Default: None</li> <li>• Values: SIP Response codes</li> </ul>

<b>out-service-response-codes</b>	<p>Enter the response codes that take a session agent out of service when they appear in its response to the Oracle Communications Session Border Controller's ping request or any dialog-creating request.</p> <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: SIP Response codes</li></ul>
<b>manipulation-string</b>	<p>Enter a string you want used in the header manipulation rules for this session-agent. Enter a value to references the \$HMR_STRING variable used to populate SIP headers and elements using HMR</p>
<b>manipulation-pattern</b>	<p>Enter the regular expression to be used in header manipulation rules for this session-agent.</p>
<b>sip-profile</b>	<p>Enter the name of the sip-profile you want to add to the session-agent</p>
<b>sip-isup-profile</b>	<p>Enter the name of the sip-isup-profile you want to add to the session-agent.</p>
<b>load-balance-dns-query</b>	<p>Sets the method the Oracle Communications Session Border Controller uses to send messages to when it queries a DNS server and receives multiple A-Records. The strategy configured here is used to select which of the multiple addresses the Oracle Communications Session Border Controller forwards the message to first.</p> <ul style="list-style-type: none"><li>• Default: hunt</li><li>• Values: hunt   round-robin</li></ul>
<b>kpml-interworking</b>	<p>Enable or disable KPML interworking.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values enabled   disabled</li></ul>
<b>monitoring-filters</b>	<p>Comma-separated list of monitoring filters used for SIP monitor and trace.</p>
<b>auth-attribute</b>	<p>Enter the auth-attribute configuration element.</p>
<b>session-recording-server</b>	<p>Name of the session-recording-server or the session-recording-group in the realm associated with the session reporting client. Valid values are alpha-numeric characters. session recording groups are indicated by prepending the groupname with SRG:</p>
<b>session-recording-required</b>	<p>Determines whether calls are accepted by the SBC if recording is not available.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• enabled—Restricts call sessions from being initiated when a recording server is not available.</li><li>• disabled—Allows call sessions to initiate even if the recording server is not available.</li></ul>

### Path

**session-agent** is an element under the session-router path. The full path from the topmost CLI prompt is: **configure terminal > session-router > session-agent**.

### Release

First appearance: 1.0 / Most recent update: S-CZ7.2.0

### RTC Status

Supported

This is a multiple instance configuration element.



## session-agent > auth-params

The auth-attribute element provides the parameters used by the Oracle Communications Session Border Controller to perform digest authentication with the parent session agent.

### Parameters

- |                          |   |
|--------------------------|---|
| <b>auth-realm</b>        | Enter the name (realm ID) of the host realm initiating the authentication challenge. This value defines the protected space in which the digest authentication is performed. Valid value is an alpha-numeric character string. <ul style="list-style-type: none"> <li>• Default: blank</li> </ul>   |
| <b>username</b>          | Enter the username of the client. Valid value is an alpha-numeric character string. <ul style="list-style-type: none"> <li>• Default: blank</li> </ul>  |
| <b>password</b>          | Enter the password associated with the username of the client. This is required for all LOGIN attempts. Password displays while typing but is saved in clear-text (i.e., *****). Valid value is an alpha-numeric character string. <ul style="list-style-type: none"> <li>• Default: blank</li> <li>• Values: round-robin   hunt</li> </ul>   |
| <b>in-dialog-methods</b> | Optionally enter the in-dialog request method(s) that digest authentication uses from the cached credentials. Specify request methods in a list form separated by a space enclosed in parentheses. Valid values are. <ul style="list-style-type: none"> <li>• Default: blank</li> <li>• Values: INVITE   BYE   ACK   OPTIONS   SUBSCRIBE   PRACK   NOTIFY   UPDATE   REFER</li> </ul> |

### Path

**auth-attributes** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-agent > auth-attributes**.

### Release

First appearance: S-CX6.3.0

### RTC Status

Supported



**Note:** This is a multiple instance configuration element.

## session-agent > rate-constraints

The rate-constraints subelement for the session-agent configuration element allows you to configure rate constraints for individual session agents, which can then be applied to the SIP interface where you want them used.

### Parameters

- |               |   |
|---------------|---|
| <b>method</b> | Enter the SIP method name for the method you want to throttle <ul style="list-style-type: none"> <li>• Values:</li> </ul> |
|---------------|---|

- NOTIFY
- OPTIONS
- MESSAGE
- PUBLISH
- REGISTER

<b>max-inbound-burst-rate</b>	For the SIP method you set in the method parameter, enter the number to restrict the inbound burst rate on the SIP interface where you apply these constraints. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 999999999</li></ul>
<b>max-outbound-burst-rate</b>	For the SIP method you set in the method parameter, enter the number to restrict the outbound burst rate on the SIP interface where you apply these constraints. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 999999999</li></ul>
<b>max-inbound-sustain-rate</b>	For the SIP method you set in the method parameter, enter the number to restrict the inbound sustain rate on the SIP interface where you apply these constraints <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 999999999</li></ul>
<b>max-outbound-sustain-rate</b>	For the SIP method you set in the method parameter, enter the number to restrict the outbound sustain rate on the SIP interface where you apply these constraints <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 999999999</li></ul>

### Path

**rate-constraints** is an element of the **session-router** path. The full path from the topmost ALCI prompt is:**configure terminal > session-router > session-agent rate-constraints**.

### Release

First appearance: 5.1.1

### RTC Status:

Supported

---

## session-agent-group

---

The session-agent-group element creates a group of Session Agents and/or groups of other SAGs. The creation of a SAG indicates that its members are logically equivalent and can be used interchangeably. This allows for the creation of constructs like hunt groups for application servers or gateways.

### Parameters

<b>group-name</b>	Enter the name of the session-agent-group element. This required entry must follow the Name Format, and it must be unique. This value cannot contain underscores.
<b>description</b>	Describe the session agent group element
<b>state</b>	Enable or disable the session-agent-group element

	<ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>app-protocol</b>	<p>Distinguish H.323 session agent groups from SIP session agent groups</p> <ul style="list-style-type: none"> <li>• Default: SIP</li> <li>• Values: H323   SIP</li> </ul>
<b>strategy</b>	<p>Select the session agent allocation options for the session-agent-group. Strategies determine how session agents will be chosen by this session-agent-group element.</p> <ul style="list-style-type: none"> <li>• Default: Hunt</li> <li>• Values: <ul style="list-style-type: none"> <li>• Hunt—Selects session agents in the order in which they are listed</li> <li>• RoundRobin—Selects each session agent in the order in which they are listed in the dest list, selecting each agent in turn, one per session. After all session agents have been used, the first session agent is used again and the cycle continues.</li> <li>• LeastBusy—Selects the session agent that has the fewest number of sessions relative to the max-outbound-sessions constraint or the max-sessions constraint (i.e., lowest percent busy) of the session-agent element</li> <li>• PropDist—Based on programmed, constrained session limits, the Proportional Distribution strategy proportionally distributes the traffic among all of the available session-agent elements</li> <li>• LowSusRate—Routes to the session agent with the lowest sustained rate of session initiations/invitations</li> </ul> </li> </ul>
<b>dest</b>	<p>Enter one or more destinations (i.e., next hops) available for use by this session-agent group. The destination value(s) must correspond to a valid IP address or hostname.</p>
<b>trunk-group</b>	<p>Enter trunk group names and trunk group contexts to match in either IPTEL or custom format. If left blank, the Oracle Communications Session Border Controller uses the trunk group in the realm for this session agent group. Multiple entries are surrounded in parentheses and separated from each other with spaces.</p> <p>Entries for this list must one of the following formats: tgrp:context or tgrp.context.</p>
<b>sag-recursion</b>	<p>Enable or disable SIP SAG recursion for this SAG</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>stop-sag-recurse</b>	<p>Enter the list of SIP response codes that terminate recursion within the SAG. On encountering the specified response code(s), the Oracle Communications Session Border Controller returns a final response to the UAC. You can enter the response codes as a comma-separated list or as response code ranges.</p> <ul style="list-style-type: none"> <li>• Default: 401, 407</li> </ul>

## Path


**session-agent-group** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-group**.

## Release

First appearance: 1.0 / Most recent update: 1.2.1

### RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

## session-constraints

---

The session-constraints configuration element allows you to create session layer constraints in order to manage and police session-related traffic including maximum concurrent sessions, maximum outbound concurrent sessions, maximum session burst rate, and maximum session sustained rate.

The SIP interface configuration's constraint-name parameter invokes the session constraint configuration you want to apply. Using the constraints you have set up, the Oracle Communications Session Border Controller checks and limits traffic according to those settings for the SIP interface. Of course, if you do not set up the session constraints or you do not apply them in the SIP interface, then that SIP interface will be unconstrained. If you apply a single session-constraint element to multiple SIP interfaces, each SIP interface will maintain its own copy of the session-constraint.

 **Note:** The Oracle Communications Session Border Controller supports five concurrent SSH and/or SFTP sessions.

### Parameters

<b>name</b>	Enter the name for this session constraint. This must be a unique identifier that you use when configuring a SIP interface on which you are applying it. This is a required parameter.
<b>state</b>	Enable or disable this session constraint <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>max-sessions</b>	Enter the maximum sessions allowed for this constraint <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 999999999</li></ul>
<b>max-inbound-sessions</b>	Enter the maximum inbound sessions allowed for this constraint <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 999999999</li></ul>
<b>max-outbound-sessions</b>	Enter the maximum outbound sessions allowed for this constraint <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 999999999</li></ul>
<b>max-burst-rate</b>	Enter the maximum burst rate (invites per second) allowed for this constraint <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 999999999</li></ul>
<b>max-inbound-burst-rate</b>	Enter the maximum inbound burst rate (number of session invitations per second) for this constraint <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0   Max: 999999999</li></ul>
<b>max-outbound-burst-rate</b>	Enter the maximum outbound burst rate (number of session invitations per second) for this constraint

	<ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>max-sustain-rate</b>	<p>Enter the maximum rate of session invitations allowed within the current window for this constraint</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>max-inbound-sustain-rate</b>	<p>Enter the maximum inbound sustain rate (of session invitations allowed within the current window) for this constraint</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>max-outbound-sustain-rate</b>	<p>Enter the maximum outbound sustain rate (of session invitations allowed within the current window) for this constraint</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>min-seizures</b>	<p>Enter the minimum number of seizures for a no-answer scenario</p> <ul style="list-style-type: none"> <li>• Default: 5</li> <li>• Values: Min: 1   Max: 999999999</li> </ul>
<b>min-asr</b>	<p>Enter the minimum ASR in percentage</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 100</li> </ul>
<b>time-to-resume</b>	<p>Enter the number of seconds that is used to place an element (like a session agent) in the standby state when it has been taken out of service because of excessive transaction timeouts</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>ttr-no-response</b>	<p>Enter the time delay in seconds to wait before changing the status of an element (like a session agent) after it has been taken out of service because of excessive transaction timeouts</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>in-service-period</b>	<p>Enter the time in seconds that elapses before an element (like a session agent) can return to active service after being placed in the standby state</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>burst-rate-window</b>	<p>Enter the time in seconds that you want to use to measure the burst rate</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>sustain-rate-window</b>	<p>Enter the time in seconds used to measure the sustained rate</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 10   Max: 999999999</li> </ul> <p>The value you set here must be higher than or equal to the value you set for the burst rate window.</p>



**Note:** If you are going to use this parameter, you must set it to a minimum value of 10.

**rate-constraints**      Access the rate-constraints subelement

### Path

**session-constraints** is an element of the session-router path. The full path from the topmost ACLI prompt is:  
**configure terminal > session-router > session-constraints.**

### Release

First appearance: 4.1.1

### RTC Status

Supported

---

## session-constraints > rate-constraints

---

The rate-constraints subelement for the session-constraints configuration element allows you to configure rate constraints for individual session constraints, which can then be applied to the SIP interface where you want them used.

### Parameters

<b>method</b>	Enter the SIP method name for the method you want to throttle <ul style="list-style-type: none"><li>Values:<ul style="list-style-type: none"><li>NOTIFY</li><li>OPTIONS</li><li>MESSAGE</li><li>PUBLISH</li><li>REGISTER</li></ul></li></ul>
<b>max-inbound-burst-rate</b>	For the SIP method you set in the method parameter, enter the number to restrict the inbound burst rate on the SIP interface where you apply these constraints. <ul style="list-style-type: none"><li>Default: 0</li><li>Values: Min: 0   Max: 999999999</li></ul>
<b>max-outbound-burst-rate</b>	For the SIP method you set in the method parameter, enter the number to restrict the outbound burst rate on the SIP interface where you apply these constraints. <ul style="list-style-type: none"><li>Default: 0</li><li>Values: Min: 0   Max: 999999999</li></ul>
<b>max-inbound-sustain-rate</b>	For the SIP method you set in the method parameter, enter the number to restrict the inbound sustain rate on the SIP interface where you apply these constraints <ul style="list-style-type: none"><li>Default: 0</li><li>Values: Min: 0   Max: 999999999</li></ul>
<b>max-outbound-sustain-rate</b>	For the SIP method you set in the method parameter, enter the number to restrict the outbound sustain rate on the SIP interface where you apply these constraints <ul style="list-style-type: none"><li>Default: 0</li></ul>

- Values: Min: 0 | Max: 999999999

**method** Enter the SIP method name for the method you want to throttle

## Path

**session-constraints**> > **rate-constraints** is an element of the session-router path. The full path from the topmost ALCI prompt is: **configure terminal** > **session-router** > **session-constraints** > **rate-constraints**.

## Release

First appearance: 5.1.1

## RTC Status

Supported

# session-router-config

The session-router-config element allows you to configure whether or not session-related functionality is enabled within your network, whether it contains a Oracle Communications Session Border Controller SR or SD.

## Parameters

<b>state</b>	<p>Enable or disable this session-related functionality on the system</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>system-number-type</b>	<p>Define the telephone number format used in local policy and local policy lookups</p> <ul style="list-style-type: none"> <li>• Default: Pots</li> <li>• Values: <ul style="list-style-type: none"> <li>• Pots—Telephone numbers are in Decimal routing number format (0-9). This is the default and recommended setting.</li> <li>• E164—Telephone numbers are in E.164 format as defined by the global-number format of the tel URI defined in RFC 3966</li> <li>• Routing—Telephone numbers are in Penta Decimal routing numbers (0-9, A-F). This value is not currently used but reserved for future enhancements.</li> </ul> </li> </ul>
<b>sr-primary-name</b>	Enter the name of the primary session router; must match the target name in the boot parameters of the primary SR
<b>sr-primary-address</b>	Enter the IP Address of the maintenance interface of the primary session router; must match the "inet on ethernet" address in the boot parameters of the primary SR
<b>sr-secondary-name</b>	Enter the name of the secondary session router; must match the target name in the boot parameters of the secondary SR
<b>sr-secondary-address</b>	Enter the IP Address of the maintenance interface of the secondary session router. This must match the "inet on ethernet" address in the boot parameters of the secondary SR.
<b>divide-resources</b>	<p>Indicate whether or not resources are divided by the number of configured session directors. This includes:</p> <ul style="list-style-type: none"> <li>• realm-config bandwidth</li> <li>• session-agent max-sessions</li> </ul>

	<ul style="list-style-type: none"><li>• session-agent max-outbound-sessions</li><li>• session-agent max-burst-rate</li><li>• session-agent max-sustain-rate</li><li>• • Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>match-lp-src-parent-realms</b>	<p>Enable or disable local policy parent realm matching based on a parent realm</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>nested-realm-stats</b>	<p>Enable or disable using session constraints for nested realms across the entire system</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>reject-message-threshold</b>	<p>Enter the minimum number of message rejections allowed in the reject-message-window time on the Oracle Communications Session Border Controller (when using the SIP manipulation action reject) before generating an SNMP trap</p> <ul style="list-style-type: none"><li>• Default: 0 (no trap is sent)</li><li>• Values: Min: 0 / Max: 4294967295</li></ul>
<b>reject-message-window</b>	<p>Enter the time in seconds that defines the window for maximum message rejections allowed before generating an SNMPS trap</p> <ul style="list-style-type: none"><li>• Default: 0 (no trap is sent)</li><li>• Values: Min: 0 / Max: 4294967295</li></ul>
<b>force-report-trunk-info</b>	<p>Enable or disable generation of VSAs for trunk group information even when you are not using trunk-group routing; VSAs 65-68 to report originating and terminating trunk group information</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>session-directors</b>	<p>Access the session-directors subelement.</p>
<b>holidays</b>	<p>Access the session-router-holidays subelement.</p>
<b>additional-lp-lookups</b>	<p>Enter the number of additional local policy per message lookups</p> <ul style="list-style-type: none"><li>• Default: 0 (disables multistaged local policy lookup)</li><li>• Values: Min: 0   Max: 5</li></ul>
<b>max-routes-per-lookup</b>	<p>Enter the maximum number of routes per local policy lookup</p> <ul style="list-style-type: none"><li>• Default: 0 (no limit on the number of returned routes)</li><li>• Values: Min: 0   Max: 4294967295</li></ul>
<b>total-lp-routes</b>	<p>Enter the total number of routes for all local policy lookups per message request</p> <ul style="list-style-type: none"><li>• Default: 0 (no limit on the number of returned routes)</li><li>• Values: Min: 0   Max: 4294967295</li></ul>
<b>multi-stage-src-realm-override</b>	<p>Sets the system to use the original received realm as the source realm for multistage local policy lookups through every stage when set to enabled. A setting of disabled sets the system to use the previous stage's next-hop as the source realm in the current stage.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>



**Path**


**session-router-config** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-router**.

**Release**

First appearance: 1.0 / Most recent update: S-C6.2.0

**RTC Status**

Supported

 **Note:** This is a single instance configuration element.

## session-router > holidays

---

The session-router-holidays configuration subelement establishes the holiday schedule to which the Oracle Communications Session Border Controller conforms.

