Oracle® Communications Session Border Controller

Maintenance and Troubleshooting Guide

Release S-Cz8.4.0

F31119-16

October 2022

Oracle Communications Session Border Controller Maintenance and Troubleshooting Guide, Release S-Cz8.4.0

F31119-16

Contents

About This Guide

Revision History

1 Logs

About This Guide

The Oracle Communications Session Border ControllerMaintenance and Troubleshooting Guide provides the information you need for understanding and troubleshooting the operation of the Oracle Communications Session Border Controller

Note:

The Upgrades chapter that has appeared in previous documentation releases has been moved to the Oracle Communications Session Border Controller Installation Guide.

Documentation Set

The following table describes the documentation set for this release.

Document Name	Document Description
Acme Packet 3900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3900.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
Acme Packet 6350 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6350.
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 Service Provider Session Border Controller (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 SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.

Document Name	Document Description
MIB Reference Guide	Contains information about Management Information Base (MIBs), Oracle Communication'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 the SBC's accounting support, including details about RADIUS and Diameter accounting.
HDR Resource Guide	Contains information about the SBC's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the SBC's support for its Administrative Security license.
SBC Family Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the SBC family of products.
Installation and Platform Preparation Guide	Contains information about upgrading system images and any pre-boot system provisioning.
Call Traffic Monitoring Guide	Contains information about traffic monitoring and packet traces as collected on the system. This guide also includes WebGUI configuration used for the SIP Monitor and Trace application.
FIPS Compliance Guide	Contains conceptual and procedural information for configuration using the tools and protocols required to manage call traffic on the SBC.
HMR Resource Guide	Contains information about configuring and using Header Manipulation Rules to manage service traffic.
TSCF SDK Guide	Contains information about the client-side SDK that facilitates the creation of secure tunnels between a client application and the TSCF of the SBC.
REST API Guide	Contains information about the supported REST APIs and how to use the REST API interface.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select 1.
   - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."

4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Revision History

The following table lists the dates and description of the revisions to this document.

Date	Description
June 2020	• Initial Release • Under View Keys, changed "show running-config ssh-key" examples to "show security <key-type> [brief | detail[" examples.
August 2020	• Removes account-config error about missing password or public-key from verify-config table.
September 2020	• Corrections to SSH key management examples. • Updates for 8.4.0p2.
October 2020	• Adds cipher to SRTP Crypto In/Out list • minidump is removed.
November 2020	• Remove ssh-password command. • Adds local-account reference.
March 2021	• Updates "Configuration Migration" to warn about copying configurations between different platforms with different capabilities.
April 2021	• Adds behavior wherein the system sets storage to read-only to prevent corruption.
June 2021	• Removes regenerate-config command. • Adds new verify-config warnings. • Removes deprecated H323 show commands.
August 2021	• Corrects log file size and rotation description.
December 2021	• Adds new SIP method counter statistics at SC-z8.4.0p8.
February 2022	• Adds missing **verify-config** error on local-policy configuration. • Adds a message for **notify berpd force** command in Log Message Graphical Display on the SBC section, applicable for S-Cz8.4.0p7 and above. • Removes Old File Remover section as this feature is no longer supported. • Adds note about virtual platform in show interfaces command in viewing network interface statistics section.
March 2022	• Adds detail about **show sessions** command in Viewing Active Audio and Video Call Statistics section. • Adds verify-config warning to Access Control.

Date	Description
June 2022	• Specifies protocol support for the advanced logging feature. • Adds Audit Log section from Admin Security Guide.
July 2022	• Adds example of 'show security tls stats'.
October 2022	• Adds explanation of ACLs not allocated message for the show acl command. • Updates the Dynamically Changing Log Level topic with tasks you cannot set with the log-level command.

1 Logs

Introduction

This chapter describes the logs available with the Oracle Communications Session Border Controller and explains how to access and view them. It also explains the relationship between logs and system events.

About Logs

Logs are a critical component of system management and security. You can use the information in logs to assist real-time debugging and management, and to track potential security breaches or other nonstandard activities on the system. The Oracle Communications Session Border Controller supports the following three types of logs:

- acmelog (syslog): contains both generic messages (not task oriented) as well as system log messages
- process logs: contain process flow from tasks
- transaction logs: contain raw messages about protocol transactions sent and received by the Oracle Communications Session Border Controller.

The Oracle Communications Session Border Controller supports SYSLOG, a protocol that lets the Oracle Communications Session Border Controller log significant system information to a remote server.

Logging Events

The Oracle Communications Session Border Controller can log events that occur on different system components, such as those associated with a protocol transaction. If logging is enabled on the system, monitored events are evaluated against the logging level set for the component that sent the event. Events that meet the logging level are written to a log file.

SNMP traps are sent when an Oracle Communications Session Border Controller generates a system log (acmelog) message and the following conditions are present:

- SNMP is enabled.
  Set the system configuration's SNMP functionality to enabled. Using the ACLI, set the **snmp-enabled** field for **system-config** to enabled.
- Sending system log (acmelog) notifications to an NMS using SNMP is enabled.
  Set the system configuration's log functionality to enabled. Using the ACLI, set the **enable-snmp-syslog-notify** field for **system-config** to enabled.
- Severity level that identifies at which severity level syslog notifications are sent is configured. For example:
  Set the system configuration's log functionality to one of the possible severity levels. Using the ACLI, set the **snmp-syslog-level** field for **system-config** to enabled.

See the *ACLI Configuration Guide* for details about configuring the Oracle Communications Session Border Controller and the *ACLI Reference Guide* for details about using the ACLI.

Event Categories

This section describes the events and the different event categories the Oracle Communications Session Border Controller can generate.

About Events

Events are the circumstances that generate one or more of the following:

- alarm
- entry in a log file
- SNMP trap

The following table lists the three categories used to define these events.

Event Category	Description
Informational	Represents non-critical conditions. For example, a configuration element has changed.
Warning	Indicates pending failures or unexpected events. For example, you typed the wrong password at the console three consecutive times.
Error	Indicates that a serious condition has occurred. For example, an internal temperature reading exceeds the recommendation.

These broad categories generally consist of the facility that generated them, along with an indication of the severity of the message. This information helps filter the more important and time-sensitive notifications from the informative messages.

Types of Events

The Oracle Communications Session Border Controller can generate the following types of events.

- process log events
- system log events
- protocol trace elements

Process Log Events

Events are logged to the process log flow from tasks and are specific to a single process running on the Oracle Communications Session Border Controller. By default they are placed into individual files associated with each process with the following name format:

```
log.<taskname>
```

> **Note:**
>
> Process logs serve as a debugging tool. When set to debug level, the quantity of events generated can become overwhelming for the Oracle Communications Session Border Controller. It should only be used by Oracle personnel, or with their assistance. It is not recommended for use on production systems.

When you configure the system, you set the default system-wide process log level and each task logs according to this setting. You can override this log level for specific tasks when configuring other elements. For example, when you configure the media manager you can set the ALGD and MBCD log levels to different severity levels.

System Log Events

System log events are a subset of the collection of all process log events. Every software process writes messages to a file called acmelog, if the severity of the event meets or exceeds the configured log level threshold. There is one system log for the whole Oracle Communications Session Border Controller (filename: `acmelog`).

System log events are also referred to as acmelog events and are analogous to a traditional syslog event. The acmelog file is typically viewed as an aggregation of notable alarms and errors from all software processes.

The Oracle Communications Session Border Controller supports logging using SYSLOG, which is an industry-standard protocol that lets a device send event notification messages across IP networks to event message collectors - also known as syslog servers. Messages are usually sent using UDP port 514.

The Oracle Communications Session Border Controller can send information to a remote SYSLOG server. You configure the server and globally set the severity level at which the Oracle Communications Session Border Controller logs events when you configure the system.

Protocol Trace Events

Protocol trace events are the events associated with a protocol transaction. They are enabled on a per-process basis using the notify command, resulting in transactional events being placed into transaction logs, such as `sipmsg.log`.

These events are helpful for troubleshooting sessions, but they are also the highest volume events the Oracle Communications Session Border Controller produces and can only be enabled for short times.

Event Granularity

You can set the reporting level for events placed into the logs by using the following methods:

- Setting the system-wide severity level (at or above which events are logged) by configuring the system’s process log level. This setting is persistent across boots.
  You set the system-wide severity level by configuring the log severity level threshold when performing the system configuration.
- Configuring individual parameters for different elements that control specific process logs. For example, you can configure the mbcd log level for the media manager. These settings are persistent across boots.

For example, to configure the process log level for monitoring all H.323 activity on the Oracle Communications Session Border Controller, you configure the log level to INFO when configuring H.323 signaling.

- Using ACLI log-level command to dynamically specify the log level for a specific task (or all tasks using the keyword all). You can specify finer granularity by including specific subtypes within the process. These settings are not persistent across boots.
- Using the ACLI or Acme Control Protocol (ACP) notify command. For example, **notify mbcd debug**. Such settings are not persistent across boots.

Event Severity

There are eight severity levels ranging from lowest severity, Debug, to the highest, Emergency.

syslog Numerical Code	syslog Severity	Oracle Log Enumeration
0	Emergency (system is unusable)	EMERGENCY (0)
1	Alert (action must be taken immediately)	CRITICAL (1)
2	Critical (critical conditions)	MAJOR (2)
3	Error (error conditions)	MINOR (3)
4	Warning (warning conditions)	WARNING (4)
5	Notice (normal but significant condition)	NOTICE (5)
6	Informational (informational messages)	INFO (6)
7	Debug (debug level messages)	TRACE (7) DEBUG (8) DETAIL (9)

SNMP Traps

The Oracle Communications Session Border Controller supports several standard SNMP traps (cold start, link up/down) and proprietary traps used to notify SNMP managers of specific events:

- apSysMgmtGroupTrap – used for different events. The trap must be parsed by a management tool to extract the specific event details.
- specific uniquely identified traps – used for specific Oracle Communications Session Border Controller events. These traps correspond exactly to the events that show up in acmelog.
  The unique traps are only generated if the **system-config**, **enable-snmp-monitor-traps** ACLI parameter is enabled:
- apSysLogGeneratedTrap – used as a catch-all for system log (syslog) events.

See the *MIB Reference Guide* for more details about traps.

Alarms

The most serious events noted by the Oracle Communications Session Border Controller are categorized as alarms. They appear in the alarm table, which is displayed in the ACLI using the command **display-alarms**. The ACLI also supports clearing alarms displayed in that table. Alarms are not sent off-box explicitly, however, at least one of the following mechanisms is usually triggered when an alarm occurs:

- A dry contact port on the back of the chassis that may be used to control a remote alarm panel.
- An SNMP trap may be generated
- A syslog event may be generated

See the *MIB Reference Guide* for details about alarms.

Process Log Events

Process log events can be sent to a log server by configuring the system to include the destination server’s IP address and port number. For example, using the ACLI you configure the following system parameters:

- **process-log-server**
- **process-log-port**
  The process log port can be any port from 1025 to 65535. It is most commonly configured as port 2500.

The Oracle Communications Session Border Controller stops logging events to RAM memory and instead sends them to the configured remote server over UDP. Because of the added overhead of sending log messages using UDP datagrams versus writing to the RAM drive, message content decreases – even at the same configured log levels.

System Log Events

System log events can be sent to one or more syslog servers using the traditional UNIX syslog mechanism as described in RFC 3164. Users can configure one or more syslog servers to which the Oracle Communications Session Border Controller will send generated syslog events by setting the following syslog parameters in the system configuration:

- **address**
- **port**
- **facility**

If the port is left empty, the default value is UDP port 514 (the well-known syslog port).

Traps

Traps are defined to be sent to a SNMP Manager using the following configuration parameters:

- **system-config**, **trap-receiver**, **ip-address**
- **system-config**, **trap-receiver**, **filter-level**
- **system-config**, **trap-receiver**, **community-name**

Alarms

Alarms can be sent off the box using the dry contact port in the rear of the chassis.

Working with Logs

This section explains how to work with logs.

Writing to Logs

You configure the Oracle Communications Session Border Controller to indicate you want messages written to logs. The system writes to these log files until they become their maximum size, and rotates them to the maximum number of files. Thresholds for size and number of files depend on whether the system is running on ramdrive or hard disk:

- If on hard-disk with a formatted system partition, the limits are 5MB per file and 25 files.
- If not using a hard-disk, the limits are 1MB per file and 12 files.

> **Note:**
>
> These sizes are fixed, based on system software parameters, and are not user configurable.

When a file reaches its maximum size, the system closes it and renames it with .1 appended to the original file name. For example, `sipmsg.log` becomes`sipmsg.log.1`. The system proceeds with writing new logs to the original filename, `sipmsg.log`, until it reaches the size limit again. At this point, the system closes `sipmsg.log` again and:

- Renames the existing `sipmsg.log.1` file to `sipmsg.log.2`.
- Renames `sipmsg.log` to `sipmsg.log.1` again.

This continues until you have the maximum number of files associated with the log. When the system reaches this limit, it discards the oldest file.

Manually Rotating Logs

You can manually rotate (close) the log file by using the following command:

```
notify * rotate-logs
```

The * can be any of the following Oracle Communications Session Border Controller tasks:

- all
- sipd
- sysmand
- berpd
- lemd
- mbcd

- h323d
- algd
- radd

You can manually rotate the log files when you are trying to isolate a specific problem. Working with Oracle Technical Support, you could close all current log files (or just for a specific task) and then run a test of your problem. You can then easily identify the log files to review.

Working with Logs Example

For example, to troubleshoot issues you suspect are media-related using the ACLI, you can look at the logs for the middlebox control daemon (MBCD).

1. Instruct the Oracle Communications Session Border Controller to write all media management transactions to mbcd.log by entering the following command:

   ```
   notify mbcd log
   ```

2. Make some test calls.
3. Set message writing to the log off by entering the following command:

   ```
   notify mbcd nolog
   ```

4. SFTP the log off the Oracle Communications Session Border Controller to view it.

> **Note:**
>
> Oracle recommends only setting the log level to DEBUG on non-production systems.

Displaying List of Log Files

You can display the list of log files by using the **display-logfiles** ACLI command. Every task writes to its own process log (`log.taskname`) and protocol trace logs (transaction logs) are enabled or disabled creating a task.log file. The log files are stored in the `/opt/logs` directory on the Oracle Communications Session Border Controller.

For example:

```
ORACLE# display-logfiles
Listing Directory /opt/logs:
drwxrwxrwx  1 0       0              512 Jul  4 18:02 ./
drwxrwxrwx  1 0       0              512 Jul  6 09:50 ../
-rwxrwxrwx  1 0       0           820707 Jul  6 11:55 acmelog
-rwxrwxrwx  1 0       0             3447 Jul  2 17:40 log.sysmand
-rwxrwxrwx  1 0       0             3724 Jul  2 15:59 log.bootstrap
-rwxrwxrwx  1 0       0              132 Jul  2 17:40 log.brokerd
-rwxrwxrwx  1 0       0              740 Jul  2 17:40 log.npsoft
-rwxrwxrwx  1 0       0              369 Jul  2 15:59 log.berpd
-rwxrwxrwx  1 0       0            26660 Jul  6 11:46 log.cliWorker
-rwxrwxrwx  1 0       0             3316 Jul  2 17:40 log.lemd
```

```
-rwxrwxrwx  1 0       0              852 Jul  2 17:40 log.atcpd
-rwxrwxrwx  1 0       0              733 Jul  2 17:40 log.atcpApp
-rwxrwxrwx  1 0       0             2877 Jul  2 17:40 log.mbcd
-rwxrwxrwx  1 0       0              757 Jul  2 17:40 log.lid
-rwxrwxrwx  1 0       0             1151 Jul  2 17:40 log.algd
-rwxrwxrwx  1 0       0              741 Jul  2 17:40 log.radd
-rwxrwxrwx  1 0       0              728 Jul  2 17:40 log.pusher
-rwxrwxrwx  1 0       0             1448 Jul  2 17:40 log.ebmd
-rwxrwxrwx  1 0       0           671322 Jul  6 11:55 log.sipd
-rwxrwxrwx  1 0       0           681011 Jul  6 11:55 log.h323d
-rwxrwxrwx  1 0       0             1169 Jul  2 15:59 log.h248d
-rwxrwxrwx  1 0       0            18294 Jul  2 17:40 log.snmpd
-rwxrwxrwx  1 0       0             1078 Jul  2 17:40 snmpd.log
-rwxrwxrwx  1 0       0              190 Jul  2 15:59 log.acliSSH0
-rwxrwxrwx  1 0       0              191 Jul  2 15:59 log.acliSSH1
-rwxrwxrwx  1 0       0              192 Jul  2 15:59 log.acliSSH2
-rwxrwxrwx  1 0       0              192 Jul  2 15:59 log.acliSSH3
-rwxrwxrwx  1 0       0              192 Jul  2 15:59 log.acliSSH4
-rwxrwxrwx  1 0       0             3043 Jul  6 11:38 log.acliConsole
-rwxrwxrwx  1 0       0             2655 Jul  2 21:07 log.acliTelnet0
-rwxrwxrwx  1 0       0              195 Jul  2 15:59 log.acliTelnet1
-rwxrwxrwx  1 0       0              195 Jul  2 15:59 log.acliTelnet2
-rwxrwxrwx  1 0       0              195 Jul  2 15:59 log.acliTelnet3
-rwxrwxrwx  1 0       0              195 Jul  2 15:59 log.acliTelnet4
-rwxrwxrwx  1 0       0          1000005 Jul  4 18:01 acmelog.1
```

Viewing Logs

You can send the log off the Oracle Communications Session Border Controller through wancom0 or retrieve it using SFTP in order to view it.

> **Note:**
>
> The view-log command currently listed in the ACLI is not supported.

Viewing a Specific Logfile

You can view a specific logfile saved on the Oracle Communications Session Border Controller using the **show logfile <filename>** command. For example:

```
ORACLE# show logfile nginx_error.log
2020/03/27 14:33:07 [notice] 4063#0: signal process started
2020/03/27 14:33:07 [notice] 2680#0: using the "epoll" event method
2020/03/27 14:33:07 [notice] 2680#0: start worker processes
2020/03/27 14:33:07 [notice] 2680#0: start worker process 4064
2020/03/27 14:33:07 [notice] 2680#0: signal 17 (SIGCHLD) received from
2681
2020/03/27 14:33:07 [notice] 2680#0: worker process 2681 exited with
code 0
2020/03/27 14:33:07 [notice] 2680#0: signal 29 (SIGIO) received
2020/03/30 09:05:45 [notice] 2678#0: using the "epoll" event method
```

Dynamically Changing Log Level

You can change the log level dynamically by using the ACLI **log-level** command in the Superuser mode. The **log-level** command sets the log level for a specific task. The following table lists the sub-commands within the **log-level** command.

log-level sub-commands	Description
task_name	Displays the log level according to the task or process name. (You do not have to enter @<system_name>.) To view all tasks, enter **all**. To list available task or process names, enter the show processes command.
log_level	Identifies the log level, either by name or by number.
log_type_list	Lets you list log types by number or by name in parentheses (()).

> **Note:**
>
> You cannot set the following tasks with the log-level command. You must go to system-config and use system-log-level and process-log-level.
>
> - authqueue
> - fragHandler
> - heap
> - healthCheckd
> - SSHD
> - tLFMiBd

To change the log level:

1. Access the ACLI in Superuser mode.
2. Type **log-level** followed by a space and one of the log level sub-commands. You can change the log level for the following:
   - system-wide

     ```
     log-level system <log level>
     ```

     For example:

     ```
     log-level system DEBUG
     ```

   - log level at which a specific task/process sends to the **acmelog** file

     ```
     log level <task name> <log level>
     ```

For example:

```
log-level sipd debug
```

3. Press **Enter**.

Requesting Log Level Data

You are able to view the current log level of processes/tasks that are running on the Oracle Communications Session Border Controller. You can do this through both the ACLI and ACP:

- ACLI—The **loglevel** subcommand has been added to the ACLI **show** command
- ACP—A new ACP method called GET_LOG_LEVEL has been added

ACLI show loglevel Command

The ACLI **show loglevel** command allows you to request log level data from the ACLI console. It takes one mandatory and two optional parameters. The mandatory parameter specifies the name of the Oracle Communications Session Border Controller task for which you are requesting information; one of the optional parameters specifies the type of log level for which you want information and the other allows you to select whether you want to view a verbose display of the task.

You can enter all as the value for either of these parameters to view information for all system tasks or all log levels. If you do not enter a parameter, the system returns an error message and provides a list of valid parameters. You can also wildcard these parameters by entering an asterisk (*), but entering partial wildcards does not work.

To view log level information for a single system task:

- Type **show loglevel**, a Space, and then the name of the system task for which you want to see log level information. Then press Enter.

```
ORACLE# show loglevel sipd
Log Levels for process sipd:
loglevel=DEBUG
```

To view log level information for a single system task with a specific log level:

- Type **show loglevel**, a Space, the name of the system task for which you want to see log level information, and the name of the log. Then press Enter.

```
ORACLE# show loglevel sipd GENERAL
Log Levels for process sipd:
        GENERAL=NOTICE
ORACLE# show loglevel sipd MINOR
Log Levels for process sipd:
        MINOR=NOTICE
ORACLE# show loglevel sipd DNS
Log Levels for process sipd:
        DNS=NOTICE
```

To view verbose log level information for a single system task:

- Type **show loglevel**, a Space, the name of the system task for which you want to see log level information, and **verbose**. Then press Enter.

```
ORACLE# show loglevel sipd verbose
Log Levels for process sipd:
GENERAL=DEBUG
EMERGENCY=DEBUG
CRITICAL=DEBUG
MAJOR=DEBUG
MINOR=DEBUG
WARNING=DEBUG
PROC=DEBUG
IPC=DEBUG
SERVICE=DEBUG
EVENT=DEBUG
MESSAGE=DEBUG
TEST=DEBUG
TRIP=DEBUG
SIP=DEBUG
MBCP=DEBUG
FLOW=DEBUG
MEDIA=DEBUG
SESSION=DEBUG
TRANS=DEBUG
TIMER=DEBUG
ALG=DEBUG
NPSOFT=DEBUG
ARP=DEBUG
SNMP=DEBUG
ANDD=DEBUG
XNTP=DEBUG
REDUNDANCY=DEBUG
SIPNAT=DEBUG
H323=DEBUG
ERROR=DEBUG
CONFIG=DEBUG
DNS=DEBUG
H248=DEBUG
BAND=DEBUG
ALI=DEBUG
SS8GI=DEBUG
COPS=DEBUG
ATCP=DEBUG
ATCPAPP=DEBUG
CLF=DEBUG
```

ACP

The new ACP command GET_LOG_LEVEL provides log level information. This ACP request requires authentication, and it must be sent to port 3000.

Because ACP message length is limited, obtaining log level information for multiple system tasks is a multi-step procedure. For a known, single task, the procedure does not require as many steps.

To obtain log level information, an ACP message with the GET_LOG_LEVEL method is sent, and its message body contains information about the log levels being requested. This message body takes the following format: process:type.

An asterisk (*) can be used instead of the process name or log type to wildcard that value. If the process name is replaced with a *, then the first message response is a list of processes; this allows the querying management software to query the level of each process directly.

Wildcarding Task Name and Log Type

When you want to wildcard the process name and log type, the ACP requests looks like this:

```
GET_LOG_LEVEL sysmand@acmesystem ACME/1.0
Object-ID:0
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
Content-Type: text/plain
CSeq: 3 GET_LOG_LEVEL
Authorization: Digest
    username="user",
    realm="intern1",
    nonce=6eccad8d8a4d7473d3725bc54bdf4a59,
    uri="sysmand@acmesystem",
    response=5a700cf8c15a0902cb8e75a02cc99f33,
    algorithm="md5-sess",
    cnonce=4c11d5,
    qop="auth",
    nc=00000002
Content-Length: 3
*:*
```

The response would return the actual list of tasks running on the system. Depending on what tasks are running, it would look like this:

```
ACME/1.0 200 Everything is OK
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
CSeq: 3 GET_LOG_LEVEL
Content-Type: text/xml
Content-Length: 253
<ProcessList>
    <process name='sysmand'/>
    <process name='brokerd'/>
    <process name='lemd'/>
    <process name='atcpd'/>
    <process name='atcpApp'/>
    <process name='mbcd'/>
    <process name='lid'/>
    <process name='radd'/>
    <process name='pusher'/>
    <process name='ebmd'/>
    <process name='sipd'/>
    <process name='snmpd'/>
</ProcessList>
```

Specific Task with Wildcard Log Level

The NMS can use the list from the above example to query each task using additional GET_LOG_LEVEL messages by specifying the name of the tasks and the levels.

The message would look like this:

```
GET_LOG_LEVEL sysmand@acmesystem ACME/1.0
Object-ID: 0
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
Content-Type: text/plain
CSeq: 3 GET_LOG_LEVEL
Authorization: Digest
    username="user",
    realm="intern1",
    nonce=5dd735490c78a0146ca06d50f47c0a50,
    uri="sysmand@acmesystem",
    response=129b882a3ee110db86565932819d017b,
    algorithm="md5-sess",
    cnonce=859dcc,
    qop="auth",
    nc=00000002
Content-Length: 9
sysmand:*
```

To which the response would look like this:

```
ACME/1.0 200 Everything is OK
Object-ID: 0
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
CSeq: 3 GET_LOG_LEVEL
Content-Type: text/xml
Content-Length: 544
<sysmand
        GENERAL=DEBUG
        EMERGENCY=DEBUG
        CRITICAL=DEBUG
        MAJOR=DEBUG
        MINOR=DEBUG
        WARNING=DEBUG
        PROC=DEBUG
        IPC=DEBUG
        SERVICE=DEBUG
        EVENT=DEBUG
        MESSAGE=DEBUG
        TEST=DEBUG
        TRIP=DEBUG
        SIP=DEBUG
        MBCP=DEBUG
        FLOW=DEBUG
        MEDIA=DEBUG
        SESSION=DEBUG
        TRANS=DEBUG
        TIMER=DEBUG
        ALG=DEBUG
        NPSOFT=DEBUG
        ARP=DEBUG
        SNMP=DEBUG
        ANDD=DEBUG
        XNTP=DEBUG
        REDUNDANCY=DEBUG
        SIPNAT=DEBUG
        H323=DEBUG
        ERROR=DEBUG
        CONFIG=DEBUG
        DNS=DEBUG
        H248=DEBUG
        BAND=DEBUG
        ALI=DEBUG
        SS8GI=DEBUG
        COPS=DEBUG
        ATCP=DEBUG
        ATCPAPP=DEBUG
        CLF=DEBUG
/>
```

Specific Task and Log Level Type

To request a specific type of log level for a specific process, specify the process name and type specified in the body of the request:

```
GET_LOG_LEVEL sysmand@acmesystem ACME/1.0
Object-ID: 0
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
Content-Type: text/plain
CSeq: 3 GET_LOG_LEVEL
Authorization: Digest
     username="user",
     realm="intern1",
     nonce=d11774ac886bf2293217b1ed894444e3,
     uri="sysmand@acmesystem",
     response=b2eb7cae77e544685ce2883b90189e78,
     algorithm="md5-sess",
     cnonce=e0ad7,
     qop="auth",
     nc=00000002
Content-Length: 14
```

```
sysmand:CONFIG
```

The response to this request would look like this:

```
ACME/1.0 200 Everything is OK
Object-ID: 0
Trans-ID: 0
From: user@10.0.0.1
To: sd@10.0.0.2
CSeq: 3 GET_LOG_LEVEL
Content-Type: text/xml
Content-Length: 26
<sysmand
     CONFIG=DEBUG
/>
```

Log Files For Offline Analysis and Defect Reporting

Current releases of the Oracle Communications Session Border Controller collect by default a large amount of information which is saved in various system logs and available after a system crash. This information is useful when debugging and submitting defects to Oracle.

The following table lists and describes the Application crash log files and includes a description and the output location of the crash log file when an HDD/SDD is present in the system or not.

file name	description	Output path on HDD/SSD	Output path with flash drive only (no HDD/SSD)
`crashlogs.gz`	compressed subset of `/opt/logs/*`	`/opt/logs`	`/code/crash`
`dump.dpwd-datapath`	Trace files for datapath watchdog initiated crash	`/opt/crash`	`/code/crash`
`trace.<timestamp>.<task-name>`	Crashing thread stack trace (text)	`/opt/crash / code/crash`	`/code/crash`
`core.<timestamp>.<task-name>.<process ID>`	Full process core dump	`/opt/crash`	not saved

The following table lists and describes the Kernel crash log files and includes a description and the output path of the crash log file when an HDD/SDD is present in the system or not.

file name	description	Output path on HDD/SSD	Output path with flash drive only (no HDD/SSD)
`vmcore.<datestamp>.dmesg`	Copy of console logs from crashed kernel	`/opt/crash`	`/code/crash`
`vmcore.<datestamp>.dump.*`	Copy of the crashed kernel system memory	`/opt/crash`	not saved

The following table lists and describes the operating system log files and includes a description and hte output path of the crash log file when an HDD/SDD is present in the system or not.

file name	description	Output path on HDD/SSD	Output path with flash drive only (no HDD/SSD)
`kernel_lgob.log`	Copied from `/opt/logs/kernel.log` at reboot	`/opt/crash`	`/code/crash`
`dmesg_lgob.log`	Copied from `/opt/logs/dmesg.log` at reboot	`/opt/crash`	`/code/crash`

For systems without SSDs or HDDs installed, persistent files are written to flash in `/code/crash`. For systems with formatted SSDs or HDDs, the core and dump files are written to `/opt/crash` on HDD. Regardless of whether an HDD/SSD is present, check both flash and HDD locations on all platforms for all available files.

lgob files are overwritten at each reboot and crashlogs are overwritten at each crash. This data must be collected immediately after system recovers from an outage. Because trace and core files are deleted automatically at reboot to free disk space, they should be moved off-box at the earliest opportunity.

For systems with HDDs/SSDs, some minidump and trace files will be saved to `/code/crash` and some will be saved to `/opt/crash`. Please check both locations.

In the event of an uncontrolled reboot (i.e. hardware reset, power cycle, watchdog trigger) the lgobs corresponding to the crash timestamp will be missing, so absence of this file on `/code/crash` is an indication of an uncontrolled reboot event.

> **Note:**
>
> Large core files (core, vmcore dumps) may be split into multiple files (.aa, .ab etc), and on some platforms these files are also compressed. Be advised to look for .gz versions of the core files.

Audit Log

The audit log records creation, modification, and deletion of all user-accessible configuration elements, access to critical security data such as public keys. For each logged event it provides associated user-id, date, time, event type, and success/failure data for each event. As a result, the log supports after the fact investigation of loss or impropriety, and appropriate management response. Only admin-level users have audit log access. These users can retrieve, read, copy, and upload the audit log. The original log cannot be deleted or edited by any operator action.

The audit log is transferred to a previously configured SFTP server or servers when one of three specified conditions is satisfied.

- A configurable amount of time has elapsed since the last transfer.

- The size of the audit log (measured in Megabytes) has reached a configured threshold.
- The size of the audit log has reached a configured percentage of the allocated storage space.

Transfer is targeted to a designated directory of each SFTP target server.

Audit logs can be viewed after they transfer.

Audit Log Syntax

The audit log file is stored on the target SFTP server or servers with a filename that takes the format:

```
<hostname>-audit<timestamp>
```

Where:

- <hostname> is the name of the host to which the log gets sent.
- <timestamp> is a 12-digit string that takes the format YYYYMMDDHHMM.

```
myhost-audit-200903051630
```

Names an audit log file transferred to an SFTP server named 'myhost' on March 5, 2009 at 4:30 PM.

Audit Log Format

Audit log events are comma-separated-values (CSV) lists that have the following format:

```
{TimeStamp,user-
id@address:port,Category,EventType,Result,Resource,Details,...}

{2009-0305 15:19:27,sftp-
elvis@192.2.0.10:22,security,login,success,authentication,,.}
```

TimeStamp specifies the time that the event was written to the log

Category takes the values: security | configuration | system

EventType takes the values: create | modify | delete | login | logout | data-access | save-config | reboot | acquire-config

Result takes the values: successful | unsuccessful

Resource identifies the configuration element accessed by the user

Details (which is displayed only in verbose mode) provides fine-grained configuration details

- If EventType = create, details is “New = element added”
- If EventType = modify, details is “Previous = oldValue New = newValue”
- If EventType = delete, details is “Element = deleted element”
- If EventType = data-access, details is “Element = accessed element”

The following lists and describes the actions that generate audit log events.

- Login—Every login attempt

  ```
  2009-03-05 17:31:14,sftp-elvis@192.2.0.10:22,security,login,
  success,authentication,,.
  ```

- Logout—Every logout attempt

  ```
  2009-03-05 18:44:03,sftp-
  elvis@192.2.0.10:22,security,logout,success,authentication,,.
  ```

- save-config—Every save-config CLI command

  ```
  2009-03-05 15:45:29,acliConsole-admin@console,configuration,
  save-config,success,CfgVersion=111,,.
  ```

- activate-config—Every activate-config CLI command

  ```
  2009-03-05 15:45:36,acliConsole-
  admin@console,configuration,activate-
  config,success,RunVersion=111,,.
  ```

- DataAccess
  - a) attempt to retrieve data using SFTP
  - b) attempt to export using ssh-key
  - c) attempt to display security info using show security
  - d) attempt to kill a session using kill

  ```
  2009-03-05 15:25:59,sftp-elvis@192.2.0.10:22,security,data-access,
  success,code/auditaudit200903051518,,.
  ```

- Create
  - a) any action that creates a configuration property
  - b) any action that creates a file

    ```
    2009-03-05 15:45:01,acliConsole-
    admin@console,configuration,create,
    success,public-key,
    Element=
    <?xml version=’1.0’ standalone=’yes’?>
    <sshPubKeyRecord
      name=’dummy’
      comment=’’
      keyType=’2’
      encrType=’1’
      keySize=’1024’
      pubKey=’’
      privKey=’’
      fingerPrint=’’
      fingerPrintRaw=’’
      lastModifiedBy=’acmin@console’
    ```

```
  lastModifiedDate=’2009-03-05 15:45:01>
</sshPubKeyRecord
```

- Modify
  - a) any action that modifies a configuration property

```
2009-03-05 15:48:01,acliConsole-admin@console,configuration,modify,
success,public-key,
Previous=
<?xml version=’1.0’ standalone=’yes’?>
<sshPubKeyRecord
  name=’dummy’
  comment=’’
  keyType=’2’
  encrType=’1’
  keySize=’1024’
  pubKey=’’
  privKey=’’
  fingerPrint=’’
  fingerPrintRaw=’’
  lastModifiedBy=’acmin@console’
  lastModifiedDate=’2009-03-05 15:45:01>
</sshPubKeyRecord

New=
<?xml version=’1.0’ standalone=’yes’?>
<sshPubKeyRecord
  name=’dummy’
  comment=’’
  keyType=’2’
  encrType=’2’
  keySize=’1024’
  pubKey=’’
  privKey=’’
  fingerPrint=’’
  fingerPrintRaw=’’
  lastModifiedBy=’acmin@console’
  lastModifiedDate=’2009-03-05 15:48:01>
</sshPubKeyRecord
```

- Delete
  - a) any action that deletes a configuration property
  - b) any action that deletes a file

```
2009-03-05 15:51:39,acliConsole-admin@console,configuration,delete,
success,public-key,
Element=
<?xml version=’1.0’ standalone=’yes’?>
<sshPubKeyRecord
  name=’dummy’
  comment=’’
  keyType=’2’
  encrType=’2’
```

```
          keySize='1024'
          pubKey=''
          privKey=''
          fingerPrint=''
          fingerPrintRaw=''
          lastModifiedBy='acmin@console'
          lastModifiedDate='2009-03-05 15:51:39>
        </sshPubKeyRecord
```

Audit Log Format for HTTP Headers

When **audit-http** is enabled, the SBC logs HTTP requests so administrators can audit which IP address requested what resource.

When logging HTTP headers with **detail-level** set to brief, the log contains one line per request, and each line contains the following information separated by a comma:

- Timestamp
- Source IP and port
- The literal string "http"
- The destination IP and port
- The HTTP request line
- The HTTP return status
- The HTTP Referer
- The HTTP User-Agent
- All headers (only if **detail-level** is set to verbose)

Audit Log Samples

Examples of audit log entries may be related to authentication, file access, configuration changes, or http headers.

Authentication

An example of a successful login from the console:

```
2020-03-27 12:59:57,console-
admin@console,security,login,success,authentication,,.
```

An example of a successful login with SSH:

```
2020-03-27 13:25:04,ssh-admin@10.0.0.1,security,login,success,keyboard-
interactive/pam for admin from 10.0.0.1 port 52687 ssh2,,.
```

An example of a failed login with SSH:

```
2020-03-27 10:34:28,ssh-admin@10.0.0.1,security,login,failure,keyboard-
interactive/pam for admin from 10.0.0.1 port 51368 ssh2,,.
```

An example of a successful login with SFTP:

```
2020-03-27 13:13:30,sftp-admin@10.0.0.1,security,data access,success,".",,.
```

File Access

An example of successfully accessing a file over SFTP:

```
2020-03-27 13:56:34,sftp-admin@10.0.0.1,security,create,success,"/opt/logs/
syslog" flags READ mode 0666,,.
```

An example of failing to access a file over SFTP because of the file permissions:

```
2020-03-27 13:57:26,sftp-admin@10.0.0.1,security,create,failure,"/code/ssh/
ssh_host_dsa_key.pub" flags READ mode 0666,,.
```

An example of successfully deleting a file over SFTP:

```
2020-03-27 13:34:25,sftp-admin@10.0.0.1,security,delete,success,name "/code/
audit/ADMINSEC-audit202003261134",,.
```

An example of failing to delete a file over SFTP because of the file permissions:

```
2020-03-27 14:23:00,sftp-admin@10.0.0.1,security,delete,failure,name "/boot/
bootloader",,.
```

An example of failing to delete a directory:

```
2020-03-27 14:09:51,sftp-admin@10.0.0.1,security,delete,failure,name "/
code/ssh/",,.
```

Configuration Changes

An example of security information:

```
2020-03-27 13:59:32,console-admin@127.0.0.1:0,configuration,data
access,failure,show security ssh-pub-key,,.
```

An example of saving the configuration:

```
2020-03-27 14:33:02,console-admin@127.0.0.1:0,configuration,save-
config,success,CfgVersion=12,,.
```

An example of activating the configuration:

```
2020-03-27 14:33:07,console-admin@127.0.0.1:0,configuration,activate-
config,success,RunVersion=12,,.
```

HTTP Headers

When **audit-http** is enabled and **detail-level** is set to brief, the following is an example log from a Web GUI HTTP request:

```
2019-11-22 12:11:44,10.0.0.1:49026,http,10.0.0.3:81,"POST /egi/
acmePacketWebService HTTP/1.1",200,"http://10.0.0.3:81/","Mozilla/5.0
(X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0",
```

And the following is an example log from a REST request:

```
2019-11-22 14:47:29,10.0.0.4:59296,http,10.0.0.3:8443,"POST /rest/v1.0/
auth/token HTTP/1.1",200,,"curl/7.29.0",
```

Configure the Audit Log

The single instance **audit-logging** configuration element enables, sizes, and locates the audit log within the local file structure. It also specifies the conditions that trigger transfer of the log to one or more SFTP servers.

1. Access the audit-logging configuration element.

   ```
   ORACLE# configure terminal
   ORACLE(configure)# security
   ORACLE(security)# admin-security
   ORACLE(admin-security)# audit-logging
   ORACLE(audit-logging)#
   ```

2. **state**—Enables or disables audit logging.

   Set to enabled to use audit logging. Retain the default value (disabled) to disable the log.

3. **detail-level**—Specifies the level of detail associated with audit log entries.

   Retain the default value (brief) to write succinct log entries; use verbose to generate more detailed entries.

4. **audit-trail**—Enables logging every command that is successfully processed by the SBC.

   Use enabled to enable the audit logging all successful commands. Retain the default value (disabled) to log only relevant information. The value of **state** must be set to enabled for **audit-trail** to work.

   > **Note:**
   >
   > When enabled, the SBC logs only commands that the SBC is able to process. For example, if a command is entered incorrectly, it will not be logged.

5. **audit-http**—Enables logging HTTP requests.

6. **audit-record-output**—Indicates how the SBC logs audit records.

- syslog—The SBC logs audit records over syslog.
- file—The SBC logs audit records to a file. This is the default value.
- both—The SBC logs audit records over both syslog and to a file.

7. **file-transfer-time**—Specifies the maximum interval (in hours) between audit-log transfers to a previously-configured SFTP server or servers.

   Allowable values are integers within the range 0 through 65535.

   The value 0 disables time-based-transfer of the audit log. Consequently, upload to an SFTP server is triggered only by exceeding the percentage-based or absolute-size-based thresholds established by the **percentage-full** and **max-file-size** properties, or by manual SFTP file transfer performed by a properly privileged admin-level user.

   Retain the default value (720 hours/30 days), or provide an alternate value to trigger time-based-transfer. With time-based-transfer enabled, automatic upload of the audit file to an SFTP server or servers is triggered when the interval decrements to 0. At that time the audit log is transferred, an alarm alerting the recipient to the transfer is generated, and the timer re-sets to its configured value. Assuming the file transfer succeeds, the audit log is deleted. If the file transfer fails, the audit log is retained until it exceeds the value specified by **max-storage-space**.

   > **Note:**
   >
   > The file-transfer-time interval is reset to its configured value with any audit log transfer regardless of cause.

8. **max-storage-space**—Specifies the maximum disk space (measured in Megabytes) available for audit log storage.

   Allowable values are integers within the range 1 through 32.

   Allocate space for the audit log by retaining the default value, or by selecting a new value from within the allowable range.

9. **percentage-full**—Specifies a file size threshold (expressed as a percentage of max-storage-space) that triggers audit file transfer to a previously-configured SFTP server or servers.

   Allowable values are integers within the range 0 through 99.

   The value 0 disables percentage-based-transfer of the audit log. Consequently, upload to an SFTP server is triggered only by exceeding the time-based and absolute-size-based thresholds established by the **file-transfer-time** and **max-file-size properties**, or by manual SFTP file transfer performed by a properly privileged admin-level user.

   Retain the default value (75 percent), or provide an alternate value to trigger percentage-based-transfer. With percentage-based-transfer enabled, automatic upload of the audit file to an SFTP server or servers is triggered when audit log size exceeds the value **max-storage-spac**e x (**percentage-full**/100). At that time the audit log is transferred, and an alarm alerting the recipient to the transfer is generated. Assuming the file transfer succeeds, the audit log is deleted. If the file transfer fails, the audit log is retained until it exceeds the value specified by **max-storage-space.**

10. **max-file-size**—Specifies a file size threshold (expressed as an absolute file size measured in Megabytes) that triggers audit file transfer to a previously-configured SFTP server or servers.

    Allowable values are integers within the range 0 through 10.

The value 0 disables absolute-size-based-transfer of the audit log. Consequently, upload to an SFTP server is triggered only by exceeding the time-based and percentage-based thresholds established by the **file-transfer-time** and **percentage-full** properties, or by manual SFTP file transfer performed by a properly privileged admin-level user.

Retain the default value (5 Megabytes), or provide an alternate value to trigger absolute-size-based-transfer. With absolute-size-based-transfer enabled, automatic upload of the audit file to an SFTP server or servers is triggered when audit log size exceeds the value **max-file-size**. At that time the audit log is transferred and an alarm alerting the recipient to the transfer is generated. Assuming the file transfer succeeds, the audit log is deleted. If the file transfer fails, the audit log is retained until it exceeds the value specified by **max-storage-space.**

11. **storage-path**—Specifies the directory that houses the audit log.

    Retain the default value (/code/audit), or identify another local directory.

12. Type **done** to save your configuration.

Example 1-1   Example Configuration

A sample audit log configuration appears below:

```
ORACLE(audit-logging)# state enabled
ORACLE(audit-logging)# file-transfer-time 1
ORACLE(audit-logging)# percentage-full 0
ORACLE(audit-logging)# max-file-size 0
ORACLE(audit-logging)# audit-http enabled
```

This configuration allocates 32MB (the default value) for audit logging HTTP headers in brief mode. Audit log transfer to a configured SFTP server or servers occurs on an hourly schedule; other transfer triggers are disabled.

Configure SFTP Audit Log Transfer

Prior to using SFTP-enabled file transfer, import a copy of the SFTP server's host key as a known host on the SBC. Then export the SBC's public key and add it to the authorized_keys file of the SFTP server.

1. Add the SBC's public key to the authorized_keys file on the SFTP server.
    a. SSH to the SBC.
    b. Run the `show security public-host-key rsa` command.