**Parameters**

- date** Enter the date of a holiday in YYYY-MM-DD format. A session router holidays entry will not function properly unless it is a valid
- description** Describe the holiday

**Path**


**session-router-holidays** is a subelement under the session-router-config element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-router > holidays**.

**Release**

First appearance: 1.0

**RTC Status**

Supported

 **Note:** This is a multiple instance configuration element.

## session-timer-profile

---

The session-timer-profile element is used to configure support for RFC 4028 Session Timers.

**Parameters**

- name** The name of this session-timer-profile element. This value is configured in a sip-interface's session-timer-profile parameter.
- session-expires** The value of the session expires header in seconds
- Default: 1800
  - Values: 64-999999999
- min-se** The value of the Min-SE header in seconds (this is a minimum session expires value).

	<ul style="list-style-type: none"><li>• Default: 90</li><li>• Values: 64-999999999</li></ul>
<b>force-reinvite</b>	Sets if the Net-Net SBC will send a reINVITE to refresh the session timer when applicable <ul style="list-style-type: none"><li>• Default: disable</li><li>• Values: enable   disable</li></ul>
<b>request-refresher</b>	Set on the outbound side of a call what the Net-Net SBC sets the refresher parameter to. Valid values are uac, uas, or none. <ul style="list-style-type: none"><li>• Default: uac</li><li>• Values: none   uac   uas</li></ul>
<b>response-refresher</b>	Set on the inbound side the value of the refresher parameter in the 200OK message. <ul style="list-style-type: none"><li>• Default: uas</li><li>• Values: uac   uas</li></ul>

### Path

**session-timer-profile** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-timer-profile**.

### Release

First appearance: S-CX6.4.0

## session-translation

---

The session-translation element defines how translation rules are applied to incoming and outgoing numbers. Multiple translation rules can be referenced and applied; this configuration element groups rules together and allows them to be referenced by a single identifier.

### Parameters

<b>id</b>	Enter the identifier or name for this set of session translation rules. This parameter is required.
<b>rules-calling</b>	Enter the rule(s) defined in the translation rules element applied to the calling number
<b>rules-called</b>	Enter the rule(s) defined in the translation rules element applied to the called number

### Path

**session-translation** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-translation**.

### Release

First appearance: 1.0

### RTC Status

Supported



**Note:** The Oracle Communications Session Border Controller applies the translation rules established in this field cumulatively, in the order in which they are entered. If this field is configured with a value of “rule1 rule2 rule3”, rule1 will be applied to the original number first, rule2 second, and rule3 last. This is a multiple instance configuration element.





## sip-config

The sip-config element is used to define the parameters for this protocol specific to the Oracle Communications Session Border Controller communicating with SIP.


### Parameters

<b>state</b>	<p>Enable or disable the SIP operations</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>operation-mode</b>	<p>Select the SIP operation mode</p> <ul style="list-style-type: none"> <li>• Default: dialog</li> <li>• Values: <ul style="list-style-type: none"> <li>• disabled—SIP operation disabled</li> <li>• stateless—Stateless proxy forwarding. SIP requests are forwarded based on the Request-URI and local policy. No transaction, session or dialog state is maintained. No media state is maintained, and session descriptions in the SIP messages are not modified.</li> <li>• transaction—Transaction stateful proxy mode. SIP requests are forwarded based on the Request-URI and local policy. The Oracle Communications Session Border Controller maintains transaction state in accordance with RFC 3261. No session or dialog state is maintained. No media state is maintained, and session descriptions in the SIP messages are not modified.</li> <li>• session—Session stateful proxy mode. SIP requests are forwarded based on the Request-URI and local policy. The Oracle Communications Session Border Controller maintains transaction state in accordance with RFC 3261. The SD also maintains session state information. A Record-Route header is inserted in requests so that the Oracle Communications Session Border Controller will remain in the path. No media state is maintained, and session descriptions in the SIP messages are not modified.</li> <li>• dialog—Dialog stateful B2BUA mode. The Oracle Communications Session Border Controller maintains full transaction, session, and dialog state. If media management is enabled, full media state is also maintained and the Oracle Communications Session Border Controller modifies session descriptions in SIP messages to cause the media to flow through the Oracle Communications Session Border Controller.</li> </ul> </li> </ul>
<b>dialog-transparency</b>	<p>Enable or disable SIP dialog transparency service to prevent the Oracle Communications Session Border Controller from generating a unique Call-ID and modifying dialog tags</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>home-realm-id</b>	<p>Enter the identifier of the home realm. This is the network to which the Oracle Communications Session Border Controller's SIP proxy (B2BUA) is logically connected. If configured, this field must correspond to a valid identifier field entry in a realm-config.</p>
<b>egress-realm-id</b>	<p>Enter the default egress realm identifier</p>
<b>nat-mode</b>	<p>Select the home realm NAT mode. This is used to indicate whether the home realm is "public" or "private" address space for application of the SIP-NAT function.</p> <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: <ul style="list-style-type: none"> <li>• none—No SIP-NAT is necessary</li> </ul> </li> </ul>

	<ul style="list-style-type: none"><li>• private—Indicates that the home realm is private address space, and all other external realms are public address space. Addresses in the home realm will be encoded in SIP URIs sent into the external realm. The addresses are decoded when the URIs enter the home realm.</li><li>• public—Indicates that the home realm is public address space. Addresses from external realms are encoded in SIP URIs as they enter the home realm. Addresses are decoded as they enter the external realm that the address originated in.</li></ul>
<b>registrar-domain</b>	Enter the domain name for identifying which requests for which Hosted NAT Traversal (HNT) or registration caching applies. The right-most portion of the "host" part of the Request-URI is matched against this value. An asterisk "*" is used to indicate any domain.
<b>registrar-host</b>	Enter the hostname or IP address of the SIP registrar for the HNT and registration caching function. An asterisk "*" is used when there are multiple SIP registrars and normal routing using the Request-URI or local policy is to be applied. An IPV6 address is valid for this parameter.
<b>registrar-port</b>	Enter the port number of the SIP registrar server <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 1024 / Max: 65535</li></ul>
<b>register-service-route</b>	Select the service-route usage for REGISTER requests. <ul style="list-style-type: none"><li>• Default: always</li><li>• Values:<ul style="list-style-type: none"><li>• never—Never use service-route for REGISTER</li><li>• always—Always use service-route for REGISTER</li><li>• removal—Use service-route for de-registration</li><li>• session—Use service-route when the UA has a session</li><li>• session+removal—Use service-route for de-registration and for when the UA has a session</li></ul></li></ul>
<b>init-timer</b>	Enter the initial timeout value in milliseconds for a response to an INVITE request, and it applies to any SIP request in UDP. In RFC 3261, this value is also referred to as TIMER_T1. <ul style="list-style-type: none"><li>• Default: 500</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>max-timer</b>	Enter the maximum retransmission timeout in milliseconds for SIP. In RFC 3261, this value is also referred to as TIMER_T2. <ul style="list-style-type: none"><li>• Default: 4000</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>trans-expire</b>	Enter the TTL1 in seconds for SIP transactions. This timer is equivalent to TIMER_B in RFC 3261, and the same value is used for TIMER_D, TIMER_F, TIMER_H, and TIMER_J as set out in the same RFC. <ul style="list-style-type: none"><li>• Default: 32</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>initial-inv-trans-expire</b>	Establishes a global, default transaction timeout value (expressed in seconds) used exclusively for initial INVITE transactions. The default value, 0, indicates that a dedicated INVITE Timer B is not enabled. Non-default integer values enable a dedicated Timer B and set the timer value. <ul style="list-style-type: none"><li>• Default: 0</li></ul>

	<ul style="list-style-type: none"> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>invite-expire</b>	<p>Enter the TTL in seconds for a SIP client transaction after receiving a provisional response. This timer is equivalent to <code>TIMER_C</code> in RFC 3261.</p> <ul style="list-style-type: none"> <li>• Default: 180</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>inactive-dynamic-conn</b>	<p>Enter the time limit in seconds for inactive dynamic connections</p> <ul style="list-style-type: none"> <li>• Default: 32</li> <li>• Values Min: 1 / Max: 999999999</li> </ul>
<b>enforcement-profile</b>	<p>Enter the name of the enforcement profile (SIP allowed methods).</p>
<b>red-sip-port</b>	<p>Enter the port for sending or receiving SIP checkpoint messages. Setting this to 0 disables SIP HA on the Oracle Communications Session Border Controller.</p> <ul style="list-style-type: none"> <li>• Default: 1988</li> <li>• Values: Min: 1024 / Max: 65535; 0</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>red-max-trans</b>	<p>Enter the size of the SIP signaling transaction list in entries stored in memory</p> <ul style="list-style-type: none"> <li>• Default: 10000</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>red-sync-start-time</b>	<p>Enter the time in milliseconds before the HA Oracle Communications Session Border Controller begins SIP signaling state checkpointing. As long as this HA Oracle Communications Session Border Controller is healthy and active, it remains in a constant cycle of (re)setting this field's timer and checking to see if it has become standby.</p> <ul style="list-style-type: none"> <li>• Default: 5000</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>red-sync-comp-time</b>	<p>Enter the time in milliseconds the standby Oracle Communications Session Border Controller waits before checkpointing with the active Oracle Communications Session Border Controller to obtain the latest SIP signaling transaction information once the initial checkpointing process is complete</p> <ul style="list-style-type: none"> <li>• Default: 1000</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported.</p>
<b>add-reason-header</b>	<p>Enable or disable adding the reason header for rfc 3326 support</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>sip-message-len</b>	<p>Set the size constraint in bytes on a SIP message</p> <ul style="list-style-type: none"> <li>• Default: 4096</li> </ul>

	<ul style="list-style-type: none"><li>• Values: Min: 0 / Max: 65535</li></ul>
<b>enum-sag-match</b>	Enable or disable matching this SAG's group name to hostname portions of ENUM NAPTR or LRT replacement URIs. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>extra-method-stats</b>	Enable or disable the expansion SIP Method tracking feature. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>extra-enum-stats</b>	Enable or disable the ENUM extra statistics tracking feature. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• enabled   disabled</li></ul>
<b>rph-feature</b>	Set the state of NSEP support for the global SIP configuration <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>nsep-user-sessions-rate</b>	Set the CPS for call rates on a per user basis for NSEP. A value of 0 disables the call admission control on a per user basis. <ul style="list-style-type: none"><li>• Default: 50</li><li>• Values: 0-999999999</li></ul>
<b>nsep-sa-sessions-rate</b>	Enter maximum acceptable number of SIP INVITES (NSEP sessions) per second to allow for SIP session agents. 0 means there is no limit. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values Min: 0 / Max: 999999999</li></ul>
<b>registration-cache-limit</b>	Set the maximum number of SIP registrations that you want to keep in the registration cache. A value of 0 means there is no limit on the registration cache, therefore disabling this feature. <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>register-use-to-for-lp</b>	Enable or disable the use of an ENUM query to return the SIP URI of the Registrar for a SIP REGISTER message for routing purposes <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>options</b>	Enter customer-specific features and/or parameters. This optional field allows for a comma separated list of "feature=<value>" or "feature" parameters for the sip-config element.
<b>refer-src-routing</b>	Enable or disable the use of the referring party's source realm lookup policy to route subsequent INVITES after static or dynamic REFER handling has been terminated. When disabled, the system derives the lookup from the source realm of the calling party. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>add-ucid-header</b>	Enable or disable the using the UCID to correlate replicated SIP message information when you use SRR. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values enabled   disabled</li></ul>

<b>proxy-sub-events</b>	Configured list of SIP event package names that you want the Oracle Communications Session Border Controller to proxy (rather than maintain state) to the destination. You can enter more than one value by enclosing multiple values in quotations marks
<b>allow-pani-for-trusted-only</b>	<p>Allow PANI header only for trusted domains</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values enabled   disabled</li> </ul>
<b>pass-gruu-contact</b>	<p>Enable or disable the sip-config to parse for GR URI parameter in the contact header in non-registered endpoints' messages.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values enabled   disabled</li> </ul>
<b>sag-lookup-on-redirect</b>	<p>Enable/disable lookup of SAG name on a redirect</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values enabled   disabled</li> </ul>
<b>set-disconnect-time-on-bye</b>	<p>Sets the disconnect time reflected in a RADIUS CDR to when the Oracle Communications Session Border Controller receives a BYE message.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>msrp-delayed-bye-timer</b>	<p>Enables the delayed transmission of SIP BYE requests, for active MSRP sessions. This parameter specifies the maximum delay period allowed before transmitting the delayed BYE request.</p> <ul style="list-style-type: none"> <li>• Default 15</li> <li>• Min: 1 / Max: 60</li> </ul> <p> <b>Note:</b> A value of 0 disables this parameter.</p>


Path: **sip-config** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-config.**

## Release

First appearance: 1.0 / Most recent update: S-C6.3.0

## RTC Status

Supported

 **Note:** This is a single instance configuration element.

## sip-feature

The sip-feature element defines how the Oracle Communications Session Border Controller's B2BUA should treat specific option tags in SIP headers.

### Parameters

<b>name</b>	Enter the option tag name that will appear in the Require, Supported, or Proxy-Require headers of SIP messages
-------------	--

<b>realm</b>	Enter the realm with which the feature is associated; to make the feature global, leave this parameter blank
<b>support-mode-inbound</b>	<p>Select the treatment of feature (option tag) in a Supported header for an inbound packet</p> <ul style="list-style-type: none"><li>• Default: pass</li><li>• Values:<ul style="list-style-type: none"><li>• pass—B2BUA should include the tag in the corresponding outgoing message</li><li>• strip—Tag should be excluded in the outgoing message. Use strip mode to not use the extension.</li></ul></li></ul>
<b>required-mode-inbound</b>	<p>Select the treatment of feature (option tag) in a Require header for an inbound packet</p> <ul style="list-style-type: none"><li>• Default: reject</li><li>• Values:<ul style="list-style-type: none"><li>• pass—B2BUA should include the tag in the corresponding outgoing message</li><li>• reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.</li></ul></li></ul>
<b>proxy-require-mode-inbound</b>	<p>Select the treatment of feature (option tag) in a Proxy-Require header for an inbound packet</p> <ul style="list-style-type: none"><li>• Default: pass</li><li>• Values:<ul style="list-style-type: none"><li>• pass—B2BUA should include the tag in the corresponding outgoing message</li><li>• reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.</li></ul></li></ul>
<b>support-mode-outbound</b>	<p>Select the treatment of feature (option tag) in a Supported header for an outbound packet</p> <ul style="list-style-type: none"><li>• Default: pass</li><li>• Values:<ul style="list-style-type: none"><li>• pass—B2BUA should include the tag in the corresponding outgoing message</li><li>• strip—Tag should be excluded in the outgoing message</li></ul></li></ul>
<b>require-mode-outbound</b>	<p>Select the treatment of feature (option tag) in a Require header for an outbound packet</p> <ul style="list-style-type: none"><li>• Default: reject</li><li>• Values:<ul style="list-style-type: none"><li>• pass—B2BUA should include the tag in the corresponding outgoing message</li><li>• reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.</li></ul></li></ul>
<b>proxy-require-mode-outbound</b>	<p>Select the treatment of feature (option tag) in a Proxy-Require header for an outbound packet</p> <ul style="list-style-type: none"><li>• Default: pass</li><li>• Values:<ul style="list-style-type: none"><li>• pass—B2BUA should include the tag in the corresponding outgoing message</li><li>• reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.</li></ul></li></ul>

### Path

**sip-feature** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-feature**.



## Release

First appearance: 1.0 / Most recent update: 2.0

## RTC Status

Supported



**Note:** If an option tag is encountered that is not configured as a SIP feature, the default treatments described in each of the field descriptions (name, support-mode, require-mode, and proxy-require-mode) included in this section will apply. Therefore, a sip-feature element only needs to be configured when non-default treatment is required.

This is a multiple instance element.

## sip-interface

The sip-interface element allows you to configure a SIP interface for your Oracle Communications Session Border Controller.

### Parameters

<b>state</b>	Enable or disable the SIP interface <ul style="list-style-type: none"> <li>Default: enabled</li> <li>Values: enabled   disabled</li> </ul>
<b>realm-id</b>	Enter the name of the realm to which the SIP interface applies
<b>description</b>	Provide a brief description of the <b>sip-interface</b> configuration element
<b>sip-ports</b>	Access the sip-ports subelement
<b>carriers</b>	Enter a list of carriers related to the sip-config. Entries in this field must follow the Carrier Format.
<b>trans-expire</b>	Set the transaction expiration timer in seconds <ul style="list-style-type: none"> <li>Default: 0</li> <li>Values: Min: 0   Max: 999999999</li> </ul>
<b>invite-expire</b>	Set the INVITE transaction expiration timer in seconds <ul style="list-style-type: none"> <li>Default: 0</li> <li>Values: Min: 0   Max: 999999999</li> </ul>
<b>max-redirect-contacts</b>	Enter the maximum number of contact and route attempts in case of a redirect <ul style="list-style-type: none"> <li>Default: 0</li> <li>Values: Min: 0   Max: 10</li> </ul>
<b>proxy-mode</b>	Set the default SIP request proxy mode <ul style="list-style-type: none"> <li>Values: <ul style="list-style-type: none"> <li>proxy—Forward all SIP requests to other session agents</li> <li>redirect—Send a SIP 3xx redirect response with contacts (found in the local policy) to the previous hop</li> <li>record-route—Forward requests with Record-Route (for stateless and transaction and operation modes only)</li> </ul> </li> </ul>
<b>redirect-action</b>	Set handling of Redirect (3xx) response messages from a session agent.


	<ul style="list-style-type: none"><li>• Default: Recurse</li><li>• Values:<ul style="list-style-type: none"><li>• Proxy—Send the response back to the previous hop</li><li>• Recurse—Recurse on the contacts in the response</li><li>• Recurse-305-only—recurse on the contacts in the 305 response</li></ul></li></ul>
<b>contact-mode</b>	<p>Select the contact header routing mode</p> <ul style="list-style-type: none"><li>• Default: none</li><li>• Values:<ul style="list-style-type: none"><li>• none</li><li>• maddr</li><li>• strict</li><li>• loose</li></ul></li></ul>
<b>nat-traversal</b>	<p>Select the type of HNT functionality for SIP</p> <ul style="list-style-type: none"><li>• Default: none</li><li>• Values:<ul style="list-style-type: none"><li>• none—NAT Traversal is disabled</li><li>• always—Performs HNT when SIP-Via and transport addresses do not match</li><li>• rport—Performs HNT when Via rport parameter is present and SIP-Via and transport addresses do not match</li></ul></li></ul>
<b>nat-interval</b>	<p>Enter the expiration time in seconds for the Net-Net SBC's cached registration entry for an endpoint doing HNT</p> <ul style="list-style-type: none"><li>• Default: 30</li><li>• Values: Min: 1   Max: 999999999</li></ul>
<b>tcp-nat-interval</b>	<p>Enter the TCP NAT traversal registration interval in seconds</p> <ul style="list-style-type: none"><li>• Default: 90</li><li>• Values: Min: 0 / Max: 999999999</li></ul>
<b>registration-caching</b>	<p>Enable or disable registration cache used for all UAs rather than those behind NATs</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>min-reg-expire</b>	<p>Enter the minimum registration expiration time in seconds for HNT registration caching</p> <ul style="list-style-type: none"><li>• Default: 300</li><li>• Values: Min: 1   Max: 999999999</li></ul>
<b>registration-interval</b>	<p>Enter the expiration time in seconds for the Oracle Communications Session Border Controller's cached registration entry for an endpoint (non-HNT)</p> <ul style="list-style-type: none"><li>• Default: 3600</li><li>• Values: Min: 1   Max: 999999999</li></ul>
<b>route-to-registrar</b>	<p>Indicate whether or not the SD should forward a request addressed to the registrar to the SIP registrar as opposed to sending the request to the registered contact in the registration cache</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>

<b>secured-network</b>	<p>Enable or disable sending messages on unsecured transport</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>teluri-scheme</b>	<p>Enable or disable the conversion of SIP URIs to Tel URIs</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>uri-fqdn-domain</b>	<p>Change the host part of the URIs to the FQDN value set here. This applies to the Request-URI, From header, and To header in non-dialog requests sent from the SIP interface.</p>
<b>trust-mode</b>	<p>Select the trust mode for this SIP interface</p> <ul style="list-style-type: none"> <li>• Default: all</li> <li>• Values: <ul style="list-style-type: none"> <li>• all—Trust all previous and next hops except untrusted session agents</li> <li>• agents-only—Trust only trusted session agents</li> <li>• realm-prefix—Trust only trusted session agents or address matching realm prefix</li> <li>• registered—Trust only trusted session agents or registered endpoints</li> <li>• None—Trust nothing</li> </ul> </li> </ul>
<b>max-nat-interval</b>	<p>Enter the amount of time in seconds that testing should not exceed for adaptive HNT. The Net-Net SBC will keep the expires interval at this value.</p> <ul style="list-style-type: none"> <li>• Default: 3600</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>nat-int-increment</b>	<p>Enter the amount of time in seconds to use as the increment in value in the SIP expires header for adaptive HNT</p> <ul style="list-style-type: none"> <li>• Default: 10</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>nat-test-increment</b>	<p>Enter the amount of time in seconds that will be added to the test timer for adaptive HNT</p> <ul style="list-style-type: none"> <li>• Default: 30</li> <li>• Values: Min: 0   Max: 999999999</li> </ul>
<b>sip-dynamic-hnt</b>	<p>Enable or disable adaptive HNT</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>stop-recurse</b>	<p>Enter a list of returned response codes that this SIP interface will watch for in order to stop recursion on the target's or contact's messages</p>
<b>port-map-start</b>	<p>Set the starting port for the range of SIP ports available for SIP port mapping. A value of 0 disables SIP port mapping.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 1025   Max: 65535</li> </ul>
<b>port-map-end</b>	<p>Set the ending port for the range of SIP ports available for SIP port mapping. A value of 0 disables SIP port mapping. This value must be larger than the port-map-start parameter's value.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 1025   Max: 65535</li> </ul>

## Configuration Elements N-Z

---

<b>in-manipulationid</b>	Enter the name of the SIP header manipulations configuration to apply to the traffic entering the Oracle Communications Session Border Controller via this SIP interface
<b>out-manipulationid</b>	Enter the name of the SIP header manipulations configuration to apply to the traffic exiting the Oracle Communications Session Border Controller via this SIP interface
<b>manipulation-pattern</b>	Number of seconds after de-registration to kill TCP connection
<b>manipulation-string</b>	Enter the string used in header manipulation rules for this sip-interface.
<b>sip-ims-feature</b>	Enable or disable IMS functionality on this SIP interface <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>subscribe-reg-event</b>	Enables the Oracle Communications Session Border Controller to generate SIP registration events. <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>operator-identifier</b>	Set the operator identifier value to be inserted into a P-Charging-Vector header. The direction of the call determines whether this value is inserted into the orig-ioi or the term-ioi parameter in the P-Charging-Vector header. This string value MUST begin with an alpha character.
<b>anonymous-priority</b>	Set the policy priority parameter for this SIP interface. It is used to facilitate emergency sessions from unregistered endpoints. This value is compared against a policy priority parameter in a local policy configuration element. <ul style="list-style-type: none"><li>• Default: none</li><li>• Values:<ul style="list-style-type: none"><li>• none</li><li>• normal</li><li>• non-urgent</li><li>• urgent</li><li>• emergency</li></ul></li></ul>
<b>max-incoming-conns</b>	Enter the maximum number of TCP/TLS connections for this sip interface <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 20000; setting a value of 0 disables this parameter</li></ul>
<b>per-scr-ip-max-incoming-conns</b>	Enter the maximum number of TCP/TLS connections per peer IP address <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 20000; setting a value of 0 disables this parameter.</li></ul>
<b>inactive-conn-timeout</b>	Enter the timeout, measured in seconds for idle TCP/TLS connections <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 999999999; setting a value of 0 disables the timer.</li></ul>
<b>untrusted-conn-timeout</b>	Enter the timeout time, in seconds, for untrusted endpoints on TCP/TLS connections <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 (disabled)   Max: 999999999</li></ul>
<b>network-id</b>	Set the value that will be inserted into the P-Visited-Network-ID header
<b>ext-policy-server</b>	Enter the name of external policy server used as the CLF for this SIP interface

<b>default-location-string</b>	Set a default location string to insert into P-Access-Network-Info header when the CLF does not return this value
<b>charging-vector-mode</b>	<p>Set the state of P-Charging-Vector header handling</p> <ul style="list-style-type: none"> <li>• Default pass</li> <li>• Values: <ul style="list-style-type: none"> <li>• none—Pass the P-Charging-Vector header received in an incoming SIP message untouched as the message is forwarded out of the Oracle Communications Session Border Controller, not extracting RADIUS information</li> <li>• pass—Pass the P-Charging-Vector header received in an incoming SIP message untouched as the message is forwarded out of the Oracle Communications Session Border Controller, extracting RADIUS information</li> <li>• delete—Delete the P-Charging-Vector header received in an incoming SIP message before it is forwarded out of the Oracle Communications Session Border Controller</li> <li>• insert—Inserts the P-Charging-Vector header in an incoming SIP message that does not contain the P-Charging-Vector header. If the incoming message contains the P-Charging-Vector header, the Oracle Communications Session Border Controller will overwrite the P-Charging-Vector header with its values.</li> <li>• delete-and-respond—Removes the P-Charging-Vector from incoming requests for a session and store it. Then the Oracle Communications Session Border Controller inserts it into outbound responses related to that session in a P-Charging-Vector header.</li> </ul> </li> </ul> <p> <b>Note:</b> Note that the default setting for the <b>charging-vector-mode</b> is pass for new SIP interface configurations. If you are upgrading and there are pre-existing SIP interfaces in your (upgraded) configuration, the default becomes none.</p>
<b>charging-function-address-mode</b>	<p>Set the state of P-Charging-Function-Address header handling</p> <ul style="list-style-type: none"> <li>• Default: pass</li> <li>• Values: <ul style="list-style-type: none"> <li>• none—Pass the P-Charging-Function-Address header received in an incoming SIP message untouched as the message is forwarded out of the Oracle Communications Session Border Controller, not extracting RADIUS information</li> <li>• pass—Pass the P-Charging-Function-Address header received in an incoming SIP message untouched as the message is forwarded out of the Oracle Communications Session Border Controller, extracting RADIUS information</li> <li>• delete—Delete the P-Charging-Function-Address header received in an incoming SIP message before it is forwarded out of the Oracle Communications Session Border Controller</li> <li>• insert—Inserts the P-Charging-Function-Address header in an incoming SIP message that does not contain the P-Charging-Function-Address header. If the incoming message contains the P-Charging-Function-Address header, the Oracle Communications Session Border Controller will prepend its configured values to the header.</li> <li>• insert-reg-cache—To be configured on the SIP interface facing the UE, configures the Oracle Communications Session Border Controller to replace the PCFA with the most recently cached values rather than the ccf-address you set to be static in your configuration. The cached values come from one of the following that the Oracle Communications Session Border Controller has received most recently: request, response, registration, or local configuration.</li> </ul> </li> </ul>

- delete-and-respond—To be configured on the SIP interface facing the S-CPCF, configures the Oracle Communications Session Border Controller to strip out the latest cached PCFA.



**Note:** Note that the default setting for the **charging-function-address-mode** is pass for new SIP interface configurations. If you are upgrading and there are pre-existing SIP interfaces in your (upgraded) configuration, the default becomes none.