    ```
    ADMINSEC# show security public-host-key rsa
    OpenSSH rsa public-key: 2048 SHA256:pslVj6X0Qau3AAKRpBr0T7WrT199/
    MEcmnbLClVl4BU root@ADMINSEC (RSA)

    ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDjKIoiW4r7g+laRMK/
    Ib+SjKSMZWeBYLJaVj/
    VAX+UtNxfw63MOmsgIVzMc29YAap1YQ6EL18BT6i9nYhRO/
    RNGCBI3GoQEB1R8fEQxuWcVENzcE5LZewVi/rQt4r/
    pNMiOKx0ftAXiy9RKIIoNdu3+CcjJqDp4noq/
    KM9puN0P+08GMCLKZKq4u8o1umIzc4zeaqDxpXNLRSLuEh2qMlxXvu5R8JFhW1Afr
    9q6BUwJvROg2c8q3B+V3Pmo+mFIZZXLdjqytU2jZHpA0hrY7SUz5gjMRqxEuae1Vm
    ```

```
LRBs+aosb5u6G7l1iO1rOUWrjqfcyAJV4KRJTsi+NfM3vIKGH root@ADMINSEC
ADMINSEC#
```

c. Copy the last line of output that begins with `ssh-rsa`.

d. SSH to the SFTP server.

e. Append the copied public key to the `.ssh/authorized_keys` file.

```
echo '[paste public key here]' >> .ssh/authorized_keys
```

For example:

```
echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDjKIoiW4r7g+laRMK/
Ib+SjKSMZWeBYLJaVj/VAX+UtNxfw63MOmsgIVzMc29YAap1YQ6EL18BT6i9nYhRO/
RNGCBI3GoQEB1R8fEQxuWcVENzcE5LZewVi/rQt4r/
pNMiOKx0ftAXiy9RKIIoNdu3+CcjJqDp4noq/
KM9puN0P+08GMCLKZKq4u8o1umIzc4zeaqDxpXNLRSLuEh2qMlxXvu5R8JFhW1Afr9q6BU
wJvROg2c8q3B+V3Pmo+mFIZZXLdjqytU2jZHpA0hrY7SUz5gjMRqxEuae1VmLRBs+aosb5
u6G7l1iO1rOUWrjqfcyAJV4KRJTsi+NfM3vIKGH root@ADMINSEC' >> .ssh/
authorized_keys
```

f. Set the correct permissions for the authorized_keys file.

```
chmod 600 .ssh/authorized_keys
```

2. Import the SFTP server's host key into the SBC.

a. SSH to the SFTP server.

b. Print the host key in RFC 4716 format.

```
[user@logserver ~]$ ssh-keygen -ef /etc/ssh/ssh_host_rsa_key.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted by user@logserver from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJXglzdoOfZ39TiU7jhywifpOpBKoDhzgbPGQTw0
qIgcI3T8J6n0jHwgZIlRtD0e5y6YBzDksvwKttObk8SSiTVB1PzMNxF0dWVoZl1mqE4xPX
j3zEVw1hBISW57PRbSulHwaiHN7ieYT/qJwZZc6nrQ56JH9Lcjej1JX96QCX6iHplfhJO4
oHWs5mDybHNnSvU64F1AMBRjLbZrclvvt8vofIzraGIUzxVse5NMYl8bbdId/4UBci1fON
rgvGKRhnmqFbV227PsOfPLy80p7IpL3RIhMzejbyhEK+e0KW7a+T6mAoq8UdGe3F9i1g49
PwNPS1/LONj0cjvcKUgQxN
---- END SSH2 PUBLIC KEY ----
[user@logserver ~]$
```

c. SSH to the SBC.

d. Import the SFTP server's host key as a known host.

```
ADMINSEC# ssh-key known-host import logserver
IMPORTANT:
Please paste SSH public key in the format defined in RFC 4716.
Terminate the key with ";" to exit.......
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted by user@logserver from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJXglzdoOfZ39TiU7jhywifpOpBKoDhzgbPGQTw0
qIgcI3T8J6n0jHwgZIlRtD0e5y6YBzDksvwKttObk8SSiTVB1PzMNxF0dWVoZl1mqE4xPX
```

```
j3zEVw1hBISW57PRbSulHwaiHN7ieYT/
qJwZZc6nrQ56JH9Lcjej1JX96QCX6iHplfhJO4
oHWs5mDybHNnSvU64F1AMBRjLbZrclvvt8vofIzraGIUzxVse5NMYl8bbdId/
4UBci1fON
rgvGKRhnmqFbV227PsOfPLy80p7IpL3RIhMzejbyhEK+e0KW7a+T6mAoq8UdGe3F9
i1g49
PwNPS1/LONj0cjvcKUgQxN
---- END SSH2 PUBLIC KEY ----
SSH public key imported successfully....
WARNING: Configuration changed, run "save-config" command to
save it
and run "activate-config" to activate the changes
ADMINSEC#
```

e. Save and activate the configuration.

Configuring SFTP Servers

The multi-instance **push-receiver** configuration element identifies remote SFTP servers that receive audit log transfers.

1. Access the audit-logging configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# security
ORACLE(security)# admin-security
ORACLE(admin-security)# audit-logging
ORACLE(audit-logging)# push-receiver
ORACLE(push-receiver)#
```

2. Select the **push-receiver** object to edit.

```
ORACLE(push-receiver)# select
<server>:<port>:
1: 192.168.54.55:22 server = 192.168.54.55, port = 22

selection: 1
ORACLE(push-receiver)#
```

3. **server**—In conjunction with **port**, specifies an SFTP server IP address:port pair.

   Provide the IP address of an SFTP server that receives transferred audit logs. For example,

```
ORACLE(push-receiver)# server 10.0.2.100
ORACLE(push-receiver)#
```

4. **port**—In conjunction with **server**, specifies an SFTP server IP address:port pair.

   Provide the port number monitored by server for incoming audit log transfers. This parameter defaults to port 22, the well-known Secure Shell (SSH) port. Retain the default value, or identify the monitored port with an integer within the range from 1 through 65535.

```
ORACLE(push-receiver)# port 22
ORACLE(push-receiver)#
```

5. **remote-path**—Specifies the absolute file path to the remote directory that stores transferred audit log files.

```
ORACLE(push-receiver)# remote-path /home/acme/auditLogs
ORACLE(push-receiver)#
```

6. **filename-prefix**—Specifies an optional prefix that can be appended to the audit log file name when transferred to an SFTP server.

```
ORACLE(push-receiver)# filename-prefix sbc01-
ORACLE(push-receiver)#
```

7. **auth-type**—Specifies the authentication type required by this remote SFTP server.

   Two authentication types are supported: simple password or public keys.

   Refer to SSH Configuration for more information on SSH authentication.

   Enter either **password** (the default) or **public-key**. For example:

```
ORACLE(push-receiver)# auth-type public-key
ORACLE(push-receiver)#
```

8. **username**—Specifies the username used to authenticate to this SFTP server.

```
ORACLE(push-receiver)# username acme
ORACLE(push-receiver)#
```

9. **password**—Specifies the password used in conjunction with **username** to authenticate the SSH client to this SFTP server.

   Required when **auth-type** is **password**, and otherwise ignored.

```
ORACLE(push-receiver)# password =yetAnotherPW!
ORACLE(push-receiver)#
```

10. **public-key**—Leave blank, regardless of authentication type.
11. Type **done** to save your configuration.

Audit Log Alarms and Traps

Three audit log alarms and traps are provided to report significant or anomalous audit log activity.

The ALARM_AUDIT_LOG_FULL trap/alarm is generated in response to (1) the expiration of the file-transfer-time interval, (2) the crossing of the percentage-full threshold, or (3) the crossing of the max-file-size threshold. This trap/alarm is cleared when storage apace becomes available, generally upon successful transfer of the audit log to a remote SFTP server or servers.

The ALARM_ADMIN_AUDIT_PUSH_FAIL trap/alarm is generated in response to failure to transfer the audit log to a designated SFTP server. This trap/alarm is cleared when a subsequent transfer to the same recipient succeeds.

The ALARM_AUDIT_WRITE_FAILED trap/alarm is generated in response to failure to record an auditable event in the audit log. This trap/alarm is cleared when a subsequent write succeeds.

Configure Login Timeouts

Use the **ssh-config** configuration element to set the SSH and TCP timeout values.

1. Access the **ssh-config** element.

   ```
   ORACLE# configure terminal
   ORACLE(configure)# security
   ORACLE(security)# admin-security
   ORACLE(admin-security)# ssh-config
   ORACLE(ssh-config)#
   ```

2. **rekey-interval**—Set the time in minutes after which the SBC rekeys an SSH or SFTP session.
   - Min: 60
   - Max: 600
   - Default: 60
3. **rekey-byte-count**—Set the number of bytes transmitted, in powers of 2, before rekeying an SSH or SFTP session.

   For example, entering a value of 24 sets this parameter to 2^24 (16777216) bytes.
   - Min: 20
   - Max: 31
   - Default: 31
4. **proto-neg-time**—Set the time in seconds to complete the SSH protocol negotiation, establishing the secure connection.
   - Min: 30
   - Max: 60
   - Default: 60
5. **keep-alive-enable**—Enable the TCP keepalive timer. Valid Values are:
   - enabled | disabled
   - Default: enabled
6. **keep-alive-idle-timer**—Set the interval in seconds between the last data packet sent and the first keepalive probe.
   - Min: 15
   - Max: 1800
   - Default: 15

7. **keep-alive-interval**—Set the interval in seconds between two successful keepalive transmissions.
   - Min: 15
   - Max: 120
   - Default: 15
8. **keepalive-retries**—Set the number of retransmission attempts before the SBC declares the remote end is unavailable.
   - Min: 2
   - Max: 10
   - Default: 2
9. Type done to save the configuration.

Log Files

This section contains information about the log files and what each contains. The log files are stored in the `/opt/logs` directory on the Oracle Communications Session Border Controller.

log.sysmand

This log contains information about the system manager task. This task is currently responsible for writing the system log (acmelog), dispatching commands to other application tasks, and starting the application-level code.

log.bootstrap

This log records information about the boot process as the system becomes operational.

log.berpd

This log contains process logs for the berpd task or the redundancy health task. This file is primarily used for storing health messages and events and for determining whether a switchover is required.

log.brokerd

This log contains information about platform-level tasks. For example, when the ARP manager wants to log information in a place other than the console, it sends a message to log-brokerd. This is also true of the various host tasks related to communicating with the network processors and/or the CAM.

This log also contains messages from the IP fragmenter, which currently takes part in the SIP NAT process. brokerd forwards these messages through sysmand to the acmelog (the overall system log). Thus, log-brokerd contains a subset of the logs that acmelog contains.

log.lemd

This log refers to the local element manager (or local database server) processes. Information in log.lemd pertains to remote retrievals of and writing of configuration data.

log.mbcd

This log contains information pertaining to the application flow manager, such as the creation, updating, and removal of media NAT entries.

miboco.log

Tasks use MIBOCO protocol processing to communicate with the mbcd task. This log can be used to determine whether the mbcd has returned any error messages or other type of messages. It is possible that sipmsg.log and algd.log contain MIBOCO messages. However, the miboco.log is used infrequently because log.sipd and log.algd also report return codes from the mbcd.

log.radd

This log is used for the accounting daemon for RADIUS. It serves as a RADIUS client to the outside world. However, it also serves as a place to concentrate RADIUS records from various signaling protocol tasks running on the SBC. Its logs reflect the latter function.

log.h323d

This log contains information pertaining to H.323 tasks.

log.sipd

This log contains information pertaining to the SIP processing task. The log contains information about how the system’s SIP proxy is processing messages.

sipmsg.log

This protocol trace log contains information about SIP messages that have been received, NAT’d, and sent by the SIP proxy. MIBOCO messages sent and received by the sipd process are also contained in this log.

log.acli

This log contains information pertaining to ACLI processing.

log.acliConsole

This log contains information about ACLI console functions.

log.SSH0-4

This log contains information about SSH processes. You can have one log for each instance.

log.tCliWorker

This log contains information about tCliWoker processes.

log.atcpApp

This log contains information about the asychronous Transport Control Protocol (TCP).

log.atcpd

This log contains information about the asychronous TCP daemon.

log.audit

This log contains information about any audits performed on the system.

log.auditpusher

This log contains information about the audits that were pushed on the system.

log.authd

This log contains information about authentication used on the system.

log.certd

This log contains information about certificate records used on the system.

log.qos

This log contains information about quality of service (qos) for call sessions.

log.lid

This log contains information about the lawful intercept daemon.

log.iked

This log contains information about the secure Internet Key Exchange (IKE) daemon.

log.bcm

This log contains information about the Business Call Management (BCM) logger used with the system to process call detail records (CDR).

log.lrtd

This log contains information about the local routing table (LRT) daemon.

log.ebmd

This log contains information about Common Open Policy Service (COPS) and Call Admission Contol (CAC) on the system. It is information about the External Bandwidth Manager (Radius/Diameter).

syslog

The term syslog refers to the protocol used for the network logging of system and network events. syslog facilitates the transmission of event notification messages across networks. Given that, the syslog protocol can be used to allow remote log access.

The syslog message functionality lets you configure more than one syslog server, and set the facility marker value used in the messages sent to that syslog server independently. All syslog messages are sent to all configured syslog servers.

> **Note:**
>
> Oracle recommends configuring no more than eight syslog servers. As the number of configured syslog servers to which the system sends logs increases, the system performance might decrease.

Configured syslog servers are keyed (identified uniquely) by IPv4 or IPv6 address and port combinations. The Oracle Communications Session Border Controller is able to send logs to multiple syslog servers on the same host.

Process Logs

Each individual process running on the system has its own process log and a server where the system sends those logs.

HA Switchover Log

The switchover log provides historical information about the role of a High Availability (HA) Oracle Communications Session Border Controller in an HA Oracle Communications Session Border Controller pair. This log lists the last 20 switchovers on an HA SBC. The switchover log is not persistent across reboot(s). The switchover log message appears in the information provided by the show health command, and it also appears immediately on the terminal screen when a switchover takes place.

Log Message Graphical Display on the SBC

The switchover log message displayed on the High Availability (HA) SBC that has moved from the Standby to the BecomingActive state (has assumed the active role) indicates the date and time that the switchover took place. It also indicates from which peer the active role was assumed and why. The peer displaying this message took the active role because a health score fell below a set threshold, because a timeout occurred, or because it was forced by a system administrator via the ACLI.

Refer to the following example of a switchover log for an HA SBC whose health score fell below a configured threshold.

```
ORACLE# Mar 28 16:36:38.226: Standby to BecomingActive, active peer ORACLE2
has unacceptable health (50)
ORACLE#
```

Refer to the following example of a switchover log for an HA SBC that has timed out.

```
ORACLE# Mar 29 13:42:12.124: Standby to BecomingActive, active peer ORACLE2
has timed out
ORACLE#
```

The peer relinquishing the active role (becoming the standby system in the HA SBC pair) also displays the date and time that the switchover took place. The peer also indicates that it has moved from the Active to the RelinquishingActive state.

Refer to the following example of a switchover log for an HA SBC that is relinquishing its active role.

```
ORACLE2# Mar 28 16:38:08.321: Active to RelinquishingActive
ORACLE2#
```

When you force a switch-over manually by running the **notify berpd force** command, the new active system displays a message - Standby to BecomingActive peer relinquishing control we're the healthiest.

Refer to the following example of a switchover log for an HA SBC that displays this message.

```
ORACLE2# Dec 17 16:38:08.321: Standby to BecomingActive peer relinquishing
control we're the healthiest
ORACLE2#
```

Advanced Logging

Advanced Logging allows targeted logging by overriding log levels, so that only a specific SIP request and its related messages get logged. The system matches criteria that you configure to determine which requests to log. The system also logs all messages related to the request, such as any responses, in-dialog messages, media, timers, and so on. Advanced Logging supports multiple matching criteria for incoming requests and rate limiting. Advanced log files are smaller than debug files because the system logs only the specified number of matches in the specified period of time. Since the files are smaller, Advanced Logging uses fewer system resources than debug logging. To make searching easier, the system labels each log.

You can deploy advanced logging by way of configuration. You configure the **sip-advanced-logging** element and **adv-log-conditions** subelement on the session router according to the logging targets.

You can control when logging occurs by enabling or disabling individual advanced logging objects using the **state** parameter. This allows you to retain advanced logging configurations on the system and simply start and stop logging against those objects when needed.

Protocol specific support includes:

- TCP—Protocol fully supported
- TLS—Protocol not supported
- UDP—Protocol not fully supported. The UDP protocol does not require port specification throughout transmission. Advanced logging uses port number to correlate traffic. As a result, advanced logging can capture UDP traffic but cannot correlate traffic when port numbers are not set and consistent.

By executing the **notify sipd conditional-log disable** command, you can disable the ability to trigger all of the configured sip-advanced-logging objects.

```
ORACLE#notify sipd conditional-log-disable
```

Any active sip-advance-logging instances continue to log because the command only disables the ability to trigger new instances. You can restore the ability to trigger new instances for all sip-advance-logging objects with the **notify sipd conditional-log-enable** command .

The system provides the following options for configuring the scope of advanced logging.

- Request-only. Logs only the matched message.
- Transaction. Logs only the request and the response.
- Session. Logs the matched message and anything else related to the session.
- Session and Media. Logs the matched message, anything related to the session, and media.

The system provides the following options for configuring the advanced logging criteria.

- Received Session-Agent, by IP address or hostname.
- Request Types, such as INVITE vs. SUBSCRIBE.
- Received Realm Name.
- Request URI. User and host. Limited to 2 condition entries, when using both types.
- To header. User and host. Limited to 2 condition entries, when using both types.
- From header. User and host. Limited to 2 condition entries, when using both types.
- Call-id. Matches the Call-id header.
- Rate Limiting. By specified number of matched requests over a specified period of time.
- Scope of Logging. Options include Request Only, Transaction, All Relating to Session, All Relating to Session and Media.

When you enable a **sip-adv-logging** object, applicable events trigger this logging by the Sipd (SIP signaling) process, resulting in log messages from it. The Sipd process also propagates advanced logging to the Atcpd (TCP connections), Ebmd (bandwidth managment), Lrtd (local routing table), Radd (accounting), and Middle Box Control Daemon (MBCD) processes, resulting in additional log messages from them. In addition, Mbcd events, including asynchronous 2833, flowguard timer and latching events, can propagate conditional logging to Sipd, resulting in log messages from Sipd.

Behavior During High Availability Synchronization

When the system is synchronizing a thread at the same time that thread is performing advanced logging, this logging continues on the standby while the replication takes place. This logging on the standby, however, stops after replication is complete, with the exception of sip-sessions and media flows.

Threads associated with sip-sessions and flows continue to store their logging state after replication. The logging state is stored in either the session or flow. When a switchover happens while a thread is processing one of these sessions or flows, the system finds the stored logging state and continues logging even though the event was triggered on the other node of the HA pair.

Configuring Advanced Logging

From Configure mode, define `sip-advanced-logging` and `advanced-log-condition`. The criteria that you configure remaps the message logging and modifies the system configuration. You must save and activate the changes to the configuration.
When configuring multiple `sip-advanced-logging` configurations, note the following:

- The system evaluates each configuration individually in an **OR** relationship.
- The system evaluates all conditions and they must all match in an **AND** relationship.

1. Access the **ifc-profile** configuration element.

   ```
   ORACLE# configure terminal
   ORACLE(configure)# session-router
   ORACLE(session-router)# sip-advanced-logging
   ORACLE(sip-advanced-logging)#
   ```

2. Configure the following parameters.
   - Name. Name to display on the log message for this set of criteria.
   - State. Activates or deactivates this advanced logging object.
   - Level. Type one: zero, none, emergency, critical, major, minor, warning, notice, info, trace, debug, or detail.
   - Scope. Type one: request-only, transaction, session, or session-and-media.
   - Matches-per-window. Type a number between 1 and 999999999 for how many matches to log per window of time.
   - Window-size. Type a number between 1 and 999999999 seconds for the length of time the logging window is open.
   - Type conditions.
     The system displays the adv-log-condition subelement.
3. Select the **sip-advanced-logging > conditions** object to edit, or create a new one.

   ```
   ORACLE(sip-advanced-logging)# adv-log-condition
   ORACLE(adv-log-condition)# select
   <name>:
   1:  name=condition1

   ORACLE(adv-log-condition)#
   ```

4. From the adv-log-condition prompt, configure the following:
    - Match-type. Type one or more of the following sip objects with either the "and" or the "or" operator between objects: request-type, recv-agent, recv-realm, request-uri-user, request-uri-host, to-header-user, to-header-host, from-header-user, from-header-host, or call-id.
    - Match-value. Type the incoming message text string that you want to match.

      For example, to match "To-header-user" to the value 1234@<companyname>.com, type "to-header-user" for Match type and type " 1234" for Match value.

    > **Note:**
    >
    > The match-value parameter does not support regex expressions.

5. Type **done** (twice) to retain your sub-element and element configuration.
6. Exit, save, and activate.

Disabling Miboco Logging

If your Oracle Communications Session Border Controller configuration is especially large—such that you deem it necessary to preserve as many system resources as possible during activation—you might want to disable Miboco logging. Miboco is a body of control messages allowing certain internal Oracle Communications Session Border Controller process to communicate with one another, and these message constitute part of the call trace logging. By turning Miboco call trace logging off, you provide additional safeguard around system resource and possibly prevent the adverse consequences that might arise from overuse.

Disabling Miboco Call Trace Logging

To disable Miboco call trace logging:

1. Access the **sip-config** configuration element.

    ```
    ORACLE# configure terminal
    ORACLE(configure)# session-router
    ORACLE(session-router)# sip-config
    ORACLE(sip-config)#
    ```

2. Select the **sip-config** object to edit.

    ```
    ORACLE(sip-config)# select


    ORACLE(sip-config)#
    ```

3. **options—Follow your entry with this value:**

- +disable-miboco-logging

  ```
  ORACLE(sip-config)# options +disable-miboco-logging
  ```

  You can enable Miboco logging again by removing the option:

  ```
  ORACLE(sip-config)# options -disable-miboco-logging
  ```

4. Type **done** to save your configuration.

2

Fault Management

Overview

This chapter explains how to access Oracle Communications Session Border Controller fault management statistics to locate faults, determine the cause, and make corrections. Fault management involves the following:

- Continuous monitoring of statistics
- Viewing alarms that warn of system problems

Accessing Fault Management Data

You can access fault management information using the following ACLI commands:

- show commands to view statistics
- display-alarms command to view alarms

You can access all show commands at the user level.

About Traps

This section defines the standard and proprietary traps supported by the system. A trap is initiated by tasks (such as the notify task) to report that an event has happened on the system. SNMP traps enable an SNMP agent to notify the NMS of significant events by way of an unsolicited SNMP message.

The system uses SNMPv2c. These notification definitions are used to send standard traps and Oracle’s own enterprise traps.

Traps are sent according to the criteria established in the following:

- IETF RFC 1907 *Management Information Base for Version 2 of the Simple Network Management Protocol*
- IETF RFC 2233 *The Interfaces Group MIB using SMIv2*
- Or the appropriate enterprise MIB (for example the Acme Packet syslog MIB or the Acme Packet System Management MIB).

For additional information about the traps and MIBS supported by the system, see the *Oracle Communications Session Border Controller MIB Reference Guide*.

Standard Traps

The following table identifies the standard traps that the system supports.

Trap Name	Description
linkUp	The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the down state to the up state. The ifOperStatus value indicates the other state.
linkDown	The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the up state to the down state. The ifOperStatus value indicates the other state.
coldStart	The SNMPv2 agent is reinitializing itself and its configuration may have been altered. This trap is not associated with a system alarm.
authenticationFailure	The SNMPv2 agent received a protocol message that was not properly authenticated. If the snmp-enabled and enable-snmp-auth-traps fields in the ACLI's system-config element are set to enabled a snmpEnableAuthenTraps object is generated. This trap is not associated with a system alarm.

Enterprise Traps

The following table identifies the proprietary traps that the system supports.

Trap Name	Description
apSyslogMessageGenerated	Generated by a syslog event. For example, this trap is generated if a switchover alarm occurs (for High Availability (HA) system peers only), or if an HA system peer times out or goes out-of-service. You enable or disable the sending of syslog messages by using the ACLI.
apSysMgmtGroupTrap	Generated when a significant threshold for a system resource use or health score is exceeded. For example, if Network Address Translation (NAT) table usage, Address Resolution Protocol (ARP) table usage, memory usage, or Central Processing Unit (CPU) usage reaches 90% or greater of its capacity, the apSysMgmtGroupTrap is generated. If the health score (for HA peers only) falls below 60, the apSysMgmtGroupTrap is generated.
apLicenseApproachingCapacityNotification	Generated when the total number of active sessions on the system (across all protocols) is within 98 - 100% of the licensed capacity.
apLicenseNotApproachingCapacityNotification	Generated when the total number of active sessions on the system (across all protocols) has gone to or below 90% of its licensed capacity (but no sooner than 15 seconds after the original alarm was triggered).
apEnvMonI2CFailNotification	Generated when the Inter-IC bus (I2C) state changes from normal (1) to not functioning (7).
apEnvMonStatusChangeNotification	Generated when any entry of any environment monitor table changes in the state of a device being monitored. To receive this trap, you need to set the system config's enable- env- monitor- table value to enabled.
apSwCfgActivateNotification	Generated when an activate-config command is issued and the configuration has been changed at running time.
apSysMgmtPowerTrap	Generated if a power supply is powered down, powered up, inserted/present or removed/not present.

Trap Name	Description
apSysMgmtTempTrap	Generated if the temperature falls below the monitoring level.
apSysMgmtFanTrap	Generated if a fan unit speed falls below the monitoring level.
apSysMgmtTaskSuspendTrap	Generated if a critical task running on the system enters a suspended state.
apSysMgmtRedundancyTrap	Generated if a state change occurs on either the primary or secondary system in a redundant (HA) pair.
apSysMgmtMediaPortsTrap	Generated if port allocation fails at a percentage higher or equal to the system’s default threshold rate. Trap is generated when there are at least 5 failures within a 30 second window and a failure rate of 5% or more.
apSysMgmtMediaBandwidthTrap	Generated if bandwidth allocation fails at a percentage higher or equal to the system’s default threshold rate. Trap is generated when there are at least 5 failures within a 30 second window and a failure rate of 5% or more.
apSysMgmtMediaOutofMemory	Generated if the media process cannot allocate memory.
apSysMgmtMediaUnknownRealm	Generated if the media process cannot find an associated realm for the media flow.
apSysMgmtRadiusDownTrap	Generated if all or some configured RADIUS accounting servers have timed out from a RADIUS server.
apSysMgmtGatewayUnreachableTrap	Generated if the gateway specified becomes unreachable by the system.
apSysMgmtH323InitFailTrap	Generated if the H.323 stack has failed to initialize properly and has been terminated.
apSysMgmtHardwareErrorTrap	Provides a text string indicating the type of hardware error that has occurred. If the message text exceeds 255 bytes, the message is truncated to 255 bytes.
apSysMgmtDOSTrap	Generated when the IP address and the realm ID is denied of service.
apSysMgmtCfgSaveFailTrap	Generated if an error occurs while the system is trying to save the configuration to memory.
apSysMgmtSystemStateTrap	Generated when the Oracle Communications Session Border Controller is instructed to change the system-state or the transition from becoming offline to online occurs. This trap contains one field called APSysMgmtSystemState, and that field has three values: • online(0) • becoming-offline(1) • offline(2)
apSysMgmtAuthenticationFailedTrap	Generated when an attempt to login to the Oracle Communications Session Border Controller fails for any reason. The trap sent to all configured trap receivers includes the following information: • administration and access level (SSH, user, enable) • connection type

Transcoding Capacity Traps

The Oracle Communications Session Border Controller sends the apSysMgmtGroupTrap as transcoding capacity nears its limit. This trap is sent and cleared for three conditions:

- Total DSP usage exceeds 95%
- Total AMR sessions exceed 95% of licensed capacity
- Total AMR-WB sessions exceed 95% of licensed capacity
- Total EVRC sessions exceed 95% of licensed capacity
- Total EVRCB sessions exceed 95% of licensed capacity

The apSysMgmtGroupTrap contains the condition observed (apSysMgmtTrapType) and the corresponding value reached (apSysMgmtTrapValue).

```
apSysMgmtGroupTrap         NOTIFICATION-TYPE
    OBJECTS        { apSysMgmtTrapType, apSysMgmtTrapValue }
    STATUS           current
    DESCRIPTION
          " The trap will generated if value of the monitoring object
          exceeds a certain threshold. "
    ::= { apSystemManagementNotifications 1 }
```

When the resource usage retreats below a defined threshold, the Oracle Communications Session Border Controller sends an apSysMgmtGroupClearTrap.

```
apSysMgmtGroupClearTrap         NOTIFICATION-TYPE
    OBJECTS        { apSysMgmtTrapType }
    STATUS           current
    DESCRIPTION
          " The trap will generated if value of the monitoring object
          returns to within a certain threshold.  This signifies that
          an alarm caused by that monitoring object has been cleared. "
    ::= { apSystemManagementNotifications 2 }
```

The following table summarizes trigger and clear conditions for transcoding capacity alerts as sent in the apSysMgmtGroupTrap:

Monitored Transcoding Resource	SNMP Object & OID in apSysMgmtTrapType	Trap Sent	Clear Trap Sent
Total DSP Usage	apSysXCodeCapacity 1.3.6.1.4.1.9148.3.2.1.1.34	95%	80%
AMR License Capacity Usage	apSysXCodeAMRCapacity 1.3.6.1.4.1.9148.3.2.1.1.35	95%	80%
AMR-WB License Capacity Usage	apSysXCodeAMRWBCapacity 1.3.6.1.4.1.9148.3.2.1.1.36	95%	80%
EVRC License Capacity Usage	apSysXCodeEVRCCapacity 1.3.6.1.4.1.9148.3.2.1.1.39	95%	80%

Monitored Transcoding Resource	SNMP Object & OID in apSysMgmtTrapType	Trap Sent	Clear Trap Sent
EVRCB License Capacity Usage	apSysXCodeEVRCBCapacity 1.3.6.1.4.1.9148.3.2.1.1.40	95%	80%
G729 License Capacity Usage	apSysXCodeG729Capacity 1.3.6.1.4.1.9148.3.2.1.1.42	95%	80%
Opus License Capacity Usage	apSysXCodeOpusCapacity 1.3.6.1.4.1.9148.3.2.1.1.46	95%	80%
Silk License Capacity Usage	apSysXCodeSilkCapacity 1.3.6.1.4.1.9148.3.2.1.1.47	95%	80%
EVRCNW License Capacity Usage	apSysXCodeEVRCNWCapacity 1.3.6.1.4.1.9148.3.2.1.1.48	95%	80%
EVS License Capacity Usage	apSysXCodeEVSCapacity 1.3.6.1.4.1.9148.3.2.1.1.49	95%	80%

The following SNMP Objects are inserted into the apSysMgmtTrapType when sending and clearing a transcoding capacity trap. You mayt query them individually with an SNMP GET.

- apSysXCodeCapacity (1.3.6.1.4.1.9148.3.2.1.1.34)
- apSysXCodeAMRCapacity (1.3.6.1.4.1.9148.3.2.1.1.35)
- apSysXCodeAMRWBCapacity (1.3.6.1.4.1.9148.3.2.1.1.36)
- apSysXCodeEVRCCapacity (1.3.6.1.4.1.9148.3.2.1.1.39)
- apSysXCodeEVRCBCapacity(1.3.6.1.4.1.9148.3.2.1.1.40)
- apSysXCodeG729Capacity(1.3.6.1.4.1.9148.3.2.1.1.42)
- apSysXCodeOpusCapacity(1.3.6.1.4.1.9148.3.2.1.1.46)
- apSysXCodeSilkCapacity(1.3.6.1.4.1.9148.3.2.1.1.47)
- apSysXCodeEVRCNWCapacity(1.3.6.1.4.1.9148.3.2.1.1.48)
- apSysXCodeEVSCapacity(1.3.6.1.4.1.9148.3.2.1.1.49)

About Alarms

This section describes system-level alarms. Alarms play a significant role in determining overall health of the system. For additional information, see the *Oracle Communications Session Border Controller MIB Reference Guide*.

Overview

An alarm is triggered when a condition or event happens within either the system’s hardware or software. This alarm contains an alarm code, a severity level, a textual description of the event, the time the event occurred, and for high severity alarms, trap information.

The system’s alarm handler processes alarms by locating the alarm ID for a particular alarm condition and then looking up that condition in an alarm table. The alarm table contains all of the actions required for following up on an alarm.

Types of Alarms

The system can generate the following types of alarms:

- Hardware alarms: generated when a problem with the chassis occurs.
- System alarms: accounts for system resource and redundancy issues. For example, CPU utilization is over threshold, memory utilization is high, the health score is under threshold, or a task is suspended. They also include low-level system calls (for example, there is not enough memory available).
- Network alarms: can occur when the software is unable to communicate with the hardware.
- Application alarms: account for application issues (for example, problems that involve protocols). These protocols include:
  - SIP
  - RADIUS

  Application alarms also include security breaches, session failures, and problems related to accounting.

About the Alarm Process

An alarm is triggered when a condition or event happens within either the hardware or software. This alarm contains the following elements:

- **Alarm ID**: a unique 32-bit integer that contains a 16-bit category name or number and a 16-bit unique identifier for the error or failure within that category.
- **Severity**: how severe the condition or failure is to the system.
- **Character string**: a textual description of the event or condition.
- **Trap information**: is not contained within every alarm, but is only sent for events of greater severity. See the *Oracle Communications Session Border Controller MIB Reference Guide* for more information.

About Alarms and the Health Score

The Oracle Communications Session Border Controller health score is used to determine the active/standby roles of the Oracle Communications Session Border Controllers participating in a High Availibility pair architecture. The healthiest Oracle Communications Session Border Controller peer (peer with the highest health score) is the active Oracle Communications Session Border Controller peer. The Oracle

Communications Session Border Controller peer with the lower health score is the standby Oracle Communications Session Border Controller peer.

The health score is based on a 100-point scoring system. When all system components are functioning properly, the health score of the system is 100.

Alarms play a significant role in determining the health score of an HA Oracle Communications Session Border Controller. Some alarm conditions have a corresponding health value, which is subtracted from the health score of the system when that alarm occurs. When that alarm is cleared or removed, the corresponding health value is added back to the system's health score.

If a key system task (for example, a process or daemon) fails, the health score of that HA Oracle Communications Session Border Controller might be decremented by 75 points, depending on how the system configuration was configured. These situations, however, do not have a corresponding system alarm.

When an alarm condition is cleared or removed, this action has a positive impact on the health score of a system.

Displaying and Clearing Alarms

You display and clear alarms using the following ACLI commands:

- **display-alarms**
- **clear-alarm**

The clear-alarm command is only available in Superuser mode. You must have that level of privilege to clear alarms.

Displaying Alarms

To display system alarms:

- Enter the **display-alarms** command.

  A list of the current alarms for the system will be displayed. For example:

  ```
  ORACLE# display-alarms
  3 alarms to show
  ID      Task    Severity        First Occurred          Last Occurred
  262147  35615744        4       2005-02-10 13:59:05     2005-02-10
  13:59:05
  Count   Description
  1       ingress realm 'test_client_realm' not found
  131075  36786224        3       2005-02-10 13:59:05     2005-02-10
  13:59:05
  Count   Description
  1       Slot 0 Port 0 DOWN
  131101  36786224        3       2005-02-10 13:59:10     2005-02-10
  13:59:10
  Count   Description
  1       health score is under threshold 50%
  done
  ORACLE#
  ```

Clearing Alarms

If an alarm situation is corrected, the corresponding alarm is cleared in the system’s alarm table and health is restored. You can also issue an ACLI command to clear a specific alarm:

To clear a specific system alarm:

1. Ensure you are in Superuser Mode by entering the **show privilege** command. at the topmost ACLI level. For example:

   ```
   ORACLE# show privilege
   console user - privilege level 1
   ```

   - **privilege level 0** refers **Level 0:User Mode**
   - **privilege level 1** refers to **Level 1: Superuser Mode.**

2. Enter **display-alarms** to list the current alarms. Note the alarm ID (ID column) and task ID (Task column) of the alarm you want to clear. You will need this reference information in order to clear the alarm.
3. Enter **clear-alarm** followed by a Space, the alarm ID, another Space, and the task ID of the task that generated the alarm.
4. Press Enter.

   With regard to redundant architectures, if you clear an alarm using the **clear-alarm** command without actually fixing the true cause of the alarm, it might have an adverse effect on the health score of the system and might, in turn, prevent future failover functionality.

About the Alarm Display on the Chassis

The alarm display appears in a two-line front panel display mode. During an alarm condition, the alarm display replaces the standard display on the chassis.

The first line of the graphic display shows the number of hardware-related alarms, if any. The second line of the graphic display shows the number of link-related alarms, if any. For example:

```
1 HW ALARM
2 LINK ALARMS
```

If the graphic display window indicates an alarm condition, the system administrator must determine the nature of the condition by using the **display-alarms** ACLI command. Executing this command allows system administrators to view specific details about the alarm.

When an alarm condition is cleared, the standard display replaces the alarm display.

Alarm Severity Levels

Five levels of alarm severity have been established for the system. These levels have been designated so that the system can take action that is appropriate to the situation.

Alarm Severity	Description
Emergency	Requires immediate attention. If you do not attend to this condition immediately, there will be physical, permanent, and irreparable damage to your system.
Critical	Requires attention as soon as it is noted. If you do not attend to this condition immediately, there may be physical, permanent, and irreparable damage to your system.
Major	Functionality has been seriously compromised. As a result, this situation might cause loss of functionality, hanging applications, and dropped packets. If you do not attend to this situation, your system will suffer no physical harm, but it will cease to function.
Minor	Functionality has been impaired to a certain degree. As a result, you might experience compromised functionality. There will be no physical harm to your system. However, you should attend to this type of alarm as soon as possible in order to keep your system operating properly.
Warning	Some irregularities in performance. This condition describes situations that are noteworthy, however, you should attend to this condition in order to keep your system operating properly. For example, this type of alarm might indicate the system is running low on bandwidth and you may need to contact Oracle to arrange for an upgrade.

System Response to Alarms

The system is capable of taking any of a range of actions when an alarm event occurs. It can present the alarms in the VED graphic display window on the front panel of the chassis, use the acmelog (syslog) to log the events off the system, create an SNMP trap with an event notification, or use three dry contacts for external alarming.

Within the system, a database holds all information related to what actions to take given an event of a specific category and severity. This section sets out and defines these actions.

Writing to syslog (acmelog)

The term syslog refers to the protocol used for the network logging of system and network events. Because syslog facilitates the transmission of event notification messages across networks, the **syslog** protocol can be used to allow remote log access.

Sending SNMP Traps

An SNMP trap is essentially an event notification that can be initiated by tasks (such as the notify task), by log messages, or by alarm reporting. When an event occurs, the Oracle Communications Session Border Controller sends a trap to the management station.

Although there is no direct correlation between system alarms and the generation of SNMP traps, there is a correlation between system alarms and the MIBs that support SNMP traps. For a list of the SNMP-related alarms and their associated traps, refer to the *Oracle Communications Session Border ControllerMIB Reference Guide*.

About Dry Contacts

The system supports three relays at the back of the Oracle Communications Session Border Controller chassis used for transmission of alarms called dry contacts. A dry contact is triggered for the following levels of severity:

- Critical
- Major
- Minor

Most often, the dry contact action is registered in the physical location of the chassis. For example, there may be an LED signal on a communications cabinet.

Displaying Alarms to the Chassis

The system can display a message concerning the alarm condition on the chassis itself. If this action is taken, a brief message appears in the VED graphic display window on the front panel of the chassis.

Hardware and Environmental Faults

This section describes the hardware and environmental faults. It includes information about fan speed, voltage, temperature, and power supply for the system.

> **Note:**
>
> If you suspect you have a hardware fault, contact Oracle Support for assistance with running the diagnostics image loaded on the Oracle Communications Session Border Controller.

Hardware Temperature Alarm

The following table describes the hardware temperature alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions	Health Score Impact
TEMPERATURE HIGH	65538		Fans are obstructed or stopped. The room is abnormally hot.	Temperature: XX.XXC (where XX.XX is the temperature in degrees)	apSyslogMessageGenerated trap generated apEnvMonStatusChangeNotification apSysMgmtTempTrap critical, major, minor dry contact	CRITICAL: -100 MAJOR: -50 MINOR: -25
SD5_TEMPERATURE_HIGH_PHY0	N/A	CRITICAL:>100°C MAJOR:>95°C MINOR:>90°C	Fans are obstructed or stopped. The room is abnormally hot.	Temperature: XX.XXC (where XX.XX is the temperature in degrees)	Temperature X is at Y degrees C over minor/major/critical threshold of Z (Where X is sensor name, Y is temperature and Z is threshold)	N/A

Note:

If this alarm occurs, the system turns the fan speed up to the fastest possible speed.

Fan Speed Alarm

The following table describes the fan speed alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions	Health Score Impact
FAN STOPPED	65537	CRITICAL: any fan speed is <50%. Or speed of two or more fans is >50% and <75%. MAJOR: speed of two or more fans is > 75% and < 90%. Or speed of one fan is >50% and <75% and the other two fans are at normal speed. MINOR: speed of one fan> 75% and <90%, the other two fans are at normal speed	Fan speed failure.	Fan speed: XXXX XXXX XXXX where xxxx xxxx xxxx is the Revolutions per Minute (RPM) of each fan on the fan module	apSyslogMessageGenerated trap generated apEnvMonStatusChangeNotification apSysMgmtFanTrap critical, major, minor dry contact	CRITICAL: -100 MAJOR: -50 MINOR: -25

Note:

If this alarm occurs, the system turns the fan speed up to the fastest possible speed.

Environmental Sensor Alarm

The following table describes the environmental sensor alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions	Health Score Impact
ENVIRONMENTAL SENSOR FAILURE	65539	CRITICAL	The environmental sensor component cannot detect fan speed and temperature.	Hardware monitor failure! Unable to monitor fan speed and temperature!	apSyslogMessageGenerated trap generated critical, major, minor dry contact syslog power cycle the standby Oracle Communications Session Border Controller peer using the power supply on/off switches located on the rear panel of the chassis force a manual switchover by executing the ACLI notify berpd force command power cycle the active Oracle Communications Session Border Controller peer	CRITICAL: -10

Media Link Alarms

Media link alarms include the following:

- Major
  If the Oracle Communications Session Border Controller’s media link goes from being up to being down, it is considered a major alarm. This alarms applies to both slots 1 and 2 on the Oracle Communications Session Border Controller. A message appears on the front panel of the Oracle Communications Session Border Controller’s chassis, similar to the following:

  ```
  MAJOR ALARM
  Gig Port 1 DOWN
  ```

- Minor
  If the Oracle Communications Session Border Controller’s media link goes from being down to being up, it is considered a minor alarm. This alarm applies to both slots 1 and 2 on the Oracle Communications Session Border Controller.

Power Supply Alarms

The following table describes the power supply alarms

Alarm	Alarm ID	Alarm Severity	Cause(s)	Log Message	Actions
PLD POWER A FAILURE	65540	MINOR (-10)	Power supply A has failed.	Back Power Supply A has failed!	apSyslogMessageGenerated trap generated minor dry contact syslog
PLD POWER A UP	65541	MINOR	Power supply A is now present and functioning.	Back Power Supply A is present!	apSyslogMessageGenerated trap generated minor dry contact syslog
PLD POWER B FAILURE	65542	MINOR (-10)	Power supply B has failed.	Back Power Supply B has failed!	apSyslogMessageGenerated trap generated minor dry contact syslog
PLD POWER B UP	65543	MINOR	Power supply B is now present and functioning.	Back Power Supply B is present!	apSyslogMessageGenerated trap generated minor dry contact syslog

Note:

If the system boots up with one power supply, the health score will be 100, and no alarm will be generated. If another power supply is then added to that same system, this same alarm will be generated, but the health score will not be decremented.

Voltage Alarms

The following table describes the voltage alarms, which are only available for Oracle Communications Session Border Controller 2:

Alarm	Alarm ID	Alarm Severity	Cause(s)	Log Message	Actions
PLD VOLTAGE ALARM 2P5V	65544	MINOR EMERGENCY	N/A	Voltage 2.5V CPU has minor alarm Voltage 2.5V CPU has emergency alarm, the system should shutdown	apSyslogMessageGenerated trap generated dry contact syslog

Alarm	Alarm ID	Alarm Severity	Cause(s)	Log Message	Actions
PLD VOLTAGE ALARM 3P3V	65545	MINOR EMERGENCY	N/A	Voltage 3.3V has minor alarm Voltage 3.3V has emergency alarm, the system should shutdown	apSyslogMessageGenerated trap generated dry contact syslog
PLD VOLTAGE ALARM 5V	65546	MINOR EMERGENCY	N/A	Voltage 5V has minor alarm Voltage 5V has emergency alarm, the system should shutdown	apSyslogMessageGenerated trap generated dry contact syslog
PLD VOLTAGE ALARM CPU	65547	MINOR EMERGENCY	N/A	Voltage CPU has minor alarm Voltage CPU has emergency alarm, the system should shutdown	apSyslogMessageGenerated trap generated dry contact syslog

Physical Interface Card Alarms

The following table describes the physical interface card alarms.

Alarm	Alarm ID	Alarm Severity	Cause(s)	Log Message	Actions
PHY0 Removed	65550	MAJOR	Physical interface card 0 was removed.	PHY card 0 has been removed.	N/A
PHY0 Inserted	65552	MAJOR	Physical interface card 0 was inserted.	None	N/A
PHY1 Removed	65553	MAJOR	Physical interface card 1 was removed.	PHY card 1 has been removed.	N/A
PHY1 Inserted	65554	MAJOR	Physical interface card 1 was inserted.	None	N/A

Transcoding Alarms

The transcoding feature employs several hardware and software alarms to alert the user when the system is not functioning properly or overload conditions are reached.

Name/ID	Severity/ Health Degredation	Cause(s)	Traps Generated
No DSPs Present with Transcoding Feature Card (DSP_NONE_PRESENT)	Minor/0	A transcoding feature card is installed but no DSP modules are discovered.	apSysMgmtHardwareErrorTrap
DSP Boot Failure (DSP_BOOT_FAILURE)	Critical/0	A DSP device fails to boot properly at system initialization. This alarm is not health affecting for a single DSP boot failure. DSPs that fail to boot will remain uninitialized and will be avoided for transcoding.	apSysMgmtHardwareErrorTrap
DSP Communications Timeout (DSP_COMMS_TIMEOUT)	Critical/100	A DSP fails to respond after 2 seconds with 3 retry messages. This alarm is critical and is health affecting.	apSysMgmtHardwareErrorTrap
DSP Alerts (DSP_CORE_HALT)	Critical/100	A problem with the health of the DSP such as a halted DSP core. The software will attempt to reset the DSP and gather diagnostic information about the crash. This information will be saved in the /code directory to be retrieved by the user.	apSysMgmtHardwareErrorTrap
DSP Temperature(DSP_TEMPERATURE_HIGH)	Clear 85°C Warning 86°C / 5 Minor 90°C / 25 Major 95°C/ 50 Critical 100°C/ 100	A DSP device exceeds the temperature threshold. If the temperature exceeds 90°C, a minor alarm will be set. If it exceeds 95°C, a major alarm will be set. If it exceeds 100°C, a critical alarm will be set. The alarm is cleared if the temperature falls below 85°C. The alarm is health affecting.	apSysMgmtHardwareErrorTrap

Name/ID	Severity/ Health Degradation	Cause(s)	Traps Generated
Transcoding Capacity Threshold Alarm (XCODE_UTIL_OVER_THRESHOLD) / 131329	Clear 80% Warning 95%	A warning alarm will be raised when the transcoding capacity exceeds a high threshold of 95%. The alarm will be cleared after the capacity falls below a low threshold of 80%. This alarm warns the user that transcoding resources are nearly depleted. This alarm is not health affecting.	apSysMgmtGroupTrap
Licensed AMR Transcoding Capacity Threshold Alarm/ 131330	Clear 80% Warning 95%	A warning alarm is triggered if the AMR transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	apSysMgmtGroupTrap
Licensed AMR-WB Transcoding Capacity Threshold Alarm/ 131331	Clear 80% Warning 95%	A warning alarm is triggered if the AMR-WB transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	apSysMgmtGroupTrap
Licensed EVRC Transcoding Capacity Threshold Alarm/ 131332	Clear 80% Warning 95%	A warning alarm is triggered if the EVRC transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	apSysMgmtGroupTrap

Name/ID	Severity/ Health Degredation	Cause(s)	Traps Generated
Licensed EVRCB Transcoding Capacity Threshold Alarm/ 131333	Clear 80% Warning 95%	A warning alarm is triggered if the EVRCB transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	apSysMgmtGroupTrap
Licensed Opus Transcoding Capacity Threshold Alarm/ 131159	Clear 80% Warning 95%	A warning alarm is triggered if the Opus transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	apSysMgmtGroupTrap
Licensed SILK Transcoding Capacity Threshold Alarm/ 131159	Clear 80% Warning 95%	A warning alarm is triggered if the SILK transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	apSysMgmtGroupTrap

Viewing PROM Information

Display PROM statistics for the following Oracle Communications Session Border Controller components by using the **show prom-info** command.

For example:

```
ORACLE# show prom-info mainboard
Contents of Main Board IDPROM
        Assy, NetNet4600
        Part Number:                002-0610-50
        Serial Number:              091132009670
        FunctionalRev:              5.06
        BoardRev:                   05.00
        PCB Family Type:            Main Board
        ID:                         NetNet 4600 Main Board
        Options:                    0
        Manufacturer:               Benchmark Electronics
        Week/Year:                  32/2017
        Sequence Number:               009670
        Number of MAC Addresses:       16
        Starting MAC Address:          00 08 25 a2 56 20
```

The following example shows the host CPU PROM contents.