<b>ccf-address</b>	Set the CCF address value that will be inserted into the P-Charging-Function-Address header
<b>ecf-address</b>	Set the ECF address value that will be inserted into the P-Charging-Function-Address header
<b>term-tgrp-mode</b>	<p>Select the mode for routing for terminating trunk group URIs</p> <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: <ul style="list-style-type: none"> <li>• none—Disable routing based on trunk groups</li> <li>• iptel—Use trunk group URI routing based on the IPTEL formats</li> <li>• egress-uri—Use trunk group URI routing based on the egress URI format</li> </ul> </li> </ul>
<b>implicit-service-route</b>	<p>Enable or disable the implicit service route behavior</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: <ul style="list-style-type: none"> <li>• enabled</li> <li>• disabled</li> <li>• strict</li> </ul> </li> </ul>
<b>rfc2833-payload</b>	<p>Enter the payload type used by the SIP interface in preferred rfc2833-mode</p> <ul style="list-style-type: none"> <li>• Default: 101</li> <li>• Values: Min: 96   Max: 127</li> </ul>
<b>rfc2833-mode</b>	<p>Choose whether the SIP interface will behave exactly the same way as before and the 2833 or UII negotiation will be transparent to the Oracle Communications Session Border Controller, transparent, or whether the sip-interface prefers to use 2833 for DTMF transfer and would signal that in its SDP, preferred. However the final decision depends on the remote endpoint.</p> <ul style="list-style-type: none"> <li>• Default: transparent</li> <li>• Values: transparent   preferred   dual</li> </ul>
<b>constraint-name</b>	Enter the name of the constraint being applied to this interface
<b>response-map</b>	Enter the name of the response map being applied to this interface
<b>local-response-map</b>	Enter the name of the local response map being applied to this interface
<b>ims-aka-feature</b>	<p>Enable or disable IMS-AKA use for a SIP interface</p> <ul style="list-style-type: none"> <li>• Default disabled</li> <li>• Values enabled   disabled</li> </ul>
<b>enforcement-profile</b>	Enter the name of the enforcement profile associated with this SIP interface
<b>route-unauthorized-calls</b>	Enter the name of the SA or SAG you want to route unauthorized calls

<b>tcp-keepalive</b>	<p>Enable or disable standard keepalive probes to determine whether or not connectivity with a remote peer is lost.</p> <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: none   enabled   disabled</li> </ul>
<b>add-sdp-invite</b>	<p>Enable or disable this SIP interface inserting an SDP into either an INVITE or a REINVITE</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: <ul style="list-style-type: none"> <li>• disabled—Do not insert an SDP</li> <li>• invite—Insert an SDP in the invite</li> <li>• reinvite—Insert an SDP in the reinvite</li> </ul> </li> </ul>
<b>add-sdp-profile</b>	<p>Enter a list of one or more media profile configurations you want to use when the Oracle Communications Session Border Controller inserts SDP into incoming INVITES that have no SDP. The media profile contains media information the Oracle Communications Session Border Controller inserts in outgoing INVITE.</p>
<b>sip-profile</b>	<p>Enter the name of the sip-profile to apply to this interface.</p>
<b>sip-isup-profile</b>	<p>Enter the name of the sip-isup-profile to apply to this interface.</p>
<b>tcp-conn-dereg</b>	<p>Number of seconds after de-registration to kill TCP connection.</p> <ul style="list-style-type: none"> <li>• Default 0 (disabled)</li> </ul>
<b>register-keep-alive</b>	<p>Sets the use of RFC 5626 CRLF Keepalives on this sip interface.</p> <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: <ul style="list-style-type: none"> <li>• none—disables this feature</li> <li>• always— Keepalive always added to SIP-Via</li> <li>• bnat— Keepalive added to SIP-Via when SIP-via and transport addresses do not match (indicates endpoint is behind a NAT)</li> </ul> </li> </ul>
<b>kpml-interworking</b>	<p>Enables or disables the KPML to RFC2833 interworking feature.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>send-380-response</b>	<p>The phrase entered in this parameter is inserted into the &lt;reason&gt; element in the &lt;alternative-service&gt; element in the XML body in the 380 response returned to an endpoint when the call cannot be completed. This is in compliance with GSMA's Voice over LTE specification (IR. 92).</p>
<b>session-timer-profile</b>	<p>A session-timer-profile name is configured here to apply that session timer profile to this SIP interface.</p>
<b>tunnel-name</b>	<p>Tunnel traffic for load balancer. Traffic sent to/from this interface will be encapsulated in an RFC 2003 compliant tunnel to/from the load balancer using the associated network-interface's tunnel name.</p>
<b>options</b>	<p>Enter optional features and/or parameters</p>

Path: **sip-interface** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-interface.**

### Release

First appearance: 1.0 / Most recent update: S-C6.3.0

### RTC Status

Supported



**Note:** This is a multiple instance configuration element.

## sip-interface > sip-ports

---

The sip-ports subelement indicates the ports on which the SIP proxy or B2BUA will listen for connections.

### Parameters

<b>address</b>	Enter the IP address of the host associated with the sip-port entry An IPV6 address is valid for this parameter.
<b>port</b>	Enter the port number for this sip-port <ul style="list-style-type: none"><li>• Default: 5060</li><li>• Values: Min: 1025 / Max: 65535</li></ul>
<b>transport-protocol</b>	Select the transport protocol associated for this sip-port <ul style="list-style-type: none"><li>• Default: UDP</li><li>• Values:<ul style="list-style-type: none"><li>• TCP</li><li>• UDP</li><li>• TLS</li><li>• SCTP</li></ul></li></ul>
<b>multi-homed-addr</b>	Enter one or more IP addresses that are multihomed on this SIP Interface, for use with SCTP. Multiple IP addresses are entered in parentheses, separated by spaces.
<b>tls-profile</b>	Select the type of anonymous connection from session agents allowed
<b>allow-anonymous</b>	Select the type of anonymous connection from session agents allowed <ul style="list-style-type: none"><li>• Default: all</li><li>• Values:<ul style="list-style-type: none"><li>• all—Allow all anonymous connections</li><li>• agents-only—Only requests from session agents allowed</li><li>• realm-prefix—Session agents and address matching realm prefix</li><li>• registered—Session agents and registered endpoints (REGISTER allowed from any endpoint)</li><li>• register-prefix—All connects from SAs that match agents-only, realm-prefix, and registered agents</li></ul></li></ul>
<b>ims-aka-profile</b>	Enter the name value for the IMS-AKA profile configuration to use for a SIP port

### Path

**sip-ports** is a subelement is under the sip-config element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-interface > sip-ports**.



## Release

First appearance: 1.0 / Most recent update: 4.1

## RTC Status

Supported



**Note:** There must be at least one sip-port entry configured within the sip-config and there can be as many entries as necessary for the sip-port. This is a multiple instance configuration element.

## sip-isup-profile

The sip-isup-profile element allows you to set up a SIP ISUP format interworking. You can apply a configured SIP ISUP profile to a realm, session agent or SIP interface.

### Parameters

<b>name</b>	Enter a unique identifier for this SIP ISUP profile. This name is used when you apply the profile to realms, session agents, and SIP interfaces.
<b>isup-version</b>	Specify the ISUP version to which you want to convert. <ul style="list-style-type: none"> <li>• Default: ansi-2000</li> <li>• Values: ansi-2000   itu-t926   gr-317   etsi-356</li> </ul>
<b>convert-isup-format</b>	Enable or disable this parameter to perform SIP ISUP format version interworking. If this feature is set to disabled, the feature is turned off. <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>

### Path

**sip-isup-profile** is an element under the session-router path. The full path from the topmost ACLI prompt is: configure terminal > session-router > sip-isup-profile.

## Release

First appearance: S-C6.2.0

## RTC Status

Supported



**Note:** This is a multiple instance configuration element.

## sip-manipulation

The sip-manipulation feature lets the Oracle Communications Session Border Controller add, modify, and delete SIP headers and SIP header elements.

### Parameters

<b>name</b>	Enter the name of this list of header rules.
<b>header-rules</b>	Access the header-rules subelement.

<b>mime-rules</b>	Access the mime-rules subelement.
<b>mime-isup-rules</b>	Access the mime-isup-rules-rules subelement.
<b>mime-sdp-rules</b>	Access the mime-sdp-rules-rules subelement which is used to configure HMR for SDP bodies.
<b>import</b>	Enter the complete file name, including .gz, of a previously exported sip-manipulation rule.
<b>export</b>	Enter the file name of a SIP manipulation to export configuration information a designated file.
<b>description</b>	Describe what the set of header rules is doing.

### Path

**sip-manipulation** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation**.

### Release

First appearance: 4.0

### RTC Status

Supported

---

## sip-manipulation > header-rules

---

The header-rules subelement is used to define one action to perform on a given SIP header.

### Parameters

<b>name</b>	Enter the name of the header to which this rule applies. This name must match a header name.
<b>action</b>	Select the action you want applied to the header specified in the name parameter. <ul style="list-style-type: none"><li>• Default: none</li><li>• Values:<ul style="list-style-type: none"><li>• add—Add a new header, if that header does not already exist</li><li>• delete—Delete the header, if it exists</li><li>• manipulate—Manipulate this header according to the element rules configured</li><li>• store—Store this header</li><li>• none—Take no action</li></ul></li></ul>
<b>match-value</b>	Enter the exact value to be matched. The action you specify is only performed if the header value matches.
<b>msg-type</b>	Select the message type to which this header rule applies <ul style="list-style-type: none"><li>• Default: any</li><li>• Values:<ul style="list-style-type: none"><li>• any—Both Requests and Reply messages</li><li>• request—Request messages only</li><li>• reply— Reply messages only</li></ul></li></ul>
<b>methods</b>	Enter a list of SIP methods that this header rule applies to. An empty value applies this header rule to all SIP method messages. <ul style="list-style-type: none"><li>• Default: none</li></ul>

<b>element-rules</b>	Access the element rules sub-subelement
<b>header-name</b>	Enter the header name for which the rules need to be applied
<b>comparison-type</b>	Select the comparison type that the match-value uses <ul style="list-style-type: none"> <li>• Default: case-sensitive</li> <li>• Values: <ul style="list-style-type: none"> <li>• case-sensitive</li> <li>• case-insensitive</li> <li>• pattern-rule</li> <li>• refer-case-sensitive</li> <li>• refer-case-insensitive</li> <li>• boolean</li> </ul> </li> </ul>
<b>new-value</b>	The new value to be used in add or manipulate actions. To clear the new-value enter an empty string.

### Path

**header-rules** is a subelement under the **sip-manipulation** configuration element, under the **session-router** path. The full path from the topmost CLI prompt is: **configure terminal > session-router > sip-manipulation > header-rules**.

### Release

First appearance: 4.0

### RTC Status

Supported

---

## sip-manipulation > header-rules > element-rules

---

The element-rules sub-subelement is used to define a list of actions to perform on a given SIP header.

### Parameters

<b>name</b>	Enter the name of the element to which this rule applies. The name parameter does not apply for the following element types: header-value, uri-user, uri-host, uri-port, uri-header. You still need to enter a dummy value here for tracking purposes.
<b>type</b>	Select the type of element on which to perform the action <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: <ul style="list-style-type: none"> <li>• header-value—Full value of the header</li> <li>• header-param-name—Header parameter name</li> <li>• header-param—Parameter portion of the header</li> <li>• uri-display—Display of the SIP URI</li> <li>• uri-user—User portion of the SIP URI</li> <li>• uri-host—Host portion of the SIP URI</li> <li>• uri-port—Port number portion of the SIP URI</li> <li>• uri-param-name—Name of the SIP URI param</li> </ul> </li> </ul>

- uri-param—Parameter included in the SIP URI
- uri-header-name—SIP URI header name
- uri-header—Header included in a request constructed from the URI
- uri-user-param—User parameter of the SIP URI
- status-code—Status code of the SIP URI
- reason-phrase—Reason phrase of the SIP URI
- uri-user-only—URI username without the URI user parameters
- uri-phone-number-only—User part of the SIP/TEL URI without the user parameters when the user qualifies for specific BNF

**action** Select the action to take to the element specified in the name parameter, if there is a match value

- Default: none
- Values:
  - none—No action taken
  - add—Add a new element, if it does not already exist
  - replace—Replace the elements
  - delete-element—Delete the specified element, if it exists
  - delete-header—Delete the specified header, if it exists
  - store—Store the elements

**match-val-type** Select the type of value that needs to be matched for the action to be performed

- Default: ANY
- Values:
  - FQDN —FQDN value
  - ANY— Both IP or FQDN values

**match-value** Enter the value to match against the element value for a manipulation action to be performed

**new-value** Enter the explicit value for a new element or replacement value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

- Use double quotes around string values
- Pre-defined parameters always start with a \$. Valid pre-defined parameters are:

Parameter	Description
\$ORIGINAL	Original value of the element is used.
\$LOCAL_IP	Local IP address is used when you receive an inbound address.
\$REMOTE_IP	Remote IP address is used.
\$REMOTE_VIA_HOST	Remote VIA host part is used.
\$TRUNK_GROUP	Trunk group is used.
\$TRUNK_GROUP_CONTEXT	Trunk group context is used.

- Operators are:

Operator	Description
+	Append the value to the end. For example: “acme”+”packet”

Operator	Description
	generates “acmepacket”
+^	Prepends the value. For example: “acme”+^”packet” generates “packetacme”
-	Subtract at the end. For example: “112311”-”11” generates “1123”
_^	Subtract at the beginning. For example: “112311”-^”11” generates “2311”

**parameter-name** Enter the element parameter name for which the rules need to be applied

**comparison-type** Select the type of comparison to be used for the match-value

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule

The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > header-rules > element-rules**.

## Path

**element-rules** is a sub-subelement under the **header-rules** subelement under the **sip-manipulation** configuration element, under the **session-router** path.

## Release

First appearance: 4.0

## RTC Status

Supported

## sip-manipulation > mime-isup-rules

The mime-isup-rules configuration allows you to perform HMR operations on SIP ISUP binary bodies.

### Parameters

**name** Enter a unique identifier for this MIME ISUP rule.

**content-type** Enter the content type for this MIME rule. This value refers to the specific body part in the SIP message body that is to be manipulated.

**isup-spec** Enter the ISUP encoding specification for the ISUP body; this specifies how the Oracle Communications Session Border Controller is to parse the binary body.

	<ul style="list-style-type: none"><li>• Default: ansi-2000</li><li>• Values: ansi-2000   itu-t926   gr-317   etsi-356</li></ul>
<b>isup-msg-types</b>	<p>Enter the specific ISUP message types (such as IAM and ACM). that the Oracle Communications Session Border Controller uses with the msg-type parameter (which identifies the SIP message) in the matching process. The values of this parameter are a list of numbers rather than enumerated values because of the large number of ISUP message types.</p> <ul style="list-style-type: none"><li>• Values: Min: 0 / Max: 255</li></ul>
<b>action</b>	<p>Select the type of action you want to be performed.</p> <ul style="list-style-type: none"><li>• Default: none</li><li>• Values: add   delete   manipulate   store   sip-manip   find-replace-all   none</li></ul>
<b>match-value</b>	<p>Enter the value to match against the body part in the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.</p>
<b>comparison-type</b>	<p>Select a method to determine how the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.</p> <ul style="list-style-type: none"><li>• Default: case-sensitive</li><li>• Values: case-sensitive   case-insensitive   pattern-rule   refer-case-sensitive   refer-case-insensitive   boolean</li></ul>
<b>msg-type</b>	<p>Enter the SIP message type on which you want the MIME rules to be performed.</p> <ul style="list-style-type: none"><li>• Default: any</li><li>• Values: any   request   reply</li></ul>
<b>methods</b>	<p>Enter the list of SIP methods to which the MIME rules apply, such as INVITE, ACK, or CANCEL. There is no default for this parameter.</p>
<b>new-value</b>	<p>When the action parameter is set to add or to manipulate, enter the new value that you want to substitute.</p>
<b>mime-headers</b>	<p>Access the mime-headers subelement.</p>
<b>isup-param-rules</b>	<p>Access the isup-param-rules subelement.</p>

### Path

**sip-mime-isup-rules** is a subelement under the sip-manipulation element. The full path from the topmost CLI prompt is: configure terminal > session-router > sip-manipulation > mime-isup-rules.

### Release

First appearance: S-C6.2.0

### RTC Status

Supported



**Note:** This is a multiple instance configuration element.

---

## sip-manipulation > mime-isup-rules > mime-header-rules

The mime-header-rules subelement of mime-isup-rules allows you to configure a SIP header manipulation to add an ISUP body to a SIP message.

## Parameters

<b>name</b>	Enter a unique identifier for this MIME header rule.
<b>mime-header-name</b>	Enter the value used for comparison with the specific header in the body part of the SIP message. There is no default for this parameter.
<b>action</b>	Choose the type of action you want to be performed. <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: add   replace   store   sip-manip   find-replace-all   none</li> </ul>
<b>comparison-type</b>	Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header. <ul style="list-style-type: none"> <li>• Default: case-sensitive</li> <li>• Values: case-sensitive   case-insensitive   pattern-rule   refer-case-sensitive   refer-case-insensitive   boolean</li> </ul>
<b>match-value</b>	Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.
<b>new-value</b>	Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

## Path


**mime-headers** is a subelement under the `sip-manipulation>mime-isup-rules` element. The full path from the topmost CLI prompt is: **configure terminal > session-router > sip-manipulation > mime-isup-rules > mime-headers**.

## Release

First appearance: S-C6.2.0

## RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

## sip-manipulation > mime-isup-rules > isup-param-rules

The `isup-parameter-rules` element is used to create, manipulate, and store different parameters in the body of ISUP message.