```
ORACLE# show prom-info cpu
Contents of CPU IDPROM
        Part Number:                   MOD-0026-62
        Manufacturer:                  RadiSys
```

Graphic Window Display

The Environment display lets you scroll through information about the operational status of the hardware displayed in the Oracle Communications Session Border Controller chassis's graphic window. For example, you can view hardware- and link-related alarm information, highest monitored temperature reading, and fan speed.

The graphic display window presents the following Environment information in the order listed:

```
Alarm state
temperature
fan speed
```

- alarm state: **HW ALARM: X (where X is the number of hardware alarms, excluding ENVIRONMENTAL SENSOR FAILURE)** and LINK ALARM: X (where X is the number of link down alarms)
- temperature: format is XX.XX C, where XX.XX is the temperature in degrees
- fan speed: XXXX, where XXXX is the RPM of the failing fan on the fan module

For example:

```
HW ALARM: 1
LINK ALARM: 2
TEMPERATURE: 38.00 C
FAN SPEED: 5800
```

From this display, pressing Enter for the Return selection refreshes the information and returns you to the main Environment menu heading.

> **Note:**
>
> Environmental sensor failure alarms are not displayed in the graphic display window on the front panel.

Fan Stopped Alarm

The fan stopped alarm presents the following in the graphic display window:

X HW ALARM(S) (where X indicates the number of HW alarms that exist on the system)

Temperature High Alarm

The temperature high alarm presents the following in the graphic display window:

X HW ALARM(S) (where X indicates the number of HW alarms that exist on the system)

System Fault Statistics

This section contains information about system faults. System faults include problems related to CPU usage, memory usage, and license capacity. System faults also include the functionality of the Address Resolution Protocol (ARP) on the system.

System State

You can use the following commands to view system uptime and state information:

- **show uptime**
- **show system-state**

Viewing System Uptime

Display current date and time information and the length of time the system has been running in days, hours, minutes, and seconds by using the **show uptime** command. For example:

```
ORACLE# show uptime
FRI FEB 25 13:02:55 2005 - up 0 days, 3 hours, 42 minutes, 30 seconds
```

Viewing System State

Display whether the Oracle Communications Session Border Controller is currently online or offline by using the show system-state command. For example:

```
ORACLE# show system-state
The current system state is online
```

System Resources

You can use the following command to view the system resource statistics:

- **show processes cpu**

Viewing CPU Usage

Display CPU usage information, categorized on a per task/process basis, for your Oracle Communications Session Border Controller by using the **show processes cpu** command.

```
ORACLE> show processes cpu
 Task Name  Task Id Pri   Status   Total CPU    Avg   Now  Load  Processor
----------- ------- ---- -------- ------------ ----- ----- ----- ---------
```

```
       tCli    1799   -2 RUNNING   0:00:00.910  0.00  2.37  4.74    1
    tAsctpd    1770  -70 SLEEPING  0:01:46.440  0.03  0.47  0.95    1
kworker/1:1     423   20 RUNNING   0:28:22.590  0.40  0.47  0.95    1
kworker/u:1    2478   20 SLEEPING  0:00:01.430  0.00  0.00  0.00    0
kworker/u:2    2477   20 SLEEPING  0:00:02.450  0.00  0.00  0.00    1
kworker/u:0    2476   20 SLEEPING  0:00:06.150  0.00  0.00  0.00    0
    telnetD    1805 -100 SLEEPING  0:00:00.000  0.00  0.00  0.00    1
  tCliTnet5    1804   -2 SLEEPING  0:00:00.000  0.00  0.00  0.00    1
  tCliTnet4    1803   -2 SLEEPING  0:00:00.000  0.00  0.00  0.00    1
  tCliTnet3    1802   -2 SLEEPING  0:00:00.000  0.00  0.00  0.00    1
  tCliTnet2    1801   -2 SLEEPING  0:00:00.000  0.00  0.00  0.00    1
  tCliTnet1    1800   -2 SLEEPING  0:00:00.000  0.00  0.00  0.00    1
       tSSH    1798 -100 SLEEPING  0:00:04.590  0.00  0.00  0.00    0
   tCliSSH4    1797   -2 SLEEPING  0:00:00.000  0.00  0.00  0.00    1
   tCliSSH3    1796   -2 SLEEPING  0:00:00.000  0.00  0.00  0.00    1
   tCliSSH2    1795   -2 SLEEPING  0:00:00.000  0.00  0.00  0.00    1
   tCliSSH1    1794   -2 SLEEPING  0:00:00.000  0.00  0.00  0.00    1
   tCliSSH0    1793   -2 SLEEPING  0:00:00.000  0.00  0.00  0.00    1
tLogCleaner    1792 -100 SLEEPING  0:00:00.100  0.00  0.00  0.00    0
     tAlarm    1791  -76 SLEEPING  0:00:29.130  0.01  0.00  0.00    1
  tifXCheck    1787 -100 SLEEPING  0:00:00.130  0.00  0.00  0.00    0
     tSnmpd    1786  -62 SLEEPING  0:00:00.070  0.00  0.00  0.00    0
```

The output of the **show processes cpu** command includes the following information:

- Task Name—Name of the system 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 system was last rebooted
- Now—CPU usage in the last second
- Load—The CPU load
- Processor—The processor number where this task runs

CPU Utilization Alarm

The following table lists the CPU utilization alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
CPU UTILIZATION	131099	MINOR	CPU usage reached 90% or greater of its capacity.	CPU usage X% over threshold X%	apSysMgmtGroupTrap trap generated minor dry contact syslog

System Task Suspended Alarm

The following table describes the system task suspended alarm information.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
SYSTEM TASK SUSPENDED	131108	CRITICAL	A system task (process) suspends or fails.	Task X suspended, which decremented health by 75! (where X is the task/process name)	apSyslogMessageGenerated trap generated major dry contact syslog reboot (if the system is configured to do so)

Memory Usage

You can use the following commands to view memory statistics:

- **show memory usage**
- **show buffers**

Viewing Memory Usage Statistics

Display memory usage statistics by using the **show memory usage** command. For example:

```
ORACLE# show memory usage
Mem Total :    3698 MB
Mem App   :    505 MB
Mem OS    :    179 MB
```

Viewing Memory Buffer Statistics

Display memory buffer statistics using the **show buffers** command. Use this command only for debugging purposes under the direction of Oracle support.

Components displayed vary based on platform and configuration, and commonly include:

- L2 Resolver
- Service Pipe
- Memory Buffer Process
- Memory Buffer Redundancy
- Memory Buffer Transport
- Network Buffer
- Network Buffer Control
- NP Application Fragments
- NP Application GARP
- NP DMA

Component statistics include:

- Pool Instances (number of pool instances)

- Memory Footprint (allocation in MB across all instances)
- Pool Size (aggregate pool size across all instances)
- Buffer Size (Bytes) (fixed buffer size)
- Allocated Buffers (aggregate allocated buffers across all instances)
- Used Buffers (aggregate in-use buffers across all instances)
- Errors (aggregate errors across all instances)

For example:

```
ORACLE# show buffers
component      refs  MB      total  size   alloc  usage  error
-------------  ----  ------  -----  -----  -----  -----  -----
L2Resolver     1     1.74    4358   418    4358   0      0
MemBufProc     62    15.88   12400  65536  254    174    0
MemBufRed      1     0.00    200    10240  0      0      0
MemBufTrans    1     0.06    200    65536  1      0      0
NetBuf         1     317.87  32000  10416  32000  0      0
NetBufCtrl     1     13.67   32000  448    32000  0      0
NpAppGarp      1     0.01    20     352    20     0      0
SvcPipe        1     130.49  16000  8552   16000  180    0
```

Subsequent, optional arguments include:

- **histogram** - Show the histogram of requested buffer sizes by the Memory Buffer Transport, Network Buffer, and Service Pipe components for use in future buffer pool optimizations.
- **usage** - Requires buffer tracking to be enabled by Oracle Support.

Memory Utilization Alarm

The following table describes the memory utilization alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
MEMORY UTILIZATION	131100	MAJOR	Memory usage reached 90% or greater of its capacity.	Memory usage X% over threshold X%	apSysMgmtGroupTrap trap generated minor dry contact syslog

License Capacity

If the total number of active sessions on the system (across all protocols) is within 98-100% of the system’s licensed capacity, an alarm and trap will be generated. The severity of this application alarm is MAJOR, but is not HA health-affecting.

The total number of active sessions is checked at an interval of 5 seconds (just as the system temperature and fans speed are). Once an approaching capacity alarm is triggered, another one will not be triggered until after the current alarm is cleared. This alarm will be cleared (and the trap sent, apLicenseNotApproachingCapacityNotification) after the total number of active sessions has gone to or below 90% of capacity, but no sooner than 15 seconds after the original alarm was triggered.

The following table describes the license capacity alarm

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
LICENSE ALARM APPROACHING SESSION CAPACITY	327684	MAJOR	Total number of active sessions on the system (across all protocols) is within 98 to 100% of the system's licensed capacity.	Total number of sessions (<#>) is approaching licensed capacity (<#>)	apLicenseApproachingCapacityNotification

Configuration Statistics

You can use the following commands to display configuration information:

- **show configuration**
- **show running-config**
- **realm-specifics <realm ID>**
- **show virtual-interfaces**

Specifying a Configuration Element

Both the **show configuration** and the **show running-config** commands let you include a configuration element name as an argument to view only instances for that configuration element. The list of valid configuration elements you can use as an argument include the following:

- account-config—Show account-config object
- h323-config—Show h323-config object
- h323-stack—Show all h323-stack objects
- iwf-stack—Show iwf-stack object
- host-route—Show all host-route objects
- local-policy—Show all local-policy objects
- media-profile—Show all media-profile objects
- media-manager—Show media-manager object
- dns-config—Show all dns-config objects
- network-interface—Show all network-interface objects
- ntp-config—Show ntp-config object
- phys-interface—Show all phys-interface objects
- realm—Show all realm objects

- MediaPolicy—Show all MediaPolicy objects
- ClassPolicy—Show all ClassPolicy objects
- redundancy-config—Show redundancy-config object
- ResponseMap—Show all ResponseMap objects
- session-agent—Show all session-agent objects
- session-group—Show all session-group objects
- session-translation—Show all session-translation objects
- translation-rules—Show all translation-rules objects
- session-router—Show session-router object
- sip-config—Show all sip-config objects
- sip-feature—Show all sip-feature objects
- sip-interface—Show all sip-interface objects
- sip-nat—Show all sip-nat objects
- snmp-community—Show all snmp-community objects
- static-flow—Show all static-flow objects
- steering-pool—Show all steering-pool objectssystem-config—show system-config object
- TrapReceiver—Show all TrapReceiver objects
- call-recording-server—Show call-recording-server configurations
- capture-receiver—Show capture-receiver configurations
- rph-profile—Show rph-profile configurations
- rph-policy—Show rph-policy configurations
- password-policy—Show password-policy configuration
- enforcement-profile—Show enforcement-profile configurations
- realm-group—Show realm-group configurations
- inventory—Displays an inventory of all configured elements on the Oracle Communications Session Border Controller

Viewing Current Configuration

Display information about the current configuration (used once the **activate-config** command is executed) by using the **show configuration** command. You can include the name of a configuration element with the **show configuration** command to display only instances for that configuration element.

For example:

```
ORACLE# show configuration media-manager
media-manager
        state                          enabled
        latching                       enabled
        flow-time-limit                86400
        initial-guard-timer            300
        subsq-guard-timer              300
        tcp-flow-time-limit            86400
        tcp-initial-guard-timer        300
        tcp-subsq-guard-timer          300
        tcp-number-of-ports-per-flow   2
        hnt-rtcp                       disabled
        mbcd-log-level                 NOTICE
        max-signaling-bandwidth        10000000
        max-untrusted-signaling        100
        min-untrusted-signaling        30
        app-signaling-bandwidth        0
        tolerance-window               30
        rtcp-rate-limit                0
        min-media-allocation           32000
        min-trusted-allocation         1000
        deny-allocation                1000
        anonymous-sdp                  disabled
        arp-msg-bandwidth              32000
        last-modified-date             2007-04-05 09:27:20
task done
```

Viewing Running Configuration

Display the running configuration information currently in use on the system by using the **show running-config** command. You can include the name of a configuration element with the show configuration command to display only the instances for that configuration element.

For example:

```
ORACLE# show running-config realm
realm-config
        identifier                     testrealm
        addr-prefix                    0.0.0.0
        network-interfaces
        mm-in-realm                    disabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   disabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        qos-enable                     disabled
        max-bandwidth                  0
        ext-policy-svr                 boffo.com
        max-latency                    0
        max-jitter                     0
        max-packet-loss                0
        observ-window-size             0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        class-profile
        average-rate-limit             0
        access-control-trust-level     low
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     758
        deny-period                    30
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow              reverse
        additional-prefixes            10.0.0.0/24
                                       172.16.0.0
        restricted-latching            peer-ip
        restriction-mask               17
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        net-management-control         disabled
        delay-media-update             disabled
        codec-policy
        codec-manip-in-realm           disabled
        last-modified-date             2006-07-06 12:43:39
```

Viewing Realm-Specific Configuration

Display realm-specific configuration based on the input realm ID by using the **realm-specifics <realm ID>** command. The information displayed includes the following:

- realm-config
- steering-pool
- session-agent
- session-translation
- class-policy
- local-policy (if the source realm or destination realm are defined)

For example:

```
ORACLE# realm-specifics testrealm
realm-config
        identifier                     testrealm
        addr-prefix                    0.0.0.0
        network-interfaces
        mm-in-realm                    disabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   disabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        qos-enable                     disabled
        max-bandwidth                  0
        ext-policy-svr                 boffo.com
        max-latency                    0
        max-jitter                     0
        max-packet-loss                0
        observ-window-size             0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        class-profile
        average-rate-limit             0
        access-control-trust-level     low
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     758
        deny-period                    30
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow              reverse
        additional-prefixes            10.0.0.0/24
                                       172.16.0.0
        restricted-latching            peer-ip
        restriction-mask               17
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        net-management-control         disabled
        delay-media-update             disabled
        codec-policy
        codec-manip-in-realm           disabled
        last-modified-date             2006-07-06 12:43:39
sip-interface
        state                          enabled
        realm-id                       testrealm
        sip-port
                address                        192.168.10.12
                port                           5060
                transport-protocol             UDP
                tls-profile
                allow-anonymous                register-prefix
        carriers
        trans-expire                   0
        invite-expire                  0
        max-redirect-contacts          0
        proxy-mode
        redirect-action
        contact-mode                   maddr
        nat-traversal                  none
        nat-interval                   30
        tcp-nat-interval               30
        registration-caching           disabled
        min-reg-expire                 300
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        options                        disable-privacy
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
        nat-test-increment             30
        sip-dynamic-hnt                disabled
        stop-recurse                   401,407
        port-map-start                 0
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        sip-ims-feature                disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout          0
        untrusted-conn-timeout         0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        last-modified-date             2006-06-12 12:08:34
```

Configuration Save Failed Alarm

The following table lists the CFG ALARM SAVE FAILED alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
CFG ALARM SAVE FAILED	393217	MAJOR	The save-config command execution failed on a standby Oracle Communications Session Border Controller peer operating as part of an HA pair.	save-config failed on targetName!/ code full, config sync stopped! or save-config failed on targetName!/ code full, config sync stopped! (where the targetName is the target name (tn) configured in the boot parameters)	apSyslogMessageGenerated trap generated syslog

HA Functionality

You can monitor HA Oracle Communications Session Border Controller functionality using the following ACLI commands:

- **show health** to view information about the HA architecture and associated HA Oracle Communications Session Border Controller peers.
- **show redundancy** to view information about the synchronization of media flows and signaling for the members of an HA Oracle Communications Session Border Controller pair.

You can also view state displays on the graphical window display of the chassis.

Viewing Health Information

Display the following information for HA architectures by using the **show health** command:

> **Note:**
>
> The spaces are intentionally used in the following examples because they appear on the screen.

- Health score
- Whether the current HA Oracle Communications Session Border Controller is active, standby, or out of service
- Whether the media flow information is synchronized for all supported protocols: SIP and H.323 (true/false)
- If media flow information is not available, Media Synchronized disabled will be displayed in the show health output.
- Whether SIP signaling information is synchronized (true/false)

- If SIP signaling is not available, SIP Synchronized disabled will be displayed in the show health output.
- Whether configuration information is synchronized (true/false)
- If configuration checkpointing is not available, Config Synchronized disabled will be displayed in the show health output.
- The IPv4 or IPv6 address of the current HA Oracle Communications Session Border Controller’s active peer (an HA Oracle Communications Session Border Controller that is currently active does not have an active Oracle Communications Session Border Controller peer and shows 0.0.0.0)
- The last message received from the HA Oracle Communications Session Border Controller peer
- A switchover log containing the last 20 switchover events (whether becoming active or relinquishing the active role)

The following example shows a currently active Oracle Communications Session Border Controller.

```
ORACLE# show health
        Media Synchronized            enabled
        SIP Synchronized              enabled
        Config Synchronized           enabled
        Collect Synchronized          enabled
        Radius CDR Synchronized       enabled
        Rotated CDRs Synchronized     enabled
        Active Peer Address           163.4.12.2
Redundancy Protocol Process (v2):
        State                           Active
        Health                          100
        Lowest Local Address            11.0.0.1:9090
        1 peer(s) on 1 socket(s):
        systest3B: v2, Standby, health=100, max silence=1050
                  last received from 11.0.0.2 on wancom1:0
        Switchover log:
        Jul 11 14:18:21.442: Active to RelinquishingActive
        Jul 11 14:24:00.872: Standby to BecomingActive, active peer
                 systest3B has timed out.
```

Viewing Redundancy Information

Display the following information about HA architecture by using the **show redundancy** command:

- General HA statistics
- Statistics related to HA transactions that have been processed
- Timestamp showing when the current period began
- The numerical identifier for the last redundant transaction processed (each transaction is numbered)

In an HA architecture that is functioning properly, the number for the last redundant transaction processed on a standby Oracle Communications Session Border

Controller peer should not be far behind (if not exactly the same as) the one shown for the active Oracle Communications Session Border Controller peer.

Several subcommands appear under the **show redundancy** command. Within this set of subcommands, system administrators can view information related to HA transactions, including specific transaction information.

The following example shows the subcommands available for the **show redundancy** command.

```
ORACLE# show redundancy ?
algd         MGCP Redundancy Statistics
collect      Collect Redundancy Statistics
config       Configuration Redundancy Statistics
iked         Iked Redundancy Statistics
manuald      Manuald Redundancy Statistics
mbcd         MBC Redundancy Statistics
radius-cdr   Radius CDR Redundancy Statistics
rec          SIPREC Redundancy Statistics
rotated-cdr  Rotated Radius CDR Redundancy Statistics
sipd         SIP Redundancy Statistics
```

HA Alarms

There are currently five alarms directly associated with the HA feature. A system alarm is triggered when any of the following HA conditions occurs:

- When the health score falls below 60. This is a hard-coded threshold value. It is not configurable.
- By the **Active-BecomingStandby** peer upon switchover.
- By the **Standby-BecomingActive** peer upon switchover.
- When the HA Oracle Communications Session Border Controller peer times out.
- When the standby system is unable to synchronize with its active Oracle Communications Session Border Controller peer within the amount of time set for the becoming standby time field of the redundancy element.

When certain alarms associated with the HA feature are triggered, traps are sent via the appropriate MIB (for example, syslog or system management). Traps for switchover alarms indicate that a switchover has occurred and identify the state transition of the HA Oracle Communications Session Border Controller reporting the switchover. For example:

- **Standby to BecomingActive**
- **BecomingStandby to BecomingActive**
- **Active to RelinquishingActive** and so on

In the case of an alarm from the **Standby to BecomingActive** peer, the associated trap also indicates the reason for switchover (as far as high availability is concerned). These reasons might include reporting the degraded health of the HA Oracle Communications Session Border Controller peer or indicating that the HA Oracle Communications Session Border Controller peer has timed out or that a switchover was forced by command.

The following table provides a list, by name, of the Oracle Communications Session Border Controller's HA-related alarms, including their alarm IDs, severities, causes, associated log messages, and actions.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
HEALTH SCORE	131101	MAJOR	System's health score fell below 60.	Health score X is under threshold (where X is the health score)	apSysMgmtGroupTrap
NAT TABLE UTILIZATION	131102	MINOR	NAT table usage reached 90% or greater of its capacity.	NAT table usage X% over threshold X%	apSysMgmtGroupTrap
ARP TABLE UTILIZATION	131103	MINOR	ARP table usage reached 90% or greater of its capacity.	ARP table X% over threshold X%	apSysMgmtGroupTrap
REDUNDANT SWITCH-TO-ACTIVE	131104	CRITICAL	A state transition occurred from Standby/ BecomingStandby to BecomingActive.	Switchover, <state to state>, active peer <name of HA peer> has timed out or Switchover, <state to state>, active peer <name of HA peer> has unacceptable health (x) (where x is the health score) or Switchover, <state to state>, forced by command	apSyslogMessageGenerated apSysMgmtRedundancyTrap
REDUNDANT SWITCH-TO-STANDBY	131105	CRITICAL	A state transition occurred from Active/ BecomingActive to BecomingStandby/ Relinquishing Active.	Switchover, <state to state>, peer <name of HA peer> is healthier (x) than us (x) (where x is the health score) or Switchover, <state to state>, forced by command	apSyslogMessageGenerated apSysMgmtRedundancyTrap

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
REDUNDANT TIMEOUT	131106	MAJOR	A HA system peer was not heard from within a time period.	Peer <name of HA peer> timed out in state x, my state is x (where x is the state (for example, BecomingStandby))	apSyslogMessageGenerated apSysMgmtRedundancyTrap
Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
REDUNDANT OUT OF SERVICE	131107	CRITICAL	Unable to synchronize with Active HA system peer within BecomingStandby timeout.	Unable to synchronize with Active redundant peer within BecomingStandby timeout, going OutOfService	apSyslogMessageGenerated apSysMgmtRedundancyTrap
CFG ALARM SAVE FAILED	393217	MAJOR	The save-config command execution failed on a standby Oracle Communications Session Border Controller peer operating as part of an HA pair.	save-config failed on targetName!/code full, config sync stopped! or save-config failed on targetName!/code full, config sync stopped! (where the targetName is the target name (tn) configured in the boot parameters)	apSyslogMessageGenerated trap generated syslog

Base Display Level

The base display level of the graphic display window on the front panel of the chassis shows the state of an HA Oracle Communications Session Border Controller. The base display appears when the Oracle Communications Session Border Controller first starts up and when the graphic display times out at any menu level.

System administrators can distinguish between an active SBC and a standby Oracle Communications Session Border Controller in an HA architecture by looking at the front of the chassis. The chassis operating as the standby Oracle Communications Session Border Controller in an HA architecture displays an (S) in the graphic display window to indicate its status as the standby system. The chassis operating as the active Oracle Communications

Session Border Controller in an HA architecture does not display anything in parentheses in the graphic display window.

HA State Display Stats

The chassis's graphic display window shows the current state of the HA Oracle Communications Session Border Controller using an abbreviation that follows the Oracle Communications Session Border Controller name. The states are defined in the following table.

State Abbreviation	Description
(I)	Initial (the Oracle Communications Session Border Controller is in this state when it is booting)
(O/S)	Out of service
(B/S)	Becoming standby
(S)	Standby
(nothing displayed after the Oracle Communications Session Border Controller name)	Active

Refer to the following sections for examples of the graphic display window output.

Initial State Displays

The following example shows the output in the graphic display window of a Oracle Communications Session Border Controller in the initial state:

```
NET - NET
SESSION DIRECTOR (I)
```

Out Of Service State Displays

The following examples show the output in the graphic display window of an out-of-service Oracle Communications Session Border Controller:

```
NET - NET
SESSION DIRECTOR (O/S)
```

Becoming Standby State Displays

The following example shows the output in the graphic display window of a Oracle Communications Session Border Controller becoming standby:

```
NET - NET
SESSION DIRECTOR (B/S)
```

Standby State Displays

The following example shows the output in the graphic display window of a standby Oracle Communications Session Border Controller:

```
NET - NET
SESSION DIRECTOR (S)
```

Active State Displays

HA Oracle Communications Session Border Controllers in the active state use the default graphic display. The following example show the display of an active Oracle Communications Session Border Controller.

```
ACME PACKET
SESSION DIRECTOR
```

For further information about the Oracle Communications Session Border Controller chassis and graphic display window, refer to the Oracle Communications Session Border Controller Installation Guide.

ARP Functionality

You can use the following command to view ARP functionality information:

- **arp-check**
- **show arp**

Testing Address Resolution

Test a specific address resolution by using the **arp-check** command; which causes a a test message to be sent. The test is successful when an OK is returned. Note that the command does not send an ARP request if the specified address is already in the ARP table or is in a different subnet.

To run this test, you must enter the following information after typing arp-check and a Space:

- media interface slot (either of two values: 1 is for the left, and 2 is for the right)
- VLAN identifier

> **Note:**
>
> If there is no VLAN identifier to be entered, enter a value of 0.

- IPv4 address (in dotted notation).

For example:

```
ORACLE# arp-check 1 6 192.168.100.1
ARP: Sending  ARP REQ port=0, vlan=6, source_ipa=192.168.200.10,
target_ipa=192.168.100.1
ORACLE#
```

Viewing Current Address Mappings

Display the current Internet-to-Ethernet address mappings in the ARP table by using the **show arp** command. The first section of this display shows the following information: destination, gateway, flags, reference count, use, and interface. The second section shows the interface, VLAN, IP address, MAC address, timestamp, and type.

The intf (interface) column in the ARP includes both slot and port information. If a value of 0/1 appears, 0 refers to the slot and 1 refers to the port. For example:

```
ORACLE# show arp
LINK LEVEL ARP TABLE
destination      gateway            flags  Refcnt  Use
Interface
-----------------------------------------------------------------------
--
172.30.0.1       00:0f:23:4a:d8:80  405    1       0
wancom0
-----------------------------------------------------------------------
--
                Total ARP Entries = 3
                -----------------------
Intf  VLAN     IP-Address             MAC          time-stamp   type
 0/0    0   010.000.045.001     00:00:00:00:00:00  1108462861  invalid
Special Entries:
 0/0    0   000.000.000.000     00:00:00:00:00:00  1108462861  gateway
 0/0    0   010.000.045.000     00:00:00:00:00:00  1108462861  network
Gateway Status:
Intf  VLAN     IP-Address           MAC          time-stamp hb status
 0/0    0   010.000.045.001  00:00:00:00:00:00  1108462861
unreachable
-- ARP table info --
Maximum number of entries  : 512
Number of used entries     : 3
Length of search key       : 1 (x 64 bits)
First search entry address : 0x3cb0
length of data entry       : 2 (x 64 bits)
First data entry address   : 0x7960
Enable aging               : 0
Enable policing            : 0
```

ARP Table Utilization Alarm

The following table describes the ARP table utilization alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
ARP TABLE UTILIZATION	131103	MINOR	ARP table usage reached 90% or greater of its capacity.	ARP table X% over threshold X%	apSysMgmtGroupTrap trap generated syslog

Local Policy

Use the following commands to view local policy statistics and information:

- **show running-config local-policy**
- **show configuration local-policy**

Viewing Running Configuration Local Policy

Display information about the local policy in the running configuration information in use on the system by using the **show running-config local-policy** command. For example:

```
ORACLE# show running-config local-policy
local-policy
        from-address
                                       192.168.0.50
        to-address
                                       10.10.10.10
        source-realm                   *
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                urgent
        last-modified-date             2006-06-12 08:48:57
        policy-attribute
                next-hop                       172.168.0.10
                realm
                action                         none
                terminate-recursion            enabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol
                state                          enabled
                media-profiles
task done
```

Viewing Current Configuration Local Policy

Display information about the local policy in the current configuration that will be used once the **activate-config** command is executed by using the **show configuration** command. For example:

```
ORACLE# show configuration local-policy
ORACLE# show running-config local-policy
local-policy
        from-address
                                       192.168.0.50
        to-address
                                       10.10.10.10
        source-realm                   *
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                urgent
        last-modified-date             2006-06-12 08:48:57
        policy-attribute
                next-hop                       172.168.0.10
                realm
                action                         none
                terminate-recursion            enabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol
                state                          enabled
                media-profiles
task done
```

Session and Protocol Statistics

You can use the following commands to access protocol tracing statistics:

- **notify**
- **monitor sessions**

Viewing Runtime Protocol Tracing

Display information about runtime protocol tracing for UDP/ TCP sockets by using the **notify** command. This command provides information for all protocol messages for ServiceSocket sockets to be written in a log file or sent out of the system to a UDP port.

This mechanism allows for tracing to be enabled for any socket, provided that the class has a logit method for displaying and formatting the protocol message. All ACP classes and SIP supports this. Tracing can be enabled for all processes, specific sockets, all sockets, or specific processes. Tracing for specific sockets is specified by the local IPv4 or IPv6 address and port on which the socket is connected.

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

The <socket-address> is the IPv4 or IPv6 address and the port on which the socket is connected. The <out-udp-port> is the UDP IPv4 or IPv6 address and port to which the log messages are sent. If the <out-udp-port> is not specified, the logs are written to the <filename>.

Viewing Real-Time SIP Session Statistics

If you have Superuser access, you can display real-time SIP session statistics by using the **monitor sessions** command. For example:

```
ORACLE# monitor sessions
09:10:26-172
SIP Status                -- Period -- -------- Lifetime --------
                Active    High   Total      Total  PerMax    High
Sessions             0       0       0          0       0       0
Subscriptions        0       0       0          0       0       0
Dialogs              0       0       0          0       0       0
CallID Map           0       0       0          0       0       0
Rejections           -       -       0          0       0
ReINVITEs            -       -       0          0       0
Media Sessions       0       0       0          0       0       0
Media Pending        0       0       0          0       0       0
Client Trans         0       0       0          0       0       0
Server Trans         0       0       0          0       0       0
Resp Contexts        0       0       0          0       0       0
Saved Contexts       0       0       0          0       0       0
Sockets              0       0       0          0       0       0
Req Dropped          -       -       0          0       0
DNS Trans            0       0       0          0       0       0
DNS Sockets          0       0       0          0       0       0
DNS Results          0       0       0          0       0       0
```

Real-time statistics for the following categories appear on the screen:

- Dialogs
- Sessions
- CallID Map
- Rejections
- ReINVITES
- Media Sessions
- Media Pending
- Client Trans
- Server Trans

- Resp Contexts
- Sockets
- Reqs Dropped
- DNS Trans
- DNS Sockets
- DNS Results

By default, the statistics refresh every second. Press any numerical digit (0-9) to change the refresh rate. For example, while viewing the statistics, you can press <6> to cause the system statistics to refresh every 6 seconds.

Pressing <q> or <Q> allows you to exit the statistics display and returns you to the ACLI system prompt.

Media and Bandwidth Statistics

You can use the following commands to display media and bandwidth statistics:

- **show mbcd errors**
- **show mbcd realms**
- monitor media

Viewing MBCD Task Errors

Display Middle Box Control Daemon (MBCD) task error statistics by using the **show mbcd errors** command. There are two categories of MBCD error statistics: Client and Server.

For example:

```
ORACLE# show mbcd errors
16:19:18-139
MBC Errors                     ---- Lifetime ----
                        Recent      Total  PerMax
Client Errors                0          0       0
Client IPC Errors            0          0       0
Open Streams Failed          0          0       0
Drop Streams Failed          0          0       0
Exp Flow Events              0          0       0
Exp Flow Not Found           0          0       0
Transaction Timeouts         0          0       0
Server Errors                0          0       0
Server IPC Errors            0          0       0
Flow Add Failed              0          0       0
Flow Delete Failed           0          0       0
Flow Update Failed           0          0       0
Flow Latch Failed            0          0       0
Pending Flow Expired         0          0       0
ARP Wait Errors              0          0       0
Exp CAM Not Found            0          2       2
Drop Unknown Exp Flow        0          0       0
Drop/Exp Flow Missing        0          0       0
```

```
Exp Notify Failed            0          0       0
Unacknowledged Notify        0          0       0
Invalid Realm                0          5       5
No Ports Available           0          0       0
Insufficient Bandwidth       0          0       0
Stale Ports Reclaimed        0          0       0
Stale Flows Replaced         0          0       0
Pipe Alloc Errors            0          0       0
Pipe Write Errors            0          0       0
```

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
- Open Streams Failed—Number of errors related to sending Add or Modify requests to MBCD
- Drop Streams Failed—Number of errors related to sending Subtract requests to MBCD
- 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
- 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—This statistic shows the 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 from the NP
- 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
- 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. Also includes when a flow for a Subtract request to MBCD cannot be found

- 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

Viewing Steering Port and Bandwidth Usage

Display steering ports and bandwidth usage for home, public, and private realms by using the **show mbcd realms** command.

For example:

```
acmepacket# show mbcd realms
18:26:39-1629
             --- Steering Ports ---  ----------- Bandwidth Usage
----------
Realm         Used   Free  No Ports    Flows Ingrss Egress  Total
Insuf BW
acme             0      0         0        0     0K     0K
0K         0
h323172          2  29999         0        0     0K     0K
0K         0
sip172           2  29999         0        0     0K     0K
0K         0
sip192           0  30001         0        0     0K     0K
0K         0
```

Information in the following categories is displayed:

- 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
- Ingrss—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

Viewing Real-Time Media Monitoring Statistics

If you have Superuser access, you can display real-time media monitoring statistics by using the **monitor media** command. For example:

```
acmepacket# monitor media
17:31:00-160
MBCD Status                -- Period -- -------- Lifetime --------
                 Active    High   Total      Total  PerMax    High
Client Sessions     143     182    1930    1218332    4225     683
Client Trans          0      18    5744    2500196    8439     625
Contexts            144     182    1930     834745    2783    2001
Flows               296     372    3860    1669498    5566    3689
Flow-Port           286     362    3860    1669488    5566    3679
Flow-NAT            294     365    3788    1658668    5563    2051
Flow-RTCP             0       0       0          0       0       0
Flow-Hairpin          0       0       0          0       0       0
Flow-Released         0       0       0          0       0       0
MSM-Release           0       0       0          0       0       0
Rel-Port              0       0       0          0       0       0
Rel-Hairpin           0       0       0          0       0       0
NAT Entries         295     365    3791    1658671    5563    2051
Free Ports         7430    7518    7828    3346410   11604    8002
Used Ports          572     724    7724    3338980   11132    8000
Port Sorts            -       -       0      14796    4156
MBC Trans          1141    1234    5748    2503147    8440    2974
MBC Ignored           -       -       0          0       0
ARP Trans             0       0       0          8       8       1
```

Real-time statistics for the following categories appear on the screen:

- Client Sessions
- Client Trans
- Contexts
- Flows
- Flow-Port
- Flow-NAT
- Flow-RTCP
- Flow-Hairpin
- Flow-Release
- MSM-Release
- NAT Entries
- Free Ports
- Used Ports
- Port Sorts
- MBC Trans

- MBC Ignored
- ARP Trans

By default, the statistics refresh every second. Press any numerical digit (0-9) to change the refresh rate. For example, while viewing the statistics, you can press <6> to cause the system statistics to refresh every 6 seconds.

Pressing <q> or <Q> allows you to exit the statistics display and returns you to the ACLI system prompt.

Media Alarms

The following table describes the Media alarms:

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
MBCD ALARM OUT OF MEMORY	262145	CRITICAL: for flow MAJOR: for media (if server cannot allocate a new context)	No further memory can be allocated for MBCD.	Flow: Cannot create free port list for realm. Media Server: Failed to allocate new context.	apSyslogMessageGenerated(ap-slog.mib) apSysMgmtMediaOutofMemory
MBCD ALARM UNKNOWN REALM	262147	MAJOR: if media server is adding a new flow	Media server is unable to find realm interface.	Realm type (ingress, egress, hairpin) X, not found	apSyslogMessageGenerated(ap-slog.mib) apSysMgmtUnknownRealm
MBCD ALARM OUT OF BANDWIDTH	262149	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of bandwidth.	Out of bandwidth	apSyslogMessageGenerated(ap-slog.mib) apSysMgmtMediaBandwidthTrap
MBCD ALARM OUT OF PORTS	262150	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of steering ports.	Out of steering ports	apSyslogMessageGenerated(ap-slog.mib) apSysMgmtMediaPortsTrap

System Problem Statistics

Packet Tracing

When you enable packet tracing (using the **packet-capture** configuration and related ACLI commands), the Oracle Communications Session Border Controller can mirror any communication between two endpoints, or between itself and a specific endpoint. To accomplish this, the Oracle Communications Session Border Controller replicates the packets sent and received, and can then send them to a trace server that you designate. Using the trace server, you can display the packets on software protocol analyzer. Currently, the Oracle Communications Session Border Controller supports:

- One configurable trace server (on which you have installed your software protocol analyzer)
- Sixteen concurrent endpoint traces

For more information about how to set up packet tracing, refer to the Oracle Communications Session Border Controller ACLI Configuration Guide.

You can see statistics for packet traces initiated on the Oracle Communications Session Border Controller by using the **show packet-trace** command. The display shows you a summary of the active packet traces on the Oracle Communications Session Border Controller. Displayed information includes: the IP address, local and remote port (which displays as 0 if no ports have been designated), slot, port, and VLAN.

```
ORACLE# show packet-trace
IP Address      Local-Port  Remote-Port  Slot Port   VLAN
---------------------------------------------------------
192.168.10.1          0            0        0    1      0
192.168.10.99      5060         5060        0    1      0
10.0.0.1             23            0        1    0      0
```

Capturing and Viewing Packets

You can capture and view packets for debugging purposes by using the **packet-capture** command. For example, if you detect an issue with the system flows, you can capture certain packets so that you can resolve the problem. Using this command, you can examine the packets in question and then perform any debugging that might be necessary.

When you use packet-capture, you work with the following subcommands:

- **packet-capture enable**
- **packet-capture show**
- **packet-capture detail**

Use the **packet-capture enable** command to enable packet-capture before using it. Because enabling this function uses system resources that should otherwise be kept free, you should enable it only when you need it and then disable it when you finish debugging.

Use the **packet-capture show** command to view a summary of the most recently captured packets, including the following:

- ingress interface
- frame format
- type/length
- VLAN identifier
- source IPv4 or IPv6 address
- destination IPv4 or IPv6 address
- protocol
- source port
- destination port

For example:

```
acmepacket# packet-capture show
Entry Ingress  Format Length VLAN-ID  Src-IP Dest-IP Prot Src-Port
Dest-Port
    1     1/0 unknown 0x0026       -      -       -    -
-        -
    2     1/0 unknown 0x0026       -      -       -    -
-        -
    3     1/0 unknown 0x0026       -      -       -    -
-        -
    4     1/0 unknown 0x0026       -      -       -    -
-        -
    5     1/0 unknown 0x0026       -      -       -    -
-        -
    6     1/0 unknown 0x0026       -      -       -    -
-        -
    7     1/0 unknown 0x0026       -      -       -    -
-        -
    8     1/0 unknown 0x0026       -      -       -    -
-        -
    9     1/0 unknown 0x0026       -      -       -    -
-        -
   10     1/0 unknown 0x0026       -      -       -    -
-        -
   11     1/0 unknown 0x0026       -      -       -    -
-        -
   12     1/0 unknown 0x0026       -      -       -    -
-        -
   13     1/0 unknown 0x0026       -      -       -    -
-        -
   14     1/0 unknown 0x0026       -      -       -    -
-        -
   15     1/0 unknown 0x0026       -      -       -    -
-        -
   16     1/0 unknown 0x0026       -      -       -    -
-        -
   17     1/0 unknown 0x0026       -      -       -    -
-        -
```

Use the **packet-capture detail** command to view the details of a particular packet, including: the ingress interface, MAC source address, MAC destination address, VLAN identifier, and the length/type. For example:

```
acmepacket# packet-capture detail 30
Ingress Slot/Port: 1/0
FF FF FF FF FF FF 00 0D 28 74 A2 01 08 00
45 00 00 4C 08 E9 00 00 40 11 61 18 AC 10 64 90 FF FF FF FF
00 7B 00 7B 00 38 00 00
1B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00

DIX header ---
MAC Src Addr       : 0x FF FF FF FF FF FF
MAC Dest Addr      : 0x 00 0D 28 74 A2 01
VLAN ID            : 0x XX
Length/Type        : 0x 0800

IP Header ---
IP Version          : 4
IP Header Length    : 5
Type-of-Service     : 0
Total Length        : 76
Identificaton       : 2281
Flags               : 0
Fragment Offset     : 0
Time-to-Live        : 64
protocol            : 17
Header Checksum     : 0x6118
Source IP Addr      : 172.16.100.144
Destination IP Addr : 255.255.255.255

UDP Header ---
Source Port         : 123
Destination Port    : 123
Length              : 56
Checksum            : 0x0000
```

System ACLs

This section provide information about system ACL removal, and about viewing system ACL statistics and configurations.

Notes on Deleting System ACLs

If you delete a system ACL from your configuration, the Oracle Communications Session Border Controller checks whether or not there are any active SFTP or SSH client was granted access when the entry was being removed. If such a client were active during ACL removal, the Oracle Communications Session Border Controller would warn you about the condition and ask you to confirm the deletion. If you confirm the deletion, then the Oracle Communications Session Border Controller’s session with the active client is suspended.

The following example shows you how the warning message and confirmation appear. For this example, and ACLI has been deleted, and the user is activating the configuration that reflects the change.

```
ORACLE # activate-config
Object deleted will cause service disruption:
 system-access-list: identifier=172.30.0.24
 ** WARNING: Removal of this system-ACL entry will result
             in the lockout of a current SFTP client
Changes could affect service, continue (y/n) y
Activate-Config received, processing.
```

Viewing System ACL Configurations

The **system-access-list** configuration has been added to the list of configurations you can display using the show configuration and show running-config ACLI commands. It will display each system ACL entry.

```
ORACLE# show running-config system-access-list
system-access-list
        dest-address                   165.31.24.2
        netmask                        225.225.0.0
        last-modified-date             2007-04-30 13:00:02
system-access-list
        dest-address                   175.12.4.2
        netmask                        225.225.225.0
        last-modified-date             2007-04-30 13:00:21
task done
```

Viewing System ACL Statistics

You can display statistics for system ACLs using the **show ip stats** ACLI command. Two new entries have been added to let you see the total number of ACL denials and the last ACL denial the Oracle Communications Session Border Controller made.

```
ORACLE# show ip stats
               total            3170
              badsum               0
            tooshort               0
            toosmall               0
             badhlen               0
              badlen               0
         infragments               0
         fragdropped               0
         fragtimeout               0
             forward               0
         fastforward               0
         cantforward              14
        redirectsent               0
     unknownprotocol               0
           delivered            1923
            localout             855
           nobuffers               0
         reassembled               0
          fragmented               0
        outfragments               0
            cantfrag               0
          badoptions               0
             noroute               0
             badvers               0
              rawout               0
             toolong               0
           notmember               0
               nogif               0
             badaddr               0
         acl-denials            1233
   last-srcip-denied    174.35.60.72
ORACLE#
```

Wancom Port Speed and Duplex Mode Display

You can display the negotiated duplex mode and speed for all system control ports by using the ACLI **show wancom** command. This command allows you to diagnose network issues more efficiently.

When you use this command, the systems shows information for all three control ports with the numbers starting at 0. It will then tell you the negotiated duplex mode and speed, or that the link is down.

To display negotiated duplex mode and speed for control interfaces:

- At the user prompt, type the ACLI **show wancom** command and press Enter.

```
ORACLE> show wancom
wancom [unit number 0]:
Duplex Mode: half
Speed: 100 Mbps
wancom [unit number 1]:
Link down
wancom [unit number 2]:
Link down
```

Application Faults

This section contains information about application fault statistics. This category of alarm accounts for problems related to applications (protocols).

- H.323
- SIP
- RADIUS and Diameter

Application alarms do not display an alarm message in the graphic display window on the front panel of the chassis.

H.323 Statistics

You can use the following command to display H.323 statistics:

- **show h323d**

There is also an alarm that occurs when stack initialization fails.

Viewing H.323 Statistics

Display H.323 statistics by using the **show h323d** command.

For example:

```
acmepacket# show h323d
18:32:26-86
Session Stats                        -- Period --  -------- Lifetime
-------
                           Active    High   Total      Total
PerMax    High
Incoming Calls                  5       5       1         18
6       5
Outgoing Calls                  1       1       1         18
6       2
Connected Calls                 1       1       1          8
2       1
Incoming Channels               2       2       2         17
4       2
Outgoing Channels               2       2       2         17
4       2
Contexts                        5       5       1         18
6       5
H323D Status     Current   Lifetime
Queued Messages        1       1608
TPKT Channels          5        404
UDP Channels           0          0
Stack                State    Type Mode       Registered Gatekeeper
h323172              enabled  H323 Gateway    No
```

In the first display section, the following statistics are displayed for period and lifetime durations in addition to an active count.

- Incoming Calls—Number of incoming H.323 calls.
- Outgoing Calls—Number of outgoing H.323 calls.
- Connected Calls—Number of currently connected H.323 calls.
- Incoming Channels—Number of established incoming channels.
- Outgoing Channels—Number of established outgoing channels.
- Contexts—Number of established H.323 contexts.

In the second section, the following statistics are displayed for current and lifetime durations.

- Queued Messages—Number of messages queued.
- TPKT Channels—Number of TPKT channels open(ed).
- UDP Channels—Number of UDP channels open(ed).

H.323 Stack Initialization Failure Alarm

The following table provides information about the H.323 ALARM STACK INITIALIZATION FAILURE application alarm, which is triggered by the failure of an H.323 stack to initialize properly.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
H.323 ALARM STACK INITIALIZATION FAILURE	327682	CRITICAL	The H.323 stack has failed to initialize properly and is terminated.	[H.323 | IWF] stack <stack-name> has failed to initialize and is terminated	apSyslogMessageGenerated trap generated critical dry contact syslog

H.323 Monitoring Stack Alarm

- Viewing the number of active calls—You can see the number of active calls using the **show h323 stack call** command at either the User or Superuser prompt.You can also access this information with an SNMP query.
- Viewing alarm information—Two ACLI commands allow you to view alarm information, but they provide different information:
  - **display-alarms**—This command shows alarm the most recently generated by an H.323 stack and the total number of stack monitoring alarms the Oracle Communications Session Border Controller has generated. Since alarms can fire simultaneously, the alarm you can see using this command will only be the most recent one.

```
ORACLE# display-alarms
1 alarms to show
ID       Task      Severity       First Occurred          Last Occurred
327694   462796192       3       2009-06-03 18:51:46     2009-10-03
18:51:46
Count    Description
2        current calls are over critical threshold of 50 percent.
Total no
         of h323 stack alarm generated are 2
```

  - **show h323 stack stack-alarms**—This command refers to specific stacks by stack name, and provides shows the alarm severity and the current percentage of max-calls that triggered the alarm. The Oracle Communications Session Border Controller keeps track of how many alarms are raised by each stacks, and the severity of each of those alarms. When the alarm clears, the information relating to it is erased from the display.

```
ORACLE# show h323 stack stack-alarms
Stack-Name   Alarm-Severity   %Max-Call
external     minor            50
internal     critical         50
```

SIP Statistics

You can use the following commands to view SIP statistics:

- **show sipd errors**
- **show processes sipd**

- **show registration**

Viewing SIP Errors

Display SIP error statistics by using the **show sipd errors** command. For example:

```
ORACLE# show sipd errors
11:34:13-194
SIP Errors/Events             ---- Lifetime ----
                       Recent      Total  PerMax
SDP Offer Errors            0          0       0
SDP Answer Errors           0          0       0
Drop Media Errors           0          0       0
Transaction Errors          0          0       0
Application Errors          0          0       0
Media Exp Events            0          0       0
Early Media Exps            0          0       0
Exp Media Drops             0          0       0
Expired Sessions            0          0       0
Multiple OK Drops           0          0       0
Multiple OK Terms           0          0       0
Media Failure Drops         0          0       0
Non-ACK 2xx Drops           0          0       0
Invalid Requests            0          0       0
Invalid Responses           0          0       0
Invalid Messages            0          0       0
CAC Session Drop            0          0       0
CAC BW Drop                 0          0       0
```

Viewing SIP Processes

Display statistics about SIP processes by using the **show processes sipd** command. For example:

```
ORACLE# show processes sipd
11:34:49-130 (sipd) ID=1b89dfd0
Process Status           -- Period -- -------- Lifetime --------
               Active    High   Total      Total  PerMax    High
Services            5       5       0          5       5       5
Messages            0       0       0          6       4       3
Transactions        0       0       0          0       0       0
Timed Objects       7       7       0         14      11       9
Total Buffers       5       5       0          5       5       5
Alloc Buffers       3       3       0          7       4       5
Memory Chunks      48      48       0         82      79      50
TOQ Entries         2       2      14      58301      19       4
Operations                         14      52997      12
Messages Received                   0          3       2
Messages Sent                       4      17681      30
Partial Message                     0          0       0
Partial Msg Expired                 0          0       0
Partial Msg Dropped                 0          0       0
Timed Events                       14      58291      12
Alarms                              0          0       0
```

```
System Logs                         4      17681      32
Process Logs                        4      17684      35
Load Rate                         0.0                0.0
CPU Usage                 0.0              8.133/529935
```

Viewing IP Session Replication for Recording (SRR) Information

The **show call-recording-server** command displays information regarding the IP call recording feature configured on the Oracle Communications Session Border Controller. Entering this command without the optional call recording server (CRS) ID displays all CRS endpoints configured on the Oracle Communications Session Border Controller along with their state.

You can specify a CRS whose information you want to view. When you specify an ID, the ACLI displays all session agents created for the CRS endpoint, its IP address, its state, and the last time a failover occurred. For example:

Viewing SIP Registration Cache Status

Display SIP registration cache status by using the show registration command. The display shows statistics for the Period and Lifetime monitoring spans.

- Cached Entries—Number of registration entries for the address of record
- Local Entries—Number of entries for Contact messages sent to a real registrar.
- 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

For example:

```
ORACLE# show registration
11:38:57-177
SIP Registrations          -- Period -- -------- Lifetime --------
                 Active    High   Total      Total  PerMax    High
User Entries          0       0       0          0       0       0
Local Contacts        0       0       0          0       0       0
Via Entries           0       0       0          0       0       0
AURI Entries          0       0       0          0       0       0
Free Map Ports        0       0       0          0       0       0
Used Map Ports        0       0       0          0       0       0
Forwards              -       -       0          0       0
Refreshes             -       -       0          0       0
Rejects               -       -       0          0       0
Timeouts              -       -       0          0       0
Fwd Postponed         -       -       0          0       0
Fwd Rejected          -       -       0          0       0
Refr Extension        0       0       0          0       0       0
Refresh Extended      -       -       0          0       0
Surrogate Regs        0       0       0          0       0       0
Surrogate Sent        -       -       0          0       0
Surrogate Reject      -       -       0          0       0
Surrogate Timeout     -       -       0          0       0
HNT Entries           0       0       0          0       0       0
Non-HNT Entries       0       0       0          0       0       0
```

SIP NSEP Statistics

To view statistics related to the NSEP feature, the ACLI **show** command has been expanded. It now allows you to see all of the statistics for NSEP support, to see them for a specific r-value (namespace and r-priority combination), or to see all of these. You can also reset the NSEP statistics counters.

When you use the ACLI **show nsep-stats** command without further arguments, the system shows you information for inbound sessions.

To display general NSEP statistics for inbound sessions:

- Type **show nsep-stats** and press Enter.

```
ORACLE# show nsep-stats
                          ------- Lifetime---------
                         Current      Total  PerMax
Inbound Sessions               0          0       0
```

NSEP Statistics per R-Value Display

You can see statistics for specific r-value by entering it with the **show nsep-stats** command. An r-value is a namespace and priority combination entered in the following format: namespace.priority. The display will also show the specified r-value for which it is displaying data.

To display general NSEP statistics for specific r-values:

- Type **show nsep-stats**, a Space, and then the r-value for which you want to display statistics. Then press Enter.

```
ORACLE# show nsep-stats ets.2
RValue = ets.2
                                    -- Period -- -------- Lifetime
--------
                          Active    High   Total      Total
PerMax    High
Incoming Sessions              0       0       0          0
0       0
Outgoing Sessions              0       0       0          0
0       0
InbSessions Rej                -       -       0          0
0       -
OutbSessions Rej               -       -       0          0
0       -
```

You can see the full set of statistics for NSEP inbound sessions and for all r-values by using the **show nsep-stats all** command. The display for r-values is divided into individual sections for each r-value shown.

To display general NSEP statistics for specific r-values:

- Type **show nsep-stats all** and press Enter.

```
ORACLE# show nsep-stats all
Session Stats
                          ------- Lifetime---------
                         Current      Total  PerMax
Inbound Sessions               0          0       0
Per RValue Stats
                                    -- Period -- -------- Lifetime
--------
                          Active    High   Total      Total  PerMax
High
RValue = ets.2
Incoming Sessions              0       0       0          0       0
0
Outgoing Sessions              0       0       0          0       0
0
InbSessions Rej                -       -       0          0       0
-
OutbSessions Rej               -       -       0          0       0
-
RValue = ets.5
Incoming Sessions              0       0       0          0       0
0
Outgoing Sessions              0       0       0          0       0
0
InbSessions Rej                -       -       0          0       0
-
OutbSessions Rej               -       -       0          0       0
-
```

Viewing NSEP Burst Statistics for SIP Session Agents

The ACLI **show sipd** command supports an **sa-nsep-burst** argument that displays the NSEP burst rate for all SIP session agents.

```
ORACLE# show sipd sa-nsep-burst
Agent             Current Rate            Lifetime High
192.168.1.139        0                       0
192.168.1.6          0                       0
192.168.200.135      4                       10
```

Resetting NSEP Statistics

You can reset the statistics for incoming sessions, for an individual r-value, or for the entire set of NSEP data. You use the same command syntax as you do when showing the statistics, except that you start your entry with the **reset** command.

In the example below, the command resets the statistics counters for the specific r-value ets.2.

To reset the counters for a specific r-value:

- For the set of statistics you want to reset, type **reset nsep-stats** and then the group that you want to reset. The press Enter.

  ```
  ORACLE# reset nsep-stats ets.2
  ```

  To reset the counters for all NSEP statistics:

- For the set of statistics you want to reset, type **reset nsep-stats** and then press Enter.

  ```
  ORACLE# reset nsep-stats
  ```

Viewing SIP Method Throttling Mechanism Statistics

You can monitor the SIP method throttling mechanism statistics for either a specific SIP interface or a session agent.

To display SIP method throttling mechanism statistics for a SIP interface:

- Type **show sipd interface**, a Space, and then the SIP interface’s name and the SIP method name for which you want statistics. Then press Enter.

  ```
  ORACLE# show sipd interface net1 NOTIFY
  NOTIFY (15:53:42-57)
                        --------- Server --------   --------- Client
  --------
  Message/Event         Recent      Total  PerMax   Recent
  Total  PerMax
                        ------  ---------  ------   ------
  ---------  ------
  NOTIFY Requests            0         49      19        0
  0       0
  Retransmissions            0          0       0        0
  0       0
  100 Trying                 0         49      19        0
  0       0
  180 Ringing                0         38      19        0
  0       0
  200 OK                     0         38      19        0
  0       0
  503 Service Unavail        0         11      11        0
  0       0
  Response Retrans           0          9       5        0
  0       0
  Transaction Timeouts       -          -       -        0
  0       0
  Locally Throttled          -          -       -        0
  0       0
  Avg Latency=0.000 for 0
  ```

```
Max Latency=0.000
BurstRate Incoming=11 Outgoing=0
```

To display SIP method throttling mechanism statistics for a session agent:

- Type show sipd agents, a Space, and then the session agent IP address and the SIP method name for which you want statistics. Then press Enter.

```
ORACLE# show sipd agents 198.167.1.60 NOTIFY
NOTIFY (15:53:34-49)
                      --------- Server --------   --------- Client
--------
Message/Event         Recent      Total  PerMax   Recent      Total
PerMax
                      ------  ---------  ------   ------  ---------
------
NOTIFY Requests            0         50      31        0          0
0
Retransmissions            0          3       3        0          0
0
200 OK                     0         25      18        0          0
0
503 Service Unavail        0         25      24        0          0
0
Transaction Timeouts       -          -       -        0          0
0
Locally Throttled          -          -       -        0         24
24
Avg Latency=0.000 for 0
Max Latency=0.000
BurstRate Incoming=5 Outgoing=0
```

Viewing SIP IP CAC Statistics

You can display CAC parameters for an IP address using the **show sipd ip-cac** command. For example:

```
ORACLE# show sipd ip-cac 192.168.200.191
CAC Parameters for IP <192.168.200.191>
 Allowed Sessions=2
 Active-sessions=0
 Allowed Bandwidth=3000000
 used-bandwidth=0
```

Viewing SIP PUBLISH Statistics

You can display statistics related to incoming SIP PUBLISH messages using the show sipd publish command. For example:

```
summer# show sipd publish
PUBLISH (10:26:43-199)
                      --------- Server --------   --------- Client --------
Message/Event         Recent      Total  PerMax   Recent      Total  PerMax
```

```
                      ------  ---------  ------   ------  ---------
------
PUBLISH Requests           1          1       1        0
0       0
Retransmissions            0          0       0        0
0       0
405 Not Allowed            1          1       1        0
0       0
Transaction Timeouts       -          -       -        0
0       0
Locally Throttled          -          -       -        0
0       0
```

RADIUS Statistics

The ACLI **show radius** command, used with the three arguments described in this section, displays the status of any established RADIUS accounting connections and authentications. A working RADIUS connection displays READY, and a disabled connection displays DISABLED.

There is also an alarm that occurs when the RADIUS connection is down.

Viewing RADIUS Statistics

The **show radius** command can take one of the three available arguments:

- **authentication**—Shows authentication statistics for primary and secondary RADIUS servers, including: server IP address and port; round trip time; information about failed and successful requests/authentications; number of rejections; number of challenges; number of time-outs, number of retransmissions
- **accounting**—Shows the information described in the following table:

Section	Description
Client Display	General accounting setup (as established in the accounting configuration element), including: Information about the state of the RADIUS client Accounting strategy used (Hunt, Failover, RoundRobin, FastestRTT, or FewestPending) IP address and port on which the server is listening Maximum message delay in seconds Number of configured accounting servers
Waiting Queue	Amount of accounting (RADIUS) messages waiting to be sent. Waiting queue capacity is 4,096 messages.
<IP Address:Port>	Information about each configured accounting server (established in the accounting servers configuration). The heading above each accounting server section is the IPv4 address and port combination of the accounting server described. This section also includes information about the accounting server's state (e.g., Connect_Attempt, INIT).

- **all**—Shows all of the information for both the authentication and accounting displays

The following is an example of the **show radius authentication** command output.

```
ORACLE# show radius authentication
Active Primary Authentication Servers:
   server ipAddr: 172.30.0.7
Active Secondary Authentication Servers:
   server ipAddr: 172.30.0.8
Authentication Statistics:
        Server:"172.30.0.7:1812"
                RoundTripTime          :0
                MalformedAccessResponse:0
                AccessRequests         :2
                BadAuthenticators      :0
                AccessRetransmissions  :5
                AccessAccepts          :0
                Timeouts               :6
                AccessRejects          :0
                UnknownPDUTypes        :0
AccessChallenges       :0
        Server:"172.30.0.8:1812"
                RoundTripTime          :0
                MalformedAccessResponse:0
                AccessRequests         :2
                BadAuthenticators      :0
                AccessRetransmissions  :9
                AccessAccepts          :0
                Timeouts               :10
                AccessRejects          :0
                UnknownPDUTypes        :0
                AccessChallenges       :0
```

The following is an example of the **show radius accounting** command output.

ORACLE# **show radius accounting**

```
*********Client Display Start************
Client State = READY, strategy=Hunt
listening on 127.0.0.1:1813
max message delay = 60 s, # of servers = 2
================= Waiting Queue ================
Waiting size = 89
================================================
------------------ 10.0.0.189:1813 ------------------
Remote = 10.0.0.189:1813, Local = 0.0.0.0:1026, sock=45 (BOUND)
conn state=READY, RTT=250 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.582, Restart
delay=30 s
------------------ 192.168.200.70:5050 ------------------
Remote = 192.168.200.70:5050, Local = 0.0.0.0:1027, sock=46 (BOUND)
conn state=DISABLED, RTT=0 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.569, Restart
delay=30 s
*********Client Display End************
```

The following is an example of the **show radius all** command output.

```
ORACLE# show radius all
*********Client Display Start************
Client State = READY, strategy=Hunt
listening on 127.0.0.1:1813
max message delay = 60 s, # of servers = 2
================= Waiting Queue ================
Waiting size = 89
================================================
----------------- 10.0.0.189:1813 ------------------
Remote = 10.0.0.189:1813, Local = 0.0.0.0:1026, sock=45 (BOUND)
conn state=READY, RTT=250 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.582,
Restart delay=30 s
----------------- 192.168.200.70:5050 ------------------
Remote = 192.168.200.70:5050, Local = 0.0.0.0:1027, sock=46 (BOUND)
conn state=DISABLED, RTT=0 ms
Min Rtt=250 ms, Max inactivity=60 s, expires at Nov 21 13:50:19.569,
Restart delay=30 s
*********Client Display End************
Active Primary Authentication Servers:
   server ipAddr: 172.30.0.7
Active Secondary Authentication Servers:
   server ipAddr: 172.30.0.8
Authentication Statistics:
        Server:"172.30.0.7:1812"
                RoundTripTime          :0
                MalformedAccessResponse:0
                AccessRequests         :2
                BadAuthenticators      :0
                AccessRetransmissions  :5
                AccessAccepts          :0
                Timeouts               :6
                AccessRejects          :0
                UnknownPDUTypes        :0
AccessChallenges       :0
        Server:"172.30.0.8:1812"
                RoundTripTime          :0
                MalformedAccessResponse:0
                AccessRequests         :2
                BadAuthenticators      :0
                AccessRetransmissions  :9
                AccessAccepts          :0
                Timeouts               :10
                AccessRejects          :0
                UnknownPDUTypes        :0
                AccessChallenges       :0
```

RADIUS Connection Down Alarm

The following table lists the alarm generated when the RADIUS accounting connection is down.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
RADIUS ACCOUNTING CONNECTION DOWN	327681	CRITICAL: if all enabled and configured Remote Authentication Dial-in User Service (RADIUS) accounting server connections have timed-out without response from the RADIUS server MAJOR: if some, but not all configured RADIUS accounting server connections have timed-out without response from the RADIUS server.	The enabled connections to RADIUS servers have timed-out without a response from the RADIUS server.	CRITICAL: All enabled accounting connections have been lost! Check accounting status for more details. MAJOR: One or more enabled accounting connections have been lost! Check accounting status for more details.	apSyslogMessageGenerated trap generated apSysMgmtRadiusDownTrap trap generated syslog

Security Breach Statistics

You can view statistics about denied ACL entries by using the following commands:

- **acl-show**
- **show acl**

Some forms of the **show acl** command includes a line showing the number of static plus dynamic entries that are "not allocated due to ACL constraints". The system tracks this statistic for each type of entry including media, trusted, untrusted and denied. For each type, the system displays the number of ACLs that could not be created by the system, because they would exceed the maximum supported by your system's resources. Dynamic and static maximums are displayed in the **show platform limits** command.

For example, the number presented by Denied Entries not allocated by the system is the number of deny ACLs that are not allocated and listed in the output because system reached its Deny Entries limit.

Viewing List of Denied ACL Entries

Display a list of denied ACL entries by using the **acl-show** command. If a IP address and realm ID is denied of service, its is added to the deny list. This command shows list of deny ACL entries. Information for each entry includes:

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

For example:

```
ORACLE# acl-show
deny entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot
type    index
Total number of deny entries = 0
Denied Entries not allocated due to ACL constraints:     0
task done
```

Viewing ACL List Entries

Display entries in the deny, untrusted, and trusted lists using the **show acl** command.

- show acl denied
- show acl untrusted
- show acl trusted
- show acl summary
- show acl all
- show acl ip

For example:

show acl denied displays summary data for denied endpoints.

```
ORACLE# show acl denied
Deny entries:
intf:vlan Source-IP/mask   port/mask dest-IP/mask port/mask prot type
index

Total number of deny entries = 0
Denied Entries not allocated due to ACL constraints:     0

ORACLE# show acl trusted
-------------
Apr 30 17:33:05.716
Static trusted entries:
```

```
intf:vlan src-ip/mask:port dest-ip/mask:port prot type  index recv drop
0/3:3000  0.0.0.0          192.168.0.123     ICMP static    2   0    0
0/2:2000  O.0.0.0          172.16.O.123:5060 UDP  static    4   0    0
Total number of static trusted entries = 2

dynamic trusted entries:
intf:vlan source-ip/mask:port dest-ip/mask:port  prot type    index
0/3:3000  192.168.0.10:5060   192.168.0.123:5060 UDP  dynamic     5
Total number of dynamic trusted entries = 1
```

show acl summary displays cumulative and per-interface statistics on ACL traffic and drops, displaying Recent, Total and PerMax counts. The parameter also separates the display of traffic from trusted versus untrusted sites.

```
ORACLEshow acl summary
14:25:04-594

          ---------------- ACL  Stats Overall     ---------------------
           Entries         Packets                         Dropped
                     Recent    Total    PerMax    Recent    Total  PerMax
Trusted          0      292      292       292         0        0       0
Untrusted        2       65       65        49         0        0       0

          -------------------- ACL Stats Per Interface ------------------
            Entries        Packets                         Dropped
                     Recent    Total    PerMax    Recent    Total  PerMax
Slot 0 /Port 0
Trusted          0      164      164       164         0        0       0
Untrusted        1       37       37        29         0        0       0

Slot 0 /Port 1
Trusted          0      128      128       128         0        0       0
Untrusted        1       28       28        20         0        0       0
```

Column definitions for this parameter include:

- Recent—-Number of packets or drops accumulated in the most recent 5 minute interval. Note that this interval is not configurable and is not calculated via the command output's time stamp
- Total—Number of packets or drops accumulated since last reboot.
- PerMax—Highest number of SIP messages and/or events that occurred during a single time period since the system was last rebooted.Identifies the highest individual Period Totals since the system was last rebooted.

show acl all displays summary data for denied endpoints, static trusted endpoints, and dynamic trusted endpoints.

```
ORACLE# show ad all
Deny entries:
intf:vlan src-IP/mask port/mask dest-IP/mask port/mask prot type index

Total number of deny entries = 0

Static trusted entries:
```

```
intf:vlan src-IP/mask:port dest-IP/mask:port prot type   index recv
drop
0/0:0     0.0.0.0          192,1680,80       ICMP static 65536    0
0
1/0:0     0.0.0.0          172.16.0.80       ICMP static 65537    0
0

Total number of static trusted entries = 2

dynamic trusted entries:
intf:vlan src-IP/mask port dest-IP/mask port prot type   index recv
drop
0/0:0     0.0.0.0          192.168.0.80      ICMP static 65536    0
0
1/0:0     0.0.0.0          172.16.0.80       ICMP static 65537    0
0

Total number of dynamic trusted entries = 2

untrusted entries:
intf:vlan src-IP/mask port  dest-IP/mask  port  prot  type    index
0/0:0     0.0.0.0           192.168.0.80  5060  UDP   static  65538
1/0:0     0.0.0.0           172.16.0.80   5060  UDP   static  65539

Total number of untrusted entries = 2

Total deny entries:             0  (0 dropped)
Total media entries:            3
Total static trusted entries:   2  (0 dropped)
Total dynamic trusted entries:  2  (0 dropped)
Total untrusted entries:        2  (0 dropped)
Total INTFC table entries:      0

Media Entries not allocated due to ACL constraints:      0
Trusted Entries not allocated due to ACL constraints:    0
untrusted Entries not allocated due to ACL constraints:  0
Denied Entries not allocated due to ACL constraints:     0
```

Viewing ACL List Entries by IP Address

You can filter the output of **show acl all** based on IP address. For example:

```
ORACLE# show acl ip 192.168.69.65
deny entries:
intf:vlan src-ip/mask:port/mask dest-ip/mask:port/mask prot type index
Total number of deny entries = 0
trusted entries:
intf:vlan src-ip/mask:port/mask dest-ip/mask:port/mask prot type index
recv drop
Total number of trusted entries = 0
untrusted entries:
intf:vlan src-ip/mask:port/mask dest-ip/mask:port/mask prot type index
Total number of untrusted entries = 0
```

Viewing ACL Entry Space in the CAM

Display how much space is used in the CAM for ACL entries, in a percentage and raw value breakdown of the use, by using the show acl info command. For example:

```
ORACLE# show acl info
Access Control List Statistics:

                   | # of entries | % utilization | Reserved Entry Count
-----------------------------------------------------------------------------
--
Denied             |     0             0.0%                 32000
Trusted            |     0             0.0%                  8000
Media              |     1             0.0%                 64000
Untrusted          |     0             0.0%                  2000
Dynamic Trusted    |     0             0.0%                250000
INTFC              |     1              -                     -
-----------------------------------------------------------------------------
--
Total CAM space used = 2 of 126976 (100.00% free)
Total HASH-table space used = 0 of 250050 (100.00% free)
-----------------------------------------------------------------------------
--
Media Entries not allocated due to ACL constraints:        0
Trusted Entries not allocated due to ACL constraints:      0
Untrusted Entries not allocated due to ACL constraints:    0
Denied Entries not allocated due to ACL constraints:       0
```

Session Agent and Session Agent Group Faults

This section explains how to view fault information about SIP and H.323 session agents and session agent groups.

SIP Agent Statistics

You can use the following commands to view SIP agent statistics:

- **show sipd agents**
- **show sipd agents <agent ID>**

Viewing SIP Session Agent Statistics

Display SIP session agent information by using the **show sipd agents** command. With this command, the Oracle Communications Session Border Controller ascertains whether a session agent is in service. When the session agent stops responding to SIP requests, it transitions to the out-of-service state. You can configure the Oracle Communications Session Border Controller to periodically ping the session agent if it has gone out-of-service, or if no requests have been sent to it.

The **show sipd agents** command shows information about the number of active sessions, the average rate of session invitations, and the number of times that the constraints established in the session-agent element have been exceeded for sessions inbound to and outbound from each session agent, as well as the average and maximum latency and the maximum burst rate related to each session agent.

For example:

```
ORACLE# show sipd agents
19:39:34-95
                ---- Inbound ---- --- Outbound ---  -Latency- --- Max
---
Session Agent   Active Rate ConEx Active Rate ConEx Avg   Max Burst In
Out
192.168.200.131      0  0.0     0      0  0.0     0 0.0   0.0     0
0   0
```

Inbound statistics:

- Active: number of active sessions sent from 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 to 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 statistics:

- Avg: average latency for packets traveling to and from each session agent listed
- Max: maximum latency for packets traveling to and from each session agent listed
- Max Burst: total number of session invitations sent to or received from the session agent within the amount of time configured for the burst rate window of the session agent

The second column, which is not labeled, of the **show sipd agents** output shows the service state of each session agent identified in the first column. In the service state column, an **I** indicates that the particular session agent is in service and an **O** indicates that the particular session agent is out of service. An **S** indicates that the session agent is transitioning from the out-of-service state to the in-service state; it remains in this transitional state for a period of time that is equal to its configured in-service period, or 100 milliseconds (whichever is greater). A **D** indicates that the session agent is disabled.

Resetting Session Agent Statistics

Reset a specific session agent’s statistics by using the reset session-agent <hostname> command.

For example:

```
ORACLE# reset session-agent agent2
Accepted
Reset SA failover timer
```

Viewing SIP Session Agent Activity

Display a specific session agent’s activity by using the **show sipd <agent ID>** command.

For example:

```
acmepacket# show sipd agent 69.69.69.22
19:32:17-47
Session Agent 172.16.0.10(sip172) [In Service]
                             -- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Inbound Sessions        0       0       0     234666      92     168
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Reg Rate Exceeded     -       -       0          0       0       -
Outbound Sessions       0       0       0     239762     126     200
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Reg Rate Exceeded     -       -       0          0       0       -
Out of Service          -       -       0          0       0       -
Trans Timeout       40928   40928     400      40928     800   40928
Requests Sent           -       -     400     519695     780       -
Requests Complete       -       -       0     478367     574       -
Seizure                 -       -       0     239762     126       -
Answer                  -       -       0     234661      93       -
  ASR Exceeded          -       -       0          0       0       -
Messages Received       -       -       0    1431343    1415       -
Latency=0.000; max=0.000
```

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

SIP Session Agent Group Statistics

You can use the following commands to display SIP agent group statistics:

- **show sipd groups**
- show sipd groups -v
- show sipd groups <group name>

Viewing Session Agent Group Statistics

Display session information for the session agent groups on the system by using the **show sipd groups** command. This information is compiled by totaling the session agent statistics for all of the session agents that make up a particular session agent group.

The Active column of the session agent group statistics output displays the first character of the session agent group state. The session agent group statistics can be in one of the following states.

- D—Disabled
- O—Out Of Service
- S—Standby
- I—In Service
- C—Constraints Exceeded
- N—This status code is Obsolete
- O—OOS Provisioned Response
- R—Reduction In Call Load. The group's sampled R-factor value (VoIP quality) is less than the configured **qos-constraints**, **major-rfactor** value. The group remains in this state until the SA's **time-to-resume** value expires.

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 for the system.

For example:

```
ORACLE# show sipd groups
11:00:21-16
           ----- Inbound -----  ----- Outbound ------   - Latency -
SAG        Active  Rate  ConEx  Active  Rate    ConEx   Avg     Max
recursion       0   0.0      0       1   0.1  0 0.005   0.005     2
```

If you carry out this command, but you do not specify the name of an existing session agent group, the system will inform you that the group statistics are not available.

Viewing List of SIP Session Agents in a Group

List the session agents that make up the session agent group, along with statistics for each by using the **show sipd groups -v** command. The -v (verbose) option must be included with this command to provide this level of detail.

For example:

```
ORACLE# show sipd groups -v
SAG:              recursion
11:00:07-32
                 ----- Inbound -----  ----- Outbound ------  -- Latency --
Session Agent    Active  Rate  ConEx  Active  Rate  ConEx    Avg      Max
150.150.150.16        0   0.0      0       0   0.0  0 0.005  0.005      1
SAG:              recursion
150.150.150.35        0   0.0      0       1   0.0  0 0.000  0.000      1

Totals:
recursion             0   0.0      0       1   0.8  0 0.005  0.005      2
```

Viewing Statistics for a SIP Session Agent

Display statistics for a specific session agent group by using the **show sipd groups <group name>** command.

For example:

```
ORACLE# show sipd groups recursion
11:00:28-23
           ----- Inbound -----  ----- Outbound ------ -- Latency --
SAG        Active  Rate  ConEx  Active  Rate    ConEx Avg       Max
recursion       0   0.0      0       0   0.0  0 0.005 0.005       2
```

Session Agent and Session Router Constraint Statistics

Oracle Communications Session Border Controller’s support for session constraints is applicable not only to the system when configured for dialog-stateful or for session-stateful mode, but also when it operates in proxy (transaction or stateless) mode.

Notes on Statistics

When it runs in transaction mode, the Oracle Communications Session Border Controller counts INVITE transactions for calculating session agent statistics that are used to apply session agent constraints. The following describes how the Oracle Communications Session Border Controller performs its count:

- For calculating the **max-burst-rate** and the **max-inbound-burst-rate**, the Oracle Communications Session Border Controller counts the server transaction created when it receives an INVITE request.
- For calculating the **max-outbound-burst-rate**, the Oracle Communications Session Border Controller counts the client transaction when it sends an INVITE request to a session agent.

- The Oracle Communications Session Border Controller counts each INVITE transaction, except for in-dialog re-INVITE transactions. It detects in-dialog re-INVITE requests by checking the To tag.
- The Oracle Communications Session Border Controller does not count retransmitted INVITE requests, which it can detect.

Example 1 Statistics from Transaction Mode

This section shows sample output from the ACLI **show sipd agents** command. The sections that do not apply to transaction mode appear in italics.

```
ORACLE# show sipd agents acme5
11:08:18-46
Session Agent acme5(private) [In Service]
                             -- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Inbound Sessions       22      22      22         22      22      22
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0      19       0          0       0      19
  Reg Rate Exceeded     -       -       0          0       0       -
Outbound Sessions       0       0       0          0       0       0
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0       0       0          0       0       0
  Reg Rate Exceeded     -       -       0          0       0       -
Out of Service          -       -       0          0       0       -
Trans Timeout           0       0       0          0       0       0
Requests Sent           -       -       0          0       0       -
Requests Complete       -       -       0          0       0       -
Seizure                 -       -       0          0       0       -
Answer                  -       -       0          0       0       -
  ASR Exceeded          -       -       0          0       0       -
Messages Received       -       -      65         65      65       -
Latency=0.000; max=0.000
```

Example 1 Statistics from Stateless Mode

This section shows sample output from the ACLI **show sipd agents** command. The sections that do not apply to stateless mode appear in italics.

```
acmesystem# show sipd agents uni
12:11:17-51
Session Agent uni(public) [In Service]
                             -- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Inbound Sessions        0       0       0          0       0       0
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0       0       0          0       0       0
  Reg Rate Exceeded     -       -       0          0       0       -
Outbound Sessions       0       1      11         11      11       1
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0      11       0          0       0      11
  Reg Rate Exceeded     -       -       0          0       0       -
Out of Service          -       -       0          0       0       -
Trans Timeout           0       0       0          0       0       0
Requests Sent           -       -       0          0       0       -
Requests Complete       -       -       0          0       0       -
Seizure                 -       -       0          0       0       -
Answer                  -       -       0          0       0       -
  ASR Exceeded          -       -       0          0       0       -
Messages Received       -       -      30         30      30       -
Latency=0.000; max=0.000
```

FQDN-resolved Session Agent Statistics

A SIP session agent can be configured with an FQDN in the hostname parameter. When the response to the DNS query for that hostname yields one or more IP addresses, the Oracle Communications Session Border Controller maintains these IP targets as all able to perform the role of the session agent object. The Oracle Communications Session Border Controller can report aggregate statistics of all IP targets that correspond to the session agent object and individual statistics per IP address (including per-method statistics) of each member of the last that the FQDN query returns. These statistics are available at the command line, via SNMP GETs, and via HDR. In addition, the Oracle Communications Session Border Controller can send traps if an individual IP target goes in or out of service.

Use the following syntax to retrieve statistics for each IP target that is returned in an FQDN query for a session agent:

```
show sipd agents <session-agent-name>#<destination-ip-address>
```

You may find the list of IP address returned for an FQDN at the bottom of the **show sipd agents <agent name>** query. In the screen capture below, a session agent is configured with sa1.dg.com FQDN in the **hostname** parameter. A DNS query returns IP addresses 192.168.26.2 and 192.168.26.3. By executing the **show sipd agent sa1.dg.com** to verify the IP routes that are used for this session agent. Their service states will also be listed. The statistics presented are the aggregate of all traffic/activity for the Oracle Communications Session Border Controller's transactions with 192.168.26.3 and 192.168.26.2.

```
ORACLE# show sipd agent sa1.dg.com
12:19:02-33
Session Agent sa1.dg.com(net192) [In Service]
                             -- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Inbound Sessions        0       0       0          0       0       0
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0       0       0          0       0       0
  Reg Rate Exceeded     -       -       0          0       0       -
  Reg Burst Rate        0       0       0          0       0       0
Outbound Sessions       0       0       0          0       0       0
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0       0       0          0       0       0
  Reg Rate Exceeded     -       -       0          0       0       -
Local Contacts          0       0       0          0       0       0
HNT Entries             0       0       0          0       0       0
Non-HNT Entries         0       0       0          0       0       0
Subscriptions           0       0       0          0       0       0
Out of Service          -       -       0          0       0       -
Trans Timeout           0       0       0          0       0       0
Requests Sent           -       -       2         20       2       -
Requests Complete       -       -       2         20       2       -
Seizure                 -       -       0          0       0       -
Answer                  -       -       0          0       0       -
  ASR Exceeded          -       -       0          0       0       -
Messages Received       -       -       2         20       2       -
Latency=0.004; max=0.005

Destination: 192.168.26.3 In Service
Destination: 192.168.26.2 In Service
```

To retrieve an individual destinations statistics, use the **show sipd agents** command again and query on the session agent name, delimited with the pound character followed by the IP destination of note. The "Rate Exceeded", "Num Exceeded", "Reg Rate Exceeded" and "ASR Exceeded" counters are not be tracked and displayed for individual routes.

```
ORACLE# show sipd agent sa1.dg.com#192.168.26.2
12:19:18-49
Session Agent sa1.dg.com#192.168.26.2(net192) [In Service]
                             -- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Inbound Sessions        0       0       0          0       0       0
  Burst Rate            0       0       0          0       0       0
  Reg Burst Rate        0       0       0          0       0       0
Outbound Sessions       0       0       0          0       0       0
  Burst Rate            0       0       0          0       0       0
Local Contacts          0       0       0          0       0       0
HNT Entries             0       0       0          0       0       0
Non-HNT Entries         0       0       0          0       0       0
Subscriptions           0       0       0          0       0       0
Out of Service          -       -       0          0       0       -
Trans Timeout           0       0       0          0       0       0
Requests Sent           -       -       1         10       1       -
Requests Complete       -       -       1         10       1       -
Seizure                 -       -       0          0       0       -
Answer                  -       -       0          0       0       -
Messages Received       -       -       1         10       1       -
Latency=0.004; max=0.004
```

To retrieve an individual destination's statistics per SIP method, use the previously explained command followed by a space and the method you wish to query.

```
ORACLE# show sipd agent sa1.dg.com#192.168.26.2 OPTIONS
OPTIONS (12:19:28-59)
                      --------- Server --------   --------- Client
--------
```

```
Message/Event          Recent      Total  PerMax   Recent      Total  PerMax
                       ------  ---------  ------   ------  ---------  ------
OPTIONS Requests            0          0       0        1         10       1
Retransmissions             0          0       0        0          0       0
200 OK                      0          0       0        1         10       1
Transaction Timeouts        -          -       -        0          0       0
Locally Throttled           -          -       -        0          0       0

Avg Latency=0.004 for 1
Max Latency=0.004
```

FQDN-resolved Session Agent Statistics Configuration

To configure FQDN-resolved Session Agent Statistics, you must add configuration to both the **sip-config** and **session-agent** configuration elements.

In the **sip-config** configuration element, set the **sa-routes-stats** parameter to enabled

```
ORACLE(configure)# exit
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# sip-config
ORACLE(sip-config)# select
ORACLE(sip-config)# sa-routes-stats enabled
ORACLE(sip-config)# done
```

In the **session-agent** configuration element, set the **ping-interval** parameter to a value greater than 0, the **ping-method** to OPTIONS, and set the **ping-all-addresses** parameter to enabled.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# session-agent
ORACLE(session-agent)# sel
<hostname>:
1:  hostname=sa1.dg.com

selection: 1
ORACLE(session-agent)# ping-interval 120
ORACLE(session-agent)# ping-all-addresses enabled
ORACLE(session-agent)# ping-method=OPTIONS
ORACLE(session-agent)# done
```

FQDN-resolved Session Agent Statistics SNMP Retrieval

When FQDN-resolved Session Agent Statistics are enabled, you can retrieve each IP target's session agent statistics via SNMP.

The apSipAgentTable returns a list of configured sessions agent with an index corresponding and configuration name. The mapping of index to configuration name is persistent across system reboot.

The index of the additional entries that correspond to the individual IP targets are identified by starting at 10000000. Because the IP targets that are retrieved from the DNS server may change on any DNS query, they are not persistent across a reboot. An snmpwalk query on asSIPAgentTable appears as:

```
SNMPv2-SMI::enterprises.9148.3.15.1.2.3.1.2.36 = STRING: "sa1.dg.com"
SNMPv2-SMI::enterprises.9148.3.15.1.2.3.1.210000000 = STRING:
"sa1.dg.com#192.168.26.2"
SNMPv2-SMI::enterprises.9148.3.15.1.2.3.1.210000001 = STRING:
"sa1.dg.com#192.168.26.3"
```

The following snmpwalk query on asSipSessionAgentStatsTable appears as:

```
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.1.36 = INTEGER: 36
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.1.10000000 = INTEGER: 1000000
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.1.10000001 = INTEGER: 1000001
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.2.36 = STRING: "sa1.dg.com"
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.2.10000000 = STRING:
"sa1.dg.com#192.168.26.2"
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.2.10000001 = STRING:
"sa1.dg.com#192.168.26.3"
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.3.36 = INTEGER: 1
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.3.10000000 = INTEGER: 1
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.3.1000001 = INTEGER: 1
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.4.36 = Gauge32: 0
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.4.10000000 = Gauge32: 0
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.4.10000001 = Gauge32: 0
```

FQDN-resolved Session Agent Statistics SNMP Traps

The apSysMgmtSAStatusChangeTrap trap is generated when a session agent's individual IP target changes state.

FQDN-resolved Session Agent Statistics HDR Retrieval

When FQDN-resolved Session Agent Statistics are enabled, each IP target's session agent statistics are written to HDR output.

For the sa1.dg.com example that retrieved 2 IP targets, the following 3 lines of HDR output are typical:

```
1380106951,sa1.dg.com,sip,inService,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,2,4
1380106951,sa1.dg.com#192.168.26.3,sip,inService,0,0,0,0,0,0,0,0,0,0,0,
0,1,0,0,0,2,4
1380106951,sa1.dg.com#192.168.26.2,sip,outOfService,0,0,0,0,0,0,0,0,0,0
,0,0,1,0,0,0,0,0
```

Note that the first entry is the aggregate of all individual targets.

Realm Faults

This section explains how to access realm fault statistics.

Signaling

Use the following command to display SIP realm statistics:

- **show sipd realms**

Viewing SIP Realm Statistics

Display SIP realm statistics by using the **show sipd realms** command. For example:

```
ORACLE# show sipd realms
19:38:17-18
               ---- Inbound ---- --- Outbound ---- -Latency- --- Max ---
Realm          Active Rate ConEx Active Rate ConEx  Avg  Max Burst In Out
external            0 0.0      0      0  0.0     0  0.0  0.0     0  0   0
external-child      0 0.0      0      0  0.0     0  0.0  0.0     0  0   0
internal            0 0.0      0      0  0.0     0  0.0  0.0     0  0   0
```

Media Statistics

You can use the following commands to display information about mbcd realms:

- **show mbcd realms**
- **show mbcd realms <realm name>**
- **show flows**

There are also alarms that occur when the following events happen:

- out of memory
- internal
- unknown realm
- realm change
- out of bandwidth
- out of ports

Viewing MBCD Steering Port and Bandwidth Usage for Realms

Display steering ports and bandwidth usage for home, public, and private realms by using the **show mbcd realms** command.

For example:

```
acmepacket# show mbcd realms
18:46:29-2819
             --- Steering Ports ---  ----------- Bandwidth Usage ----------
Realm         Used   Free  No Ports    Flows Ingrss Egress  Total  Insuf BW
acme             0      0         0        0     0K     0K     0K         0
h323172          0  30001         0        0     0K     0K     0K         0
sip172           2  29999         0        0     0K     0K     0K         0
sip192           2  29999         0        0     0K     0K     0K         0
```

The information displayed includes the following:

- 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.

Viewing MBCD Statistics for a Specific Realm

Display media statistics for a specific realm by using the **show mbcd realms <realm-name>** command. This information is given for period and lifetime durations.

- 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

For example:

```
acmepacket# show mbcd realms sip172
18:47:31-2881 Realm=sip172
                            -- Period -- -------- Lifetime --------
                  Active    High   Total      Total  PerMax    High
Ports Used             2       2      18         18      18       2
Free Ports         29999   30001   30017      30017   30017   30001
No Ports Avail         -       -       0          0       0       -
Ingress Band          0K      0K       0          0       0      0K
Egress Band           0K      0K       0          0       0      0K
BW Allocations         0       0       0          0       0       0
Band Not Avail         -       -       0          0       0       -
Total Bandwidth=0K
Steering Ports: 100% Success
```

Viewing MBCD Task Errors

The **show mbcd errors** command displays MBCD task error statistics, starting with a time stamp that shows when the current period began.

For example:

```
ORACLE# show mbcd errors
11:42:37-198
MBC Errors/Events              ---- Lifetime ----
                        Recent      Total  PerMax
Client Errors                0          0       0
Client IPC Errors            0          0       0
Open Streams Failed          0          0       0
Drop Streams Failed          0          0       0
Exp Flow Events              0          0       0
Exp Flow Not Found           0          0       0
Transaction Timeouts         0          0       0
Server Errors                0          0       0
Server IPC Errors            0          0       0
Flow Add Failed              0          0       0
Flow Delete Failed           0          0       0
Flow Update Failed           0          0       0
Flow Latch Failed            0          0       0
Pending Flow Expired         0          0       0
ARP Wait Errors              0          0       0
Exp CAM Not Found            0          0       0
Drop Unknown Exp Flow        0          0       0
Drop/Exp Flow Missing        0          0       0
Exp Notify Failed            0          0       0
Unacknowledged Notify        0          0       0
Invalid Realm                0          0       0
No Ports Available           0          0       0
Insufficient Bandwidth       0          0       0
Stale Ports Reclaimed        0          0       0
Stale Flows Replaced         0          0       0
Telephone Events Gen         0          0       0
Pipe Alloc Errors            0          0       0
Pipe Write Errors            0          0       0
```

There are two categories of MBCD error statistics: Client and Server.

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
- 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
- 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—This statistic shows the 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 from the NP
- 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

Viewing Realm Configurations

You can use the **show realm** command to display all realm-specific configurations. For example:

```
ORACLE# show realm
14:27:38-56SIP Realm Statistics
                                  -- Period -- ------- Lifetime -------
Realm               Active  Rate   High  Total      Total PerMax   High
realm1
```

```
    Inbound              0   0.0      0      0          0      0      0
    Outbound             0   0.0      0      0          0      0      0
```

Viewing Realm Configurations for a Specific Realm

```
ORACLE# show realm realm1
realm stats for : Realm: realm1
14:29:22-40
Realm realm1 NO ACTIVITY
```

Viewing Monthly Minutes for a Specific Realm

You can use the **show monthly minutes <realm-id>** command to display the monthly minutes for a specified realm. For example:

```
ORACLE# show monthly-minutes realm1
14:31:33-51
Realm            MinutesAllowed  MinutesLeft         Minutes Exceed Rejects
------------     -------------   -----------         --------------------
                                                     Recent   Total  PerMax
realm1           10              10                    0          0       0
```

Media Alarms

The following table lists information about the different media alarms.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
MBCD ALARM OUT OF MEMORY	262145	CRITICAL: for flow MAJOR: for media (if server cannot allocate a new context)	No further memory can be allocated for MBCD.	Flow: Cannot create free port list for realm. Media Server: Failed to allocate new context.	apSyslogMessageGenerated apSysMgmtMediaOutofMemory trap generated
MBCD ALARM INTERNAL	262146	MINOR	An internal software error.	Internal Error. No agent for socket <IPPort>.	None
MBCD ALARM UNKNOWN REALM	262147	MAJOR: if media server is adding a new flow	Media server is unable to find realm interface.	Realm type (ingress, egress, hairpin) X, not found	apSyslogMessageGenerated apSysMgmtUnknownRealm
MBCD ALARM OUT OF BANDWIDTH	262149	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of bandwidth.	Out of bandwidth	apSyslogMessageGenerated apSysMgmtMediaBandwidthTrap

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
MBCD ALARM OUT OF PORTS	262150	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of steering ports.	Out of steering ports	apSyslogMessageGenerated apSysMgmtMediaPortsTrap

Viewing Deny ACL List

Display a list of deny ACLI entries by using the **acl-show** command at the topmost ACLI prompt. The following information is displayed:

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

For example:

```
ORACLE# acl-show
deny entries:
intf:vlan source-ip/mask:port/mask dest-ip/mask:port/mask   prot
type    index
Total number of deny entries = 0
Denied Entries not allocated due to ACL constraints:     0
task done
```

Network Faults

This section explains how to access network fault information. Network alarms account for problems related to low-level network issues and might occur when the software is unable to communicate with the hardware.

NAT Statistics

Use the following command to display NAT table information.

- **show nat**

There is also an alarm that occurs when the NAT table usage reaches 90% or greater of its capacity.

Viewing Information from the NAT Table

Display information from the NAT table by using the **show nat** command along with one of the following subcommands.

> **Note:**
>
> Do not display the entire contents of the NAT table on your screen. The size of the table can interfere with call processing.