## Parameters

<b>name</b>	Enter a unique identifier for this ISUP parameter rule. This parameter is required and has no default.
<b>parameter-type</b>	Using ISUP parameter mapping, enter the ISUP parameters on which you want to perform manipulation. This parameter takes values between 0 and 255, and you must know the correct ISUP mapping value for your entry. The Oracle Communications Session Border Controller calculates the offset and location of this parameter in the body.



**Note:** The value returned from the body does not identify the type or length, only the parameter value. For example, a parameter-type value of 4 acts on the Called Party Number parameter value.

- Default: 0
- Values: Min: 0 / Max: 255

**parameter-format**

Enter the method for the Oracle Communications Session Border Controller to convert a specific parameter to a string representation of that value.

- Default: hex-ascii
- Values: number-param | hex-ascii | binary-ascii | ascii-string | bcd

**action**

Choose the type of action you want to be performed.

**comparison-type**

Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

**match-value**

Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

**new-value**

When the action parameter is set to add or to manipulate, enter the new value that you want to substitute.

### Path

**isup-param-rules** is a subelement under the `sip-manipulation>mime-isup-rules` element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-isup-rules > isup-param-rules**.

### Release

First appearance: S-C6.2.0

### RTC Status

Supported



**Note:** This is a multiple instance configuration element.

## sip-manipulation > mime-rules

---

The mime-rules configuration element allows you to set parameters in the MIME rules that the Oracle Communications Session Border Controller uses to match against specific SIP methods and message types.

### Parameters

**name**

Enter a unique identifier for this MIME rule.

**action**

Choose the type of action you want to be performed.

- Default: none



	<ul style="list-style-type: none"> <li>Values: add   delete   manipulate   store   sip-manip   find-replace-all   none</li> </ul>
<b>match-value</b>	Enter the value to match against the body part in the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.
<b>comparison-type</b>	<p>Select a method to determine how the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.</p> <ul style="list-style-type: none"> <li>Default: case-sensitive</li> <li>Values: case-sensitive   case-insensitive   pattern-rule   refer-case-sensitive   refer-case-insensitive   boolean</li> </ul>
<b>msg-type</b>	<p>Enter the SIP message type on which you want the MIME rules to be performed.</p> <ul style="list-style-type: none"> <li>Default: any</li> <li>Values: any   request   reply</li> </ul>
<b>methods</b>	Enter the list of SIP methods to which the MIME rules apply. There is no default for this parameter.
<b>new-value</b>	When the action parameter is set to add or to manipulate, enter the new value that you want to substitute
<b>mime-headers</b>	access the mime-headers subelement.
<b>name</b>	Enter a unique identifier for this MIME rule.

## Path


**mime-rules** is a subelement under the sip-manipulation element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-rules**.

## Release

First appearance: S-C6.2.0

## RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

## sip-manipulation > mime-rules > mime-headers

The mime-headers configuration allows you to configure MIME headers, which operate on the specific headers in the match body part of the SIP message.

### Parameters

<b>name</b>	Enter a name for this MIME header rule. This parameter is required and has no default.
<b>mime-header-name</b>	Enter the value to be used for comparison with the specific header in the body part of the SIP message. There is no default for this parameter.
<b>action</b>	<p>Choose the type of action you want to be performed.</p> <ul style="list-style-type: none"> <li>Default: none</li> <li>Values: add   replace   store   sip-manip   find-replace-all   none</li> </ul>

<b>comparison-type</b>	Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header. <ul style="list-style-type: none"><li>• Default: case-sensitive</li><li>• Values: case-sensitive   case-insensitive   pattern-rule   refer-case-sensitive   refer-case-insensitive   boolean</li></ul>
<b>match-value</b>	Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.
<b>new-value</b>	Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

### Path


**mime-headers** is a subelement under the sip-manipulation>mime-rules element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-rules>mime-headers**.

### Release

First appearance: S-C6.2.0

### RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

---

## sip-manipulation > mime-sdp-rules

---

The mime-sdp-rules configuration allows you to configure HMR for SDP.

### Parameters

<b>name</b>	Enter a name for this SDP header rule. This parameter is required and has no default.
<b>msg-type</b>	Select the message type to which this header rule applies <ul style="list-style-type: none"><li>• Default: any</li><li>• Values:<ul style="list-style-type: none"><li>• any—Both Requests and Reply messages</li><li>• request—Request messages only</li><li>• reply—Reply messages only</li><li>• out-of-dialog—</li></ul></li></ul>
<b>methods</b>	Enter the list of SIP methods to which the MIME rules apply, such as INVITE, ACK, or CANCEL. There is no default for this parameter.
<b>action</b>	Choose the type of action you want to be performed. <ul style="list-style-type: none"><li>• Default: none</li><li>• Values: add   replace   store   sip-manip   find-replace-all   none   reject   log</li></ul>

<b>comparison-type</b>	Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header. <ul style="list-style-type: none"> <li>• Default: case-sensitive</li> <li>• Values: case-sensitive   case-insensitive   pattern-rule   refer-case-sensitive   refer-case-insensitive   boolean</li> </ul>
<b>match-value</b>	Enter the value to match against the SDP body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.
<b>new-value</b>	When the action parameter is set to <b>add</b> or to <b>manipulate</b> enter the new value that you want to substitute.
<b>mime-header-rules</b>	See "sip-manipulation mime-isup-rules > mime-header-rules"
<b>sdp-session-rules</b>	list of sdp-session-rules. See "sip-manipulation > mime-sdp-rules > sdp-session-rules"
<b>sdp-media-rules</b>	list of sdp-media-rules. See "sip-manipulation > mime-sdp-rules > sdp-media-rules"

## Path


**mime-headers** is a subelement under the sip-manipulation>mime-rules element. The full path from the topmost CLI prompt is: **configure terminal > session-router > sip-manipulation > mime-sdp-rules**.

## Release

First appearance: S-C6.3.0

## RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

# sip-manipulation > mime-sdp-rules > sdp-session-rules > sdp-line-rules

The sdp-line-rules configuration allows you to configure HMR for SDP.

## Parameters

<b>name</b>	Enter a name for this SDP header rule. This parameter is required and has no default.
<b>type</b>	descriptor type specifying which line of the SDP will be manipulated <ul style="list-style-type: none"> <li>• Values: a-z</li> </ul>
<b>action</b>	Choose the type of action you want to be performed. <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: none   add   delete   manipulate   replace   store   sip-manip   find-replace-all   reject   log</li> </ul>
<b>comparison-type</b>	Select a method to determine how the header in the body part of the SDP is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

**match-value** Enter the value to match against the SDP body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

**new-value** When the action parameter is set to add or to manipulate, enter the new value that you want to substitute

### Path

**sdp-line-rules** is a subelement under the `sip-manipulation>mime-sdp-rules > sdp-session-rules` (and `sdp-media-rules`) subelement. The full path from the topmost ACLI prompt is: `configure terminal > session-router > sip-manipulation > mime-sdp-rules > sdp-session-rules` (or `sdp-media-rules`) `> sdp-line-rules`.

### RTC Status

Supported

### Release

First appearance: S-C6.3.0



**Note:** This is a multiple instance configuration element.

## sip-manipulation > mime-sdp-rules > sdp-session-rules > sdp-line-rules

---

The `sdp-line-rules` configuration allows you to configure HMR for SDP.

### Parameters

**name** Enter a name for this SDP header rule. This parameter is required and has no default.

**type** descriptor type specifying which line of the SDP will be manipulated

- Values: a-z

**action** Choose the type of action you want to be performed.

- Default: none
- Values: none | add | delete | manipulate | replace | store | sip-manip | find-replace-all | reject | log

**comparison-type** Select a method to determine how the header in the body part of the SDP is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

**match-value** Enter the value to match against the SDP body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

**new-value** When the action parameter is set to add or to manipulate, enter the new value that you want to substitute

### Path


**sdp-line-rules** is a subelement under the `sip-manipulation>mime-sdp-rules > sdp-session-rules` (and `sdp-media-rules`) subelement. The full path from the topmost ACLI prompt is: `configure terminal > session-router > sip-manipulation > mime-sdp-rules > sdp-session-rules` (or `sdp-media-rules`) `> sdp-line-rules`.

### RTC Status

Supported

### Release

First appearance: S-C6.3.0

 **Note:** This is a multiple instance configuration element.

## sip-manipulation > mime-sdp-rules > sdp-media-rules

The `sdp-media-rules` configuration allows you to configure HMR for SDP.

### Parameters

<b>name</b>	Enter a name for this SDP header rule. This parameter is required and has no default.
<b>action</b>	Choose the type of action you want to be performed. <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: none   add   delete   manipulate   replace   store   sip-manip   find-replace-all   reject   log</li> </ul>
<b>comparison-type</b>	Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header. <ul style="list-style-type: none"> <li>• Default: case-sensitive</li> <li>• Values: case-sensitive   case-insensitive   pattern-rule   refer-case-sensitive   refer-case-insensitive   boolean</li> </ul>
<b>match-value</b>	Enter the value to match against the SDP body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.
<b>new-value</b>	When the action parameter is set to add or to manipulate, enter the new value that you want to substitute.
<b>sdp-line-rules</b>	Where you configure the list of SDP line rules. See <a href="#">sip-manipulation mime-sdp-rules sdp-session-rules sdp-line-rules</a>

### Path

**sdp-media-rules** is a subelement under the `sip-manipulation>mime-sdp-rules` element. The full path from the topmost ACLI prompt is: `configure terminal > session-router > sip-manipulation > mime-sdp-rules > sdp-media-rules`.

### Release

First appearance: S-C6.3.0

### Release



**Note:** This is a multiple instance configuration element.

## sip-nat

---

The sip-nat element is used for configuring SIP-NAT across realms.

### Parameters

<b>realm-id</b>	Enter the name of the external realm. This required realm-id must be unique.
<b>domain-suffix</b>	Enter the domain name suffix of the external realm. This suffix is appended to encoded hostnames that the SIP-NAT function creates. This is a required field.
<b>ext-proxy-address</b>	Enter the IP address of the default next-hop SIP element (a SIP proxy) in the external network. This is a required field. Entries in this field must follow the IP Address Format.
<b>ext-proxy-port</b>	Enter the port number of the default next-hop SIP element (a SIP proxy) in the external network <ul style="list-style-type: none"><li>• Default: 5060</li><li>• Values: Min: 1025 / Max: 65535</li></ul>
<b>ext-address</b>	Enter the IP address on the network interface in the external realm. This required entry must follow the IP address format.
<b>home-address</b>	Enter the IP address on the network interface in the home realm. This required entry must follow the IP address format.
<b>home-proxy-address</b>	Enter the IP address for the home proxy (from the perspective of the external realm). An empty home-proxy-address field value signifies that there is no home proxy, and the external address will translate to the address of the Oracle Communications Session Border Controller's SIP proxy. Entries in this field must follow the IP Address Format.
<b>home-proxy-port</b>	Enter the home realm proxy port number <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0; 1025 / Max: 65535</li></ul>
<b>route-home-proxy</b>	Enable or disable requests being routed from a given SIP-NAT to the home proxy <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled   forced</li></ul>
<b>address-prefix</b>	Enter the address prefix subject to SIP-NAT encoding. This field is used to override the address prefix from the realm config for the purpose of SIP-NAT encoding. <ul style="list-style-type: none"><li>• Default: *</li><li>• Values:<ul style="list-style-type: none"><li>• &lt;IP address&gt;:[/num-bits]</li><li>• *—indicates that the addr-prefix in the realm-config is to be used</li><li>• 0.0.0.0—indicates that addresses NOT matching the address prefix of the home realm should be encoded</li></ul></li></ul>
<b>tunnel-redirect</b>	Enable or disable certain headers in a 3xx Response message being received and NATed when sent to the initiator of the SIP INVITE message

	<ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>use-url-parameter</b>	<p>Select how SIP headers use the URL parameter (parameter-name) for encoded addresses that the SIP-NAT function creates. A value of none indicates that Oracle Communications Session Border Controller functionality remains unchanged and results in the existing behavior of the Oracle Communications Session Border Controller. From-to and phone are used for billing issues related to extracting digits from the encoded portion of SIP messages along with the parameter-name field.</p> <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: <ul style="list-style-type: none"> <li>• none</li> <li>• from-to</li> <li>• phone</li> <li>• all</li> </ul> </li> </ul>
<b>parameter-name</b>	<p>Enter the URL parameter name used when constructing messages. This field is used in SIP-NAT encoding addresses that have a use-url-parameter field value of either from-to or all. This field can hold any value, but it should not be a recognized name that another proxy might use.</p>
<b>user-nat-tag</b>	<p>Enter the username prefix used for SIP URLs</p> <ul style="list-style-type: none"> <li>• Default: -acme-</li> </ul>
<b>host-nat-tag</b>	<p>Enter the hostname prefix used for SIP URLs</p> <ul style="list-style-type: none"> <li>• Default: ACME-</li> </ul>
<b>headers</b>	<p>Enter the type of SIP headers to be affected by the Oracle Communications Session Border Controller's sip-nat function. The URIs in these headers will be translated and encrypted, and encryption will occur according to the rules of this sip-nat element. Entries in this field must follow this format: &lt;header-name&gt;=&lt;tag&gt;.</p> <ul style="list-style-type: none"> <li>• Default: Type headers -d &lt;enter&gt;</li> </ul> <p>The default behavior receives normal SIP-NAT treatment. SIP-NAT header tags for SIP IP address replacement are listed below:</p> <ul style="list-style-type: none"> <li>• fqdn-ip-tgt—Replaces the FQDN with the target address</li> <li>• fqdn-ip-ext—Replaces the FQDN with the SIP-NAT external address</li> <li>• ip-ip-tgt—Replaces FROM header with target IP address</li> <li>• ip-ip-ext—Replaces FROM header with SIP-NAT external address</li> </ul>
<b>delete-headers</b>	<p>Remove headers from the list of SIP headers configured in the headers field</p>

## Path

**sip-nat** is an element under the session-router path. The full path from the topmost CLI prompt is: **configure terminal > session-router > sip-nat**.

## Release

First appearance: 1.0 / Most recent update: 2.0

## RTC Status

Supported



**Note:** This is a multiple instance configuration element.

### sip-profile

---

The sip-profile configuration element allows you to configure SIP profiles on the Oracle Communications Session Border Controller.

#### Parameters

<b>name</b>	Enter a unique identifier for this SIP profile. You will need this SIP profile's name when you want to apply this profile to a realm, SIP interface, or SIP session agent
<b>redirection</b>	<p>Set this value to specify the redirection action, within the context of SIP Diversion interworking.</p> <ul style="list-style-type: none"><li>• Default: none</li><li>• Values: inherit   none   isup   diversion   history-info</li></ul>
<b>ingress-conditional-cac-admit</b>	<p>Set this parameter to enabled to use conditional bandwidth CAC for media release on the ingress side of a call. Set this parameter to inherit for the value to be inherited from the realm-config, sip-interface, or sip-interface</p> <ul style="list-style-type: none"><li>• Default: inherit</li><li>• Values: enabled   disabled   inherit</li></ul>
<b>egress-conditional-cac-admit</b>	<p>Set this parameter to enabled to use conditional bandwidth CAC for media release on the egress side of a call.</p> <ul style="list-style-type: none"><li>• Default: inherit</li><li>• Values: enabled   disabled   inherit</li></ul>
<b>forked-cac-bw</b>	<p>Select the method for the CAC bandwidth to be configured between the forked sessions.</p> <ul style="list-style-type: none"><li>• Default: inherit</li><li>• Values:<ul style="list-style-type: none"><li>• per-session—The CAC bandwidth is configured per forked session</li><li>• shared—The CAC bandwidth is shared across the forked sessions</li><li>• inherit—Inherit value from realm-config or sip-interface</li></ul></li></ul>
<b>cnam-lookup-server</b>	Enter the name of an <b>enum-config</b> to query ENUM servers for CNAM data.
<b>cnam-lookup-dir</b>	<p>Set this parameter to ingress or egress to identify where the Net-Net SBC performs a CNAM lookup with respect to where the call traverses the system.</p> <ul style="list-style-type: none"><li>• Default: egress</li><li>• Values: ingress   egress</li></ul>
<b>cnam-unavailable-ptype</b>	Set this parameter to a string, no more than 15 characters, to indicate that the unavailable=parameter was returned in a CNAM response.
<b>cnam-unavailable-utype</b>	Set this parameter to a string, no more than 15 characters, to indicate that the unavailable=uparameter was returned in a CNAM response.
<b>replace-dialogs</b>	Enables the SBC to process messages with the Replaces: header. It also adds the replaces parameter to the to the Supported header in the realms where it is applied. The inherit value falls back to the higher level of configuration precedence.