- **by-index**: specify the range of entries to display, up to a maximum of 5024 entries. For example, to see entries on lines 10 through 50 of the NAT table, enter the following:

  ```
  show nat by-index 10 50
  ```

  A Space separates the two numbers defining the range. If you do not specify a range, the system uses the default range of 1 through 200. The range you enter here corresponds to line numbers in the table, and not to the number of the entry itself.
- **by-addr**: specify the entries to display according to SA and DA values. For example, to view entries with an SA of 192.168.112.25 and a DA 101.102.103.104, enter the following:

  ```
  show nat by-addr 192.168.112.25 101.102.103.104
  ```

  The system matches these values to the NAT table entries and displays the pertinent information. If no addresses are entered, the system displays all of the table entries (all of the table entries will match).
- 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>
- 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. The syntax is:
  show nat flow-info <all | by-addr | by-switchid>

Viewing NAT information By Index

The following example shows the output of the **show nat by-index** command:

```
ORACLE# show nat by-index 1 2
-------------------------------------------------------------
Total number of entries in the Database = 395
NAT table search address 1, xsmAddr 62580 :
Flow type: Traditional weighted flow
SA_flow_key       : 192.168.200.041       SA_prefix          : 32
DA_flow_key       : 000.000.000.000       DA_prefix          : 0
SP_flow_key       : 0                     SP_prefix          : 0
DP_flow_key       : 0                     DP_prefix          : 0
VLAN_flow_key     : 0
Protocol_flow_key : 0
```

```
Ingress_flow_key  : 64
Ingress Slot      : 64
Ingress Port      : 0
XSA_data_entry    : 000.000.000.000
XDA_data_entry    : 000.000.000.000
XSP_data_entry    : 0
XDP_data_entry    : 0
Egress_data_entry : 0
Egress Slot       : 0
Egress Port       : 0
flow_action       : 0X1
optional_data     : 0
FPGA_handle       : 0xffffffff
assoc_FPGA_handle : 0xffffffff
VLAN_data_entry   : 0
host_table_index  : 1
Switch ID         : 0x00034000
average-rate      : 0
weight            : 0x10
init_flow_guard   : 4294967295
inact_flow_guard  : 4294967295
max_flow_guard    : 4294967295
q - quit, return - next entry, space - through to the end :
```

Viewing NAT Information By Address

```
ORACLE# show nat by-addr
sip_key = (null), dip_key = (null)
-- Total number of entries in the NAT table is 407
---------------------------------
NAT table search address 1 :
Flow type: Traditional weighted flow.  Weight = 16
SA_flow_key       : 192.168.200.041       SA_prefix         : 32
DA_flow_key       : 000.000.000.000       DA_prefix         : 0
SP_flow_key       : 0                     SP_prefix         : 0
DP_flow_key       : 0                     DP_prefix         : 0
VLAN_flow_key     : 0
Protocol_flow_key : 0
Ingress_flow_key  : 64
Ingress Slot      : 64
Ingress Port      : 0
XSA_data_entry    : 000.000.000.000
XDA_data_entry    : 000.000.000.000
XSP_data_entry    : 0
XDP_data_entry    : 0
Egress_data_entry : 0
Egress Slot       : 0
Egress Port       : 0
flow_action       : 0X1
optional_data     : 0
FPGA_handle       : 0xffffffff
assoc_FPGA_handle : 0xffffffff
VLAN_data_entry   : 0
host_table_index  : 1
```

```
Switch ID         : 0x00034000
average-rate      : 0
weight            : 0x10
init_flow_guard   : 4294967295
inact_flow_guard  : 4294967295
max_flow_guard    : 4294967295
q - quit, return - next entry, space - through to the end :
```

Viewing NAT Information In Tabular

```
acmepacket# show nat in-tabular
  NAT      SA_key           DA_key        SP_key     DP_key   VLAN_key
ING      PROTO     WEIGHT
addr=1, sip=0xac100056, dip=0x00000000, SP=0x0000, DP=0x0000, VLAN=  0,
Intf=64, proto= 0, weight=0x10
addr=2, sip=0x7f000064, dip=0x00000000, SP=0x0000, DP=0x0000, VLAN=999,
Intf=64, proto= 0, weight=0x10
addr=3, sip=0x00000000, dip=0xac100056, SP=0x0000, DP=0x0000, VLAN=  0,
Intf= 0, proto= 6, weight=0x9
addr=4, sip=0x00000000, dip=0xac100056, SP=0x0000, DP=0x0000, VLAN=  0,
Intf= 0, proto=17, weight=0x9
addr=5, sip=0x00000000, dip=0x7f000064, SP=0x0000, DP=0x13c4, VLAN=999,
Intf= 0, proto=17, weight=0xd
addr=6, sip=0x00000000, dip=0xac100058, SP=0x0000, DP=0x13c4, VLAN=  0,
Intf= 0, proto=17, weight=0xd
addr=7, sip=0x00000000, dip=0xc0a86458, SP=0x0000, DP=0x13c4, VLAN=  0,
Intf= 1, proto=17, weight=0xd
addr=8, sip=0x00000000, dip=0xac100056, SP=0x0000, DP=0x0001, VLAN=  0,
Intf= 0, proto= 6, weight=0x63
```

Viewing General NAT Table Information

```
ORACLE# show nat info
-- NAT table info --
Maximum number of entries  : 7768
Number of used entries     : 10
Length of search key       : 2 (x 64 bits)
First search entry address : 0x0
length of data entry       : 4 (x 64 bits)
First data entry address   : 0x0
Enable aging               : 1
Enable policing            : 0
```

Viewing Network Address Translation (NAT) Flow Information

To confirm that network interfaces are properly created, use the **show nat flow-info by-addr** command to view the NAT flow information table.

The following illustration is a sample NAT flow information table.

```
ORACLE# show nat flow-info by-add 192.168.225.1
```

```
Index   Prot   Intf:Vlan  Src IP:Port                    Dst IP:Port
-----------------------------------------------------------------------
-------
9       udp    I=0/0:33   192.168.225.6:0
192.168.225.1:10006
               O=0/0:33   192.168.225.1:10004
192.168.225.4:10000
11      udp    I=0/0:33   192.168.225.4:0
192.168.225.1:10004
               O=0/0:33   192.168.225.1:10006
192.168.225.6:10000
----------------------------------------------
ORACLE#
```

NAT Table Utilization Alarm

The following table describes the NAT table utilization alarm:

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
NAT TABLE UTILIZATION	131102	MINOR	NAT table usage reached 90% or greater of its capacity.	NAT table usage X% over threshold X%	apSysMgmtGroupTrap trap generated syslog

TCP and SCTP State Connection Counters

The Oracle Communications Session Border Controller (SBC) can provide systemwide counts of Transmission Control Protocol (TCP) and Stream Control Transmission Protocol (SCTP) states by way of the **show ip tcp** and **show ip sctp** commands from the ACLI.

The **show ip tcp** command includes the following section of counters that correspond to counts of TCP states per active connections, including counts differentiated by inbound, outbound, listen and IMS-AKA connections.

```
Connections By State:
        0       CLOSED
        0       LISTEN
        0       SYN_SENT
        0       SYN_RCVD
        0       ESTABLISHED
        0       CLOSE_WAIT
        0       FIN_WAIT_1
        0       CLOSING
        0       LAST_ACK
        0       FIN_WAIT_2
        0       TIME_WAIT

Inbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
         50    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


Outbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          1    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


Listen Socket Connection By State:
          0    CLOSED
          2    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


IMSAKA Inbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


IMSAKA Outbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


IMSAKA Listen Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


        Number of Connections Counted = 0
        Maximum Connection Count = 0
        Maximum Number of Connections Supported = 220000
```

The **show ip sctp** command includes the following section of counters that correspond to counts of SCTP states per active connections.

```
Connections By State:
                0       CLOSED
                0       BOUND
                0       LISTEN
                0       COOKIE_WAIT
                0       COOKIE_ECHOED
                0       ESTABLISHED
                0       SHUTDOWN_SENT
                0       SHUTDOWN_RECEIVED
                0       SHUTDOWN_ACK_SENT
                0       SHUTDOWN_PENDING

        Number of Connections Counted = 0
        Maximum Connection Count = 0
        Maximum Number of Connections Supported = 10000
```

The output of the state counters indicates the number of connections currently in each state. The statistics from the counters do not accumulate like many of the other statistics in the **show ip** command tree. Most states are ephemeral, and you may see many "0" counters for states other than LISTEN and ESTABLISHED.

TCP Connection Tools

Transmission Control Protocol (TCP) connection tools can assist you in gauging performance, identifying potential memory leaks, and debugging connections for performance tracking and improvement.

The **show ip tcp** command shows the following socket connections by state:

- inbound
- outbound
- listen
- IMS-AKA

The **show sipd tcp** and **show sipd tcp connections** commands display counters to track usage. Use the **reset sipd** command to reset the counters.

TCP and SCTP State Connection Counters

The Oracle Communications Session Border Controller (SBC) can provide systemwide counts of Transmission Control Protocol (TCP) and Stream Control Transmission Protocol (SCTP) states by way of the **show ip tcp** and **show ip sctp** commands from the ACLI.

The **show ip tcp** command includes the following section of counters that correspond to counts of TCP states per active connections, including counts differentiated by inbound, outbound, listen and IMS-AKA connections.

```
Connections By State:
        0       CLOSED
        0       LISTEN
        0       SYN_SENT
        0       SYN_RCVD
        0       ESTABLISHED
        0       CLOSE_WAIT
        0       FIN_WAIT_1
        0       CLOSING
        0       LAST_ACK
        0       FIN_WAIT_2
        0       TIME_WAIT

Inbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
         50    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT
```

```
Outbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          1    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


Listen Socket Connection By State:
          0    CLOSED
          2    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


IMSAKA Inbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


IMSAKA Outbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT
```

```
IMSAKA Listen Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


        Number of Connections Counted = 0
        Maximum Connection Count = 0
        Maximum Number of Connections Supported = 220000
```

The **show ip sctp** command includes the following section of counters that correspond to counts of SCTP states per active connections.

```
Connections By State:
                0       CLOSED
                0       BOUND
                0       LISTEN
                0       COOKIE_WAIT
                0       COOKIE_ECHOED
                0       ESTABLISHED
                0       SHUTDOWN_SENT
                0       SHUTDOWN_RECEIVED
                0       SHUTDOWN_ACK_SENT
                0       SHUTDOWN_PENDING

        Number of Connections Counted = 0
        Maximum Connection Count = 0
        Maximum Number of Connections Supported = 10000
```

The output of the state counters indicates the number of connections currently in each state. The statistics from the counters do not accumulate like many of the other statistics in the **show ip** command tree. Most states are ephemeral, and you may see many "0" counters for states other than LISTEN and ESTABLISHED.

show sipd tcp connections

The **show sipd tcp connections** command displays Transmission Control Protocol (TCP) connection information details on remote and local address/port and connection states for analysis. Oracle recommends that you use the command only during non-peak times or maintenance windows.

The s**how sipd tcp connections** command displays all SIP/TCP connections including each connection's direction, type, state, local and remote addresses, SIP interface and IMS-AKA details. Arguments include:

- sip-interface—Optional parameter that limits output to sockets in the specified sip-interface
- start start—Integer indicating which connection to start displaying. This can be a negative number. When the number selected for the start variable is greater than the number of TCP connections, the system displays nothing.
- start-count start—Integer as per above plus the count integer, specifying how many TCP connections to display from the start.
- all—Display all of the sipd tcp connections. Exercise caution due to the possibility of consuming all CPU time; preferably use during a maintenance window

For example:

```
ORACLE# show sipd tcp connections

sipd tcp connections

Dir Type    State          Local Address         Remote Address
sip-interface-id     isImsaka

    LISTEN  TCP_LISTENING  172.16.101.149:5060
net172
in  FORKED  TCP_CONNECTED  172.16.101.149:5060   172.16.23.100:51678
net172
in  FORKED  TCP_CONNECTED  172.16.101.149:5060   172.16.23.100:51679
net172
[...]
in  FORKED  TCP_CONNECTED  172.16.101.149:5060   172.16.23.100:51727
net172
in  FORKED  TCP_CONNECTED  172.16.101.149:5060   172.16.23.100:51728
net172
in  FORKED  TCP_CONNECTED  172.16.101.149:5060   172.16.23.100:51729
net172
    LISTEN  TCP_LISTENING  192.168.101.149:5060
net192
out CONNECT TCP_CONNECTED  192.168.101.149:8192  192.168.23.100:5060
net192

Connections Displayed:       53
Total Connections:           53
```

show sipd tcp

.

The **show sipd tcp** command displays TCP connection state information for the following:

- inbound
- outbound
- listen

- total
- IMS-AKA

For example:

```
ORACLE# show sipd tcp
11:11:54-110
SIP TCP Sockets               -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States              53      53     108        108     108      53
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       1      51         51      51       1
TCP_BOUND                0       1       3          3       3       1
TCP_CONNECTED           51      51      51         51      51      51
TCP_CONNECTING           0       1       1          1       1       1
TCP_LISTENING            2       2       2          2       2       2
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------

SIP Inbound TCP Sockets       -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States              50      50     100        100     100      50
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       1      50         50      50       1
TCP_BOUND                0       0       0          0       0       0
TCP_CONNECTED           50      50      50         50      50      50
TCP_CONNECTING           0       0       0          0       0       0
TCP_LISTENING            0       0       0          0       0       0
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------

SIP Outbound TCP Sockets      -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States               1       1       4          4       4       1
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       1       1          1       1       1
TCP_BOUND                0       1       1          1       1       1
TCP_CONNECTED            1       1       1          1       1       1
TCP_CONNECTING           0       1       1          1       1       1
TCP_LISTENING            0       0       0          0       0       0
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------

SIP Listen TCP Sockets        -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States               2       2       4          4       4       2
```

```
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       0       0          0       0       0
TCP_BOUND                0       1       2          2       2       1
TCP_CONNECTED            0       0       0          0       0       0
TCP_CONNECTING           0       0       0          0       0       0
TCP_LISTENING            2       2       2          2       2       2
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------
```

IMS-AKA portion of show **sipd tcp command**:

```
ORACLE# show sipd tcp
15:28:51-197
[...]

SIP IMSAKA In TCP Sockets     -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States               0       0       0          0       0       0
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       0       0          0       0       0
TCP_BOUND                0       0       0          0       0       0
TCP_CONNECTED            0       0       0          0       0       0
TCP_CONNECTING           0       0       0          0       0       0
TCP_LISTENING            0       0       0          0       0       0
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------

SIP IMSAKA Out TCP Sockets    -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States               0       0       0          0       0       0
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       0       0          0       0       0
TCP_BOUND                0       0       0          0       0       0
TCP_CONNECTED            0       0       0          0       0       0
TCP_CONNECTING           0       0       0          0       0       0
TCP_LISTENING            0       0       0          0       0       0
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------

SIP IMSAKA Listen TCP Sockets -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States               1       1       0          2       2       1
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       0       0          0       0       0
```

```
TCP_BOUND                0       0       0          1       1       1
TCP_CONNECTED            0       0       0          0       0       0
TCP_CONNECTING           0       0       0          0       0       0
TCP_LISTENING            1       1       0          1       1       1
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0
----------------------------------------------------------------------
```

ARP Statistics

You can use the following command to view ARP statistics:

- **show arp statistics**

There is also an alarm that occurs when a gateway is unreachable.

Viewing Address Mappings

Display the current Internet-to-Ethernet address mappings in the ARP table by using the **show arp** command. The first section of this display shows the following information: destination, gateway, flags, reference count, use, and interface. The second section shows the interface, VLAN, IP address, MAC address, timestamp, and type.

The intf (interface) column in the ARP includes both slot and port information. If a value of 0/1 appears, 0 refers to the slot and 1 refers to the port.

```
ORACLE# show arp
LINK LEVEL ARP TABLE
destination      gateway            flags  Refcnt  Use           Interface
-------------------------------------------------------------------------
172.30.0.1       00:0f:23:4a:d8:80  405    1       0             wancom0
-------------------------------------------------------------------------
                Total ARP Entries = 3
                -----------------------
Intf  VLAN     IP-Address             MAC          time-stamp   type
 0/0    0   010.000.045.001     00:00:00:00:00:00  1108462861  invalid
Special Entries:
 0/0    0   000.000.000.000     00:00:00:00:00:00  1108462861  gateway
 0/0    0   010.000.045.000     00:00:00:00:00:00  1108462861  network
Gateway Status:
Intf  VLAN     IP-Address          MAC          time-stamp hb status
 0/0    0   010.000.045.001  00:00:00:00:00:00  1108462861    unreachable
-- ARP table info --
Maximum number of entries  : 512
Number of used entries     : 3
Length of search key       : 1 (x 64 bits)
First search entry address : 0x3cb0
length of data entry       : 2 (x 64 bits)
First data entry address   : 0x7960
Enable aging               : 0
Enable policing            : 0
```

Gateway Unreachable Alarm

The Oracle Communications Session Border Controller supports polling for and detection of front interface links to the default gateway when monitoring ARP connectivity. Based on configured gateway link parameter, the Oracle Communications Session Border Controller detects connectivity loss, generates an alarm when it loses ARP-connectivity to the front interface gateway, and decrements its health score accordingly.

The GATEWAY UNREACHABLE network-level alarm is generated in the following circumstances:

- If the ARP manager has not received any ARP messages from a front interface gateway (assigned when the network interface was configured) within the configured heartbeat time period, it will send out ARP requests and wait for a reply.
  You can set this heartbeat time period when configuring the gateway heartbeat interval for the redundancy element or when configuring the gw heartbeat's heartbeat field for the network interface element.
- If no reply is received after retrying (re-sending) ARP requests for a configured number of times.
  You can set this retry value when configuring the gateway heartbeat retry field for the redundancy element or the gw heartbeat's retry count field for the network interface element.

The GATEWAY UNREACHABLE alarm decrements the health score of the Oracle Communications Session Border Controller by the amount you set for either the gateway heartbeat health field of the redundancy element or the gw heartbeat's health score field for the network interface. The alarm is cleared once a front interface gateway ARP entry is valid again.

After the initial alarm is triggered, the Oracle Communications Session Border Controller continues to attempt to connect to the front interface gateway. It issues ARP requests (retries) every five seconds until front interface gateway ARP connectivity is achieved.

You can set the gateway link failure detection and polling parameters, and the health score decrement (reduction) value for the entire Oracle Communications Session Border Controller by configuring the redundancy element or for each individual network interface by configuring the gw heartbeat for the network interface.

The following table lists information about the GATEWAY UNREACHABLE alarm.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
GATEWAY UNREACHABLE	dynamicID	MAJOR	The Oracle Communications Session Border Controller lost ARP connectivity to the front interface gateway.	gateway X.X.X.X unreachable on slot Y port Z subport ZZ (where X.X.X.X is the IPv4 address of the front interface gateway, Y is the front interface slot number, Z is the front interface port number, and ZZ is the subport ID)	apSysMgmtGatewayUnreachableTrap generated syslog

Note:

The value of this alarm changes based on a number of factors. The total alarm ID range falls between 196608 and 262143. The alarm ID is calculated based on a compilation of a hexadecimal number that represents the VLAN ID and the front interface slot/port numbers.

System Reboot after Gateway Unreachable Event

Oracle Communications Session Border Controllers in an HA pair can be configured so that after a gateway unreachable event initiates a switchover, the newly standby system (where the event occurred) is rebooted.

In some HA scenarios when a system or NIU-based processor error occurs, and a gateway unreachable condition is experienced, the Oracle Communications Session Border Controller fails-over to its standby as expected. The new standby system will not reboot to recover because only a typical gateway unreachable event occurred. When the HA pair returns to its initial role states, the first Oracle Communications Session Border Controller has never recovered from the NIU error and an outage results from the system or NIU error persisting.

Such scenarios can be mitigated by configuring the **reboot=Gateway-Unreachable** option in the **system-config**. This option is disabled by default and must be explicitly configured for use.

The **system**, **network-interface**, **gw-heartbeat**, **health-score** parameter must be a value other than the default of 0.

The syntax below shows how to set this option.

```
ORACLE#configure terminal
ORACLE(configure)#system
ORACLE(system)#system-config
ORACLE(system-config)#select
ORACLE(system-config)#options +reboot=Gateway-Unreachable
ORACLE(system-config)#done
```

This feature contains an additional mechanism to prevent runaway failover-and-reboots.

After the failover, but just prior to the reboot, the system creates a time-stamped logfile indicating that the reboot-and-failover occurred. When the gateway-unreachable alarm is cleared, this file is deleted. When the next gateway unreachable event occurs on an active system, and would otherwise prompt a failover-and-reboot via health score degradation, the system checks for the presence of the logfile. If the logfile's creation date is less than one hour old, the system will failover but not reboot. If the logfile's creation date is greater than or equal to one hour old, the failover-and-reboot will proceed as expected.

View Network Interfaces Statistics

Display statistics for network interfaces by using **show interfaces** command. The following is an example of the Version S-CZ7.1.2 output:

```
ORACLE# show interfaces
lo:
     Flags: (0x49) UP LOOPBACK TRAILERS ARP RUNNING
     Type: LOOPBACK_INTERFACE
     inet is: 127.0.0.1 Vlan: 0
     Metric is 0:
     Maximum Transfer Unit size is 16436
     46001 octets received
     46001 octets sent
     364 packets received
     364 packets sent
     0 multicast packets received
     0 incoming packets discarded
     0 outgoing packets discarded
     0 incoming errors
     0 outgoing errors
     0 invalid frames
     0 collisions; 0 carrier errors
     0 input queue drops
     0 output queue drops
wancom0:
     Flags: (0x1043) UP BROADCAST MULTICAST TRAILERS ARP RUNNING
     Type: GIGABIT_ETHERNET
     inet is: 172.30.46.20 Vlan: 0
     Netmask: 255.255.0.0
     Gateway: 172.30.0.1
     Ethernet address is 00:08:25:a2:56:20
     Metric is 0:
     Maximum Transfer Unit size is 1500
     809490537 octets received
     775555 octets sent
     10768436 packets received
     9449 packets sent
     73012 multicast packets received
     74839 incoming packets discarded
     0 outgoing packets discarded
     0 incoming errors
     0 outgoing errors
     0 invalid frames
     0 collisions; 0 carrier errors
     0 input queue drops
     0 output queue drops
left-left (media slot 0, port 0)
     Flags: UP BROADCAST MULTICAST ARP RUNNING
     Type: GIGABIT_ETHERNET
     Admin State: enabled
     Auto Negotiation: enabled
     Internet address: 192.168.0.10     Vlan: 0
     Broadcast Address: 192.168.0.255
     Netmask: 255.255.255.0
     Gateway: 192.168.0.1
     Maximum Transfer Unit size is 1500
     Ethernet address is 00:08:25:a2:56:23
     Virtual Ethernet address is 00:08:25:a2:56:23
     Metric is 0
     0 octets received
     4668396 octets sent
     0 packets received
     72942 packets sent
     0 non-unicast packets received
     0 unicast packets received
     0 input discards
     0 input unknown protocols
     0 input errors
     0 output errors
     0 collisions; 0 dropped
```

You can also view key running statistics about the interfaces within a single screen by using the **show interfaces [brief]** command.

For example:

```
show interfaces brief
Slt Prt Vlan Interface  IP                     Gateway                 Adm
Oper
Num Num   ID Name       Address                Address                 Stat
Stat
--- --- ---- ---------- ---------------------- ----------------------- ----
----
  -   -    - lo         127.0.0.1              -                        up
up
  -   -    - wancom0    172.30.46.20/16        172.30.0.1               up
up
  0   0    0 left-left  192.168.0.10/24        192.168.0.1              up
up
-----------------------------------------------------------------------------
---
```

Physical Interface Faults

This section contains information about the statistics you can view for network and media interfaces, and alarms that occur for physical interface faults.

Viewing Network Interface Statistics

Display information about the network interfaces by using the show interfaces command.

For example:

```
ORACLE# show interfaces
lo:
     Flags: (0x49) UP LOOPBACK TRAILERS ARP RUNNING
     Type: LOOPBACK_INTERFACE
     inet is: 127.0.0.1 Vlan: 0
     Metric is 0:
     Maximum Transfer Unit size is 16436
     46001 octets received
     46001 octets sent
     364 packets received
     364 packets sent
     0 multicast packets received
     0 incoming packets discarded
     0 outgoing packets discarded
     0 incoming errors
     0 outgoing errors
     0 invalid frames
     0 collisions; 0 carrier errors
     0 input queue drops
     0 output queue drops
wancom0:
     Flags: (0x1043) UP BROADCAST MULTICAST TRAILERS ARP RUNNING
     Type: GIGABIT_ETHERNET
     inet is: 172.30.46.20 Vlan: 0
     Netmask: 255.255.0.0
     Gateway: 172.30.0.1
     Ethernet address is 00:08:25:a2:56:20
     Metric is 0:
     Maximum Transfer Unit size is 1500
     809490537 octets received
     775555 octets sent
     10768436 packets received
     9449 packets sent
     73012 multicast packets received
     74839 incoming packets discarded
     0 outgoing packets discarded
     0 incoming errors
     0 outgoing errors
     0 invalid frames
     0 collisions; 0 carrier errors
     0 input queue drops
     0 output queue drops
left-left (media slot 0, port 0)
     Flags: UP BROADCAST MULTICAST ARP RUNNING
     Type: GIGABIT_ETHERNET
     Admin State: enabled
     Auto Negotiation: enabled
```

```
Internet address: 192.168.0.10     Vlan: 0
Broadcast Address: 192.168.0.255
Netmask: 255.255.255.0
Gateway: 192.168.0.1
Maximum Transfer Unit size is 1500
Ethernet address is 00:08:25:a2:56:23
Virtual Ethernet address is 00:08:25:a2:56:23
Metric is 0
0 octets received
4668396 octets sent
0 packets received
72942 packets sent
0 non-unicast packets received
0 unicast packets received
0 input discards
0 input unknown protocols
0 input errors
0 output errors
0 collisions; 0 dropped
```

> **Note:**
>
> When run on a virtual platform, the show interfaces and show interfaces ethernet commands display auto-negotiation as disabled whenever media port is down, regardless of the ACLI configurations.

Viewing Media Interface Statistics

Display information about the system's media interfaces, if any, by using the show media command. You can also display information about loopback (internal) interfaces, which are logical interfaces used for internal communications.

You can use the following arguments to specify the information you want to view:

- classify—network processor statistics; requires slot and port arguments
- host-stats—host processor statistics, including number of packets received at a specific port and types of packets received; requires slot and port arguments
- frame-stats—frame counts and drops along the host path; does not require port and slot specification
- network—network interface details; does not require port and slot specification
- physical—physical interface information; does not require port and slot specification
- phy-stats—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

For the slot arguments, 1 corresponds to the left Phy slot and 2 corresponds to the right Phy slot on the front of the chassis. For the port argument, the values are 0, 1, 2, and, 3, with 0 corresponding to the leftmost port and 3 corresponding to the rightmost port.

For example:

The RECEIVE STATISTICS and TRANSMIT STATISTICS in the following examples have been abbreviated.

Viewing Network Interface Statistics

The **show media network** command displays configured network interfaces according to IPv4 and IPv6 types.

```
ORACLE# show media  network
 nPApp_Media_max_slots = 3
IPv4 Enabled Interfaces:
Slot/Port:   Vlan   IPAddress      Mask            Gateway       Status
  0/0:       0      192.168.0.10   255.255.255.0   192.168.0.1   enable
IPv6 Enabled Interfaces:
Slot/Port:   Vlan   IPAddress      Mask            Gateway       Status
  0/0:       -      -                              -             -
```

Viewing Physical Interface Statistics

```
ORACLE# show media physical
Slot/Port:      MAC Address             Encap   Connection ID   Frames
Rx
   1/1:  0:          8:25: 1: 0:53       0x0     0x0     0x0
   2/3:  0:          8:25: 1: 0:54       0x0     0x0     0x0
```

Viewing Physical Interface Level Statistics

```
ORACLE# show media phy-stats 0 0
*** RECEIVE STATISTICS ***
 Statistics Counter Name       :     Count (hex)      :  Count
(decimal)
 Rx bytes recd - Upper 32 bits :   0x0000    0x002E   :  46
 Rx bytes recd - Lower 32 bits :   0xB132    0xE69D   :  2972903069
 Rx 64 (Bad + Good)            :   0x0005    0x3392   :  340882
 Rx 65 to 127 (Bad + Good)     :   0x006F    0x6F88   :  7303048
 Rx 128 to 255 (Bad + Good)    :   0x36BA    0xB44C   :  918205516
 Rx 256 to 511 (Bad + Good)    :   0x0004    0x531C   :  283420
 Rx 512 to 1023 (Bad + Good)   :   0x0000    0x02D0   :  720
 Rx 1024 to 1518 (Bad + Good)  :   0x0000    0x0000   :  0
 Rx 1519 to 1530 (Bad + Good)  :   0x0000    0x0000   :  0
 Rx > 1530 (Good)              :   0x0000    0x0000   :  0
 Rx Error Oversized > 1530     :   0x0000    0x0000   :  0
 Rx Good Undersized < 64       :   0x0000    0x0000   :  0
 Rx Error Undersized < 64      :   0x0000    0x0000   :  0
 Rx Unicast Frames In (Good)   :   0x3732    0xBCF4   :  926072052
 Rx Multicast Frames In (Good) :   0x0000    0x93A2   :  37794
 Rx Broadcast Frames In (Good) :   0x0000    0x5CBC   :  23740
 Rx Sync loss / Rx PHY Error   :   0x0000    0x0000   :  0
 Rx GMAC Fifo Full Errors      :   0x0000    0x0000   :  0
 Rx FCS Errors                 :   0x0000    0x0000   :  0
 Rx Delimiter Sequence Errors  :   0x0000    0x0000   :  0
 Rx GMAC Drop count            :   0x0000    0x0000   :  0
 Rx Symbol Error/Alignment err :   0x0000    0x0000   :  0
 Rx Pause Control Frames In    :   0x0000    0x0000   :  0
 Rx Control Frames In          :   0x0000    0x0000   :  0
 Rx Threshold Oversize         :   0x0000    0x0000   :  0
 *** TRANSMIT STATISTICS ***
 Statistics Counter Name       :     Count (hex)      :  Count (decimal)
 Total Xmitted - Upper 32 bits :   0x0000    0x002E   :  46
 Total Xmitted - Lower 32 bits :   0xC35B    0x3BCC   :  3277536204
 Tx 64                         :   0x0011    0x3635   :  1127989
 Tx 65 to 127                  :   0x0084    0xC730   :  8701744
 Tx 128 to 255                 :   0x36AC    0xEA43   :  917301827
 Tx 256 to 511                 :   0x0000    0x0000   :  0
 Tx 512 to 1023                :   0x0000    0x0000   :  0
 Tx 1024 to 1518               :   0x0000    0x0000   :  0
 Tx 1519 to 1530               :   0x0000    0x0000   :  0
 Tx > 1530                     :   0x0000    0x0000   :  0
 Tx Unicast Frames Out         :   0x3742    0xE767   :  927131495
 Tx Multicast Frames Out       :   0x0000    0x0000   :  0
 Tx Broadcast Frames Out       :   0x0000    0x0041   :  65
 Tx FCS Error                  :   0x0000    0x0000   :  0
 Tx Pause Control Frames Out   :   0x0000    0x0000   :  0
 Tx Control Frames Out         :   0x0000    0x0000   :  0
 Tx Bad Frames Fifo Underrun   :   0x0000    0x0000   :  0
 Tx Bad Frames Fifo Overrun    :   0x0000    0x0000   :  0
 Tx Drop Frames Fifo Overrun   :   0x0000    0x0000   :  0
 Tx Bad Frames Parity Error    :   0x0000    0x0000   :  0
 Tx Drop Frames Parity Error   :   0x0000    0x0000   :  0
 Tx Bad Frames Sequence Error  :   0x0000    0x0000   :  0
 Tx Drop Frames Sequence Error :   0x0000    0x0000   :  0
 Tx Bad Frames Jam Bit Error   :   0x0000    0x0000   :  0
 Tx Drop Frames Jam Bit Error  :   0x0000    0x0000   :  0
 Tx Undersized < 64            :   0x0000    0x0000   :  0
 Tx Excess Collisions          :   0x0000    0x0000   :  0
 Tx One Collision              :   0x0000    0x0000   :  0
 Tx > One Collision            :   0x0000    0x0000   :  0
```

show media classify

The **show media classify** command displays counts of packets by type for a given interface. The command is entered as:

```
ORACLE# show media classify <slot> <port>
```

Global packet counters are displayed and classified according to direction and L2/L3. The interface identified by the supplied slot and port combination. The following screen capture is Version S-CZ7.1.2 executed on a Server Edition/VM platform.

```
ORACLE> show media classify 0 0
GLOBAL counters:
    L2 to userspace    : 0
    L3 to userspace    : 0
    L2 from userspace  : 0
    L3 from userspace  : 0
    L2 miss            : 0
INTETERFACE counters: (slot 0, port 0):
    IP pkts received       : 0
    IP VLAN pkts received  : 0
    ARP pkts received      : 0
    VLAN ARP pkts received : 0
    Invalid protocol drops : 0
    NAT miss               : 0
    IP Frag drops          : 0
    Crypto drops           : 0
    Drop error             : 0
    L2 miss                : 0
    L2 miss incomplete     : 0
```

The following screen capture is Version S-CZ7.1.2 executed on the Acme Packet 6300 platform.

```
ORACLE# show media classify 0 0
Slot 0 Port 0 Fastpath Statistics
--------- Ingress Packet Counts ----------|---------Egress Packet 
Counts  -------------
IPv4              :  4545                 | IPv4                :  
114504
IPv6              :  9                    | IPv6                :  12
UDP               :  4545                 | L4                  :  0
TCP               :  0                    | IPSec               :  0
SCTP              :  0                    | vlan                :  0
IPIP              :  0                    | non-vlan            :  
113424
ARP               :  89                   | From Host           :  3335
ICMPv4            :  0                    | Packet Trace Hit    :  0
ICMPv6            :  1                    | Packet Trace Miss   :  0
IPSec             :  0                    | L2 Success          :  1092
vlan              :  0                    | L2 Drop(incomplete) :  0
non-vlan          :  4554                 | L2 Lookup Index     :  0
Frag              :  0                    | L2 Lookup Miss      :  0
Multicast         :  186                  | L2 Lookup Drop      :  0
Latch             :  1092                 | L2 Drop Key1        :  
[0x0000000000000000]
Packet Trace Hit  :  0                    | L2 Drop Key2        :  
[0x0000000000000000]
Packet Trace Miss :  0                    | L2 Drop Key3        :  
[0x0000000000000000]
Nat Match         :  4368                 |
Host Packets      :  3276                 |
Media Packets     :  1092                 |
MAC Filter Drop   :  3794                 |
NAT Miss Drop     :  367                  |
Standby Drop      :  0                    |
IP Drop           :  0                    |
Deny Drop         :  0                    |
Frag Drop         :  0                    |
Rate Drop         :  0                    |
IPsec Drop        :  0                    |
```

Physical Interface Alarms

The following table lists the physical interface alarms.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
LINK UP ALARM GIGPORT	131073	MINOR	Gigabit Ethernet interface 1 goes up.	Slot 1 port 0 UP	linkUp trap generated syslog
LINK UP ALARM GIGPORT	131074	MINOR	Gigabit Ethernet interface 2 goes up.	Slot 2 port 0 UP	linkUp trap generated syslog
LINK DOWN ALARM GIGPORT	131075	MAJOR	Gigabit Ethernet interface 1 goes down.	Slot 1 port 0 DOWN	linkDown trap generated minor dry contact syslog
LINK DOWN ALARM GIGPORT	131076	MAJOR	Gigabit Ethernet interface 2 goes down.	Slot 2 port 0 DOWN	linkDown trap generated minor dry contact syslog
LINK UP ALARM VXINTF	131077	MINOR	Control interface 0 goes up.	Port 0 UP	linkUp trap generated syslog
LINK UP ALARM VXINTF	131078	MINOR	Control interface 1 goes up.	Port 1 UP	linkUp trap generated syslog
LINK UP ALARM VXINTF	131079	MINOR	Control interface 2 goes up.	Port 2 UP	linkUp trap generated syslog
Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
LINK DOWN ALARM VXINTF	131080	MAJOR	Control interface 0 goes down.	Port 0 DOWN	linkDown trap generated minor dry contact syslog
LINK DOWN ALARM VXINTF	131081	MAJOR	Control interface 1 goes down.	Port 1 DOWN	linkDown trap generated minor dry contact syslog
LINK DOWN ALARM VXINTF	131082	MAJOR	Control interface 2 goes down.	Port 2 DOWN	linkDown trap generated minor dry contact syslog
LINK UP ALARM FEPORT	131083	MAJOR	Fast Ethernet slot 1, port 0 goes up.	Slot 1 port 0 UP	linkUp trap generated syslog
LINK UP ALARM FEPORT	131084	MAJOR	Fast Ethernet slot 2, port 0 goes up.	Slot 2 port 0 UP	linkUp trap generated syslog

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
LINK UP ALARM FEPORT	131085	MINOR	Fast Ethernet slot 1, port 1 goes up.	Slot 1 port 1 UP	linkUp trap generated syslog
LINK UP ALARM FEPORT	131086	MINOR	Fast Ethernet slot 2, port 1 up.	Slot 2 port 1 UP	linkUp trap generated syslog
LINK UP ALARM FEPORT	131087	MINOR	Fast Ethernet slot 1, port 2 goes up.	Slot 1 port 2 UP	linkUp trap generated syslog
LINK UP ALARM FEPORT	131088	MINOR	Fast Ethernet slot 2, port 2 goes up.	Slot 2 port 2 UP	linkUp trap generated syslog
LINK UP ALARM FEPORT	131089	MINOR	Fast Ethernet slot 1, port 3 goes up.	Slot 1 port 3 UP	linkUp trap generated syslog
LINK UP ALARM FEPORT	131090	MINOR	Fast Ethernet slot 2, port 3 goes up.	Slot 2 port 3 UP	linkUp trap generated syslog
LINK DOWN ALARM FEPORT	131091	MAJOR	Fast Ethernet slot 1, port 0 goes down.	Slot 1 port 0 DOWN	linkDown trap generated minor dry contact syslog
LINK DOWN ALARM FEPORT	131092	MAJOR	Fast Ethernet slot 2, port 0 goes down.	Slot 2 port 0 DOWN	linkDown trap generated minor dry contact syslog
LINK DOWN ALARM FEPORT	131093	MAJOR	Fast Ethernet slot 1, port 1 goes down.	Slot 1 port 1 DOWN	linkDown trap generated minor dry contact syslog
LINK DOWN ALARM FEPORT	131094	MAJOR	Fast Ethernet slot 2, port 1 goes down.	Slot 2 port 1 DOWN	linkDown trap generated minor dry contact syslog
LINK DOWN ALARM FEPORT	131095	MAJOR	Fast Ethernet slot 1, port 2 goes down.	Slot 1 port 2 DOWN	linkDown trap generated minor dry contact syslog
LINK DOWN ALARM FEPORT	131096	MAJOR	Fast Ethernet slot 2, port 2 goes down.	Slot 2 port 2 DOWN	linkDown trap generated minor dry contact syslog
Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
LINK DOWN ALARM FEPORT	131097	MAJOR	Fast Ethernet slot 1, port 3 goes down.	Slot 1 port 3 DOWN	linkDown trap generated minor dry contact syslog

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Actions
LINK DOWN ALARM FEPORT	131098	MAJOR	Fast Ethernet slot 2, port 3 goes down.	Slot 2 port 3 DOWN	linkDown trap generated minor dry contact syslog

Verifying an IP Address

This section explains how to determine the existence of an IP address, and whether it is up and accepting requests.

You can use the ping command with the IPv4 address to send echo messages that indicate whether a given address is available. In addition the ping command returns the following information:

- time in milliseconds it took the ICMP packets to reach the destination and return
- statistics that indicate the number of packets transmitted, the number of packets received, and the percentage of packet loss.
- time in milliseconds for the minimum, average, and maximum RTTs. The default timeout is 64 milliseconds.

The following example shows the ping command used with IPv4 address 10.0.0.1:

```
ORACLE# ping 172.30.1.150
PING 172.30.1.150: 56 data bytes
64 bytes from 172.30.1.150: icmp_seq=0. time=1. ms
64 bytes from 172.30.1.150: icmp_seq=1. time=0. ms
64 bytes from 172.30.1.150: icmp_seq=2. time=0. ms
64 bytes from 172.30.1.150: icmp_seq=3. time=0. ms
----172.30.1.150 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/1
```

> **Note:**
>
> The system does not allow you to ping from a secondary SBC media interface, presenting a warning if you try. This prevents you from creating conflicts in the resolution of your interfaces in neighboring switches.

Specifying a Source Address for ICMP Pings

The Oracle Communications Session Border Controller's **ping** command can also be used to set the source IP address (a valid network interface) to use when sending ICMP pings. You must enter the IP address for the entity you want to ping first, followed by the source IP address.

To specify a source address for an ICMP ping:

- At the main system prompt, type ping and a Space, the IP address of the entity you want to ping, the network interface, and then the source IP address you want to use, and then press Enter.

  ```
  ORACLE # ping 124.7.58.6 core:0 172.30.56.6
  ```

Traceroute Command

The system can trace the route of an IP packet to an Internet host by sending probe packets and listening to responses from gateways along the route. Use the traceroute command to see each host route and the round trip time of packets received from each host in a route for diagnostic purposes.

The traceroute command sends probe packets that start with a maximum time-to-live (TTL) value of one. The system listens for an Internet Control Message Protocol (ICMP) error message in response to the TTL expiry, and records the source that sent the ICMP error message. The system repeats this process and increments the TTL value by 1 for each hop in the route to the final destination.

The traceroute command returns the following information, which allows tracing the packet route to its destination.

- TTL value
- IP address of each host along the route
- Amount of time that it takes for each probe packet to travel to each host in the route

Notes:

- Unless otherwise specified, the system sends three probe packets to each host.
- The traceroute command is only available in software versions of the Oracle Communications Session Border Controller, for example, Server Edition (SE) and Virtual Machine Edition (VME). For more information on supported platforms, see "Platform Support."

For traceroute command syntax and arguments, see "Traceroute Command Specifications."

Examples

The following example traces the route to IP address 172.30.0.167, identifying each host in the route and the amount of time that it takes for each of three probe packets to travel to each host. The first three probe packets reach the host at 172.44.0.1 in times ranging from less than one to a little over two milliseconds. The next three probe packets reach the route destination at IP address 172.30.0.167 all in less than one millisecond.

```
ORACLE# traceroute 172.30.0.167
traceroute to 172.30.0.167
1 172.44.0.1 (0.669003 ms) (2.140045 ms) (2.290964 ms)
2 172.30.0.167 (0.25602 ms) (0.219822 ms) (0.604868 ms)
```

The following example traces the route to IP address 172.30.0.167 but specifies the use of 4 probe packets instead of the default of 3.

```
ORACLE traceroute 172.30.0.167 probes 4
traceroute to 172.30.0.167
1 172.44.0.1 (0.549003 ms) (1.180045 ms) (2.920584 ms) (2.48541 ms)
2 172.30.0.167 (0.25802 ms) (0.220822 ms) (0.454868 ms) (0.387574)
```

The following example specifies that the traceroute command is issued to the IP address over the user-specified network interface private and VLAN 123.

```
ORACLE traceroute 10.1.2.6 intf-name:vlan private:123
traceroute to 10.1.2.6
1 10.1.2.6 (0.265121 ms) (0.599080 ms) (0.0184195 ms)
```

The following example specifies that the wait for a response timeout is 4 seconds. The default value is three seconds.

```
ORACLE traceroute 10.1.2.6 timeout 4
traceroute to 10.1.2.6
1 10.1.2.6 (0.265121 ms) (0.199080 ms) (0.0284195 ms)
```

The following example specifies that the traceroute starts at a user-specified source IP address of 172.20.22.31 to a destination IP address of 10.25.2.10.

```
ORACLE traceroute 172.20.22.31 source-ip 10.25.2.10
traceroute to 172.20.22.31
172.20.22.31 (0.284121 ms) (0.499770 ms) (0.084595 ms)
```

Traceroute Command Specifications

The traceroute command traces the route of an IP packet to an Internet host by sending probe packets with small maximum time-to-live (TTL) values and listening to responses from gateways along the path. This diagnostic command provides the route (path) and the round trip times of packets received from each host in a route.

The traceroute command works by sending probe packets starting with a maximum time-to-live (TTL) value of one, listening for an ICMP error message in response to the TTL expiry, and recording the source that sent it. This process is repeated by incrementing the TTL value by 1 each time until the final destination is reached. This information allows the path to be traced for the packet to reach its destination.

Syntax

```
traceroute <destination-address> <options>
```

Arguments

<destination-address> — Specifies the destination IP address for the route to be traced.

<intf-name:vla> — Specifies the network interface and VLAN to use.

<max_ttl> — Specifies the maximum number of hops before timeout.

- Default — 30
- Values — Min: 1 / Max: none

<probes> — Specifies the number of probes to send.

<source-ip> — Specifies the source IP address from which to trace the route to the destination IP address.

<timeout> — Specifies the maximum time (in seconds) to wait for a response.

- Default — 3
- Values — Min: 1 / Max: none

Mode

Superuser

Example

```
ORACLE# traceroute 172.30.0.167 probes 4
traceroute to 172.30.0.167
1 172.44.0.1 (0.669003 ms) (2.140045 ms) (2.290964 ms) (2.40891 ms)
2 172.30.0.167 (0.25602 ms) (0.219822 ms) (0.604868 ms) (0.398874)
```

DNS Statistics

You can monitor DNS statistics using the ACLI **show dns** command. The information displayed includes the following:

- Queries—The number of DNS queries initiated.
- Successful—The number of DNS queries completed successfully.
- NotFound—The number of DNS queries that did not result in DNS resolution.
- TimedOut—The number of DNS queries that timed out.

To get DNS statistics, use either the ACLI **show dns** or **show dns stats** command. Both return the same output. For example:

```
ORACLE# show dns
18:20:18-16
             ---Queries----  --Successful--  ---NotFound---  ---
TimedOut---
DNS Intf Name   Current  Total  Current  Total  Current  Total  Current
Total
M10                 1       1       0       0       0       0       1
1
```

Viewing DNS Statistics for Specific Cache Entries

To view DNS statistics for specific cache entries, use the **show dns cache-entry** command. You must include both the realm name and the entry ID as arguments to avoid receiving an error message. Your cache key entries must appear in one of the following formats:

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

A successful inquiry appears as follows:

```
ORACLE# show dns cache-entry core A:abc.sipp.com
Query-->
        Q:A abc.sipp.com ttl=86329
Answers-->
         172.16.0.191
```

DNS Queries on the Command Line

Users can perform Domain Name Services (DNS) queries from the command line. Positive results are added to the DNS cache.

Currently the SIP proxy agent issues DNS queries to find the Serving Call Session Control Function (S-CSCF) from a SIP invite or a SIP registration event. A user can perform these same DNS queries from the command line, both with and without the use of the local DNS cache.