- Default: inherit
- inherit | enabled | disabled


Path: **sip-profile** is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-profile**.

### Release

First appearance: S-C6.2.0

### RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

---

## sip-q850-map

The sip-q850-map configuration element is used to map SIP response codes to q850 cause codes.

### Parameters

<b>entries</b>	Enter the entries configuration subelement
<b>delete</b>	Delete a SIP to q850 mapping. Enter the SIP code.
<b>edit</b>	Edit a response map by number

### Path

**sip-q850-map** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-q850-map**

### Release

First appearance: 4.0

### RTC Status

Supported

---

## sip-q850-map > entries

The entries subelement is used to create the mapping of q850 cause to SIP reason code.

### Parameters

<b>q850-cause</b>	Enter the q850 cause code to map to a SIP reason code
<b>sip-status</b>	Enter the SIP response code that maps to this q850 cause code <ul style="list-style-type: none"> <li>• Values: Min: 100 / Max: 699</li> </ul>
<b>q850-reason</b>	Describe text to accompany the mapped SIP response code

### Path

Entries is a subelement under the **sip-q850-map** configuration element, which is located under the session-router path. The full path from the topmost CLI prompt is: **configure terminal > session-router > sip-q850-map > entries**.

### Release

First appearance: 4.0

### RTC Status

Supported

## sip-response-map

---

The sip-response-map element establishes SIP response maps associated with the upstream session agent.

### Parameters

<b>name</b>	Name of SIP response map
<b>entries</b>	Access the entries subelement
<b>delete</b>	Remove the selected response-map entry

### Path


**sip-response-map** is an element under the session-router path. The full path from the topmost CLI prompt is: **configure terminal > session-router > sip-response-map**.

### Release

First appearance: 1.1

### RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

## sip-response-map > entries

---

The entries subelement establishes the status code(s) for both received and transmitted messages and the reason phrase(s) of a SIP response map.

### Parameters

<b>recv-code</b>	Enter the original SIP response code received <ul style="list-style-type: none"><li>Values: Min: 1 / Max: 699</li></ul>
<b>xmit-code</b>	Enter the setting of translated SIP response code transmitted <ul style="list-style-type: none"><li>Values: Min: 1 / Max: 699</li></ul>
<b>reason</b>	Enter the setting of translated response comment or reason phrase to send denoted by an entry in quotation marks

<b>method</b>	Enter the SIP method name you want to use for this SIP response map entry
<b>register-response-expires</b>	<p>Enter the time you want to use for the expires time when mapping the SIP method you identified in the method parameter. By default, the expires time is the Retry-After time (if there is one in the response) of the expires value in the Register request (if there is no Retry-After expires time). Any value you configure in this parameter (when not using the defaults) should never exceed the Register request's expires time.</p> <ul style="list-style-type: none"> <li>• Values: Min: 0 / Max: 999999999</li> </ul>

### Path


**entries** is a subelement of the sip-response-map element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-response-map > entries**

### Release

First appearance: 1.1

### RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

## sipura-profile

The **sipura-profile** element is analogous to existing sdes-profiles, mikey-profiles, or IKE security associations in that all these objects specify materials (certificates, protocol suites, etc.) available in support of cryptographic operations.

### Syntax

```
sipura-profile <name | crypto-list | certificate-file-name>
```

### Parameters

<b>name</b>	A unique name for this sipura profile.
<b>crypto-list</b>	<p>Cryptographic algorithm for this profile.</p> <ul style="list-style-type: none"> <li>• Default: AES_CM_128_HMAC_MD5</li> <li>• AES_CM_128_HMAC_MD5</li> </ul>
<b>certificate-file-name</b>	Required parameter to specify the file name of the minicertificate presented by the SBC in support of Linksys/sipura operations. This file must have been previously installed in the /code/sipura directory. When identifying the file, use the complete file name, to include the file extension, but omit the directory path.

### Path

**sipura-profile** is an element of the media-security path. The full path from the topmost ACLI prompt is: **configure terminal > system > security > media-security > sipura-profile**.

### Release

First appearance: S-CX6.4.0

### snmp-community

---

The snmp-community element defines the NMSs from which the Oracle Communications Session Border Controller will accept SNMP requests.

#### Parameters

- community-name** Enter the name of the SNMP community to which a particular NMS belongs. This required entry must follow the Name Format. The community-name field values must be unique.
- access-mode** Select the access level for each snmp-community element
- Default: READ-ONLY
  - Values:
    - READ-ONLY—Allows GET requests
    - READ-WRITE—Allows both GET and SET requests
- ip-addresses** Enter the IP address(es) for SNMP communities for authentication purposes. Entries must follow the IP Address Format. Path: **snmp-community** is an element under the system path.

#### Path

The full path from the topmost ACLI prompt is: **configure terminal > system > snmp-community**.

#### Release

First appearance: 1.0

#### RTC Status

Unsupported



**Note:** This is a multiple instance configuration element.

### snmp-user-entry

---

The snmp-user-entry element is used to create SNMP users for use with SNMPv3.

#### Parameters

- user-name** Enter the name of the user authorized for retrieving SNMPv3 information.
- auth-password** Enter the authorization password for this user. This value will be obscured when displayed at the ACLI.
- priv-password** Enter the privacy password for this user. This value will be obscured when displayed at the ACLI.

#### Path

**snmp-community** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > snmp-user-entry**.

#### Release

First appearance: 6.3



**Note:** This is a multiple instance configuration element.

## spl-config

---

### Parameters

**plugins** Use this parameter to enter the plugins path as described next. In the plugins path you will configure local plugin files for use.

### Path

**spl-config** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** > **system** > **spl-config**.

### Release

First appearance: 6.3

## spl-config > plugins

---

### Parameters

**name** Enter the SPL package to load. The default location is /code/spl. You may enter a single SPL plugin within a package as follows: SPL\_PACKAGE:MODIFY-HEADER

**move** Move plugin

### Path

**spl-config** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** > **system** > **spl-config** > **plugins**.

### Release

First appearance: 6.3

## static-flow

---

The static-flow element sets preconfigured flows that allow a specific class of traffic to pass through the Oracle Communications Session Border Controller unrestricted.

### Parameters

**in-realm-id** Enter the ingress realm or interface source of packets to match for static flow translation. This in-realm-id field value must correspond to a valid identifier field entry in a realm-config. This is a required field. Entries in this field must follow the Name Format.

**description** Provide a brief description of this static-flow configuration object.

**in-source** Enter the incoming source IP address and port of packets to match for static flow translation. IP address of 0.0.0.0 matches any source address. Port 0 matches packets received on any port. The port value has no impact on system operation if either ICMP or ALL is the selected protocol. The in-source parameter takes the format: in-source <ip-address>[:<port>]

	<ul style="list-style-type: none"><li>• Default: 0.0.0.0</li><li>• Values: Port: Min: 0 / Max: 65535</li></ul>
<b>in-destination</b>	<p>Enter the incoming destination IP address and port of packets to match for static-flow translation. An IP address of 0.0.0.0 matches any source address. Port 0 matches packets received on any port. The port value has no impact on system operation if either ICMP or ALL is the selected protocol. The in-destination parameter takes the format: in-destination &lt;ip-address&gt;[:&lt;port&gt;]</p> <ul style="list-style-type: none"><li>• Default: 0.0.0.0</li><li>• Values: Port: Min: 0 / Max: 65535</li></ul>
<b>out-realm-id</b>	<p>Enter the egress realm or interface source of packets to match for static flow translation. This out-realm-id field value must be a valid identifier for a configured realm. This required entry must follow the Name Format.</p>
<b>out-source</b>	<p>Enter the outgoing source IP address and port of packets to translate to for static flow translation. IP address of 0.0.0.0 translates to any source address. Port 0 translates to packets sent on any port. The port value has no impact on system operation if either ICMP or ALL is the selected protocol. The out-source parameter takes the format: out-source &lt;ip-address&gt;[:&lt;port&gt;]</p> <ul style="list-style-type: none"><li>• Default: 0.0.0.0</li><li>• Values: Port: Min: 0 / Max: 65535</li></ul>
<b>out-destination</b>	<p>Enter the outgoing destination IP address and port of packets to translate to for static-flow translation. An IP address of 0.0.0.0 matches any source address. Port 0 translates to packets sent on any port. The port value has no impact on system operation if either ICMP or ALL is the selected protocol. The out-destination parameter takes the format: out-destination &lt;ip-address&gt;[:&lt;port&gt;]</p> <ul style="list-style-type: none"><li>• Default: 0.0.0.0</li><li>• Values: Port: Min: 0 / Max: 65535</li></ul>
<b>protocol</b>	<p>Select the protocol for this static-flow. The protocol selected must match the protocol in the IP header. The protocol remains the same for the inbound and outbound sides of the packet flow.</p> <ul style="list-style-type: none"><li>• Default: UDP</li><li>• Values:<ul style="list-style-type: none"><li>• UDP—UDP used for this static-flow element</li><li>• TCP—TCP used for this static-flow element</li><li>• ICMP—ICMP used for this static-flow element</li><li>• ALL—Static-flow element can accept flows via any of the available protocols.</li></ul></li></ul>
<b>alg-type</b>	<p>Select the type of NAT ALG to use</p> <ul style="list-style-type: none"><li>• Default: none</li><li>• Values:<ul style="list-style-type: none"><li>• none—No dynamic ALG functionality</li><li>• NAPT—Configure as NAPT ALG</li><li>• TFTP—Configure as TFTP ALG</li></ul></li></ul>
<b>average-rate-limit</b>	<p>Enter the maximum speed in bytes per second for this static flow</p> <ul style="list-style-type: none"><li>• Default 0</li><li>• Values: Min: 0 / Max: 125000000</li></ul>
<b>start-port</b>	<p>Enter the internal starting ALG ephemeral port</p> <ul style="list-style-type: none"><li>• Default: 0</li></ul>

	<ul style="list-style-type: none"> <li>Values: Min: 1025 / Max: 65535</li> </ul>
<b>end-port</b>	Enter the internal ending ALG ephemeral port <ul style="list-style-type: none"> <li>Default: 0</li> <li>Values: Min: 1025 / Max: 65535</li> </ul>
<b>flow-time-limit</b>	Enter the time limit for a flow, measured in seconds <ul style="list-style-type: none"> <li>Values: Min: 0 / Max: 999999999</li> </ul>
<b>initial-guard-timer</b>	Enter the initial flow guard timer, measured in seconds <ul style="list-style-type: none"> <li>Values: Min: 0 / Max: 999999999</li> </ul>
<b>subsq-guard-timer</b>	Enter the subsequent flow guard timer, measured in seconds <ul style="list-style-type: none"> <li>Values: Min: 0 / Max: 999999999</li> </ul>

## Path


**static-flow** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > static-flow**.

## Release

First appearance: 1.0 / Most recent update: 4.1

## RTC Status

Supported

 **Note:** This is a multiple instance configuration element.

# steering-pool

The steering-pool element defines sets of ports that are used for steering media flows through the Oracle Communications Session Border Controller. The Oracle Communications Session Border Controller can provide packet steering in order to ensure a determined level of quality or routing path.

## Parameters

<b>ip-address</b>	Enter the target IP address of the steering pool. This required entry must follow the IP Address Format. The combination of entries in the ip-address, start-port, and realm-id fields must be unique. No two steering-pool elements can have the same entries in the ip-address, start-port, and realm-id fields.  An IPV6 address is valid for this parameter.
<b>start-port</b>	Enter the port number that begins the range of ports available to this steering pool element. This is a required entry. The steering pool will not function properly unless this entry is a valid port. <ul style="list-style-type: none"> <li>Default: 0</li> <li>Values: Min: 0 / Max: 65535</li> </ul>
<b>end-port</b>	Enter the port number that ends the range of ports available to this steering-pool element. This is a required field. The steering-pool element will not function properly unless this field is a valid port value.

- Default: 0
- Values: Min: 0 / Max: 65535

<b>realm-id</b>	Enter the steering-pool element's realm identifier used to restrict this steering pool to only the flows that originate from this realm. This required entry must be a valid identifier of a realm.
<b>network-interface</b>	Enter the name of network interface this steering pool directs its media toward. A valid value for this parameter must match a configured name parameter in the network-interface configuration element.

### Path


**steering-pool** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > steering-pool**.

### Release

First appearance: 1.0 / Most recent update: 2.1

### RTC Status

Supported


 **Note:** This is a multiple instance configuration element.

---

## surrogate-agent

The surrogate-agent configuration element allows you to configure the Oracle Communications Session Border Controller for surrogate registration. This feature lets the Oracle Communications Session Border Controller explicitly register on behalf of Internet Protocol Branch Exchange (IP-PBX).

### Parameters

<b>register-host</b>	Enter the registrar's hostname to be used in the Request-URI of the REGISTER request
<b>register-user</b>	Enter the user portion of the Address of Record
<b>state</b>	Enable or disable this surrogate agent <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>realm-id</b>	Enter the name of the realm where the surrogate agent resides
<b>description</b>	Describe the surrogate agent. This parameter is optional.
<b>customer-host</b>	Enter the domain or IP address of the IP-PBX, which is used to determine whether it is different than the one used by the registrar. This parameter is optional.
<b>customer-next-hop</b>	Enter the next hop to this surrogate agent <p> <b>Note:</b> Even though the customer-next-hop field allows specification of a SAG or FQDN, the functionality will only support these values if they resolve to a single IP address. Multiple IP addresses, via SAG, NAPTR, SRV, or DNS record lookup, are not allowed.</p>
<b>register-contact-host</b>	Enter the hostname to be used in the Contact-URI sent in the REGISTER request. This should always point to the Oracle Communications Session Border Controller. If specifying a IP



	address, use the egress interface's address. If there is a SIP NAT on the registrar's side, use the home address in the SIP NAT.
<b>register-contact-user</b>	Enter the user part of the Contact-URI that the Oracle Communications Session Border Controller generates
<b>password</b>	Enter the password to be used for this agent
<b>register-expires</b>	Enter the expire time in seconds to be used in the REGISTER <ul style="list-style-type: none"> <li>• Default: 600,000 (1 week)</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>replace-contact</b>	Specify whether the Oracle Communications Session Border Controller needs to replace the Contact in the requests coming from the surrogate agent <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>route-to-registrar</b>	Enable or disable requests coming from the surrogate agent being routed to the registrar if they are not explicitly addressed to the Oracle Communications Session Border Controller <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>aor-count</b>	Enter the number of registrations to do on behalf of this IP-PBX <ul style="list-style-type: none"> <li>• Default: 1</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>auth-user</b>	Enter the authentication user name you want to use for the surrogate agent
<b>max-register-attempt</b>	Enter the number of times to attempt registration; a 0 value means registration attempts are unlimited <ul style="list-style-type: none"> <li>• Default: 3</li> <li>• Values: Min: 0 / Max: 10</li> </ul>
<b>register-retry-time</b>	Enter the amount of time in seconds to wait before reattempting registration <ul style="list-style-type: none"> <li>• Default: 300</li> <li>• Values: Min: 10 / Max: 3600</li> </ul>
<b>count-start</b>	Enter the number of registrations to do on behalf of this IP-PBX <ul style="list-style-type: none"> <li>• Default: 1</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>options</b>	Enter non-standard options or features

## Path

**surrogate-agent** is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > surrogate-agent.**

## Release

First appearance: 4.1; Last update: 5.1

### system-access-list

---

The system-access-list configuration element allows you to configure system access control of the management interface on your Oracle Communications Session Border Controller. Once configured, any access from hosts that are not part of the system access IP address or subnet are denied. When this element is not configured, any host can access management ports.