The command to first query the local DNS cache and then perform an external DNS query (if needed) is **show dns lookup** with the following parameters:

- realm—Realm name to use for DNS cache lookup key.
- type—Type of DNS query.
  - A for IPv4 lookup
  - AAAA for IPv6 lookup
  - SRV for service recod
  - NAPTR for naming authority pointers
- name—FQDN of DNS name to lookup.

To perform a manual external DNS query with no cache lookup, issue the **show dns query** command with the following parameters:

- realm—Realm name to use for DNS cache lookup key.
- type—Type of DNS query.
  - A for IPv4 lookup
  - AAAA for IPv6 lookup
  - SRV for service recod
  - NAPTR for naming authority pointers
- name—FQDN of DNS name to lookup.

Clearing ENUM and DNS Statistics

To clear statistics for DNS, you can use additions to the ACLI **reset** command. Before you reset the counters, however, you might want to confirm the current statistics on the system are not zero. You can do so using the **show dns** command.

The **reset** command takes the DNS arguments to clear those sets of statistics. When you use the command, the system notifies you whether it has successfully cleared the statistics (even if the counter are zero) or if it has run into an error causing the command to fail.

You can **reset all** system statistics using the reset all command.

This section shows you how to clear DNS statistics. The sample below shows the error message that appears if the command fails.

To clear DNS statistics:

- At the command line, type **reset dns** and then press Enter.

  ```
  ORACLE# reset dns
  SIP DNS statistics not available
  ```

System Support Information for Troubleshooting

The **show support-info** command allows you to gather a set of information commonly requested by Oracle Support when troubleshooting customer issues.

The **show support-info** syntax is as follows:

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

- custom—Uses the /code/supportinfo.cmds file to determine what commands should be encompassed. If the file does not exist, then the system notifies you.
- standard—Displays information for all commands the **show support-info** command encompasses.
- media—Executes and writes out only the show media commands to the support-info.log file.
- signaling—Executes and writes all but the ACLI commands that display signaling data to the support-info.log file.
- config—Add the **show running-config** output to the output of the standard arguments.
- file-only—Disables the output of commands to stdout and instead appends that output to the file support-info.log.

In all cases, the system displays the command's output on the screen and writes the output to the support-log.info file (stored in /opt/logs).

Each time the **show support-info** command is executed a new support-info.log file is created. The previous support-info.log file is renamed by appending a .1 to the end of the file name. All additional support-info.log files are renamed to their previous number, plus 1. The Oracle Communications Session Border Controller maintains up to 6 support-info files: support-info.log and support-info.log.1 through support-info.log.5.

For example, when executing the **show support-info** command, a new support-info.log file is created. The existing support-info.log file is renamed to support-info.log.1. The existing support-info.log.1 file is renamed to support-info.log.2, and so on. If a support-info.log.5 exists prior to executing the **show support-info** command, it is deleted from the system when rotating the files.

The **show support-info** command combines the output of several ACLI commands into a single command. These include:

Included Data

This command combines the output of several other ACLI commands into a single command, which are listed in the table below.

Data Group	Included Data
General System Commands	• show clock • show version image • show version boot • show sipd spl • show prom-info all • display-alarms • show process • show arp • show sessions • show features • show memory • show buffers • show health • display-current • display-run • show user • check-space-remaining code • check-space-remaining ramdrv • check-space-remaining hard-disk • show process cpu all • show spl
Physical Interface Commands	• show interfaces • show media physical • show media phy-stats • show media host-stats • show media classify • show media network • show media frame-stats • show media tm-stats • dump-etc-stats
SIP Commands	• show registration • show sipd all • show sipd agent
H323 Commands	• show h323 • show h323 h323stats • show h323 agentstats • show h323 stackCallstats • show h323 stackPvtStats • show h323 stackDisconnectInstate • show h323 stacklist

Data Group	Included Data
Call Media Commands	• show mbcd all • show mbcd realms • stack mbcd
Security Commands	• show security certificates brief • show security ssh-key • show security ssm-accelerator • show security tls session-cache
Other Commands	• ipt show all • show acl info • show acl summary • show acl all (only in signaling) • show ip connections (only in signaling) • show dns stats • show enum stats • show routes

Using the ACLI show support-info command

To gather and ship information to Oracle Support using the **show support-info** command:

1. Select a meaningful filename for the file to which you will send data.
2. In either User or Superuser mode, type **show support-info** at the prompt. Include the name of the file you want to send the information to as follows:

   ```
   ORACLE# show support-info 10102006
   ```

3. SFT the file to Oracle Support.

support-info command

To Display information on the screen gathered from the show support-info command:

1. In either User or Superuser mode, type **show support-info** at the prompt. Include more if you want to view the information one page at a time.

   ```
   ORACLE# show support-info more
   ```

2. At the prompt at the bottom of the window, select one of the following ways to view further information:
   - Enter a **q** to exit and return to the system prompt
   - Press the <enter> key to view the next page
   - Press the <space> bar to view the information through the end

System Configuration Listing

The show support info command can append the complete running config output (**show running-config**) to the end of the support output file by adding the config argument to the end of any show support-info command, except show support-info custom. For example:

ORACLE# **show support-info standard config**

SLB Information

The following show commands have been added so that more SLB-related debug information is available in the **show support-info** output.

- **show sip tunnels** is added to show **support-info** and **show support-info** signaling
- **show sip ccp** is added to show **support-info** and **show support-info** signaling
- **show sip lb-endpoints** is added to **show support-info** and **show support-info** signaling

The following changes have been made to avoid this situation on the Oracle Session Load Balancer image (LCX image):

- **show ccd ccp** is added **show support-info**

SIP Interface Constraints Monitoring

The session constraints configuration allows you to set up a body of constraints that you can then apply them to a SIP interface. 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.

SIP interfaces have two states: “In Service” and “Constraints Exceeded.” When any one of the constraints is exceeded, the status of the SIP interface changes to Constraints Exceeded and remains in that state until the time-to-resume period ends. The session constraint timers that apply to the SIP interface are the time-to-resume, burst window, and sustain window.

You can view information about constraints for a SIP interface by using the **show sipd interface** command. Using that command, you can show statistics for all SIP interfaces, or for one that you specify when you carry out the command.

All SIP Interfaces

To display statistical information for all SIP interfaces:

- Type **show sipd interface** at the command line and then press Enter. The results will resemble the following example.

```
ORACLE# show sipd interface
19:38:17-18
          ---- Inbound ---- --- Outbound ---- -Latency-  --- Max ---
Realm     Active Rate ConEx Active Rate ConEx  Avg  Max Burst In Out
external       0 0.0      0      0  0.0     0  0.0  0.0     0  0   0
```

Single SIP Interface

To display statistical information for a single SIP interfaces:

- Type **show sipd interface** at the command line, followed by the realm identifier for that interface, and then press Enter. The results will resemble the following example.

```
ORACLE# show sipd interface internal
19:46:10-37
Sip Interface internal(internal) [In Service]
                             -- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Inbound Sessions        0       0       0          0       0       0
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
Outbound Sessions       1       1       1          1       1       1
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
Out of Service          -       -       0          0       0       -
Trans Timeout           0       0       0          0       0       0
Requests Sent           -       -       1          1       1       -
Requests Complete       -       -       1          1       1       -
Messages Received       -       -       3          3       2       -
Latency=0.013; max=0.013
```

Displaying and Clearing Registration Cache Entries

The Oracle Communications Session Border Controller’s registration cache management for all protocols offers detailed information (beyond basic registration cache displays) and flexible ways to work with SIP and H.323 registrations. You can query, clear and audit entries.

Working with the SIP Registration Cache

There are two ways to view basic SIP registration cache statistics. The **show sipd endpoint-ip** command displays information regarding a specific endpoint, and the **show registration** command displays statistics for the SIP registration. These commands still remain.

There are additional commands let you view SIP registration cache information, and to clear and audit information from the cache.

Displaying the SIP Registration Cache

You can view the SIP registration cache by using one of the following commands:

- **show registration sipd by-ip <ipaddress>**—Displays the Oracle Communications Session Border Controller’s SIP process registration cache for a specified IP address. The IP address value can be a single IP address or a wildcarded IP address value that has an asterisk (*) as its final character.
  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.
- **show registration sipd by-realm <realm>**—Display information for calls that have registered through a specified ingress realm. Enter the realm whose registration cache information you want to view. This value can be wildcarded.

- **show registration sipd by-registrar <ipaddress>**—Display information for calls that use a specific registrar. Enter the IP address of the registrar whose registration cache information you want to view. This value can be wildcarded.
- **show registration sipd by-route <ipaddress>**—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.
- **show registration sipd by-user <endpoint>**—Displays the Oracle Communications Session Border Controller’s SIP process registration cache for a specified phone number or for a user name. That is, the **<endpoint>** portion of the command you enter depends on how the SIP endpoint is registered. For example, an endpoint might be registered as 7815551234@10.0.0.3 or as username@10.0.0.3. The value preceding the at-sign (@) is what you enter for the **<endpoint>**.
  The phone number can be a single number (such as 7815551234) or a single number wildcarded by placing an asterisk (*) (such as 7815551*) at the end of the phone number. The user name can be a single name (such as user), or a single name wildcarded by using an asterisk at the end of the user name (such as us*).

  There are brief and detailed versions of this display. To see the detailed version, add the **detail** argument to the end of your entry.

  The following is a sample of this command’s output for the brief view:

```
ORACLE> show registration sipd by-user user*
Registration Cache                                TUE JUL  11:29:50 UTC
2007
                                        Num
User                              Contacts   Registered at
--------------------------------- --------   -------------------
sip:user@acme.com                        1   2007-07-26-11:29:50
sip:username@acme.com                    1   2007-07-26-11:29:51
sip:username2@acme.com                   1   2007-07-26-11:29:51
ORACLE>
```

  You can add the **detail** argument to view this command’s output with detailed information:

```
ORACLE> show registration sipd by-user user@acme.com detail
Registration Cache (Detailed View)                TUE JUL  11:32:21 UTC
2007
User: sip:user@acme.com
      Registered at:  2007-07-26-11:32:21    Surrogate User: false
  Contact Information:
    Contact Name: sip:user@acme.com valid: false, challenged: false
              Via-Key: 172.30.80.4
              Registered at: 2007-07-26-11:32:21
              Last Registered at: 2007-07-26-11:32:21
              state:  <expired>
              Transport: <none>,   Secure: false
              Local IP: 172.30.80.180:5060
              User Agent Info:
              Contact: sip:user-acc-
m2vmeh72n09kb@127.0.0.15:5060;transport=udp
              Realm: access,  IP: 172.30.80.4:5060
              SD Contact: sip:user-p3rrurjvp0lvf@127.0.0.10:5060
              Realm: backbone
ORACLE>
```

The following is a sample of the **show registration sipd by-realm** command’s output:

```
ORACLE# show registration sipd by-realm access
Registration Cache                    WED JUN 25 2008  09:12:03
  Realm           User                             Registered at
----------------- --------------------------------
------------------
  access          sip:16172345687@192.168.12.200
2008-06-25-09:00:32
  access          sip:3397654323@192.168.12.200
2008-06-25-09:00:40
----------------- --------------------------------
------------------
Total: 2 entries
```

The following is a sample of the **show registration sipd by-registrar** command’s output:

```
ORACLE# show registration sipd by-registrar *
Registration Cache                    WED JUN 25 2008  09:06:28
  Registrar
  IP Address      User                             Registered at
----------------- --------------------------------
------------------
  0.0.0.0         sip:16172345687@192.168.12.200
2008-06-25-09:00:32
  0.0.0.0         sip:3397654323@192.168.12.200
2008-06-25-09:00:40
----------------- --------------------------------
------------------
Total: 2 entries
```

The following is a sample of the **show registration sipd by-route** command’s output:

```
ORACLE# show registration sipd by-route 192.168.11.101
Registration Cache                    WED JUN 25 2008  09:06:04
  Routable
  IP Address      User                             Registered at
----------------- --------------------------------
------------------
  192.168.11.101  sip:3397654323@192.168.12.200
2008-06-25-09:00:40
----------------- --------------------------------
------------------
Total: 1 entry
```

Clearing the SIP Registration Cache

You can clear the SIP registration cache by using one of the following commands:

- **clear-cache registration sipd all**—Clears all SIP registrations in the cache.
- **clear-cache registration sipd by-ip <ipaddress>**—Clears the Oracle Communications Session Border Controller's SIP process registration cache of a particular IP address. The IP address value can be a single IP address or an IP address range in the form n.n.n.n/nn.
- **clear-cache registration sipd by-user <endpoint>**—Clears the Oracle Communications Session Border Controller's SIP process registration cache of a particular phone number. The phone number can be a single number (7815554400). You can also enter a user name for this value.

Note that you cannot wildcard values for commands to clear the SIP registration cache. When you use one of these commands, the system asks you to confirm clearing the applicable cache entries.

Auditing the SIP Registration Cache

You can audit the SIP registration cache by using one of the following commands:

- **request audit registration sipd by-ip <ipaddress>**—Audits a specified IP address in the SIP registration cache.
- **request audit registration sipd by-user <endpoint>**—Audits a specific user by specifying the phone number in the SIP registration cache. You can also enter a user name for this value.

Note that you cannot wildcard values for commands to audit the SIP registration cache. Expired entries are automatically cleared.

Working with the H.323 Registration Cache

The ACLI displays the number of cached H.323 entries when you use the basic **show h323d registrations** command. Using this command with a registration key displays information about a single H.323 cached entry.

Additions to this command allow you to view detailed H.323 registration cache information based on a specific phone number or terminal identifier. You can also clear and audit the cache.

Displaying the H.323 Registration Cache

You can view the H.323 registration cache by using the **show registration h323d by-alias <endpoint>** command. For the **<endpoint>** portion of the entry, use a phone number or terminal identifier. You can wildcard the **<endpoint>** value by using an asterisk (*) as the final character in the terminalAlias string.

There are brief and detailed versions of this display. To see the detailed view, add the **detail** argument to the end of your entry.

The following is a sample of this command’s output for the brief view:

```
ORACLE# show registration h323d by-alias 4278_endp
Registration Cache                                FRI AUG  20:22:00
2007
Endpoint                          Expiration      Registered at
--------------------------------- --------------- -------------------
4278_endp                         27              2007-08-03-19:58:34
ORACLE#
```

You can add the **detail** argument to view this command’s output with detailed information:

```
ORACLE# show registration h323d by-alias 4224_endp detail
Registration Cache (Detailed View)                TUE JUL 14:51:59 007
Endpoint: 4224_endp,  state: Registered
  Registered at: 2007-04-24-14:50:05
  Expiration: 204
  Gatekeeper: open-gk1
  Endpoint NAT Address: 192.168.200.56:1372
  SD Call Signaling Address: 150.150.150.10:2048
  SD RAS Address: 150.150.150.10:8200
  Terminal Alias(s):
    Alias: e164: 17815552222,  Registered: true
  Call Signaling Address(s):
    Address: 192.168.200.56:1720
  RAS Address(s):
    Address: 192.168.200.56:1372
```

Clearing the H.323 Registration Cache

You can clear the H.323 registration cache by entering one of the following commands:

- **clear-cache registration h323d all**—Clears all H.323 registrations in the registration cache.
- **clear-cache registration h323d by-alias <endpoint>**—Clears H.323 registrations from the registration cache based on a phone number or terminal identifier.

Note that you cannot wildcard values for commands to clear the H.323 registration cache. When you use one of these commands, the system asks you to confirm clearing the appropriate cache entries.

Auditing the H.323 Registration Cache

You can audit the H.323 registration cache by entering one of the following commands:

- **request audit registration h323 <terminalAlias>**—Audits the H.323 registration cache based on a phone number or terminal identifier.

Session Management for SIP H.323 and IWF

Using the session management feature, you can display and manage SIP, H.323, and IWF sessions using a range of new ACLI commands. You can choose to view summary or detailed displays.

If you choose to terminate a session that is already in progress, the Oracle Communications Session Border Controller tears down the session and returns:

- SIP BYE with a reason header naming administrative preemption as a cause, and where the cause code is 3
- H.323 Disconnect with Q.850 disconnect cause code 8, preemption

Note that if your system is carrying a heavy traffic load, it could take a good amount of time to display or clear sessions. When you use these commands, a reminder will appear about the fact that it can take up to thirty seconds for the command to complete.

Displaying Sessions

You can display SIP, H.323 and IWF sessions using the ACLI **show <protocol type> sessions** command. This command now takes the following additional arguments:

- **all**—Displays all SIP or H.323 sessions for the protocol you specify.
- **by-agent**—When entered with the name of a configured session agent, displays session information for the specified session agent: adding **iwf** to the very end of the command shows sessions for IWF; adding **detail** to the very end of the command expands the displayed information
- **by-ip**—When entered with the IP address of an endpoint, displays session information for the specific endpoint; adding **iwf** to the very end of the command shows sessions for IWF; adding **detail** to the very end of the command expands the displayed information Entries for the IP address portion of this command must be enclosed in quotation marks ()
- **by-user**—When entered with the calling or called number, displays session information for the specified user; adding **iwf** to the very end of the command shows sessions for IWF; adding **detail** to the very end of the command expands the displayed information
- **by-callid**—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

Example 1 Displaying All SIP Sessions

The following is an example of a display showing all SIP sessions.

```
ORACLE# show sipd sessions all
-----------------------------------------------------------------
Displaying Sessions 'all' expression ''
 This may take up to 30 seconds
-----------------------------------------------------------------
   CallID(S)  1139b3d8-1d0010ac-13c4-12557b-146c746b-12557b@127.0.0.11
(ESTABLISHED)
   CallID(C)  SDo6d9601-05da1dd13301cad1523806354168b28b-v3000i1
 IWF Call Leg is = SERVER
  From (Server)
    Realm       sip172 SA=127.0.0.11
    From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=113783f0-1d0010ac-13c4-
12557b-426bb44b-12557b
    To-URI
<sip:1180000@127.0.0.100:5060;transport=UDP>;tag=SDo6d9699-000001200008
8798
    Contact-URI <sip:2180000@127.0.0.11:5060;transport=UDP>
  To (Client)
    Realm       h323192fs; SA=192.168.200.29
    From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SDo6d9601-113783f0-1d00
10ac-13c4-12557b-426bb44b-12557b
    To-URI
<sip:1180000@192.168.200.29:1720;acme_sa=192.168.200.29;acme_realm=h323
192fs;acme_irealm=sip172;acme_iwf_itrusted>;tag=0000012000088798
    Contact-URI
<sip:1180000@127.0.0.1:5070;acme_sa=192.168.200.29;acme_realm=h323192fs
;acme_iwf_itrusted>
------------------------------------------------------------------
Displayed 1 out of total of 1 Sessions (msg=1)
------------------------------------------------------------------
ORACLE#
```

Example 2 Displaying All H.323 Sessions

The following is an example of a display showing all H.323 sessions.

```
ORACLE# show h323d sessions all
------------------------------------------------------------------
Displaying Sessions 'all' expression ''
 This may take up to 30 seconds
------------------------------------------------------------------
   CallID(S)  SDo6d9601-05da1dd13301cad1523806354168b28b-v3000i1 ()
   CallID(C)  80834d3a4200001f0110090e2f3cc51b
 IWF Call Leg is = SERVER
  From (Server)
    Realm
    From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SDo6d9601-113783f0-1d00
10ac-13c4-12557b-426bb44b-12557b
    To-URI      <sip:1180000@127.0.0.100:5060;transport=UDP>
  To (Client)
    Realm    ; SA=192.168.200.29
    From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SDo6d9601-113783f0-1d00
10ac-13c4-12557b-426bb44b-12557b
    To-URI      <sip:1180000@127.0.0.100:5060;transport=UDP>
------------------------------------------------------------------
Displayed 1 out of total of 1 Sessions (msg=1)
------------------------------------------------------------------
ORACLE#
```

Example 3 Displaying SIP Sessions for a Session Agent

The following is an example of a display showing SIP sessions for a specified session agent.

```
ORACLE# show sipd sessions by-agent 127.0.0.11
------------------------------------------------------------------
Displaying Sessions 'by-agent' expression '127.0.0.11'
 This may take up to 30 seconds
------------------------------------------------------------------
   CallID(S)  1139b3d8-1d0010ac-13c4-12557b-146c746b-12557b@127.0.0.11
(ESTABLISHED)
   CallID(C)  SDo6d9601-05da1dd13301cad1523806354168b28b-v3000i1
 IWF Call Leg is = SERVER
  From (Server)
    Realm       sip172 SA=127.0.0.11
    From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=113783f0-1d0010ac-13c4-12557b
-426bb44b-12557b
    To-URI
<sip:1180000@127.0.0.100:5060;transport=UDP>;tag=SDo6d9699-0000012000088798
    Contact-URI <sip:2180000@127.0.0.11:5060;transport=UDP>
  To (Client)
    Realm       h323192fs; SA=192.168.200.29
    From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SDo6d9601-113783f0-1d0010ac-1
3c4-12557b-426bb44b-12557b
    To-URI
<sip:1180000@192.168.200.29:1720;acme_sa=192.168.200.29;acme_realm=h323192fs;
acme_irealm=sip172;acme_iwf_itrusted>;tag=0000012000088798
    Contact-URI
<sip:1180000@127.0.0.1:5070;acme_sa=192.168.200.29;acme_realm=h323192fs;acme_
iwf_itrusted>
------------------------------------------------------------------
Displayed 1 out of total of 1 Sessions (msg=1)
------------------------------------------------------------------
ORACLE#
```

Example 3 Displaying H.323 Sessions for a Session Agent

The following is an example of a display showing H.323 sessions for a specified session agent.

```
ORACLE# show h323d sessions by-agent 192.168.200.29
------------------------------------------------------------------
Displaying Sessions 'by-agent' expression '192.168.200.29'
 This may take up to 30 seconds
------------------------------------------------------------------
   CallID(S)  SDo6d9601-05da1dd13301cad1523806354168b28b-v3000i1 ()
   CallID(C)  80834d3a4200001f0110090e2f3cc51b
 IWF Call Leg is = SERVER
  From (Server)
    Realm
    From-URI
```

```
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SDo6d9601-113783f0-1d00
10ac-13c4-12557b-426bb44b-12557b
    To-URI      <sip:1180000@127.0.0.100:5060;transport=UDP>
  To (Client)
    Realm    ; SA=192.168.200.29
    From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SDo6d9601-113783f0-1d00
10ac-13c4-12557b-426bb44b-12557b
    To-URI      <sip:1180000@127.0.0.100:5060;transport=UDP>
------------------------------------------------------------------
Displayed 1 out of total of 1 Sessions (msg=1)
------------------------------------------------------------------
ORACLE#
```

Example 4 Displaying SIP Sessions for a Call ID

The following is an example of a display showing SIP sessions for a specified call ID.

```
ORACLE# show sipd sessions by-callId A899FD1C-8D4F-4E6C-921C-
F45F5CD5DFC9@192.168.11.101
<call-id>                     Call-Id
< sessions by-callId A899FD1C-8D4F-4E6C-921C-
F45F5CD5DFC9@192.168.11.101
------------------------------------------------------------------
Displaying Sessions 'by-callId' expression 'A899FD1C-8D4F-4E6C-921C-
F45F5CD5DFC9@192.168.11.101'
 This may take up to 30 seconds
------------------------------------------------------------------
   CallID     A899FD1C-8D4F-4E6C-921C-F45F5CD5DFC9@192.168.11.101
(ESTABLISHED)
  From (Server)
    Realm       access SA=192.168.12.100
    From-URI    "poza"<sip:333@192.168.12.200:5060>;tag=43629539029921
    To-URI      <sip:1234@192.168.12.200:5060>;tag=EE9B4A00-BFF07BF1
    Contact-URI <sip:333@192.168.11.101:5060>
  To (Client)
    Realm       core
    From-URI    "poza"<sip:333@192.168.12.200:5060>;tag=43629539029921
    To-URI      <sip:1234@192.168.12.200:5060>;tag=EE9B4A00-BFF07BF1
    Contact-URI <sip:1234-
dcgkuvfb53ne8@192.168.12.100:5060;transport=udp>
------------------------------------------------------------------
   CallID     A899FD1C-8D4F-4E6C-921C-F45F5CD5DFC9@192.168.11.101
(ESTABLISHED)
  From (Server)
    Realm       core
    From-URI    "poza"<sip:333@192.168.12.200:5060>;tag=43629539029921
    To-URI      <sip:1234@192.168.12.200:5060>;tag=EE9B4A00-BFF07BF1
    Contact-URI
<sip:333-3sd0uq3ad3a65@192.168.12.100:5060;transport=udp>
  To (Client)
    Realm       access
    From-URI    "poza" <sip:333@192.168.12.200:5060>;tag=43629539029921
    To-URI      <sip:1234@192.168.12.200:5060>;tag=EE9B4A00-BFF07BF1
    Contact-URI <sip:1234@192.168.11.102>
------------------------------------------------------------------
Displayed 2 out of total of 2 Sessions (msg=1)
```

Clearing Sessions

You can clear sessions from the Oracle Communications Session Border Controller with the **clear-sess** command. You can clear all sessions, or you can:

- Clear sessions for a specific session agent (**by-agent**)
- Clear sessions for a specific call by using the call identifier (**by-callid**)
- Clear sessions for a specific IP address (**by-ip**, where you enter the IP address in quotation marks ())
- Clear sessions for a specific user by using the called or calling number (**by-user**)

Example 1 Clearing All SIP Sessions

The following is an example of clearing all SIP sessions from the Oracle Communications Session Border Controller.

```
ORACLE# clear-sess sipd sessions all
------------------------------------------------------------------
Clearing Sessions 'all' expression ''
 This may take up to 30 seconds
------------------------------------------------------------------
   CallID(S)  1139b3d8-1d0010ac-13c4-12568b-333eb709-12568b@127.0.0.11
(ESTABLISHED)
   CallID(C)  SDpmd9601-8a9346384f02a41972cf4e65d7b692be-v3000i1
 IWF Call Leg is = SERVER
  From (Server)
    Realm       sip172 SA=127.0.0.11
    From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=113783f0-1d0010ac-13c4-12568b
-3ce7f7a6-12568b
    To-URI
<sip:1180000@127.0.0.100:5060;transport=UDP>;tag=SDpmd9699-0000022c000a0e38
    Contact-URI <sip:2180000@127.0.0.11:5060;transport=UDP>
  To (Client)
    Realm       h323192fs; SA=192.168.200.29
    From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SDpmd9601-113783f0-1d0010ac-1
3c4-12568b-3ce7f7a6-12568b
    To-URI
<sip:1180000@192.168.200.29:1720;acme_sa=192.168.200.29;acme_realm=h323192fs;
acme_irealm=sip172;acme_iwf_itrusted>;tag=0000022c000a0e38
    Contact-URI
<sip:1180000@127.0.0.1:5070;acme_sa=192.168.200.29;acme_realm=h323192fs;acme_
iwf_itrusted>
Clear Call [y/n]?: y
*** Call Cleared ***
------------------------------------------------------------------
Cleared 1 Sessions
```

```
-------------------------------------------------------------------
ORACLE#
```

Example 2 Clearing an H.323 Session by User

The following is an example of clearing an H.323 session for a specific user from the Oracle Communications Session Border Controller.

```
ORACLE# clear-sess h323d sessions by-user 2180000
-------------------------------------------------------------------
Clearing Sessions 'by-user' expression '2180000'
 This may take up to 30 seconds
-------------------------------------------------------------------
   CallID(S)  SD70bp801-c3ab2f185aa73aca37d1fc619ec16a2f-v3000i1 ()
   CallID(C)  c080c5f0c600001f0112090e2f3cc51b
 IWF Call Leg is = SERVER
  From (Server)
    Realm
    From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SD70bp801-1138cd28-1d00
10ac-13c4-1257b5-1a5eebc4-1257b5
    To-URI      <sip:1180000@127.0.0.100:5060;transport=UDP>
  To (Client)
    Realm    ; SA=192.168.200.29
    From-URI
<sip:2180000@127.0.0.11:5060;transport=UDP>;tag=SD70bp801-1138cd28-1d00
10ac-13c4-1257b5-1a5eebc4-1257b5
    To-URI      <sip:1180000@127.0.0.100:5060;transport=UDP>
Clear Call [y/n]?: y
*** Call Cleared ***
 Retrying the command
-------------------------------------------------------------------
Cleared 1 Sessions
-------------------------------------------------------------------
ORACLE#
```

Datapath monitor alarm

The datapath monitor alarm monitors the load on some of the major hardware components that packets traverse within the Oracle Communications Session Border Controller. These components collectively make up the datapath. The datapath overload alarm is non-health affecting, but when enabled, new SIP calls received by the Oracle Communications Session Border Controller are rejected. Existing calls remain unaffected.

The datapath monitor alarm identifies the physical interface over which the offending traffic was received.

```
ORACLE# display-alarms
4 alarms to show
131200      0       4       2006-05-23 06:35:49    2006-05-23 06:35:49
```

```
Count       Description
1    Datapath Interface slot 0 port 0 is overloaded
```

For the alarm to clear, ETC CPU and ETC Memory loads must all fall below overload threshold.

Valid alarm IDs for the datapath monitor alarm are: 131200-131328

Datapath Watchdog Timer and SNMP Trap Generation

The Oracle Communications Session Border Controller's datapath watchdog timer performs periodic background checks on the continuity of the data path.

Under certain conditions, the internal data path may be interrupted. If packets do not flow long enough for the datapath watchdog timer to expire, a core dump is created and the system can automatically restart or fail over to a standby. This feature is enabled by default and is not configurable.

If SNMP is enabled, the system can also send a trap. Specifically, the system would send the **apSysMgmtHardwareErrorTrap** with the message **Datapath Watchdog: Failures detected on the mainboard**.

Software Worker Threads Watchdog Timer and Health Check Trap

The Oracle Communications Session Border Controller monitors specific software threads for faults and provides the user with configurable actions to take in case of thread failure. The system registers applicable threads to this watchdog and assumes a thread has failed when it does not respond. By default, the Oracle Communications Session Border Controller generates information about the event and reboot history. For HA configurations, the system synchronizes this watchdog configuration and simultaneously operates on both the active and standby Oracle Communications Session Border Controllers.

You can query the system to show the actual threads being monitored with the **show platform health-check command**. The output include these columns:

- Name: name of the thread that registered with HealthCheck
- Count: Health Count of the thread
- State: State of thread as either: STOPPED, RUNNING, EXCLUDE
- Duration: Stop Expire time in seconds. Shows 0 for RUNNING and EXCLUDE states.

```
ORACLE# show platform health-check
------------------------------------------------
Name Count STATE DURATION
------------------------------------------------
tLrtd 3 RUNNING 0
lrtdWorkerThrea 3 RUNNING 0
dnsWorker01 3 RUNNING 0
loseld 3 RUNNING 0
npsoft 3 RUNNING 0
tFlowGdTmr 3 RUNNING 0
tLemd 3 RUNNING 0
```

```
tServiceHealth 3 RUNNING 0
tAtcpd 3 RUNNING 0
atcpd02 0 EXCLUDE 0
atcpd01 0 EXCLUDE 0
[...]
------------------------------------------------
Total Displayed: 39
-----------------------------------------------
```

When an applicable thread is not responding, the Oracle Communications Session Border Controller's default behavior includes:

- Generate a log message
- Issue an alarm
- Issue a SNMP trap
- Generate a core dump
- Reboot

The user configures the Software Worker Threads Watchdog action by configuring the **sw-health-check-action** option in the **system-config** with one of the following values:

- **logonly** — Generate log message only
- **logandreboot** — Generate log message and reboot
- **logcoreandreboot** — Generate log message, generate a core dump and reboot [default]

By default, the system checks thread status every 16 seconds. The user can change this interval with the **task-health-check-time** option configured in the **system-config**.

When the system identifies an unresponsive thread, it sends out the following trap: **apUsbcSysThreadNotRespondingTrap**. This trap is defined within the **apUsbc** MIB. The system sends it once by default; this value can be overridden by the trap configuration. This function does not include a clear trap.

Be aware that the **tHealthCheckd** task monitors only the application tasks that are registered with it. It does not monitor any platform tasks.

None of the configuration options are real-time configurable; the user must reboot after changing the option.

Software Worker Thread Health Check Interval Configuration

Use this procedure to set the timing and action for the Software Worker Thread Health Check and Watchdog Timer.

1. Access the **system-config** configuration element.

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

2. Type **select** to begin editing the **system-config** object.

```
ORACLE(system-config)# select
ORACLE(system-config)#
```

3. Set the task-health-check-time option to the preferred interval (in seconds)

```
ORACLE(system-config)# option +task-health-check-time=10
```

4. Set the watchdog timer action option that indicates the action on thread failure.

```
ORACLE(system-config)# option +sw-health-check-action=logonly
```

5. Type **done** to save your configuration.

NIU-Based Processor Buffer Depletion Recovery

The following suite of three features will failover an Oracle Communications Session Border Controller in an HA pair for certain related NIU-based processor and input buffer conditions.

Fast Failover after NIU-processor Core Crash

In some scenarios when a single core on an NIU-based processor crashes, the Oracle Communications Session Border Controller can be configured to failover to the standby HA node. To enable it, configure the **etc-fast-failover=enabled** option in the system-config. This option is disabled by default and must be explicitly configured for use.

The syntax below shows how to set this option.

```
OC-SBC#configure terminal
ORACLE(configure)#system
ORACLE(system)#system-config
ORACLE(system-config)#select
ORACLE(system-config)#options + etc-fast-failover=enabled
ORACLE(system-config)#done
```

Failover After Non-responsive NIU-processor Core

The Oracle Communications Session Border Controller polls NIU-processor cores for health every second. If the Oracle Communications Session Border Controller determines that a core is unresponsive for 10 consecutive seconds, and then determines that a NIU-processor's input queue is not processing frames, the system degrades its health score to the point where it fails over to the standby HA node. Following the failover, the system reboots. If the input queue can continue to process frames, no failover occurs.

This non-configurable watchdog process is always enabled and represents a behavioral change from previous releases without this feature.

Failover and Reboot on Filling up Input Queue

If at least one core is flagged as non-responsive for 10 consecutive seconds, and the NIU-processor's input queue is filling up, the system will failover and reboot. The relative amount that the input queue must fill before initiating this failover and reboot action is configurable by setting the **etc-buf-depletion-threshold=<low | medium | high | critical>** option in the system-config.

The default value for the **etc-buf-depletion-threshold** is low. Oracle recommends that the user retains the default setting of low.

The syntax below shows how to set this option.

```
OC-SBC#configure terminal
ORACLE(configure)#system
ORACLE(system)#system-config
ORACLE(system-config)#select
ORACLE(system-config)#options + etc-buf-depletion-threshold=medium
ORACLE(system-config)#done
```

Crash and Log File Maintenance

Transferring Log and Crash Files to External Systems

Users can transfer both log files and crash files to separate external devices for analysis or storage.

To remove logfiles, use the **package-logfiles** command to compress multiple log files into a single file while preserving the timestamps. The syntax for the **package-logfiles** command is:

```
package-logfiles [name <file>.tar.gz] [newer-than <days>] <all>
```

The **package-logfiles** command takes three arguments:

- **name**—Specify the path and name of the saved file. Generally, the files should be saved to /opt. If the system's hard drive has been formatted with partitions, /mnt may be used instead. For example:

  ```
  ORACLE# package-logfiles name /opt/logs/recentlogs.tar.gz
  Tar/gzip file /opt/logs/recentlogs.tar.gz to include 61 files of
  447 kiB (uncompressed)
  Proceed? [y/n]?: y
  Tar/gzip file created /opt/logs/recentlogs.tar.gz with 61 files
  with final size 62 kiB
  ORACLE#
  ```

  If the name argument is omitted, the Oracle Communications Session Border Controller saves the compressed log files to a file named logs-<date>.tar.gz, where <date> is the current date.

  ```
  ORACLE# package-logfiles
  Tar/gzip file /opt/logs/logs-130528.tar.gz to include 61 files of
  447 kiB (uncompressed)
  Proceed? [y/n]?: y
  Tar/gzip file created /opt/logs/logs-130528.tar.gz with 61 files
  with final size 62 kiB
  ORACLE#
  ```

- **newer-than**—Specify a time limit, in days, on log files to be compressed and saved. This option counts backwards, starting with the current day. Thus the option newer-than 5 would compress and save log files for the past 5 days only.

  ```
  ORACLE# package-logfiles name /opt/logs/5dlogs.tar.gz newer-than 5
  Tar/gzip file /opt/logs/5dlogs.tar.gz to include 61 files of 271 kiB
  (uncompressed)
  Proceed? [y/n]?: y
  Tar/gzip file created /opt/logs/5dlogs.tar.gz with 61 files with final
  size 45 kiB
  ORACLE#
  ```

  If the newer-than argument is omitted, the Oracle Communications Session Border Controller compresses and saves all log files.

- all—Collect the np-stats info, support-info.log, running configuration, and log files. Use this argument with caution as it may impact system performance.

  ```
  ORACLE# package-logfiles all
  Executing the command with argument 'all' may impact performance of system
  Proceed? [y/n]?: y
  writing stats to file /opt/logs/dump.datapath, it may take a while ...
  task done
  Provisioned Entitlements:
  -------------------------
  Session Border Controller Base    : enabled
  Session Capacity                  : 512
    Accounting                      : enabled
    BFD                             : enabled
    IPv4 - IPv6 Interworking        : enabled
    IWF (SIP-H323)                  : enabled
    Load Balancing                  : enabled
    Policy Server                   : enabled
    Quality of Service              : enabled
    Routing                         : enabled
    SIPREC Session Recording        : enabled
  Admin Security                    :
  ANSSI R226 Compliance             :
  IMS-AKA Endpoints                 : 1000
  IPSec Trunking Sessions           : 1024
  MSRP B2BUA Sessions               : 512
  SRTP Sessions                     : 2000
  Transcode Codec AMR Capacity      : 102
  Transcode Codec AMRWB Capacity    : 103
  Transcode Codec EVS Capacity      : 0
  Transcode Codec OPUS Capacity     : 0
  Transcode Codec SILK Capacity     : 0
  Wrote /opt/logs/support-info.log file
  Tar/gzip file /opt/logs/logs-180921.tar.gz to include 232 files of 95 MiB
  (uncompressed)
  Proceed? [y/n]?: y
  Tar/gzip file created /opt/logs/logs-180921.tar.gz with 232 files with
  final size 10 MiB
  ```

To preserve system resources, users should remove the compressed file as soon as possible.

To remove crash files, use the **package-crashfiles** command to compress multiple crash files into a single file while preserving the timestamps. The syntax for the **package-crashfiles** command is:

```
package-crashfiles [name <file>.tar.gz] [newer-than <days>] <all>
```

The **package-crashfiles** command takes three arguments:

- **name**—Specify the path and name of the saved file. Generally, the files should be saved to /opt. If the system’s hard drive has been formatted with partitions, /mnt may be used instead. For example:

  ```
  ORACLE# package-crashfiles name /opt/crash/recentcrashes.tar.gz
  Tar/gzip file /opt/crash/recentcrashes.tar.gz to include 6 files of
  1 MiB (uncompressed)
  Proceed? [y/n]?: y
  Tar/gzip file created /opt/crash/recentcrashes.tar.gz with 6 files
  with final size 169 kiB
  ORACLE#
  ```

  If the name argument is omitted, the Oracle Communications Session Border Controller saves the compressed crash files to a file named crash-<date>.tar.gz, where <date> is the current date.

  ```
  ORACLE# package-crashfiles
  Tar/gzip file /code/crash/crash-130529.tar.gz to include 6 files of
  1 MiB (uncompressed)
  Proceed? [y/n]?: y
  Tar/gzip file created /code/crash/crash-130529.tar.gz with 6 files
  with final size 169 kiB
  ORACLE#
  ```

- **newer-than**—Specify a time limit, in days, on the crash files to be compressed and saved. This option counts backwards, starting with the current day. Thus the option newer-than 5 would compress and save crash files for the past 5 days only.

  ```
  ORACLE# package-crashfiles name /opt/crash/recentcrashes.tar.gz
  newer-than 5
  Tar/gzip file /opt/crash/recentcrashes.tar.gz to include 6 files of
  1 MiB (uncompressed)
  Proceed? [y/n]?: y
  Tar/gzip file created /opt/crash/recentcrashes.tar.gz with 6 files
  with final size 169 kiB
  ORACLE#
  ```

  If the newer-than argument is omitted, the Oracle Communications Session Border Controller compresses and saves all crash files.

- **all**—Collects all formed crash files and available log files. Use this argument with caution as it may impact system performance.

  ```
  ORACLE# package-crashfiles all
  Executing the command with argument 'all' may impact performance of system
  Proceed? [y/n]?: y
  writing stats to file /opt/logs/dump.datapath, it may take a while ...
  task done
  Provisioned Entitlements:
  -------------------------
  Session Border Controller Base    : enabled
  Session Capacity                  : 512
    Accounting                      : enabled
    BFD                             : enabled
    IPv4 - IPv6 Interworking        : enabled
    IWF (SIP-H323)                  : enabled
    Load Balancing                  : enabled
    Policy Server                   : enabled
    Quality of Service              : enabled
    Routing                         : enabled
    SIPREC Session Recording        : enabled
  Admin Security                    :
  ANSSI R226 Compliance             :
  IMS-AKA Endpoints                 : 1000
  IPSec Trunking Sessions           : 1024
  MSRP B2BUA Sessions               : 512
  SRTP Sessions                     : 2000
  Transcode Codec AMR Capacity      : 102
  Transcode Codec AMRWB Capacity    : 103
  Transcode Codec EVS Capacity      : 0
  Transcode Codec OPUS Capacity     : 0
  Transcode Codec SILK Capacity     : 0
  Wrote /opt/logs/support-info.log file
  Tar/gzip file /opt/crash/crash-180921.tar.gz to include 235 files of 95
  MiB (uncompressed)
  Proceed? [y/n]?: y
  Tar/gzip file created /opt/crash/crash-180921.tar.gz with 235 files with
  final size 10 MiB
  ```

To preserve system resources, users should remove the compressed file as soon as possible.

delete-crashfiles

The **delete-crashfiles** command deletes all closed crash-files located in the /opt/crash directory. You may specify the age of the crash-files to delete. The command is entered as

```
delete-crashfile all
```

or

```
delete-crashfile older-than <days>
```

delete-logfiles

The **delete-logfiles** command deletes all closed log-files located in the /opt/logs directory. Files currently being written to remain untouched. You may specify the age of the log-files to delete. The command is entered as

```
delete-logfile all
```

or

```
delete-logfile older-than <days>
```

3

Performance Management

Overview

This chapter explains how to access and view statistics to help you monitor and manage Oracle Communications Session Border Controller performance. Gathering statistical information to help monitor system performance effectively helps you decide on the actions you need to take to correct or improve system behavior. For example, you can access statistics to monitor the calls per second capability of the Oracle Communications Session Border Controller and make decisions based on that information.

You can collect performance data to establish a baseline before making changes to the system. This helps determine what effect the change has on performance. You can use the baseline to compare future trends. You can collect performance data on a daily, weekly, and monthly basis for trend analysis. This allows you to pro-actively solve problems before they result in degraded performance.

Viewing System Information

This section explains how to access system level performance statistics. All the commands defined in this section are accessible in User mode.

ACLI Credit Information

Display the credit information, including the version number, for the ACLI that you are running on your system by using the **show about** command. This command also displays current third party licenses applicable to the software image you are running.

User Privilege Mode

Display the current level of privilege at which the user is operating on the system by using the **show privilege** command.

```
ORACLE> show privilege
console user - privilege level 0
ORACLE>
```

Privilege level 0 means the current user is in User mode and privilege level 1 means the current user is in Superuser mode.

System Uptime

Display 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) by using the **show uptime** command.

```
ORACLE# show uptime
FRI SEP 25 12:57:23 2017 - up 0 days, 22 hours, 58 minutes, 57 seconds
ORACLE#
```

Current Date and Time

Display the current date and time for your system by using the **show clock** command.

```
ORACLE# show clock
11:51:41 est  MON SEP 25 2017
```

Software Release Current Version

Display the version information for the release, including: the version number, the date that the current copy of the OS was made, and other information by using the **show version** command.

```
ACMESYSTEM# show version
ACME PACKET 4600 SCZ8.0.0 GA (WS Build 299)
Build Date=04/14/18
```

Viewing System Resource Information

This section explains how to access system resource statistics.

System Memory

Display the memory statistics for the system by using the show memory command. It displays the number of bytes, the number of blocks, the average block size in both free and allocated memory, and the maximum block size of free memory in table form. In addition, it displays the number of blocks currently allocated, the average allocated block size, and the maximum number of bytes allocated at any given time (peak use, for example).

```
ORACLE# show memory
  status      bytes     blocks    avg block  max block
 -------- ---------- --------- ---------- ----------
current
 free      826292736       179    4616160  825573472
 alloc     211642160      3398      62284          -
 internal        448         2        224          -
cumulative
 alloc     212286912      5105      41584          -
```

```
peak
 alloc     211643792         -          -          -
Memory Errors:
  Links Repaired            0
  Padding Modified          0
  Nodes Removed             0
  Removal Failures          0
  Fatal Errors              0
```

Listing Memory Subcommands

You can access a list of available **show memory** subcommands.

```
ORACLE# show memory ?
application                   application memory usage statistics
l2                            layer 2 cache status
l3                            layer 3 cache status
usage                         memory usage statistics
```

Application Object Allocation and Use

Display information about application object allocations and usage by displaying counters associated with the **show memory application** command.

```
ORACLE# show memory application
14:06:47-153
Memory Statistics             -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
Processes               27      27       0         29      28      27
Messages                 3       4      12      23768     298      27
Services               133     133       0        142     139     134
Sockets                120     120       0        129     126     121
Buffers                338     338       0        350     325     338
Transactions             0       0       0         22      11      11
Timed Objects        16164   16164       0      16486   16218   16176
TOQ Entries             25      25    1893    4178055    1334      37
SIP Messages             0       0       0          0       0       0
MBC Messages             0       0       0          0       0       0
Pipe Messages           30      30       0         30      30      30
Message Blocks           0       0       0          0       0       0
Mutexes              18492   18493       0      43732   18660   18494
Mutex Locks             68      73  186539   1096480k  117493      78
Mutex Waits              0       3       3     117461     173       9
Mutex Timeouts           -       -       0          0       0       -
Rcr Mutex-Timeouts       -       -       0        499     166       -
```

The following table lists and defines the counters of the **show memory application** command.

show memory application Subcommand	Description
Processes	Process object statistics

show memory application Subcommand	Description
Message	Message class and all derived classes statistics
Services	Service class and all derived classes statistics
Sockets	ServiceSocket class and all derived classes statistics
Buffers	Malloced buffers in various classes statistics
Transactions	All classes derived from the transactions template statistics
Timed Objects	TimedObject class and all derived classes statistics
TOQ Entries	Timed out queue (TOQEntry) class statistics
SIP Messages	Sip request (SipReq) and SIP response (SipResp) entry classes statistics
MBC Messages	MbcpMessage class statistics
Pipe Messages	Pipe message class statistics
Mutex Messages	Mutually exclusive class statistics

Worker Threads Deadlock Condition SNMP Trap

An SNMP trap is generated when a worker thread experiences a deadlock.