#### Parameters

<b>source-address</b>	Enter the network source address
<b>netmask</b>	Enter the source subnet mask
<b>description</b>	Provide a brief description of this system-access-list configuration.
<b>protocol</b>	<p>Enter a specified protocol or the special value all that specifies by protocol the type of management traffic allowed to access the system. The default value (all) matches all supported transport layer protocols.</p> <ul style="list-style-type: none"><li>• Default: all</li><li>• Values: all   icmp   telnet   ftp   ftp-passive   ssh   snmp</li><li>• ip-prot/well-known-port: 6/21</li><li>• for non-tcp and non-udp port must be 0</li><li>• for single entry: telnet</li><li>• for multiple entry: (telnet 6/20 ssh)</li></ul>

#### Path

**system-access-list** is an element of the system path. The full path from the topmost ACLI prompt is: **configure terminal > system> system-access-list**

#### Release

First appearance: 5.0 / Most recent update: S-C6.2.0

#### RTC Status

Supported

### system-config

---

The system-config element establishes general system information and settings.

#### Parameters

<b>hostname</b>	Enter the main hostname that identifies the Oracle Communications Session Border Controller. Entries must follow either the Hostname (or FQDN) Format or the IP Address Format.
<b>description</b>	Describe the Oracle Communications Session Border Controller. Entries must follow the Text Format
<b>location</b>	Enter the physical location of the Oracle Communications Session Border Controller used for informational purposes. Entries must follow the Text Format.
<b>mib-system-contact</b>	Enter the contact information for this Oracle Communications Session Border Controller for SNMP purposes. This field value is the value reported for MIB-II when an SNMP GET is issued by the NMS. Entries must follow the Text Format.

<b>mib-system-name</b>	Enter the identification of the Oracle Communications Session Border Controller for SNMP purposes. This value has no relation to the <b>system-config &gt; hostname</b> field. By convention, this is the node's FQDN. If this field remains empty, the Oracle Communications Session Border Controller name that appears in SNMP communications will be the target name configured in the boot parameters and nothing else.
<b>mib-system-location</b>	Enter the physical location of the Oracle Communications Session Border Controller for SNMP purposes. This parameter has no direct relation to the location field identified above. Entries must follow the Text Format
<b>snmp-enabled</b>	<p>Enable or disable SNMP is enabled. If SNMP is enabled, then the system will initiate the SNMP agent. If SNMP is disabled, then the SNMP agent will not be initiated, and the trap-receiver and snmp-community elements will not be functional.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>enable-snmp-auth-traps</b>	<p>Enable or disable the SNMP authentication traps</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>enable-snmp-syslog-notify</b>	<p>Enable or disable sending syslog notifications to an NMS via SNMP; determines whether SNMP traps are sent when a Oracle Communications Session Border Controller generates a syslog message</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>enable-snmp-monitor-traps</b>	<p>Determine whether traps are sent out in ap-smgmt.mib trap. (See 400-0010-00, MIB Reference Guide for more information)</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>enable-env-monitor-traps</b>	<p>Determine whether the environmental monitoring MIB is sent from the Oracle Communications Session Border Controller. This trap will be sent any time there is a change in state in fan speed, temperature, voltage (SD 2 only), power supply (SD 1 for rev 1.32 or higher, SD 2 w/QoS for rev 1.32 or higher, SD II no QoS for rev 1.3 or higher), phy-card insertion, or I2C bus status. If this parameter is set to enabled, fan speed, temperature, and power supply notifications are not sent out in other traps.</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>snmp-syslog-his-table-length</b>	<p>Enter the maximum entries that the SNMP Syslog message table contains. The system will delete the oldest table entry and add the newest entry in the vacated space when the table reaches maximum capacity.</p> <ul style="list-style-type: none"> <li>• Default: 1</li> <li>• Values: Min: 1 / Max: 500</li> </ul>
<b>snmp-syslog-level</b>	<p>Set the log severity levels that send syslog notifications to an NMS via SNMP if snmp-syslog-notify is set to enabled. If the severity of the log being written is of equal or greater severity than the snmp-syslog-level value, the log will be written to the SNMP syslog history table. If the severity of the log being written is of equal or greater severity than the snmp-syslog-level field value and if enabled-snmp-syslog-notify field is set to enabled, the system will send the syslog message to an NMS via SNMP. If the severity of the log being written is of lesser severity than the snmp-syslog-level value, then the log will not be written to the SNMP syslog history table and it will be disregarded.</p>

	<ul style="list-style-type: none"><li>• Default: warning</li><li>• Values:<ul style="list-style-type: none"><li>• emergency</li><li>• critical</li><li>• major</li><li>• minor</li><li>• warning</li><li>• notice</li><li>• info</li><li>• trace</li><li>• debug</li><li>• detail</li></ul></li></ul>
<b>syslog-servers</b>	Access the syslog-servers subelement
<b>system-log-level</b>	<p>Set the system-wide log severity levels write to the system log</p> <ul style="list-style-type: none"><li>• Default: warning</li><li>• Values:<ul style="list-style-type: none"><li>• emergency</li><li>• critical</li><li>• major</li><li>• minor</li><li>• warning</li><li>• notice</li><li>• info</li><li>• trace</li><li>• debug</li><li>• detail</li></ul></li></ul>
<b>process-log-level</b>	<p>Set the default log level that processes running on the Oracle Communications Session Border Controller start</p> <ul style="list-style-type: none"><li>• Default: notice</li><li>• Values:<ul style="list-style-type: none"><li>• emergency</li><li>• critical</li><li>• major</li><li>• minor</li><li>• warning</li><li>• notice</li><li>• info</li><li>• trace</li><li>• debug</li><li>• detail</li></ul></li></ul>
<b>process-log-ip-address</b>	<p>Enter the IP address of server where process log files are stored. Entries must follow the IP Address Format. The default value of 0.0.0.0 causes log messages to be written to the local log file.</p> <ul style="list-style-type: none"><li>• Default: 0.0.0.0</li></ul>

<b>process-log-port</b>	<p>Enter the port number associated with server IP address where process log files are stored. The default value of 0 writes log messages to the local log file.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0; 1025 / Max: 65535</li> </ul>
<b>collect</b>	<p>Accesses the collect subelement</p>
<b>call-trace</b>	<p>Enable or disable protocol message tracing for sipmsg.log for SIP and alg.log for MGCP</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>internal-trace</b>	<p>Enable or disable internal ACP message tracing for all processes</p> <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>log-filter</b>	<p>Set to logs or all to send the logs to the log server</p> <ul style="list-style-type: none"> <li>• Default: all</li> <li>• Values: <ul style="list-style-type: none"> <li>• none</li> <li>• traces</li> <li>• traces-fork</li> <li>• logs</li> <li>• log-fork</li> <li>• all</li> <li>• all-fork</li> </ul> </li> </ul>
<b>default-gateway</b>	<p>Enter the IP address of the gateway to use when IP traffic sent by the Oracle Communications Session Border Controller is destined for a network other than one of the LANs on which the 10/100 Ethernet interfaces could be. Entries must follow the IP Address Format. A value of 0.0.0.0 indicates there is no default gateway.</p> <ul style="list-style-type: none"> <li>• Default: 0.0.0.0</li> </ul>
<b>restart</b>	<p>Enable or disable the Oracle Communications Session Border Controller rebooting when a task is suspended. When set to enabled, this field causes the Oracle Communications Session Border Controller to reboot automatically when it detects a suspended task. When this field is set to disabled and a task is suspended, the Oracle Communications Session Border Controller does not reboot.</p> <ul style="list-style-type: none"> <li>• Default: enabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>exceptions</b>	<p>Select system tasks that have no impact on system health or cause the system to restart. This field contains the name(s) of the task(s) surrounded by quotation marks. If there are multiple entries, they should be listed within quotation marks, with each entry separated by a &lt;Space&gt;.</p>
<b>telnet-timeout</b>	<p>Enter the time in seconds the Oracle Communications Session Border Controller waits when there is no Telnet activity before an administrative telnet session, or SSH connection, is terminated. A value of 0 disables this functionality, meaning no time-out is being enforced.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 65535</li> </ul>
<b>console-timeout</b>	<p>Enter the time in seconds the Oracle Communications Session Border Controller waits when there is no activity on an ACLI administrative session before it terminates the session. The</p>

	<p>ACLI returns to the User Access Verification login sequence after it terminates a console session. A value of 0 disables this functionality.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 65535</li></ul>
<b>remote-control</b>	<p>Enable or disable listening for remote ACP config and control messages before disconnecting</p> <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>cli-audit-trail</b>	<p>Enable or disable the ACLI command audit trail. The cli-audit-trail outputs to cli.audit.log.</p> <ul style="list-style-type: none"><li>• Default: enabled</li><li>• Values: enabled   disabled</li></ul>
<b>link-redundancy-state</b>	<p>Enable or disable the link redundancy</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>source-routing</b>	<p>Enable or disable source routing egress HIP packets based on source IP addresses. This parameter is used to route packets based on their source address, and not on the system's routing table. This feature is only used for management applications within the Oracle Communications Session Border Controller that utilize HIP interfaces.</p> <p>A few things to note: This feature only affects media-network interfaces The bootparam flag (0x80008) does not work in C-Series 5.x and D-Series 5.x and up. You must use the system-config source-routing parameter. The source-routing parameter is not RTC-supported. You must reboot after enabling it.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>cli-more</b>	<p>Enable this parameter to have the ACLI “more” paging feature working consistently across console, Telnet, or SSH sessions with the Oracle Communications Session Border Controller. When this parameter is disabled, you must continue to set this feature on a per session basis.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>terminal-height</b>	<p>Set the Oracle Communications Session Border Controller terminal height when the more prompt option is enable</p> <ul style="list-style-type: none"><li>• Default: 24</li><li>• Values: Minimum: 5 / Maximum: 1000</li></ul>
<b>debug-timeout</b>	<p>Enter the time, in seconds, you want to the Oracle Communications Session Border Controller to timeout log levels for system processes set to debug using the ACLI notify and debug commands. A value of 0 disables this parameter.</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 65535</li></ul>
<b>trap-event-lifetime</b>	<p>Set this parameter to the number of days you want to keep the information in the alarm synchronization table; 0 turns alarm synchronization off</p> <ul style="list-style-type: none"><li>• Default: 0</li><li>• Values: Min: 0 / Max: 7</li></ul>

<b>ids-syslog-facility</b>	Enter a syslog facility, as entered in the syslog-config configuration element, facility parameter to send IDS-type syslog messages to that syslog server. The default value of -1 disables selective message transfer.  • Default: -1
<b>default-v6-gateway</b>	Set the IPv6 default gateway for this Oracle Communications Session Border Controller. This is the IPv6 egress gateway for traffic without an explicit destination. The application of your Oracle Communications Session Border Controller determines the configuration of this parameter. An IPV6 address is valid for this parameter.
<b>ipv6-signaling-mtu</b>	This sets the system-wide, default IPv6 MTU size.  • Default: 1500 • Values: 1280-4096
<b>ipv4-signaling-mtu</b>	This sets the system-wide, default IPv4 MTU size.  • Default: 1500 • Values: 576-4096
<b>alarm-threshold</b>	Accesses the alarm-threshold subelement.
<b>cleanup-time-of-day</b>	Enter the local time the Oracle Communications Session Border Controller begins inspecting directories to perform the clean up process.  directory-cleanup—Enters the directory-cleanup subelement.
<b>snmp-engine-id-suffix</b>	Sets a unique suffix for the SNMPEngineID. This value is entered as a string.
<b>snmp-agent-mode</b>	Determines which version of SNMP is supported on this system.  • Default: v1v2 • Values: v1v2   secure-trap
<b>options</b>	Enter any customer-specific features and/or parameters for this global system configuration. This parameter is optional.

## Path

**system-config** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config**.

## Release

First appearance: 1.0 / Most recent update: 6.3

## RTC Status

Supported



**Note:** Under the system-config element, options are not RTC supported. This is a single instance configuration element.

## system-config > alarm-threshold

The alarm-threshold configuration element allows you to configure custom alarms for certain system conditions based on those conditions reaching defined operating levels.

### Parameters

- type** The type of custom alarm-threshold this object creates.
- Values:
    - **cpu** — Alarm based on CPU usage
    - **space** — Alarm based on used space on an identified disk volume
    - **memory** — Alarm based on memory usage
    - **sessions** — Alarm based on percentage of licensed sessions in use
    - **rfactor** — unused
    - **deny-allocation** — Alarm based on remaining number of reserved deny entries
- volume** — Identifies the disk volume that this alarm threshold monitors. This parameter is only configured when the type parameter is set to space.
- Values for the volume parameter include active volume names on your system, such as "opt" and "boot".
- severity** The system severity of this alarm.
- Default: minor
  - Values: major | minor | critical
- value** The percentage usage of the resource identified in the type parameter that triggers this alarm.
- Default: 2
  - Values: 1 - 100

### Path

**alarm-threshold** is a subelement of the **system-config** element. The full path from the topmost ACLI prompt is:  
**configure terminal > system > system-config > alarm-threshold**

### RTC Status

Supported

---

## system-config > collect


---

The collect configuration element allows you to configure general collection commands for data collection on the Oracle Communications Session Border Controller.

### Parameters

- sample-interval** Enter the data collection sampling interval, in minutes
- Default: 0
  - Values: Min: 1 / Max: 120
- push-interval** Enter the data collecting push interval, in minutes
- Default: 0
  - Values: Min: 0 / Max: 120
- start-time** Enter the date and time to start data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hours; m=minutes; s=seconds)
- Default: now



<b>end-time</b>	Enter the date and time to stop data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hours; m=minutes; s=seconds) <ul style="list-style-type: none"> <li>• Default: never</li> </ul>
<b>boot-state</b>	Enable or disable group collection on reboot <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul> <p> <b>Note:</b> This parameter is not RTC supported</p>
<b>red-collect-state</b>	Enable or disable HA support for the collection function <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>
<b>red-max-trans</b>	Enter the maximum number of redundancy sync transactions to keep on active <ul style="list-style-type: none"> <li>• Default: 1000</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>red-sync-start-time</b>	Enter the time to start redundancy sync timeout, in milliseconds. <ul style="list-style-type: none"> <li>• Default: 5000</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>red-sync-comp-time</b>	Enter the time to complete a redundancy sync, in milliseconds <ul style="list-style-type: none"> <li>• Default: 1000</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>push-receiver</b>	Access the push-receiver subelement
<b>group-settings</b>	Access the group-settings subelement
<b>push-success-trap-state</b>	Enable this parameter if you want the Oracle Communications Session Border Controller to send a trap confirming successful data pushes to HDR servers

## Path

collect is a subelement of the system-config element. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > collect**

## Release

First appearance: 5.0

## RTC Status

Supported

## system-config > collect > push-receiver

The push-receiver configuration subelement allows you to configure the Oracle Communications Session Border Controller to push collected data to a specified node.

### Parameters

- address** Enter the hostname or IP address to which the Oracle Communications Session Border Controller pushes collected data
- user-name** Enter the hostname or IP address to which the Oracle Communications Session Border Controller pushes collected data
- password** Enter the login password for the specified server used when pushing collected data
- data-store** Enter a directory on the specified server in which to put collected data
- protocol** Set the protocol with which to send HDR collection record files.
- Default FTP
  - Values FTP | SFTP

### Path

**push-receiver** is a subelement of the **system-config>collect** subelement. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > collect > push-receiver**.