When a worker thread experiences a deadlock, the **apMutexDeadLockTrap** will be set. This trap contains the name of the thread on which the deadlock was encountered. Immediately following the above operation, the **apMutexDeadLockClearTrap** will be set. The operational setting of the trap and then immediate clearing of it functions more like a warning or alarm than the traditional SNMP trap functionality.

Memory Buffer

Display memory buffer statistics information by using the **show buffers** command.

```
ORACLE# show buffers
type        number
---------   ------
FREE    :    20990
DATA    :        1
HEADER  :        1
TOTAL   :    20992
number of mbufs: 20992
number of times failed to find space: 0
number of times waited for space: 0
number of times drained protocols for space: 0
__________________
CLUSTER POOL TABLE
__________________________________________________________________
size      clusters  free      usage     minsize   maxsize   empty
------------------------------------------------------------------
64        8192      8192      116       4         56         0
128       8192      8191      169342    128       128        0
256       2048      2047      35893     131       255        0
512       2048      2048      20357     258       512        0
```

```
1024      256       256       4         595       718       0
2048      256       256       7         1444      2048      0
------------------------------------------------------------------
```

The first column of the two column list shows the type of buffer, and the second column shows the number of buffers of that type. The first line of the list shows the number of buffers that are free; all subsequent lines show buffers of each type that are currently in use. Next you see four lines that describe the total number of buffers and how many times the system failed, waited, or had to empty a protocol to find space.

Following this information, the next section of the displayed information shows the cluster pool table. The size column lists the size of the clusters. The clusters column lists the total number of clusters of a certain size that have been allocated. The free column lists the number of available clusters of that size. The usage column lists the number of times that clusters have been allocated (and not the number of clusters currently in use).

Control and Maintenance Interfaces

Display all information concerning the system’s control and maintenance interfaces by using the **show interfaces** command.

```
ORACLE# show interfaces
lo (unit number 0):
     Flags: (0xc8049) UP LOOPBACK MULTICAST TRAILERS ARP RUNNING INET_UP
INET6_UP
     Type: SOFTWARE_LOOPBACK
     inet: 127.0.0.1
     Netmask 0xff000000 Subnetmask 0xff000000
     inet6:  ::1 prefixlen 128
     Metric is 0
     Maximum Transfer Unit size is 1536
     0 packets received; 5262 packets sent
     0 multicast packets received
     0 multicast packets sent
     0 input errors; 0 output errors
     0 collisions; 0 dropped
     0 output queue drops
wancom (unit number 0):
     Flags: (0xe8043) UP BROADCAST MULTICAST ARP RUNNING INET_UP INET6_UP
     Type: ETHERNET_CSMACD
     inet6:  fe80::208:25ff:fe01:760%wancom0 scopeid 0x2 prefixlen 64
     inet: 172.30.55.127
     Broadcast address: 172.30.255.255
     Netmask 0xffff0000 Subnetmask 0xffff0000
     Ethernet address is 00:08:25:01:07:60
     Metric is 0
     Maximum Transfer Unit size is 1500
     0 octets received
     0 octets sent
     259331 unicast packets received
     2069 unicast packets sent
     0 non-unicast packets received
     5 non-unicast packets sent
     0 incoming packets discarded
     0 outgoing packets discarded
     0 incoming errors
     0 outgoing errors
     0 unknown protos
     0 collisions; 0 dropped
     0 output queue drops
f00 (media slot 0, port 0)
     Flags: Down
     Type: GIGABIT_ETHERNET
     Admin State: enabled
     Auto Negotiation: enabled
     Internet address: 10.10.0.10     Vlan: 0
     Broadcast Address: 10.10.255.255
     Netmask: 0xffff0000
     Gateway: 10.10.0.1
     Ethernet address is 00:08:25:01:07:64
     Metric is 0
     Maximum Transfer Unit size is 1500
     0 octets received
     0 octets sent
     0 packets received
     0 packets sent
     0 non-unicast packets received
     0 non-unicast packets sent
     0 unicast packets received
     0 unicast packets sent
     0 input discards
     0 input unknown protocols
     0 input errors
     0 output errors
     0 collisions; 0 dropped
f01 (media slot 1, port 0)
     Flags: Down
     Type: GIGABIT_ETHERNET
     Admin State: enabled
     Auto Negotiation: enabled
     Internet address: 10.10.0.11     Vlan: 0
     Broadcast Address: 10.10.255.255
     Netmask: 0xffff0000
     Gateway: 10.10.0.1
     Ethernet address is 00:08:25:01:07:6a
     Metric is 0
     Maximum Transfer Unit size is 1500
     0 octets received
     0 octets sent
     0 packets received
     0 packets sent
     0 non-unicast packets received
     0 non-unicast packets sent
     0 unicast packets received
     0 unicast packets sent
     0 input discards
     0 input unknown protocols
     0 input errors
     0 output errors
     0 collisions; 0 dropped
```

The following information is listed for each interface:

- Internet address
- broadcast address
- netmask
- subnet mask
- Ethernet address
- route metric
- maximum transfer unit
- number of octets sent and received
- number of packets sent and received
- number of input discards
- number of unknown protocols
- number of input and output errors
- number of collisions
- number of drops
- flags (such as loopback, broadcast, promiscuous, ARP, running, and debug)

This command also displays information for loopback (internal) interfaces, which are logical interfaces used for internal communications.

You can also view key running statistics about the interfaces within a single screen by using the **show interfaces [brief]** command.

For example:

```
ORACLE# show interfaces brief
Slot Port Vlan Interface  IP                  Gateway          Admin Oper
Num  Num    ID Name       Address             Address          State State
---- ---- ---- ---------- ------------------- ---------------- ----- -----
lo (unit number 0):
     Flags: (0xc8049) UP LOOPBACK MULTICAST TRAILERS ARP RUNNING INET_UP
INET6_U
P
     Type: SOFTWARE_LOOPBACK
     inet: 127.0.0.1
     Netmask 0xff000000 Subnetmask 0xff000000
     inet6:  ::1 prefixlen 128
     Metric is 0
     Maximum Transfer Unit size is 1536
     238 packets received; 238 packets sent
     0 multicast packets received
     0 multicast packets sent
     0 input errors; 0 output errors
     0 collisions; 0 dropped
     0 output queue drops
```

```
wancom (unit number 0):
     Flags: (0xe8043) UP BROADCAST MULTICAST ARP RUNNING INET_UP
INET6_UP
     Type: ETHERNET_CSMACD
     inet6:  fe80::208:25ff:fe02:2280%wancom0 scopeid 0x2 prefixlen 64
     inet: 172.30.1.186
     Broadcast address: 172.30.255.255
     Netmask 0xffff0000 Subnetmask 0xffff0000
     Ethernet address is 00:08:25:02:22:80
     Metric is 0
     Maximum Transfer Unit size is 1500
     0 octets received
     0 octets sent
     638311 unicast packets received
     129 unicast packets sent
     0 non-unicast packets received
     5 non-unicast packets sent
     0 incoming packets discarded
     0 outgoing packets discarded
     0 incoming errors
     0 outgoing errors
     21 unknown protos
     0 collisions; 0 dropped
     0 output queue drops
sp (unit number 0):
     Flags: (0x68043) UP BROADCAST MULTICAST ARP RUNNING INET_UP
     Type: ETHERNET_CSMACD
     inet: 1.0.2.3
     Broadcast address: 1.0.2.255
     Netmask 0xff000000 Subnetmask 0xffffff00
     Ethernet address is 00:08:25:02:22:84
     Metric is 0
     Maximum Transfer Unit size is 1500
     0 octets received
     0 octets sent
     0 unicast packets received
     0 unicast packets sent
     0 non-unicast packets received
     0 non-unicast packets sent
     0 incoming packets discarded
     0 outgoing packets discarded
     0 incoming errors
     0 outgoing errors
     0 unknown protos
     0 collisions; 0 dropped
     0 output queue drops
   0    0    0 lefty      192.168.50.1/24     192.168.0.1      up
down
   1    0    0 righty     192.168.50.5/24     192.168.0.1      up
down
---------------------------------------------------------------------
```

Platform information

show platform cpu

The **show platform cpu** command displays an overview of the system's CPU(s), including number of CPUs, speed in MHz, model, flags, and CPU workload. For example:

```
ORACLE# show platform cpu
CPU count :       8
CPU speed :       2301 MHz
CPU model :       Intel(R) Core(TM) i7-3615QE CPU @ 2.30GHz
CPU flags :       fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx
rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology
nonstop_tsc aperfmperf pni pclmulqdq dtes64 monitor ds_cpl vmx smx est tm2
ssse3 cx16 xtpr pdcm sse4_1 sse4_2 x2apic popcnt aes xsave avx f16c rdrand
lahf_lm ida arat epb xsaveopt pln pts dts tpr_shadow vnmi flexpriority ept
vpid fsgsbase smep erms
CPU workload:
Capacity  :       80000 bogoMIPS
App load  :       4599 bogoMIPS
```

show platform cpu-load

Depending on platform, the show **show platform cpu-load** command displays 1 or 2 sets of CPU status statistics.

On VM and COTS platforms, the command displays a timestamp and the percentage of CPU consumed on each core during the last 10 second window using calculations similar to the linux top command.

On Acme platforms, the command omits the timestamp, displays CPU load as above, and also displays the load average for all CPUs and IO over time using 5 statistics, including:

1. CPU and IO utilization in the last 1 minute
2. CPU and IO utilization in the last 5 minutes
3. CPU and IO utilization in the last 10 minutes
4. Number of currently running processes and the total number of processes
5. Last process ID used

```
ORACLE> show platform cpu-load
Total load:       0%
          CPU#00  0%
          CPU#01  0%
          CPU#02  0%
          CPU#03  0%
          CPU#04  0%
          CPU#05  0%
          CPU#06  0%
```

```
              CPU#07   0%
    Load average: 0.61 0.42 0.19 2/231 3101
```

Viewing Active Processes

This section explains how to display statistics for active processes by displaying the task information for the system. By using the **show processes** command, you can view the system tasks in a table.

The information in this table is useful not only for viewing the process running on the system, but also for obtaining task names and identification numbers (TIDs in this table) for carrying out **notify** and **stop-task** commands.

This table contains the following information: names of tasks, entries, task identification codes, priority of a task, status, program counter, error numbers, and protector domain identification.

```
ORACLE# show processes
TaskName   Id  PPID Pri   Status    EIP       Up Time     RSS(kb)
vMEM(kb) Proc
--------  ---- ---- --- -------- ------------ ----------- -------
-------  ----
    uscc  2115 1557  20 SLEEPING 7fe09fa86974 0:16:37.660 1366524
5932844   0
    intt  2110    1  20 SLEEPING 7fafeee76350 0:16:37.670     412
19100   3
    intt  2109    1  20 SLEEPING 7fafeee76350 0:16:37.670     412
19100   2
dropberr  1984    1  20 SLEEPING 7fdaa36169c3 0:16:38.710     668
22668   1
   getty  1849    1  20 SLEEPING 7f75dae9c350 0:16:39.010    1016
19104   5
 syslod)  1840    1  20 SLEEPING 7f5def91b350 0:16:39.030     660
19100   0
   klogd  1838    1  20 SLEEPING 7ff68d78a267 0:16:39.030     660
19100   0
```

Accessing Process Subcommands

Display the help text for the **show processes** command to access the following subcommands:

```
ORACLE# show processes ?
```

The following table lists and defines some of the subcommands and additional capabilities of the **show processes** command.

show processes Subcommand	Description
sysmand	Statistics for the sysmand process, which is related to the system startup tasks. sysmand starts and keeps track of many of the system tasks. All application tasks send their system log messages to the sysmand task and all notify requests go through sysmand.
lemd	Statistics for the local element management (lemd) process, which is responsible for maintaining and providing local and remote access to data (including configuration and policy data) stored in the system.
brokerd	Statistics for the brokerd process, which is a log concentrator and sequencer used for forwarding path and hardware monitor tasks.
mbcd	Statistics for the mbcd process, which is the process for the middlebox control daemon. It provides signalling applications with the ability to dynamically manage (crete, modify, delete, and receive flow event notifications) NAT entries (pinholes) for media flows via the MIBOCO protocol.
sipd	Statistics for sipd process statistic, which acts as a SIP server that receives and forwards them on the behalf of the requestor. sipd is responsible for processing SIP (RFC 3261) messages. It NATs the Layer 5 signaling content (for example, SIP message headers) and manages the associated media flows via tMBCD.
current	Current statistics for all processes.
total	Total statistics for all processes.
all	All statistics for all processes.
cpu	Percentage of CPU utilization by all processes.

Viewing Totals for all Processes

Display total statistics for all processes by using the **show processes total** command.

```
ORACLE# show processes total
12:32:34-94
Process  Svcs      Rcvd      Sent    Events  Alarm    Slog     Plog   CPU Max
sysmand    29     35961        45      5340      0      11       58   0.0   0
acliSSH0    4         0         3         0      0       6        6   0.0   0
brokerd     2        20         4         0      3       4        4   0.0   0
cliWorke    2         0         2         0      0       5        6   0.0   0
lemd        5         5        28         3      0      26       36   0.0   0
collect     3         1         6         0      0       8        8   0.0   0
atcpd       5         1         8   1062468      0      10       12   0.0   0
atcpApp     4         1         5         0      0       7        8   0.0   0
mbcd        9         1        30     23112      0      32       38   0.0   0
lid         3         1         6         0      0       8        8   0.0   0
algd        6         1         9      5334      0      11       13   0.0   0
radd        3         1         9      5333      0      11       11   0.0   0
pusher      3         1         6         0      0       8        8   0.0   0
ebmd        5         1         9     10668      0      11       11   0.0   0
sipd        5         3     17796     58671      0   17796    17799   0.0   0
lrtd        4         1         5         0      0       7       10   0.0   0
h323d       6         1     17835     80005      0   17837    17843   0.0   0
h248d       2         0        24      5334      0      27       27   0.0   0
secured     5         1         6         0      0       8       10   0.0   0
snmpd       4         1         7         0      0       9        9   0.0   0
acliSSH1    4         0         3         0      0       6        6   0.0   0
```

```
acliSSH2    4         0         3         0      0       6        6
0.0   0
acliSSH3    4         0         3         0      0       6        6
0.0   0
acliSSH4    4         0         3         0      0       6        6
0.0   0
acliCons    3         1        16         0      0      18       18
0.0   0
acliTeln    4        22        92         3      0      73       73
0.0   0
acliTeln    4         6        20         0      0      16       16
0.0   0
acliTeln    4         0         3         0      0       6        6
0.0   0
acliTeln    4         0         3         0      0       6        6
0.0   0
acliTeln    4         0         3         0      0       6        6
0.0   0
tTaskChe    0         0         0         0      0       0        0
0.0   0
```

Viewing Current Statistics

Display the current statistics for all processes by using the **show processes current** command.

```
ORACLE# show processes current
12:35:12-52
Process  Svcs    TOQ     Ops   Rcvd   Sent Events Alrm  Slog    Plog
CPU Now
sysmand    29      2      15     11      0      1    0     0      0
0.0   0
acliSSH0    4      1       1      0      3      0    0     6      6
0.0   0
brokerd     2      0       8      3      0      0    0     0      0
0.0   0
cliWorke    2      0       2      0      0      0    0     0      0
0.0   0
lemd        5      0       3      0      0      0    0     0      0
0.0   0
collect     3      0      34      0      0      0    0     0      0
0.0   0
atcpd       5      1     307      0      0    304    0     0      0
0.0   0
atcpApp     4      0       3      0      0      0    0     0      0
0.0   0
mbcd        9      2       7      0      0      6    0     0      0
0.0   0
lid         3      0       3      0      0      0    0     0      0
0.0   0
algd        6      1       4      0      0      1    0     0      0
0.0   0
radd        3      1       5      0      0      2    0     0      0
0.0   0
```

```
pusher      3      0       3      0      0      0    0     0      0   0.0   0
ebmd        5      2       4      0      0      2    0     0      0   0.0   0
sipd        5      2      16      0      5     16    0     5      5   0.0   0
lrtd        4      0       3      0      0      0    0     0      0   0.0   0
h323d       6      3      16      0      5     22    0     5      5   0.0   0
h248d       2      1       4      0      0      1    0     0      0   0.0   0
secured     5      0       3      0      0      0    0     0      0   0.0   0
snmpd       4      0       3      0      0      0    0     0      0   0.0   0
acliSSH1    4      1       1      0      3      0    0     6      6   0.0   0
acliSSH2    4      1       1      0      3      0    0     6      6   0.0   0
acliSSH3    4      1       1      0      3      0    0     6      6   0.0   0
acliSSH4    4      1       1      0      3      0    0     6      6   0.0   0
acliCons    3      0       3      0      0      0    0     0      0   0.0   0
acliTeln    4      0      48      0      0      0    0     0      0   0.0   0
acliTeln    4      1       4      0      4      0    0     3      3   0.0   0
acliTeln    4      1       1      0      3      0    0     6      6   0.0   0
acliTeln    4      1       1      0      3      0    0     6      6   0.0   0
acliTeln    4      1       1      0      3      0    0     6      6   0.0   0
tTaskChe    0      0       1      0      0      0    0     0      0   0.0   0
```

Realtime CPU usage

The **show processes top** command displays realtime updates of per-process CPU utilization. To quit, press "q".

```
ORACLE> show processes top
top - 13:57:22 up 23:48,  0 users,  load average: 0.00, 0.01, 0.05
Tasks: 117 total,   2 running, 115 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,
0.0%st
Mem:   2966240k total,   398016k used,  2568224k free,    66536k buffers
Swap:        0k total,        0k used,        0k free,   116032k cached
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      20   0  3724 1100  936 S    0  0.0   0:30.13 init
    2 root      20   0     0    0    0 S    0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S    0  0.0   0:04.49 ksoftirqd/0
    6 root      RT   0     0    0    0 S    0  0.0   0:00.00 migration/0
    7 root      RT   0     0    0    0 S    0  0.0   0:00.33 watchdog/0
    8 root      RT   0     0    0    0 S    0  0.0   0:00.00 migration/1
    9 root      20   0     0    0    0 S    0  0.0   0:00.00 kworker/1:0
   10 root      20   0     0    0    0 S    0  0.0   0:00.08 ksoftirqd/1
   11 root      20   0     0    0    0 R    0  0.0   0:02.16 kworker/0:1
   12 root      RT   0     0    0    0 S    0  0.0   0:00.17 watchdog/1
   13 root       0 -20     0    0    0 S    0  0.0   0:00.00 khelper
  418 root      20   0     0    0    0 S    0  0.0   0:00.13 sync_supers
  420 root      20   0     0    0    0 S    0  0.0   0:00.00 bdi-default
  421 root       0 -20     0    0    0 S    0  0.0   0:00.00 kblockd
  423 root      20   0     0    0    0 S    0  0.0  11:31.98 kworker/1:1
  559 root       0 -20     0    0    0 S    0  0.0   0:00.00 ata_sff
  570 root      20   0     0    0    0 S    0  0.0   0:00.00 khubd
```

Checking Remaining Space

Check the amount of storage space is available on the flash file system on the following devices by using the **check-space-remaining** command:

- /boot
- /code
- /crash
- /opt
- the data-disk, system-disks or a combination

For example:

```
ORACLE# check-space-remaining boot
boot: 20127744/29760512 bytes (67%) remaining
```

SMP-Aware Task Load Limiting

The ability to manage CPU load is critical for highly available devices. SMP architectures require unique load limiting because a task's threads may be spread out over several cores. The Oracle Communications Session Border Controller employs a method of determining aggregate load in its SMP environment so that resources may be evenly spread across all CPUs and applications can decrease their load when necessary. In turn, traffic may be dropped or rejected depending on the application to reduce the CPU load to an acceptable value.

Load limiting can be performed on three fundamental processing areas of the Oracle Communications Session Border Controller:

- Transport Limiting — When the system's CPU load rises above the transport limiting value, traffic received from endpoints is dropped. The system scales back the load of the processes where network packets (TCP, SCTP, and UDP) are disassembled.
- Media Limiting — When the system's CPU load rises above the Media limiting value, the process that creates end-to-end media interface connections begins to drop requests (changes to existing transport sessions can still occur) thereby reducing CPU load. The system replies to SIP requests that initiate transport sessions with 503 Service Unavailable (this would typically be an INVITE with SDP).
- SIP Limiting — The system can manage percent CPU utilization by limiting the number of SIP messages it processes, as follows:
  - Begins rejecting SIP requests when the CPU reaches its throttling threshold, and
  - Rejects all SIP requests when the CPU reaches its maximum utilization.

Calculating CPU Load Limits

This section explains how and when the Oracle Communications Session Border Controller performs SIP message throttling to limit CPU utilization. This configuration also affects IDS management information.

The Oracle Communications Session Border Controller limits CPU utilization by SIP requests using two utilization percentage points. When CPU utilization reaches the first point, the system begins to reject SIP requests. When it reaches the second point, the system rejects all SIP requests. By default, these values are 90% and 99%. The user can change these values using a sip-config option called **load-limit**.

The **load-limit** option accepts two parameters, from which it determines these levels, including:

- Minimum CPU Utilization - The CPU utilization percentage at which the system begins to throttle back on the SIP requests it processes.
- CPU Limit for Headroom Calculation - A variable the system uses to compute maximum CPU utilization, at which it stops accepting SIP requests.

Syntax for this option is:

```
 load-limit= < Minimum CPU Utilization  > [-< CPU Limit for Headroom
Calculation >]
```

User settings include:

- Minimum CPU Utilization - The range is 15% to 100%, and the default is 90%.
- (Optional) CPU Limit for Headroom Calculation - The range is 15 to 100, and the default is 100.

The calculation the system uses to determine the maximum CPU percent utilization is shown below, with X representing the Minimum CPU Utilization, and Y representing the CPU Limit for Headroom Calculation.

```
 X + ((Y - X) * X/Y)%
```

The example setting below sets the throttling threshold to 60% and the maximum utilization to 75%.

```
 load-limit= 60-80
```

The calculation the system uses is 60 + (80 - 60) * 60/80 = 75

The system progressively rejects requests as CPU utilization increases. When CPU utilization is between X% and the maximum, the system accepts some new SIP requests, depending on CPU utilization and utilization configuration. The system calculates this acceptance rate using the formula below.

```
100 - ((Current CPU Util - X) * 100 / ((Y - X) * X/Y))
```

When CPU utilization reaches its maximum, it drops all new SIP requests. The system resumes accepting requests when CPU utilization falls below its maximum, and stops throttling when it falls below the Minimum CPU Utilization.

While rejecting a SIP request, the system returns a 503 service unavailable message, along with a Retry-After header. The user can configure the reject-interval using the sip-config's **reject-interval=X** option. The default value is 1 second.

The actual value of reject interval header embedded in the 503 message is:

```
RetryAfter = (100 - Acceptance Rate) /10 * rejectInterval
```

If this value is smaller than the configured reject-interval, the system overwrites it with the configured reject-interval value.

Note the table below, which displays some valid and invalid configuration entries.

User Configuration	Headroom	Max CPU Limit	Configuration Valid?
load-limit=60	(100 - 60) * 60 /100 = 24	60+24 = 84	Yes
load-limit=60-80	(80 - 60) * 60/80 = 15	60+15 = 75	Yes
load-limit=80-60	(100 - 80) * 80 / 100 = 16	80+16 = 96	No - (Upper limit < Lower limit)
load-limit=80-101	(100 - 80) * 80 / 100 = 16	80+16 = 96	No - (Upper limit > 100)
load-limit=-70	(100 - 90) * 90 / 100 = 9	90 + 9 = 99	No - default of 90% is used for lower limit, 100% for upper limit
load-limit=70-	(100 - 70) * 70 / 100 = 21	70 + 21 = 91	No - upper limit default - 100% is used
load-limit=-	(100 - 90) * 90 / 100 = 9	90 + 9 = 99	No - default - 90% is used.
load-limit=80-ABC	(100 - 80) * 80 / 100 = 16	80 + 16 = 96	No - the upper limit default of 100% is used
load-limit=80 90	(100 - 80) * 80 / 100 = 16	80 + 16 = 96	No - the upper limit default of 100% is used

SIP Application Load Limiting Configuration

To set SIP application load limiting:

1. Access the **sip-config** configuration element.

   ```
   ORACLE# configure terminal
   ORACLE(configure)# session-router
   ORACLE(session-router)# sip-config
   ORACLE(sip-config)#
   ```

2. Set the **load-limit= < Minimum CPU Utilization > [-< CPU Limit for Headroom Calculation >]** option as shown in the example below, and then press Enter. The example shows the throttling threshold set to 45% and the variable set to 70.

   ```
   ORACLE(sip-config)# options +load-limit=45-70
   ```

   The first value specifies the percent CPU utilization at which the system starts rejecting some SIP requests. The valid range is 15 to 100. The default is 90%.

   The second value specifies the calculation variable the system uses to determine maximum percent CPU utilization and is optional. The default is 100 and the valid range is 15 to 100. If this value is greater than the first value, the system defaults it to 100.

3. Type **done**.
4. Save and activate your configuration.

Transport Limiting Configuration

To set transport application load limiting:

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

   ```
   ORACLE# configure terminal
   ORACLE(configure)#
   ```

2. Type **system** and press Enter.

   ```
   ORACLE(configure)# system
   ORACLE(system)#
   ```

3. Type **system-config** and press Enter.

   ```
   ORACLE(system)# system-config
   ORACLE(system-config)#
   ```

   From this point, you can configure system-config configuration parameters. To view all system-config parameters, enter a **?** at the system prompt.

4. **options**—Set the options parameter by typing **options**, a Space, the option name **transport-load-limit=<value>** with a plus sign in front of it, and then press Enter.

   ```
   ORACLE(media-manager)# options +transport-load-limit=80
   ```

   Set this option's value to between 10 and 100 to set the CPU load point at which the transport application threads begin rejecting requests to disassemble packets. A value of 0 disables transport load limiting.

   If you type the option without the plus sign, you will overwrite any previously configured options. In order to append the new options to the realm configuration's options list, you must prepend the new option with a plus sign as shown in the previous example.

5. Save and activate your configuration.

Media Limiting Configuration

To set Media load limiting:

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

   ```
   ORACLE# configure terminal
   ORACLE(configure)#
   ```

2. Type **media-manager** and press Enter to access the media-level configuration elements.

   ```
   ORACLE(configure)# media-manager
   ORACLE(media-manager)#
   ```

3. Type **media-manager** and press Enter to begin configuring media over TCP.

   ```
   ORACLE(media-manager)# media-manager
   ORACLE(media-manager-config)#
   ```

   From this point, you can configure media-manager-config configuration parameters. To view all media-manager-config parameters, enter a **?** at the system prompt.

4. **options** — Set the options parameter by typing **options**, a Space, the option name **media-load-limit=<value>** with a plus sign in front of it, and then press Enter.

   ```
   ORACLE(media-manager)# options +media-load-limit=80
   ```

   Set the option’s value to between 0 and 100 to set the CPU load point at which the media traffic setup begin rejecting requests. The **media-load-limit=<value>** default is 80. A value of 0 disables media task limiting.

   If you type the option without the plus sign, you will overwrite any previously configured options. In order to append the new options to the realm configuration’s options list, you must prepend the new option with a plus sign as shown in the previous example.

5. Save and activate your configuration.

Viewing Active Audio and Video Call Statistics

The **show sessions** and **show sipd codec** CLI commands identify and display media processing statistics, such as the aggregate call count for active audio and video calls, and codec information per call.

show sessions

The **show sessions** command displays the statistics for SIP, H.323 and IWF along with the cumulative SIP audio and video call counters for the active calls. The system uses the following assumptions and interpretations of the calls to have separate counters for audio and video calls:

- The system determines the type of call, whether audio or video, by checking the m-line for media-type and a valid media-port. When the SDP uses only one m-line with media-type 'video' and media-port > 0, the system increments the video call count. Same logic applies for audio calls.
- The system considers multiple m lines for same media-type as a single call and increments the call by one.

```
ORACLE# show sessions
01:47:46-189 Capacity=84000
Session Statistics          -- Period -- -------- Lifetime --------
                           Active    High      Total      Total     PerMax     High
```

```
Established Tunnel          1          1          1           1        1        1
Total Sessions              1          1          1           1        1        1
SIP Sessions                0          0          0           0        0        0
H.323 Calls                 0          0          0           0        0        0
H.248 ALG Contexts          0          0          0           0        0        0

IWF Statistics                -- Period -- -------- Lifetime --------
                           Active    High      Total      Total     PerMax     High
H.323-to-SIP Calls          0          0          0           0        0         0
SIP-to-H.323 Calls          0          0          0           0        0         0

SIP Audio/Video Statistics    -- Period -- -------- Lifetime --------
                           Active    High      Total      Total     PerMax     High
Audio Calls                 1          1          1           1        1          1
Video Calls                 1          1          1           1        1          1
```

- When the system renegotiates SDP during the call, the call counters reflect the active SDP m-lines.

The scenarios in consideration are :

- Initial offer and answer SDP:

Offer	Answer

`OFFER:`
`m=audio 10000 RTP/AVP 8 0`
`a=rtpmap:8 PCMA/8000`
`a=rtpmap:0 PCMU/8000`
`m=audio 0 RTP/AVP 0`
	`ANSWER:`
	`m=audio 10000 RTP/AVP 8 0`
	`a=rtpmap:8 PCMA/8000`
	`a=rtpmap:0 PCMU/8000`
	`m=audio 0 RTP/AVP 0`

The following is an example of the **show sessions output** command.

```
ORACLE# show sessions
01:47:46-189 Capacity=84000
Session Statistics          -- Period -- -------- Lifetime --------
                           Active    High      Total      Total
PerMax     High
Established Tunnel          1          1          1           1
1          1
Total Sessions              1          1          1           1
1          1
SIP Sessions                0          0          0           0
0          0
H.323 Calls                 0          0          0           0
0          0
H.248 ALG Contexts          0          0          0           0
0          0

IWF Statistics              -- Period -- -------- Lifetime --------
                           Active    High      Total      Total
PerMax      High
H.323-to-SIP Calls          0          0          0          0
0          0
SIP-to-H.323 Calls          0          0          0          0
0          0

SIP Audio/Video Statistic   -- Period -- -------- Lifetime --------
                           Active    High      Total      Total
PerMax      High
```

```
Audio Calls                 1          1          1          1
1          1
Video Calls                 0          0          0          0
0          0
```

- Renegotiated offer answer SDP (with audio and video):

Offer	Answer

`OFFER:`
`m=audio 10000 RTP/AVP 8 0`
`a=rtpmap:8 PCMA/8000`
`a=rtpmap:0 PCMU/8000`
`m=audio 0 RTP/AVP 0`
	`ANSWER:`
	`m=audio 10000 RTP/AVP 8 0`
	`a=rtpmap:8 PCMA/8000`
	`a=rtpmap:0 PCMU/8000`
	`m=audio 0 RTP/AVP 0`

The following is an example of the **show sessions output** command.

```
ORACLE# show sessions
01:47:46-189 Capacity=84000
Session Statistics          -- Period -- -------- Lifetime --------
                           Active    High      Total      Total     PerMax      High
Established Tunnel          1          1          1           1        1          1
Total Sessions              1          1          1           1        1          1
SIP Sessions                0          0          0           0        0          0
H.323 Calls                 0          0          0           0        0          0
H.248 ALG Contexts          0          0          0           0        0          0

IWF Statistics              -- Period -- -------- Lifetime --------
                           Active    High      Total      Total     PerMax      High
H.323-to-SIP Calls          0          0          0          0         0          0
SIP-to-H.323 Calls          0          0          0          0         0          0

SIP Audio/Video Statistics  -- Period -- -------- Lifetime --------
                           Active    High      Total      Total     PerMax      High
Audio Calls                 1          1          1          1         1          1
Video Calls                 1          1          1          1         1          1
```

- Renegotiated offer answer SDP (with audio only):

Offer	Answer

`OFFER:`
`m=video 0 RTP/AVP 98`
`a=rtpmap:98 H264/90000`
`m=audio 6000 RTP/AVP 0`
`a=rtpmap:0 PCMU/8000`
	`ANSWER:`
	`m=video 0 RTP/AVP 98`
	`a=rtpmap:98 H264/90000`
	`m=audio 6000 RTP/AVP 0`
	`a=rtpmap:0 PCMU/8000`

The following is an example of the **show sessions output** command.

```
ORACLE# show sessions
01:47:46-189 Capacity=84000
Session Statistics          -- Period -- -------- Lifetime --------
                           Active    High      Total      Total     PerMax    High
Established Tunnel          1          1          1           1          1        1
Total Sessions              1          1          1           1          1        1
SIP Sessions                0          0          0           0          0        0
H.323 Calls                 0          0          0           0          0        0
H.248 ALG Contexts          0          0          0           0          0        0

IWF Statistics              -- Period -- -------- Lifetime --------
                           Active    High      Total      Total     PerMax    High
H.323-to-SIP Calls          0          0          0           0          0        0
```

```
SIP-to-H.323 Calls          0          0          0           0          0        0

SIP Audio/Video Statistics  -- Period -- -------- Lifetime --------
                           Active    High      Total      Total     PerMax    High
Audio Calls                 1          1          1           1          1        1
Video Calls                 0          1          1           1          1        1
```

The **show session** command displays these statistics.

- Total Sessions—The aggregation of all current active subscriber sessions (H.323 call/SIP session) and is the total session count against the capacity license.
- SIP Sessions—The total current active SIP sessions.
- H.323 Calls—The total current active H.323 calls.
- SIP Audio Calls - The audio call count.
- SIP Video Calls - The video call count.
- Messaging Sessions - The session-based messaging session count.
- Period Statistics:
  - Active - The current number of active counts.
  - High - The highest number during the recent window.
  - Total - The total accumulated count during the recent window.
- Lifetime Statistics:
  - Total - The total accumulated count.
  - PerMax - The maximum recorded in one period.
  - High - The highest momentary count.

show sipd codec

The **show sipd codec** command displays the media-processing statistics per SIP traffic. Note that the **show sipd codec** command displays the statistics per realm and requires a realm argument. The system displays the statistics of the active video sessions in the rows: H.261 Count, H.263 count, H.264 Count.

```
show sipd codec <realm-name>
07:11:28-45 Realm peer
Codec Statistics
                             ---- Recent ---- -------- Lifetime --------
                       Active    High   Total      Total  PerMax    High
Transcoded                  0       0       0          0       0       0
Transrated                  0       0       0          0       0       0
Transparent                 0       0       0          0       0       0
PCMU Count                  0       0       0          0       0       0
PCMA Count                  0       0       0          0       0       0
G722 Count                  0       0       0          0       0       0
G723 Count                  0       0       0          0       0       0
G726-16 Count               0       0       0          0       0       0
G726-24 Count               0       0       0          0       0       0
G726-32 Count               0       0       0          0       0       0
G726-40 Count               0       0       0          0       0       0
G728 Count                  0       0       0          0       0       0
G729 Count                  0       0       0          0       0       0
GSM Count                   0       0       0          0       0       0
iLBC Count                  0       0       0          0       0       0
H261 Count                  0       0       0          0       0       0
H263 Count                  0       0       0          0       0       0
H264 Count                  0       0       0          0       0       0
T38 Count                   0       0       0          0       0       0
AMR Count                   0       0       0          0       0       0
AMR-WB Count                0       0       0          0       0       0
EVRC Count                  0       0       0          0       0       0
```

```
EVRC0 Count                  0       0       0          0       0       0
EVRC1 Count                  0       0       0          0       0       0
EVRCB Count                  0       0       0          0       0       0
EVRCB0 Count                 0       0       0          0       0       0
EVRCB1 Count                 0       0       0          0       0       0
opus Count                   0       0       0          0       0       0
SILK Count                   0       0       0          0       0       0
T140 Count                   0       0       0          0       0       0
BAUDOT Count                 0       0       0          0       0       0
H264 Count                   0       0       0          0       0       0
EVS Count                    0       0       0          0       0       0
Other Count                  0       0       0          0       0       0
```

Media Session Traffic and QoS Reporting

The Oracle Communications Session Border Controller (SBC) Quality of Service (QoS) monitor reports statistics on Real-time Transport Protocol (RTP) call flows.

QoS monitoring reports the following statistics on RTP call flows:

- Bytes and packets received
- Lost packets
- Jitter
- Maximum jitter
- Latency
- Maximum latency

These statistics are captured in the CDR for each call leg (calling and called) and for up to 2 media streams. The SBC gathers information for media internetworking calls and SRTP sessions. Both the RADIUS and Diameter protocols are supported.

The system captures the preceding statistics in the Call Detail Record (CDR) for both the calling leg and the called leg for up to two media streams. The system gathers information for media internetworking calls and Secure Real-time Transport Protocol (SRTP) sessions. The system supports the RADIUS protocol.

> **Note:**
>
> You must own the QoS license to use media session traffic and QoS reporting. The system does not support pooled transcoding.

Viewing Redundancy Statistics

This section explains how to check the redundancy status for Acme Packet High Availability (HA) pairs by using the **show redundancy** command. Viewing the redundancy statistics provides the following information:

- General HA statistics
- Statistics related to HA transactions that have been processed
- Numerical identifier for the last redundant transaction processed (each transaction is numbered)

In an HA architecture that is functioning properly, the number for the last redundant transaction processed on a standby Oracle Communications Session Border Controller peer should not be far behind (if not exactly the same as) the one shown for the active Oracle Communications Session Border Controller peer.

The **show redundancy** command’s output displays a time stamp showing when the current period began, the statistics and transactions for high availability and the numerical identifier for the last redundant transaction processed.

Accessing Redundancy Subcommands

The following example shows the **show redundancy** subcommands. You can display the redundancy statistics for applicable components, including the Middlebox Control (MBC), SIP and for the configuration. Display the subcommands using the ACLI's question mark argument.

```
ORACLE# show redundancy ?
```

Configuration Checkpoint Example

The following example shows the configuration checkpointing statistics you can display by using the **show redundancy config** subcommand.

```
ORACLE# show redundancy config
18:35:05-105
Redundancy Statistics         -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
Queued Entries           0       0       0          5       2       1
Records Dropped          -       -       0          0       0
Server Trans             1       1      44        593      78       27
Client Trans             0       0       0          0       0       0
Redundancy Transactions          ---- Lifetime ----
                          Recent      Total  PerMax
Requests received             44        593      78
Duplicate requests             0          2       1
Success responses             44        593      78
Error responses                0          0       0
Request sent                   0          0       0
Retransmissions sent           0          0       0
Success received               0          0       0
Errors received                0          0       0
Transaction timeouts           0          0       0
Avg Latency=0.000 for 0
Max Latency=0.000
Last redundant transaction processed: 5
ORACLE#
```

About High Availability Transactions

The following table lists the redundancy statistics for the HA transactions for the Lifetime monitoring span. A standby Oracle Communications Session Border Controller (SBC) always acts as the client side in a client-server relationship with an active SBC peer; the active SBC acts as the server. The standby SBC peer always sends HA requests to its active SBC peer, which always acts as receiver of HA transactions from the standby peer.

Statistic	Description
Queued entries	Number of transactions the active SBC has not yet sent to its standby SBC peer.
Red Records	Total number of HA transactions created. This set of statistics should be the same as those for Queued entries.
Records Dropped	Number of HA transaction records that were lost (i.e., dropped) because the standby SBC fell behind in synchronization.
Server Trans	This statistic shows the number of HA transactions in which the SBC acted as the server side in the client-server relationship. The active HA SBC peer is the server.
Client Trans	This statistic shows the number of HA transactions in which the SBC acted as the client side in the client-server relationship. The standby HA SBC peer is the client.
Request-Response Round-Trip Times	Combined processing and network round-trip transaction times (RTT). The system displays Request-Response RTT values as the number of times the RTT time result fell into the following ranges: • 0 – 2 ms • 2 – 4 ms • 4 – 8 ms • 8 – 16 ms • 16 – 33 ms • 33 - 67 ms • > 67 ms These statistics measure the time from issuing a request to receiving a response, and therefore, apply only to the standby SBC. Recent statistics on the active are always zero. Period statistics on the active are not reset during a switchover.
Request-Response Loss	Recent and lifetime percent packets dropped by the SBC during HA transactions. These statistics apply only to the standby. Recent statistics on the active are always zero. Period statistics on the active are not reset during a switchover.

Viewing Border Element Redundancy Protocol Information

You can view Border Element Redundancy Protocol statistics by using the **show berpd** command.

The border element redundancy protocol responds to alarms, advertisements, and checkpointing. This protocol manages switchovers between active and standby Oracle Communications Session Border Controllers and checkpoints health, media flow, and signaling state information. Using the border element redundancy protocol, HA Oracle Communications Session Border Controller peers communicate through their configured interfaces with User Datagram Protocol (UDP) messages.

In HA operation, each HA Oracle Communications Session Border Controller peer in an HA Oracle Communications Session Border Controller pair uses the border element redundancy protocol to advertise its current state and health so that an active peer can be elected. Using the border element redundancy protocol, HA Oracle Communications Session Border Controller peers communicate with UDP (advertisement or checkpoint) messages which are sent out on one or more rear interfaces (destinations). These checkpoint messages are sent by both HA Oracle Communications Session Border Controller peers in the HA Oracle Communications Session Border Controller pair on a regular basis.

The border element redundancy protocol is sometimes referred to as BERP (e.g., the berpd task/process) by the internal system components

Viewing Redundancy Health

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

- Health score
  The health score of a Oracle Communications Session Border Controller is used to determine the active/standby roles of the Oracle Communications Session Border Controllers participating in an HA pair architecture. The healthiest Oracle Communications Session Border Controller peer (the Oracle Communications Session Border Controller peer with the highest health score) is the active Oracle Communications Session Border Controller peer. The Oracle Communications Session Border Controller peer with the lower health score is the standby Oracle Communications Session Border Controller peer.

  The health score is based on a 100-point scoring system. When all system components are functioning properly, the health score of the system is 100.

  If the health score of an active Oracle Communications Session Border Controller peer drops below a configurable threshold, the standby Oracle Communications Session Border Controller peer takes control and initiates an automatic switchover (assumes the active role). The standby Oracle Communications Session Border Controller peer only takes over the active role if its own health score is greater than that of the active Oracle Communications Session Border Controller peer. In the case where an active Oracle Communications Session Border Controller's health score has reached an unsatisfactory level and therefore the standby Oracle Communications Session Border Controller has taken over, the Oracle Communications Session Border Controller that was originally active assumes the role of the standby system.
- Whether the current HA Oracle Communications Session Border Controller is active, standby, or out of service
- The last 20 switchover events in the switchover log

HA States

Refer to the following table for information about each potential HA state.

State	Description
Initial	HA Oracle Communications Session Border Controller is booting and looking for its configured peers.
BecomingActive	HA Oracle Communications Session Border Controller has negotiated to become the active system, but it is waiting for the length of time equal to its configured becoming-active-time to become fully active. It is important to note that packets cannot be processed in this state. An HA Oracle Communications Session Border Controller must be in the Active state before packet processing can occur.

State	Description
Active	HA Oracle Communications Session Border Controller has waited for the length of time set in the becoming-active-time field and is healthy enough. This HA Oracle Communications Session Border Controller is handling all media flow and signaling processing.
RelinquishingActive	HA Oracle Communications Session Border Controller has been in the Active state, but has begun the switchover process to the Standby state. This state is very brief (i.e., the HA Oracle Communications Session Border Controller quickly transitions from the Active state through the RelinquishingActive state to the BecomingStandby state).
BecomingStandby	HA Oracle Communications Session Border Controller has negotiated to become the standby system, but is waiting to become synchronized and fully standby. It remains in this state for the length of time equal to its configured becoming-standby-time.
Standby	HA Oracle Communications Session Border Controller is fully synchronized with an active peer.
OutOfService	HA Oracle Communications Session Border Controller is not able to synchronize with its peer within the length of time set in the becoming-standby-time field. The HA Oracle Communications Session Border Controller can only transition to this state from the BecomingStandby state. An active Oracle Communications Session Border Controller will consider its HA Oracle Communications Session Border Controller peer to be in this state if the peer has timed out and not sent a checkpoint message to the active peer within a time period (equal to the percent-drift value multiplied by the advertisement-time value).

HA Logs

The SBC logs information about HA operation to assist in troubleshooting and other operational procedures.

The SBC performs the following procedures to log HA operations. The SBC logs this information to each task's log file regardless of the **redundancy-config**'s **log-level** setting.

- Both HA systems log a message for each redundancy journal every 5 minutes, including synchronization state, current size, lifetime record drops, maximum latency, enqueue rate and dequeue rate.
- The Active SBC logs the reason for the status change when the active SBC changes the status of the standby SBC to Out of Service, along with journal statistics.
- The Standby SBC logs the time it starts resynchronization and the time it becomes synchronized.
- The Active SBC logs the Request-Response RTT and Request-Response Loss Percentage statistics when the standby SBC changes to Out of Service.
- For sipd and mbcd, the number of redundancy objects to be synchronized is logged on the active SBC at the start of re-synchronization.

These log messages are logged to task log files regardless of the log-level of **redundancy-config**.

Command Examples

Display information about redundancy health by using the **show health** command.

(available in User Mode)

Active

The following example shows a currently active Oracle Communications Session Border Controller.

```
ORACLE# show health
        Media Synchronized            enabled
        SIP Synchronized              enabled
        Config Synchronized           enabled
        Collect Synchronized          enabled
        Radius CDR Synchronized       enabled
        Rotated CDRs Synchronized     enabled
        Active Peer Address           163.4.12.2
Redundancy Protocol Process (v2):
        State                           Active
        Health                          100
        Lowest Local Address            11.0.0.1:9090
        1 peer(s) on 1 socket(s):
        systest3B: v2, Standby, health=100, max silence=1050
                  last received from 11.0.0.2 on wancom1:0
        Switchover log:
        Jul 11 14:18:21.442: Active to RelinquishingActive
        Jul 11 14:24:00.872: Standby to BecomingActive, active
peer             systest3B has timed out. The following example that follows
shows a         currently standby Oracle Communications Session Border
Controller.
```

Standby

The following example shows a becoming standby Oracle Communications Session Border Controller.

```
ORACLE# show health
        Media Synchronized             true
        SIP Synchronized               disabled
        Config Synchronized            true
        Active Peer Address            0.0.0.0
Redundancy Protocol Process (v2):
        State                           Active
        Health                          100
        Lowest Local Address            11.0.0.1:9090
        1 peer(s) on 1 socket(s):
        systest3B: v2, Standby, health=100, max silence=1050
                  last received from 11.0.0.2 on wancom1:0
        Switchover log:
        Jul 11 14:18:21.442: Active to RelinquishingActive
        Jul 11 14:24:00.872: Standby to BecomingActive, active peer systest3B
```

```
 has timed out
ORACLE2#
```

The following table lists the health statistics along with a brief description.