### Release

First appearance: 5.0

### RTC Status

Supported

---

## system-config > collect > group-settings

---

The group-settings subelement allows you to configure and modify collection parameters for specific groups.

### Parameters

- group-name** Enter the name of the object the configuration parameters are for. There can only be one object per group.
- Values:
    - system
    - interface
    - session-agent
    - session-realm
    - voltage
    - fan
    - temperature
    - sip-sessions
    - sip-ACL-oper
    - sip-ACL-status
    - sip-client
    - sip-server
    - sip-policy
    - sip-errors
    - sip-status

- sip-invites
- enum-stats
- mgcp-state
- mgcp-trans
- mgcp-media-events
- mgcp-ACL
- mgcp-oper
- h323-stats
- network-util
- space
- registration-realm

<b>sample-interval</b>	Enter the group data collection sampling interval, in minutes <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 120</li> </ul>
<b>start-time</b>	Enter the date and time to start group data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hour; m=minute; s=second)
<b>end-time</b>	Enter the date and time to stop group data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hour; m=minute; s=second)
<b>boot-state</b>	Enable or disable data collection for this group. <ul style="list-style-type: none"> <li>• Default: disabled</li> <li>• Values: enabled   disabled</li> </ul>

### Path

First appearance: 5.0 / Last update: S-C6.2.0 **group-settings** is a subelement of the **configure terminal > system > system-config > collect > subelement**. The full path from the topmost CLI prompt is: **configure terminal > system > system-config > collect > group-settings**

### Release

First appearance: 5.0 / Last update: S-C6.2.0

### RTC Status

Supported

## system-config > syslog-servers

The syslog-servers subelement configures multiple syslog servers.

### Parameters

<b>address</b>	Enter the syslog server's IP address
<b>port</b>	Enter the port number on the syslog server that the Oracle Communications Session Border Controller sends log <ul style="list-style-type: none"> <li>• Default 514</li> </ul>
<b>facility</b>	Enter the user-defined facility value sent in every syslog message from the Oracle Communications Session Border Controller to the syslog server. This value must conform to IETF RFC 3164.

- Default 4

### Path

**syslog-servers** is a subelement under the **system-config** element. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > syslog-servers**.

### Release

First appearance: 1.2.1

### RTC Status

Supported



**Note:** We recommend configuring no more than 8 syslog-config subelements. This is a multiple instance configuration subelement.

## system-config > directory-cleanup

---

The **syslog-servers** subelement configures multiple syslog servers.

### Parameters

- directory-path** name of the directory path where you want the Oracle Communications Session Border Controller to perform file clean-up. Subdirectories are not examined or cleaned, they must be explicitly identified.
- admin-state** State of cleanup for this directory.
- Default: enabled
  - Values: enabled | disabled
- age** age in number of days after which to delete files in this directory

### Path

**directory-cleanup** is a subelement under the **system-config** element. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > directory-cleanup**.

## tcp-media-profile

---

The **tcp-media-profile** configuration element allows you to enter individual tcp media profile entry elements. These are used for MSRP functionality.

### Parameters

- name** Name of this tcp media profile.
- profile-list** Used to enter individual tcp media profiles.

## Release

### Path

**tcp-media-profile** is an element of the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > tcp-media-profile**.

## Release

First appearance S-CX6.4.0

## tcp-media-profile > tcp-media-profile-entry

The **tcp-media-profile-entry** configuration element allows you to enter individual tcp media profile entry elements. These are used for MSRP functionality.

### Parameters

<b>media-type</b>	<p>A string used to match with the media type &lt;media&gt; in the SDP message's media description (m=). For example: "message" for MSRP.</p> <ul style="list-style-type: none"> <li>Default: message</li> </ul>
<b>transport-protocol</b>	<p>The string used to match with the transport protocol &lt;proto&gt; in the media description (m=). For example: "TCP/TLS" for MSRP over TCP/TLS.</p>
<b>listen-port</b>	<p>The listening port on which the SBC listens for incoming connections to establish a TCP connection for a media session. If the value of this field is 0, the listening port will be chosen automatically by the SBC from the steering pool of the realm (which the tcp-media-profile belongs to).</p> <ul style="list-style-type: none"> <li>Default: 0</li> <li>Values: 0-65535</li> </ul>
<b>preferred-setup-role</b>	<p>The value used by the Net-Net SBC for the a=setup attribute when negotiating the setup role, regardless of whether the SBC is an offer or answer in the SDP offer/answer exchange.</p> <ul style="list-style-type: none"> <li>Default: passive</li> <li>Values: active   passive</li> </ul>
<b>tls-profile</b>	<p>Identify the TLS profile that specifies the cryptographic resources available to support TLS operations. This is configured when transport protocol is set to TCP/TLS/MSRP. This parameter can be safely ignored if transport-protocol is TCP/MSRP.</p>
<b>require-fingerprint</b>	<p>If transport-protocol is TCP/TLS/MASP, use the require-fingerprint parameter to enable or disable endpoint authentication using the certificate fingerprint methodology defined in RFC 4572. This parameter can be ignored if transport-protocol is TCP/MSRP.</p> <ul style="list-style-type: none"> <li>Default: disabled</li> <li>Values: enabled   disabled</li> </ul>

Release First appearance: S-CX6.4.0

### Path

**tcp-media-profile-entry** is a subelement of **tcp-media-profile**. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > tcp-media-profile > tcp-media-profile-entry**.

### test-policy

---

The test-policy element tests and displays local policy routes from the ACLI.

#### Parameters

<b>source-realm</b>	Enter the name set in the source-realm field of a configured local policy. Entering an "*" in this field matches for any source realm. Leaving the field empty indicates that only the "global" realm will be tested.
<b>from-address</b>	Enter the "from" address of the local policy to look up/test. From addresses should be entered as SIP-URLs in the form of sip:19785551212@netnetsystems.com.
<b>to-address</b>	Enter the "to" address of the local policy to look up/test. To addresses should be entered as SIP-URLs in the form of sip:19785551212@netnetsystems.com.
<b>time-of-day</b>	Enable or disable use of the time of day value set in the start-time and end-time fields you set in configured local-policy elements <ul style="list-style-type: none"><li>Values: enabled   disabled</li></ul>
<b>carriers</b>	Enter the names of permitted carriers set in the carriers fields set in configured local-policy elements. This field is formatted as a list of comma separated text strings enclosed in quotation marks.
<b>media-profile</b>	Enter a list of media profiles
<b>show</b>	Show the next hop and the associated carrier information for all routes matching the "from" and "to" addresses entered

#### Path

test-policy is available under the session-router path.

#### Release

First appearance: 1.0 / Most recent update: 1.2.1

#### RTC Status

Supported

#### Notes

Type the show command to perform the actual test lookup after parameters have been entered.

The test-policy element can also be configured in Superuser mode as a command.

### test-translation

---

The test-translation element tests translation rules configured for the Address Translation feature.

#### Parameters

<b>called-address</b>	Enter the address on which the called rules will be applied. This entry is required.
<b>calling-address</b>	Enter the address on which the calling rules will be applied. This entry is required.
<b>translation-id</b>	Enter the translation rules to test. This entry is required.

**show** Show results of translation

### Path

**test-translation** is available under the session-router path.

### Release

First appearance: 1.3

### RTC Status

Supported.



**Note:** The test-translation element can also be configured in Superuser mode as a command.

## tls-global

The **tls-global** configuration element allows you to configure global TLS parameters.

### Parameters

**session-caching** Enable or disable the Oracle Communications Session Border Controller's session caching capability

- Default: disabled
- Values: enabled | disabled

**session-cache-timeout**

Enter the session cache timeout in hours

- Default: 12
- Values: Min: 0 (disabled) / Max: 24

### Path

**tls-global** is an element of the security path. The full path from the topmost ACLI prompt is: **configure terminal > security > tls-global**.

### Release

First appearance: 5.0

### RTC Status

Supported

## tls-profile

The **tls-profile** configuration element holds the information required to run SIP over TLS.

### Parameters

**name** Enter the name of the TLS profile

**end-entity-certificate** Enter the name of the entity certification record

<b>trusted-ca-certificates</b>	Enter the names of the trust CA Certificate records
<b>cipher-list</b>	<p>Enter the default ALL, or enter a list of supported ciphers which you can find in the TLS section of the ACLI Configuration Guide's Security chapter. As of Release S-C6.1.0, TLSv1 and SSLv3 have been removed made redundant by the <code>tls-version</code> parameter).</p> <ul style="list-style-type: none"><li>• Default: all</li></ul>
<b>verify-depth</b>	<p>Enter the maximum depth of the certificate chain that will be verified</p> <ul style="list-style-type: none"><li>• Default: 10</li><li>• Values: Min: 0 / Max: 10</li></ul>
<b>mutual-authenticate</b>	<p>Enable or disable mutual authentication on the Oracle Communications Session Border Controller</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>tls-version</b>	<p>Enter the TLS version you want to use with this TLS profile</p> <ul style="list-style-type: none"><li>• Default: compatability</li><li>• Values: TLSv1   SSLv3   compatibility</li></ul>
<b>cert-status-check</b>	<p>Enable or disable OCSP in conjunction with an existing TLS profile.</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>
<b>cert-status-profile-list</b>	<p>Select an object from the <code>cert-status-profile</code> parameter. In order to enable this parameter, this list must not be empty. If multiple <code>cert-status-profile</code> objects are assigned to <code>cert-status-profile-list</code>, the Oracle Communications Session Border Controller will use a hunt method beginning with the first object on the list.</p> <ul style="list-style-type: none"><li>• Values: Any valid certificate status profile from <code>cert-status-profile</code> parameter</li></ul>
<b>ignore-dead-responder</b>	<p>Allows local certificate based authentication by the Oracle Communications Session Border Controller in the event of unreachable OCSRs</p> <ul style="list-style-type: none"><li>• Default: disabled</li><li>• Values: enabled   disabled</li></ul>

### Path

`tls-profile` is an element under the security path. The full path from the topmost prompt is: **configure terminal > security > tls-profile**

### Release

First appearance: 4.1 / Most recent update S-C6.2.0

### RTC Status

Supported



## translation-rules

The translation-rules element creates unique sets of translation rules to apply to calling and called party numbers. The fields within this element specify the type of translation to be performed, the addition for deletion to be made, and where in the address that change should be made.

### Parameters

<b>id</b>	Enter the identifier or name for this translation rule. This field is required.
<b>type</b>	<p>Select the address translation type to be performed</p> <ul style="list-style-type: none"> <li>• Default: none</li> <li>• Values: <ul style="list-style-type: none"> <li>• add—Adds a character or string of characters to the address</li> <li>• delete—Deletes a character or string of characters from the address</li> <li>• replace—Replaces a character or string of characters within the address</li> <li>• none—Translation rule is disabled</li> </ul> </li> </ul>
<b>add-string</b>	<p>Enter the string to be added during address translation to the original address. The value in this field should always be a real value; i.e., this field should not be populated with at-signs (@) or dollar-signs (\$).</p> <p>When the type is set to replace, this field is used in conjunction with the delete-string value. The value specified in the delete-string field is deleted and the value specified in the add-string field is inserted. If no value is specified in the delete-string field and the type field is set to replace, then nothing will be inserted into the address.</p> <ul style="list-style-type: none"> <li>• Default: blank string</li> </ul>
<b>add-index</b>	<p>Enter the location in the original address where the string specified in the add-string value is inserted. This value is the character position starting at 0 to insert the add-string value.</p> <p>When a dollar-sign (\$) is used for the add-index, it appends the add-string to the end of the number. This is represented by “999999999” when a show is performed.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>
<b>delete-string</b>	<p>Enter the string to be deleted from the original address during address translation. Unspecified characters are denoted by the at-sign symbol (@).</p> <p>When the type is set to replace, this value is used in conjunction with the add-string value. The value specified in the delete-string field is deleted and the value specified in the add-string field is inserted. If no value is specified in the delete-string parameter and the type field is set to replace, then nothing will be inserted into the address.</p> <ul style="list-style-type: none"> <li>• Default: blank string</li> </ul>
<b>delete-index</b>	<p>Enter the location in the address to delete the string specified in the delete-string field. This value of this field is the character position starting at 0 to insert the add-string value. This is not used when only deleting a given string.</p> <ul style="list-style-type: none"> <li>• Default: 0</li> <li>• Values: Min: 0 / Max: 999999999</li> </ul>

### Path

**translation-rules** is an element under the session-router path. The full path from the topmost CLI prompt is: **configure terminal > session-router > translation-rules**.

### Release

First appearance: 1.3

### RTC Status

Supported



**Note:** You can delete unspecified characters from an original address by using the at-sign (@). This is a multiple instance configuration element.

## trap-receiver

---

The trap-receiver element defines the NMSs to which the Oracle Communications Session Border Controller sends SNMP traps for event reporting.

### Parameters

<b>ip-address</b>	Enter the IP address and port for an NMS. If no port value is specified, the Oracle Communications Session Border Controller uses a default port of 162. This required field must follow the IP Address format.
<b>filter-level</b>	Set the filter level for the NMS identified within this trap-receiver element <ul style="list-style-type: none"><li>• Default: critical</li><li>• Values:<ul style="list-style-type: none"><li>• All—All alarms, syslogs, and other traps will be trapped out. That is, the corresponding NMS will receive informational, warning, and error events.</li><li>• Minor—All syslogs generated with a severity level greater than or equal to MINOR and all alarms generated with a severity level greater than or equal to MINOR will be trapped out</li><li>• Major—All syslogs generated with a severity level greater than or equal to MAJOR and all alarms generated with a severity level greater than or equal to MAJOR will be trapped out</li><li>• Critical—Syslogs generated with a severity level greater than or equal to CRITICAL and all alarms generated with a severity level greater than or equal to CRITICAL will be trapped out</li></ul></li></ul>
<b>community-name</b>	Enter the name of the community to which a particular NMS belongs. This required entry must follow the Name format.
<b>user-list</b>	This parameter is configured with the name of one or more snmp-user-entry configuration element user-names for authorizing access to SNMPv3 functionality.

### Path

**trap-receiver** is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > trap-receiver**.

### Release

First appearance: 1.0 / Most recent update: 1.3

### RTC Status

Unsupported



**Note:** This is a multiple instance configuration element.

---

## tunnel-orig-params

---

The tunnel-orig-params configuration element defines a single remote IKEv2 peer.

### Parameters

- |                    |  |
|--------------------|--|
| <b>name</b>        | Enter the name of this instance of the <b>tunnel-orig-params</b> configuration element <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: A valid configuration element name, that is unique within the <b>tunnel-orig-params</b> namespace</li></ul> |
| <b>remote-addr</b> | Enter the IPv4 address of a remote IKEv2 peer <ul style="list-style-type: none"><li>• Default: None</li><li>• Values: Any valid IPv4 address</li></ul>   |
| <b>retry-limit</b> | Set the number of times IKEv2 tries to initiate the tunnel. If this value is exceeded, IKEv2 abandons the initiation attempt and issues an SNMP trap. <ul style="list-style-type: none"><li>• Default: 3</li><li>• Values: Min: 1   Max: 5</li></ul>                       |
| <b>retry-time</b>  | Set the interval (in seconds) between initiation attempts. <ul style="list-style-type: none"><li>• Default: 10 seconds</li><li>• Values: Min: 5   Max: 60</li></ul>  |

### Path

**tunnel-orig-params** is a subelement under the ike element. The full path from the topmost ACLI prompt is: **configure-terminal > security > ike > tunnel-orig-params**

### Release

First appearance: S-C6.2.0

### RTC Status

Supported



**Note:** This is a multiple instance configuration element.



# Glossary