Statistic	Description
Media Synchronized	Whether or not the media flow is synchronized for both supported protocols: SIP and H.323, (true/false). If media flow information is not available, the Media Synchronized displayed message is displayed in the show health output.
SIP Synchronized	Whether or not SIP signaling information is synchronized (true/false). If SIP signaling is not available, the SIP Synchronized disabled message is displayed in the show health output.
Config Synchronized	Whether or not configuration information is synchronized (true/false).
Active Peer Address	IPv4 address of the current HA Oracle Communications Session Border Controller's active peer (an HA Oracle Communications Session Border Controller that is currently active does not have an active Oracle Communications Session Border Controller peer and will show 0.0.0.0)

Viewing Routing Statistics

This section explains how to view the routing statistics.

Viewing Routing Table Entries

Display entries in the routing table by using the **show routes** command. The routing table displays IP layer information about the destination, mask, TOS, gateway, flags, reference count, use, interface, and protocol information.

```
ORACLE# show routes
Destination/Pfx    Gateway         Flags    RefCnt Use     Proto Tos
I/f
0.0.0.0/0          172.30.0.1      2010003  0      0            1   0
wancom0
10.0.0.0/16        172.30.0.1      2010003  1      0            1   0
wancom0
10.0.200.164       172.30.0.1      2020007  1      13801        2   0
wancom0
127.0.0.1          127.0.0.1       2200005  82     36220        2   0
lo0
172.30.0.0/16      172.30.55.127   2000101  2      0            2   0
wancom0
```

Viewing Routing Stats

Display statistics for the application layer routes shown in the routing table by using the **show route-stats** command.

```
ORACLE# show route-stats
routing:
        0 bad routing redirect
        3 dynamically created route
        1 new gateway due to redirects
        9 destinations found unreachable
        2 use of a wildcard route
ORACLE#
```

Testing Routing Policies

Use the **test policy** command to test application layer routes from the ACLI by specifying a from and to address. You can also specify a source realm, time of day, and carriers.

The **test-policy** command works similarly to the way a configuration element does. This command allows you to test and display local policy routes from the ACLI by specifying From and To addresses. After you have entered these addresses, use the **show** command to perform the actual lookup.

```
ORACLE# test-policy ?
carriers                      sets list of permitted carriers
from-address                  From address list
media-profiles                list of media profiles
show                          shows local policy test results
source-realm                  Source realm
time-of-day                   enables/disables time of day
to-address                    To address
exit                          end test
```

The following table lists the test-policy specification formats.

Specification	Format
source-realm	A string that indicates the name set in the source-realm field of a configured local-policy element. If you enter a “*” in this specification, any configured source realms will be matched. An empty source-realm value indicates that only the global realm will be tested
time-of-day	A Boolean value that can be set to either enabled or disabled that indicates whether or not to use the time of day value set in the start-time and end-time fields set in configured local-policy elements
carriers	A list of comma-separated text strings enclosed in quotation marks of the names of permitted carriers set in the carriers fields set in configured local-policy elements.

Test Policy Subcommands

The following table lists and describes the **test-policy** subcommands.

test-policy Subcommand	Description
from-address	Set the From address of the local policy you want to look up/test. From addresses should be entered as SIP-URLs (e.g., sip:19785551212@netnetsystem.com).

test-policy Subcommand	Description
to-address	Set the To address of the local policy you want to look up/test. To addresses should be entered as SIP-URLs (for example, sip:19785551212@netnetsystem.com).
show	Performs the actual policy lookup and shows the next hop and the associated carrier information for all routes matching the From and To addresses entered.
exit	Exits the test-policy session.

Testing Address Translations

Oracle Communications Session Border Controller number translation is used to change a Layer-5 endpoint name according to prescribed rules. Number translations can be performed on both the inbound and the outbound call legs independently, before and after routing occurs. Number translation is used for SIP, H.323, and SIP/ H.323 interworking. configurations.

```
ORACLE# test-translation
called-address                called address
calling-address               calling address
show                          shows local translation test results
translation-id                Translation Id
exit                          end test
```

Viewing QoS Based Routing Statistics

You can view statistics about QoS based routing for realms, and see what realms are in service or whether a call load reduction has been applied. In the ACLI **show realms** display, the following values show you QoS based routing information:

- QoS Major Exceeded
- QoS Critical Exceeded
- QoS R-Factor Avg.

You can see these statistics in the following example of a **show realm** display:

```
ORACLE# show realm
13:34:24-167   Realm Statistics
                                  -- Period -- ------- Lifetime -------
Realm               Active  Rate   High  Total      Total PerMax   High
external                [Reduction In Call Load]
    Inbound              0   0.0      0      0          0      0      0
    Outbound             0   0.0      2      1          2      2      1
internal                [In Service]
    Inbound              0   0.0      3      1          3      3      1
    Outbound             0   0.0      0      0          0      0      0
ORACLE# show realm external
13:33:00-82
Realm external() [Reduction In Call Load]
-- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
```

```
Inbound Sessions        0       0       0          0       0       0
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0       0       0          0       0       0
  Reg Rate Exceeded     -       -       0          0       0       -
  Reg Burst Rate        0       0       0          0       0       0
Outbound Sessions       0       1       2          2       2       1
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0       2       0          0       0       2
  Reg Rate Exceeded     -       -       0          0       0       -
Out of Service          -       -       0          0       0       -
Trans Timeout           0       0       0          0       0       0
Requests Sent           -       -       0          0       0       -
Requests Complete       -       -       0          0       0       -
Seizure                 -       -       4          4       4       -
Answer                  -       -       4          4       4       -
  ASR Exceeded          -       -       0          0       0       -
Requests Received       -       -       0          0       0       -
QoS Major Exceeded      -       -       2          2       2       -
QoS Critical Exceeded   -       -       0          0       0       -
Latency=0.000; max=0.000
QoS R-Factor Avg=82.39; max=93.21
```

Local Route Table Statistics and Management

This section ACLI commands that have been added so that you can troubleshooting this feature, and view monitoring statistics and other information about it.

Setting the Log Level

Log files for the local routing system task are log.lrtd and lrt.log. The lrt.log file contains the DNS request and response communication between the system's SIP and local routing tasks.

Using the new ACLI **notify lrtd** command, you can set the local routing task's log level to any of the following:

- log
- nolog
- debug
- nodebug
  To set the log level for the local routing task:

- In Superuser mode, type **notify lrtd**, followed by the log level you want to set. Then press Enter.

```
ORACLE# notify lrtd log
```

Updating the Local Cache

When you want to update the cache file with new entries, delete old ones, or edit existing entries, you can refresh the local cache for a specific local routing policy.

To update the cache file for a local routing policy:

- In Superuser mode, type **notify lrtd refresh**, followed by the name of the local routing policy you want updated.

```
ORACLE# notify lrtd refresh lookup
```

Testing a Lookup in the Local Cache

To test a lookup in the local cache:

- In User or Superuser mode, enter the **show enum lookup lrt=** command. After the equal sign (=), type the name of the local routing configuration you want to test followed by a Space. Then type in the E.164 number you want to look up, and press Enter.

```
ORACLE# show enum lookup lrt=lookup +123
Enum Lookup Result:
Query Name -->
        +123
Answers -->
        sip:123@192.168.1.191 ttl= 60
```

Displaying a Route Entry in the Local Cache

To see a route entry in the local cache:

- In User or Superuser mode, enter the **show lrt route-entry** command. Then type in the name of the local routing configuration, a Space, the key you want to use, and then press Enter.

```
ORACLE# show lrt route-entry lookup 123
UserName <123>
 User Type= E164
NextHop= !^.*$!sip:123@192.168.1.191!
 NextHop Type= regexp
```

Displaying Statistics for a Local Route Tables

There are two ways to see statistics for local route tables:

- Collectively—Viewing all of the statistics for all of the local route tables at once (using the **show lrt stats** command)

- Individually—Viewing the statistics for a local route table that you specify (using the **show lrt stats** command with the name of a specific local routing configuration)

The Oracle Communications Session Border Controller shows you the following information:

- Queries—Number of queries from the application includes those that resulted in a cache hit, and those that caused an actual query to be sent
- Success—Number of successful results; includes cache hits and queries sent
- NotFound—Number of note found results; includes cache hits and queries sent
- Number of Valid Entries—Total number of valid entries in the cache
- Number of Invalid Entries—Total number of invalid entries in the cache
- Last Modified—Date and time the cache was last modified

Resetting ENUM Statistic Counters

To clear statistics for ENUM, you can use the ACLI **reset** command. Before you reset the counters, however, you might want to confirm the current statistics on the system are not zero. You can do so using the show command—by typing, for example, **show enum stats**.

The **reset** command takes the ENUM arguments to clear those sets of statistics. When you use the command, the system notifies you whether it has successfully cleared the statistics (even if the counter are zero) or if it has run into an error causing the command to fail.

You can **reset all** system statistics using the reset all command.

The ENUM example confirms successful completion of the command.

To clear ENUM statistics:

- At the command line, type **reset enum** and then press Enter.

```
ORACLE# reset enum
Successful reset of the ENUM Agent stats
```

Viewing SIP Protocol Performance Statistics

This section contains the commands you use to access SIP protocol statistics. These statistics provide information about the SIP protocol performance.

Accessing SIP Statistics

You can access SIP statistics for both client and server SIP transactions by using the **show sipd** command. You can then use additional subcommands to display more specific information, including specific types of SIP messages.

Example

The following example show s the output of the **show sipd** command.

```
ORACLE# show sipd
14:10:32-178
SIP Status                  -- Period -- -------- Lifetime --------
```

```
                Active    High   Total      Total  PerMax    High
Sessions             0       0       0          0       0       0
Subscriptions          0       0       0          0       0       0
Dialogs              0       0       0          0       0       0
CallID Map           0       0       0          0       0       0
Rejections           -       -       0          0       0
ReINVITEs            -       -       0          0       0
Media Sessions       0       0       0          0       0       0
Media Pending        0       0       0          0       0       0
Client Trans         0       0       0          0       0       0
Server Trans         0       0       0          0       0       0
Resp Contexts        0       0       0          0       0       0
Saved Contexts       0       0       0          0       0       0
Sockets              0       0       0          0       0       0
Req Dropped          -       -       0          0       0
DNS Trans            0       0       0          0       0       0
DNS Sockets          0       0       0          0       0       0
DNS Results          0       0       0          0       0       0
Session Rate = 0.0
Load Rate = 0.0
```

The display organizes the SIP transaction statistics for the system into two categories: **Client Trans(actions)** and **Server Trans(actions)**. The remainder of the display provides information regarding dialogs, sessions, sockets, and DNS transactions.

Viewing SIP Status Information

The following example shows the output of the **show sipd status** command.

```
ORACLE# show sipd status
14:11:15-121
SIP Status                -- Period -- -------- Lifetime --------
                Active    High   Total      Total  PerMax    High
Sessions             0       0       0          0       0       0
Subscriptions        0       0       0          0       0       0
Reg Evt Subs         0       0       0          0       0       0
Dialogs              0       0       0          0       0       0
CallID Map           0       0       0          0       0       0
Rejections           -       -       0          0       0
ReINVITEs            -       -       0          0       0
Media Sessions       0       0       0          0       0       0
Media Pending        0       0       0          0       0       0
Client Trans         0       0       0          0       0       0
Server Trans         0       0       0          0       0       0
Resp Contexts        0       0       0          0       0       0
Saved Contexts       0       0       0          0       0       0
Sockets              0       0       0          0       0       0
Req Dropped          -       -       0          0       0
DNS Trans            0       0       0          0       0       0
DNS Sockets          0       0       0          0       0       0
DNS Results          0       0       0          0       0       0
Replaced Dialogs     -       -       1          1       1
```

```
Session Rate = 0.0
Load Rate = 0.0
```

The following table lists the SIP status statistics.

Statistic	Description
Dialogs	Number of SIP signaling connections between the Oracle Communications Session Border Controller and a SIP UA (for example, a call leg)
Sessions	Number of sessions established by an INVITE request. A session consists of all dialogs created by one INVITE transaction.
Sockets	Number of active SIP communication ports (the number of open UDP and TCP sockets)
DNS Transactions	Number of outstanding DNS requests

SIP Monitoring by Transaction Type

You can view statistics about SIP monitoring by transaction type.

SIP Server Transactions

Display statistics SIP server transactions by using the **show sipd server** command.

```
ORACLE# show sipd server
15:40:05-65
SIP Server Trans          -- Period -- -------- Lifetime --------
                Active    High   Total      Total  PerMax    High
All States           0     346    2213      67975    3729     365
<Initial>            0       1    2213      67975    3729       1
<Trying>             0      48    1504      44773    2431      63
<Proceeding>         0       9     709      23202    1310       9
<Cancelled>          0       2      75       1370     182       4
<Established>        0       2     545      20201     971       3
<Completed>          0     148     959      24572    1489     149
<Confirmed>          0     157     716      23202    1309     161
<Terminated>         0       1     545      20201     972       1
ORACLE#
```

The following table lists the specifics along with a brief description.

Statistic	Description
All States	Total number of all server transactions.
Initial	State when the server transaction is created after a request is received.
Trying	Number of times the 100 Trying message has been sent, meaning that a request has been received and action is being taken.
Proceeding	Number of times a server transaction has been constructed for a request.
Cancelled	Number of INVITE transactions for which the system receives a CANCEL.
Established	Situation in which the server sends a 2xx response to an INVITE.

Statistic	Description
Completed	Number of times that the server has received a 300 to 699 status code and therefore entered the completed state.
Confirmed	Number of times that an ACK was received while the server was in the completed state and therefore transitioned to the confirmed state.
Terminated	Number of times that the server has received a 2xx response or has never received an ACK while in the completed state, and has therefore transitioned to the terminated state.

SIP Client Transactions

Display statistics for SIP client transactions by using the **show sipd client** command.

```
ORACLE# show sipd client
15:40:09-69
SIP Client Trans          -- Period -- -------- Lifetime --------
                Active    High   Total      Total  PerMax    High
All States           0     382    2042      64973    3371     387
<Initial>            0       1    2042      64973    3371       2
<Trying>             0     128    1333      41771    2073     128
<Calling>            0       2     709      23202    1310       2
<Proceeding>         0       8     613      21570    1130       9
<Cancelled>          0       2      75       1370     182       4
<EarlyMedia>         0       0       0          0       0       0
<Completed>          0     146     959      24571    1489     167
<SetMedia>           0       2     545      20201     972       2
<Established>        0     127     545      20201     971     127
<Terminated>         0       0       0          0       0       0
ORACLE#
```

The following table lists the statistics along with a brief description.

Statistic	Description
All States	Total number of all client transactions.
Initial	State before a request is sent out.
Trying	Number of times the trying state was entered due to the receipt of a request.
Calling	Number of times that the calling state was entered due to the receipt of an INVITE request.
Proceeding	Number of times that the proceeding state was entered due to the receipt of a provisional response while in the calling state.
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 300 to 699 status code when either in the calling or proceeding state.
SetMedia	Number of transactions in which the system is setting up NAT and steering ports (setting up the steering of the RTP flow).

Statistic	Description
Established	Number of situations in which the client receives a 2xx response to an INVITE, but can not forward it on because it requires NAT and steering port information.
Terminated	Number of times that the terminated state was entered due to the receipt of a 2xx message.

Viewing SIP Media Event Errors

Display statistics for SIP media event errors by using the **show sipd errors** command.

```
ORACLE# show sipd errors
13:06:59-159
SIP Errors/Events             ---- Lifetime ----
                       Recent      Total  PerMax
SDP Offer Errors            0          0       0
SDP Answer Errors           0          0       0
Drop Media Errors           0          0       0
Transaction Errors          0          0       0
Application Errors          0          0       0
Media Exp Events            0          0       0
Early Media Exps            0          0       0
Exp Media Drops             0          0       0
Expired Sessions            0          0       0
Multiple OK Drops           0          0       0
Multiple OK Terms           0          0       0
Media Failure Drops         0          0       0
Non-ACK 2xx Drops           0          0       0
Invalid Requests            0          0       0
Invalid Responses           0          0       0
Invalid Messages            0          0       0
CAC Session Drop            0          0       0
CAC BW Drop                 0          0       0
Replace Dialog Fails        0          0       0
```

The information displayed is divided into the following categories:

- **Recent**: number of errors that occurred within the number of seconds defined by the figure that appears directly after the time. In the example above, the Recent period of time is 60 seconds.
- **Total**: number of errors that occurred since the system was last rebooted.
- **PerMax**: period maximum number of errors that occurred since the system was last rebooted. This value identifies the highest individual Period Total value calculated over the lifetime of the monitoring.

These statistics record exceptional events encountered by the SIP application in processing SIP media sessions, dialogs, and sessions descriptions (SDP). Serious errors will be accompanied by a log message in **log.sipd** and **acmelog** (depending of the current **log level** setting) of the appropriate severity which will indicate the nature of the error.

Statistic	Description
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 defined in RFC 3264. This may be a failure to send the transaction to MBCD or an error response from MBCD. These errors may also be counted in one of the show mbcd errors.
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). This may be a failure to send the transaction to MBCD or an error response from MBCD. These errors may also be counted in the show mbcd errors.
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 Oracle Communications Session Border Controller due to a timeout notification from MBCD. This may be a failure to send the transaction to MBCD or an error response from MBCD. These errors may also be counted in the show mbcd errors.
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. Usually, this event will also be counted as a 481 (Does Not Exist) server response for the method of the SIP request. This event will occur quite often particularly when both endpoints send a BYE request at approximately the same time.
Application Errors	Number of miscellaneous errors that occur in the SIP application that are otherwise uncategorized.
Media Exp Events	Number of flow timer expiration notifications received from MBCD. These may be fairly common particularly if endpoints stop sending media (or do not start sending media) without sending the appropriate signaling message (BYE) to terminate the dialog/session. These events may also be counted in the show mbcd errors.
Early Media Exps	Number of flow timer expiration notifications received for media sessions that have not been completely set up due to an incomplete or still pending INVITE transaction (e.g., 200 OK response to the INVITE has not been received yet). This can occur if an INVITE transaction takes longer than the initial-guard-timer or subsq-guard-timer fields defined in the media-manager-config element. This event does not result in the dialog/session being terminated if the INVITE is still pending. Note that this statistic is a subset of the Media Exp Events above.
Exp Media Drops	Number of flow timer expiration notifications from MBCD which resulted in the SIP application terminating the dialog/session.

Statistic	Description
Multiple OK Drops	Number of dialogs that were terminated upon reception of a 200 OK response from multiple UASs for a given INVITE transaction which was forked by a downstream proxy. When multiple UASs accept an INVITE with a 200 OK responses, only the first one is passed on by the Oracle Communications Session Border Controller. If the subsequent 200 OK were processed and passed on the media session established by the first 200 OK would be disrupted. The Oracle Communications Session Border Controller will ACK the 200 OK response and then send a BYE request to terminate the dialog for the subsequent 200 OK response. The proscribed behavior for the proxy is to cancel outstanding branches of the fork when a 200 OK is received. However, there is a race condition where a subsequent 200 OK is generated by a UAS before the CANCEL reaches the UAS.
Multiple OK Terms	Number of dialogs that were terminated upon reception of a 200 OK response which conflicts with an existing established dialog on the Oracle Communications Session Border Controller. This is similar to the Multiple OK Drops statistic. The difference is that an upstream proxy forked the INVITE resulting in multiple INVITE transactions which have the same Call-ID and session description (SDP). The Oracle Communications Session Border Controller will accept only the first 200 OK received. If the subsequent 200 OK were processed, the media session established by the initial 200 OK would be disrupted. The Oracle Communications Session Border Controller will ACK the 200 OK response and then send a BYE request to terminate the dialog for the subsequent 200 OK response. The Oracle Communications Session Border Controller will send a 487 (Terminated) response upstream in order to complete the client transaction which conflicted with an established dialog. The prescribed behavior for the proxy is to cancel outstanding branches of the fork when a 200 OK is received. However, there is a race condition where a subsequent 200 OK is generated by a UAS before the CANCEL reaches the UAS.
Media Failure Drops	Number of dialogs that had to be terminated due to a failure in setting up the media session. This situation occurs when an SDP offer is sent downstream in a request, but the SDP answer in a response to that request encounters a failure. Rather than passing the successful response upstream to the User Agent Client (UAC), the Oracle Communications Session Border Controller terminates the session. For an INVITE transaction, the Oracle Communications Session Border Controller sends an ACK for the 200 OK response and then sends a BYE request. The Oracle Communications Session Border Controller then sends an error response to the UAC.
Expired Sessions	Number of sessions that were terminated due to the session timer expiring. When the media for a dialog/session does not traverse the Oracle Communications Session Border Controller, the SIP application sets a session timer (equal to the flow-time-limit defined in the media-manager-config). This to ensure that the session is properly cleaned up in the event that the endpoints do not send the appropriate signaling to terminate the session (e.g., BYE). Note that when the media session does traverse the Oracle Communications Session Border Controller, the flow timers are used by MBCD and the SIP application does not set a session timer.

Viewing SIP Session Agent Statistics

Display SIP session agent information by using the **show sipd agents** command. With this command, the Oracle Communications Session Border Controller ascertains whether a session agent is in service. When the session agent stops responding to SIP requests, it transitions to the out-of-service state. You can configure the Oracle Communications Session Border Controller to periodically ping the session agent if it has gone out-of-service, or if no requests have been sent to it.

The **show sipd agents** command shows information about the number of active sessions, the average rate of session invitations, and the number of times that the constraints established in the session-agent element have been exceeded for sessions inbound to and outbound from each session agent, as well as the average and maximum latency and the maximum burst rate related to each session agent.

For example:

```
ORACLE# show sipd agents
19:39:34-95
                ---- Inbound ----  --- Outbound ----  -Latency-  ---
Max ---
Session Agent   Active Rate ConEx  Active Rate ConEx  Avg   Max  Burst
In Out
192.168.200.131      0  0.0     0       0  0.0     0  0.0   0.0
0  0   0
```

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 statistics:

- Avg: average latency for packets traveling to and from each session agent listed
- Max: maximum latency for packets traveling to and from each session agent listed
- Max Burst: total number of session invitations sent to or received from the session agent within the amount of time configured for the burst rate window of the session agent

The second column, which is not labeled, of the **show sipd agents** output shows the service state of each session agent identified in the first column. In the service state column, an I indicates that the particular session agent is in service and an O indicates that the particular session agent is out of service. An S indicates that the session agent is in transition from the out-of-service state to the in-service state; it remains in this transitional state for a period of time that is equal to its configured in-service period, or 100 milliseconds (whichever is greater). A D indicates that the session agent is disabled.

Viewing SIP Session Agent Group Statistics

Display session information for the session agent groups on the system by using the **show sipd groups** command. 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 for the system.

If you carry out this command, but you do not specify the name of an existing session agent group, the system informs you that the group statistics are not available.

Viewing Session and Dialog States

Display session and dialog states by using the **show sipd sessions** command. For example:

```
SIP Session Status        -- Period -- -------- Lifetime --------
                Active    High   Total      Total  PerMax    High
Sessions             0       0       0          0       0       0
  Initial            0       0       0          0       0       0
  Early              0       0       0          0       0       0
  Established        0       0       0          0       0       0
  Terminated         0       0       0          0       0       0
Dialogs              0       0       0          0       0       0
  Early              0       0       0          0       0       0
  Confirmed          0       0       0          0       0       0
  Terminated         0       0       0          0       0       0
```

Sessions

- Initial—state of a new session for which an INVITE or SUBSCRIBE is being forwarded.
- Early—state the session enters when it receives the first provisional response (1xx other than 100).
- Established—state the session enters when it receives a success (2xx) response.
- Terminated—state the session enters when 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 remains in the Terminated state until all the resources for the session are freed.

Dialogs

A dialog is created when a dialog establishing method (INVITE or SUBSCRIBE) receives a provisional (1xx other than 100) or success (2xx) response.

- Early—dialog is created by a provisional response.
- Confirmed—dialog is created by a success response; an Early dialog transitions to Confirmed when it receives a success response.
- Terminated—dialog enters this state when the session is ended by receiving/sending a BYE for an Established session, or by receiving/sending error response Early dialog. The dialog remains in the Terminated state until all the resources for the session are freed.

Viewing SIP Endpoint

The **show sipd sip-endpoint-ip** command supports the look-up and display of registration information for a designated endpoint. This command uses the following syntax: show sipd endpoint-ip <phone number>. For the phone number value, you can enter as many components of the particular phone number about which you would like information—including information about adaptive HNT.

This command must be entered with the numerical value representing the endpoint to look up. The ACLI help menu prompts you for this information.

```
ORACLE# show sipd endpoint-ip ?
----------  ACLI v1.0  -----------
<phone number>  enter phone number to look up endpoint
```

There is no support for wildcard matches or lists of users. The first entry that matches the phone number given as an argument will be returned. The following examples show a range of matching values.

```
ORACLE# show sipd endpoint-ip 1781
Reg[sip:17815551111@69.69.69.10]
RegEntry[sip:17815551111@69.69.69.10] ID=4 exp=28
UA-
contact='sip:17815551111@69.69.69.69:5062;acme_nat=192.168.201.50:5060'
SD-contact='sip:17815551111-1ke1g79h75pu8@69.69.69.10'
hnt-test-status='IN-PROGRESS'
successful-test-time='40 secs'

ORACLE# show sipd endpoint-ip 17815551111
Reg[sip:17815551111@69.69.69.10]
RegEntry[sip:17815551111@69.69.69.10] ID=4 exp=20
UA-
contact='sip:17815551111@69.69.69.69:5062;acme_nat=192.168.201.50:5060'
SD-contact='sip:17815551111-1ke1g79h75pu8@69.69.69.10'
hnt-test-status='COMPLETED'
successful-test-time='40 secs'
ORACLE# show sipd endpoint-ip 17815559999
Reg[sip:17815559999@69.69.69.80]
RegEntry[sip:17815559999@69.69.69.80] ID=5 exp=29
UA-
contact='sip:17815559999@69.69.69.69:5063;acme_nat=192.168.201.155:5060
'
SD-contact='sip:17815559999-2se308dh81p29@69.69.69.10'
hnt-test-status='IN-PROGRESS'
successful-test-time='40 secs'
ORACLE# show sipd endpoint-ip 1781555
Reg[sip:17815551111@69.69.69.10]
RegEntry[sip:17815551111@69.69.69.10] ID=4 exp=17
UA-
contact='sip:17815551111@69.69.69.69:5062;acme_nat=192.168.201.50:5060'
SD-contact='sip:17815551111-1ke1g79h75pu8@69.69.69.10'
hnt-test-status='IN-PROGRESS'
successful-test-time='40 secs'
```

```
hnt-test-status='IN-PROGRESS'
successful-test-time='40 secs'
ORACLE# show sipd endpoint-ip 1781555555
Reg[sip:17815555555@69.69.69.80]
RegEntry[sip:17815555555@69.69.69.80] ID=3 exp=19
UA-contact='sip:17815555555@69.69.69.69:5060;user=phone'
SD-contact='sip:17815555555-v3etv61h55om8@69.69.69.10'
hnt-test-status='COMPLETED'
successful-test-time='40 secs'
```

Viewing SIP Per User CAC Statistics

The commands in this section allow you to view information about SIP per user CAC.

IP-Based CAC Information

If you want to see information about the operation of SIP per user CAC for the IP address mode, you can use the new ACLI **show sipd ip-cac** command. You enter this command with the IP address for which you want to view data.

The Oracle Communications Session Border Controller will display the number of configured sessions allowed, number of active sessions, amount of configured bandwidth allowed, and the amount of bandwidth used.

To view information about SIP per user CAC using the IP address mode:

- In either User or Superuser mode, type **show sipd ip-cac**, a Space, and the IP address for which you want to view data. Then press Enter.

```
ORACLE# show sipd ip-cac 192.168.200.191
CAC Parameters for IP <192.168.200.191>
 Allowed Sessions=2
 Active-sessions=0
 Allowed Bandwidth=3000000
 used-bandwidth=0
```

AoR-Based CAC Information

If you want to see information about the operation of SIP per user CAC for the AoR mode, you can use the **show sipd endpoint-ip** command. You enter this command with the AoR for which you want to view data.

- In either User or Superuser mode, type **show sipd endpoint-ip**, a Space, and the AoR for which you want to view data. Then press Enter.

```
ORACLE# show sipd endpoint-ip 123
User <sip:123@192.168.200.191>
  Contact local-exp=47 exp=97
    UA-Contact: <sip:123@192.168.200.191:5061>
    SD-Contact: <sip:123-rrbgdlubs3e66@192.168.1.190:5060>
    Call-ID: 00078555-47260002-3dde9eea-259763e2@10.10.10.16'
 Allowed Sessions=2
 Active-sessions=0
```

```
    Allowed Bandwidth=3000000
    used-bandwidth=0
```

Number of Calls Dropped because of Per User CAC Limits

The **show sipd errors** command allows you to view how many calls were dropped:

- Because the per user CAC session limit was exceeded
- Because the per user CAC bandwidth limit was exceeded

Viewing Statistics for SIP Per User Subscribe Dialog Limit

You can display the number of subscription dialogs per SUBSCRIBE event type using the ACLI **show registration sipd subscriptions-by-user** command. You can display this information per event type, or you can show data for all event types by wildcarding the event type argument.

The following example shows you how to use this command with a wildcard.

```
ORACLE# show registration sipd subscriptions-by-user *
Registration Cache                    FRI NOV 21 2008  13:40:14
User: sip:7815550001@192.168.1.206
  AOC: <sip:7815550001@192.168.1.206:5060;transport=udp>
    Event-Type: dialog  -->  Subscriptions: 2
----------------- -------------------------------- ------------------
```

Message Rate Statistics

The Oracle Communications Session Border Controller provides message rate statistics for SIP traffic. You must first enable extra method statistics generation in the sip config.

To enable full SIP message rate statistics:

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

   ```
   ORACLE# configure terminal
   ```

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

   ```
   ORACLE(configure)# session-router
   ORACLE(session-router)#
   ```

3. Type **sip-config** and press Enter.

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

4. **extra-method-stats**—Set this parameter to enabled for the Oracle Communications Session Border Controller to collect and track SIP method statistics per second.
5. Save and activate your configuration.

Message rate statistics are listed per message type. This command is entered as:

```
ORACLE# show sipd rate [interface <interface-name> | agent agent-name]
```

show sipd rate

The **show sipd rate** command displays request and response rates for messages (per method) on a system-wide basis. The rates are calculated based on the time in the current monitoring window (100+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ORACLE# show sipd rate
17:24:28-103
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                 Rate      Rate      Rate      Rate       Rate       Rate
INVITE            0.0       0.0       0.0       0.0        0.0        0.0
ACK               0.0       0.0       0.0       0.0        0.0        0.0
BYE               0.0       0.0       0.0       0.0        0.0        0.0
REGISTER          0.0       0.0       0.0       0.0        0.0        0.0
CANCEL            0.0       0.0       0.0       0.0        0.0        0.0
PRACK             0.0       0.0       0.0       0.0        0.0        0.0
OPTIONS           0.0       0.0       0.0       0.0        0.0        0.0
INFO              0.0       0.0       0.0       0.0        0.0        0.0
SUBSCRIBE         0.0       0.0       0.0       0.0        0.0        0.0
NOTIFY            0.0       0.0       0.0       0.0        0.0        0.0
REFER             0.0       0.0       0.0       0.0        0.0        0.0
UPDATE            0.0       0.0       0.0       0.0        0.0        0.0
MESSAGE           0.0       0.0       0.0       0.0        0.0        0.0
PUBLISH           0.0       0.0       0.0       0.0        0.0        0.0
OTHER             0.0       0.0       0.0       0.0        0.0        0.0
ALL               0.0       0.0       0.0       0.0        0.0        0.0
clank#
```

show sipd rate interface

The **show sipd rate interface** command displays request and response rates for messages (per method) for all configured sip-interfaces. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ORACLE# show sipd rate interface
17:24:33-58
Sip Interface core
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                 Rate      Rate      Rate      Rate       Rate       Rate
INVITE            0.0       0.0       0.0       0.0        0.0        0.0
ACK               0.0       0.0       0.0       0.0        0.0        0.0
BYE               0.0       0.0       0.0       0.0        0.0        0.0
REGISTER          0.0       0.0       0.0       0.0        0.0        0.0
CANCEL            0.0       0.0       0.0       0.0        0.0        0.0
PRACK             0.0       0.0       0.0       0.0        0.0        0.0
OPTIONS           0.0       0.0       0.0       0.0        0.0        0.0
```

```
INFO              0.0       0.0       0.0       0.0        0.0
0.0
SUBSCRIBE         0.0       0.0       0.0       0.0        0.0
0.0
NOTIFY            0.0       0.0       0.0       0.0        0.0
0.0
REFER             0.0       0.0       0.0       0.0        0.0
0.0
UPDATE            0.0       0.0       0.0       0.0        0.0
0.0
MESSAGE           0.0       0.0       0.0       0.0        0.0
0.0
PUBLISH           0.0       0.0       0.0       0.0        0.0
0.0
OTHER             0.0       0.0       0.0       0.0        0.0
0.0
17:24:33-58
Sip Interface peer
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp
Sent
                 Rate      Rate      Rate      Rate       Rate
Rate
INVITE            0.0       0.0       0.0       0.0        0.0
0.0
ACK               0.0       0.0       0.0       0.0        0.0
0.0
BYE               0.0       0.0       0.0       0.0        0.0
0.0
REGISTER          0.0       0.0       0.0       0.0        0.0
0.0
CANCEL            0.0       0.0       0.0       0.0        0.0
0.0
PRACK             0.0       0.0       0.0       0.0        0.0
0.0
OPTIONS           0.0       0.0       0.0       0.0        0.0
0.0
INFO              0.0       0.0       0.0       0.0        0.0
0.0
SUBSCRIBE         0.0       0.0       0.0       0.0        0.0
0.0
NOTIFY            0.0       0.0       0.0       0.0        0.0
0.0
REFER             0.0       0.0       0.0       0.0        0.0
0.0
UPDATE            0.0       0.0       0.0       0.0        0.0
0.0
MESSAGE           0.0       0.0       0.0       0.0        0.0
0.0
PUBLISH           0.0       0.0       0.0       0.0        0.0
0.0
OTHER             0.0       0.0       0.0       0.0        0.0
0.0
```

By entering a configured interface, the ACLI displays aggregate statistics for that interface and then displays all Session Agents’ counts configured on that SIP interface. Displays have been truncated below. For example:

```
ORACLE# show sipd rate interface peer
17:24:40-34
Sip Interface peer
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                 Rate      Rate      Rate      Rate       Rate       Rate
INVITE            0.0       0.0       0.0       0.0        0.0        0.0
[...]
OTHER             0.0       0.0       0.0       0.0        0.0        0.0
clank#
_____________________________________________________________________________
_____
Session Agent 172.16.202.102
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                 Rate      Rate      Rate      Rate       Rate       Rate
INVITE            0.0       0.0       0.0       0.0        0.0        0.0
ACK               0.0       0.0       0.0       0.0        0.0        0.0
BYE               0.0       0.0       0.0       0.0        0.0        0.0
REGISTER          0.0       0.0       0.0       0.0        0.0        0.0
CANCEL            0.0       0.0       0.0       0.0        0.0        0.0
PRACK             0.0       0.0       0.0       0.0        0.0        0.0
OPTIONS           0.0       0.0       0.0       0.0        0.0        0.0
INFO              0.0       0.0       0.0       0.0        0.0        0.0
SUBSCRIBE         0.0       0.0       0.0       0.0        0.0        0.0
NOTIFY            0.0       0.0       0.0       0.0        0.0        0.0
REFER             0.0       0.0       0.0       0.0        0.0        0.0
UPDATE            0.0       0.0       0.0       0.0        0.0        0.0
MESSAGE           0.0       0.0       0.0       0.0        0.0        0.0
PUBLISH           0.0       0.0       0.0       0.0        0.0        0.0
OTHER             0.0       0.0       0.0       0.0        0.0        0.0
17:26:21-46
Session Agent 192.168.202.100
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
                 Rate      Rate      Rate      Rate       Rate       Rate
INVITE            0.0       0.0       0.0       0.0        0.0        0.0
[...]
OTHER             0.0       0.0       0.0       0.0        0.0        0.0
ORACLE#
```

show sipd rate agent

The **show sipd rate agent** command displays request and response rates for messages (per method) for all session agents. By adding a session agent name in the form show sipd rate agent <session-agent-name>, you can view statistics for the identified agent only. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ORACLE# show sipd rate agent 192.168.202.100
17:26:47-42
Session Agent 192.168.202.100
```

```
Method Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp 
Sent
                 Rate      Rate      Rate      Rate       Rate      
Rate
INVITE            0.0       0.0       0.0       0.0        0.0       
0.0
ACK               0.0       0.0       0.0       0.0        0.0       
0.0
BYE               0.0       0.0       0.0       0.0        0.0       
0.0
REGISTER          0.0       0.0       0.0       0.0        0.0       
0.0
CANCEL            0.0       0.0       0.0       0.0        0.0       
0.0
PRACK             0.0       0.0       0.0       0.0        0.0       
0.0
OPTIONS           0.0       0.0       0.0       0.0        0.0       
0.0
INFO              0.0       0.0       0.0       0.0        0.0       
0.0
SUBSCRIBE         0.0       0.0       0.0       0.0        0.0       
0.0
NOTIFY            0.0       0.0       0.0       0.0        0.0       
0.0
REFER             0.0       0.0       0.0       0.0        0.0       
0.0
UPDATE            0.0       0.0       0.0       0.0        0.0       
0.0
MESSAGE           0.0       0.0       0.0       0.0        0.0       
0.0
PUBLISH           0.0       0.0       0.0       0.0        0.0       
0.0
OTHER             0.0       0.0       0.0       0.0        0.0       
0.0
```

SNMP Reporting of Message Rate Statistics pointer

Message Rate Statistics are available via SNMP. See the MIB Reference Guide, SNMP Reporting of Message Rate Statistics section for detailed information.

Viewing IMS-AKA Statistics

The ACLI **show sipd endpoint-ip** command is updated to show the IMS-AKA parameters corresponding to each endpoint. The display shows the algorithms used, the ports used, and the security parameter indexes (SPIs) used.

In addition, the **show sa stats** command now shows the security associations information for IMS-AKA.

```
ORACLE# show sa stats
05:28:32-107
SA Statistics                   ---- Lifetime ----
                            Recent      Total  PerMax
IKE Statistics
```

```
ADD-SA Req Rcvd                0          0       0
ADD-SA Success Resp Sent       0          0       0
ADD-SA Fail Resp Sent          0          0       0
DEL-SA Req Rcvd                0          0       0
DEL-SA Success Resp Sent       0          0       0
DEL-SA Fail Resp Sent          0          0       0
ACQUIRE-SA Req Sent            0          0       0
ACQUIRE-SA Success Resp        0          0       0
ACQUIRE-SA Fail Resp Rcv       0          0       0
ACQUIRE-SA Trans Timeout       0          0       0
SA Added                       0          0       0
SA Add Failed                  0          0       0
SA Deleted                     0          0       0
SA Delete Failed               0          0       0
IMS-AKA Statistics
ADD-SA Req Rcvd                0          0       0
ADD-SA Success Resp Sent       0          0       0
ADD-SA Fail Resp Sent          0          0       0
DEL-SA Req Rcvd                0          0       0
DEL-SA Success Resp Sent       0          0       0
DEL-SA Fail Resp Sent          0          0       0
SA Added                       0          0       0
SA Add Failed                  0          0       0
SA Deleted                     0          0       0
SA Delete Failed               0          0       0
```

STUN Server Statistics and Protocol Tracing

This section describes how you can monitor STUN server statistics and perform STUN protocol tracing.

STUN Server Statistics

You can display statistics for the STUN server using the ACLI **show mbcd stun** command when the STUN server has been enabled. However, if the STUN server has not been enabled since the last system reboot, the command does not appear and no statistics will be displayed.

```
ORACLE# show mbcd stun
09:05:21-193
STUN Statistics              -- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Servers                 1       1       0          2       1       1
Server Ports            4       4       0          8       4       4
Binding Requests        -       -       4        861       4
Binding Responses       -       -       4        861       4
Binding Errors          -       -       0          0       0
Messages Dropped        -       -       0          0       0
```

The table below lists and describes the STUN server statistics.

STUN Server Display Category	Description
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.

STUN Protocol Tracing

You can enable STUN protocol tracing two ways: by configuration or on demand.

- By configuration—The Oracle Communications Session Border Controller’s STUN protocol trace file is called stun.log, which is classified as a call trace. This means that when the system configuration’s call-trace parameter is set to enabled, you will obtain STUN protocol information for the system. As with other call protocol traces, tracing data is controlled by the log-filter in the system configuration.

On demand—Using the ACLI **notify mbcd log** or **notify mbcd debug** commands, you enable protocol tracing for STUN. Using **notify mbcd debug** sets the STUN log level to TRACE. You can turn off tracing using the **notify mbcd nolog** or **notify mbcd nodebug** commands. Using **notify mbcd nodebug** returns the STUN log level back to its configured setting.

Local and Remote Call Termination Counters

The SBC maintains counters of gracefully terminated calls for cases where the BYE is generated both locally within the system and call is terminated externally, as expected. Each case is maintained in a unique counter. These counters are maintained for each session agent, realm, SIP Interface, and globally.

Local and Remote Call Termination Counters are displayed in the following show commands:

- show sipd agents
- show sipd realms
- show sipd interface
- show sipd status

For each of these four show commands, Local and Remote call termination appear as follows (using show sipd agents as an example):

```
# show sipd agents EP2
06:22:24-40
Session Agent EP2(Realm192) [In Service]
                            -- Period --                --------
```

```
Lifetime --------
                            Active    High   Total      Total  PerMax    High
Inbound Sessions            0          0          0         0
0          0
[...]
Local Call Drops            -           -         1         1
0          -
Normal Call Drops           -           -         0         0
0          -
```

Local call drops include scenarios wherein the SBC generates BYE messages because of internal triggers such as a media guard timer expiring, a negative Rx response after call establishment, or internal processing errors (SIP application exception or other MBCD drops). The SBC displays this counter in applicable show commands as `Local Call Drops`.

Remote call release scenarios include flows that terminate gracefully, such as the SBC receiving a BYE . The SBC increments the counter on the ingress and the egress sides, and displays this counter in applicable show commands as `Normal Call Drops`.

SIP Method Counters

The Oracle Communications Session Border Controller (SBC) displays detailed counts of SIP messages (methods) via the **show sipd** command. You append this command with the applicable message name to view information about individual SIP messages types, including: INVITEs, REGISTERs, OPTIONS, CANCELs, BYEs, ACKs, INFOs, PRACKs (provisional ACKs), SUBSCRIBEs, NOTIFYs, MESSAGE, REFERs, and UPDATEs.

Counts for messages are grouped by the SIP response code that was sent or received for each method. If the SBC has not recorded an instance of the method, it is omitted from the output.

```
ORACLE# show sipd invite
INVITE (19:38:49-110)
                      --------- Server --------   --------- Client --------
Message/Event         Recent      Total  PerMax   Recent      Total  PerMax
                      ------  ---------  ------   ------  ---------  ------
INVITE Requests          146        146     107      146        146     107
Retransmissions            0          0       0        0          0       0
100 Trying               146        146     107        0          0       0
180 Ringing              146        146     107      146        146     107
200 OK                   146        146     107      146        146     107
Response Retrans           0          0       0        0          0       0
Transaction Timeouts       -          -       -        0          0       0
Locally Throttled          -          -       -        0          0       0

Avg Latency=0.000 for 146
Max Latency=0.001
```

The information is divided in two sections: Server and Client and includes information for recent, total, and period maximum messages or events.

- Recent: number of specific SIP messages and/or events that occurred within the current time period—in one-second increments, and always is between 100 and 199 and never below 100, constituting a 100-200 second recent period. This is done in order to keep the statistics from zeroing out between transition periods

- Total: current number of SIP messages and/or events that occurred since the system was last rebooted.
- PerMax: maximum number of SIP messages and/or events that occurred during a single time period since the system was last rebooted.

This display also shows information regarding the average and maximum latency. For each type of SIP message, the SBC displays only those transactions for which there are statistics, displaying the text below to indicate it has not yet received a REFER method.

```
ORACLE# ---< NO DATA AVAILABLE >----(REFER)
```

You can configure the SBC to display the information above on a per sip-interface, realm and session-agent basis by enabling the **extra-method-stats** parameter in the **sip-config**.

HDR Output for SIP Method Counters

SIP Method Counters may be accessed through the following HDR groups:

- sip-method
- sip-realm-method
- sip-interface-method
- sip-agent-method

These groups can be configured within the collect-group configuration element or from the request collection ACLI command.

SNMP Output for SIP Method Counters

System level method statistics are output with the apSipMethodStatsTable, available in ap-sip.mib.

Additional Rate Statistics for Specific Methods

The SBC also displays success, timeout and failure rates for both client and server statistics on recent and cumulative (lifetime) requests and responses for the following methods:

- SUBSCRIBE
- NOTIFY
- MESSAGE

These rates, displayed as percentages, include:

- Success Rate—Calculated using the number of 200 and, for the MESSAGE method only, 202 responses and the number of requests processed within the measurement window.
  Success rate = (Number of 200 Responses to the method/Total number of method transactions) * 100

- Timeout Rate—Calculated for client transactions only, using the number of 408, 504 responses to the message, the number of transaction timeouts, and the number of requests processed within the measurement window.
  Timeout rate = (Number of (408 plus 504 Responses plus timeout transactions to the method)/Total number of method transactions) * 100
- Failure Rate—Calculated using the number of responses between 4xx, 5xx and 6xx other than 408 and 504 response to requests, and the number of requests processed within the measurement window.
  Failure rate = (Number of (4xx, 5xx and 6xx Responses to the method, excluding 408 and 504)/Total number of method transactions) * 100

> **Note:**
>
> There is no HDR support for reporting on these success, timeout and failure rate statistics.

The example below displays the output when you specify the SUBSCRIBE method.

```
ORACLE# show sipd subscribe
INVITE (19:38:49-110)
                      --------- Server --------   --------- Client --------
Message/Event         Recent      Total  PerMax   Recent      Total  PerMax
                      ------  ---------  ------   ------  ---------  ------
INVITE Requests          146        146     107      146        146     107
Retransmissions            0          0       0        0          0       0
100 Trying               146        146     107        0          0       0
180 Ringing              146        146     107      146        146     107
200 OK                   146        146     107      146        146     107
Response Retrans           0          0       0        0          0       0
Transaction Timeouts       -          -       -        0          0       0
Locally Throttled          -          -       -        0          0       0
Success Rate           33.33      33.33       -    33.33      33.33       -
Timeouts Rate          33.33      33.33       -    33.33      33.33       -
Failure Rate           33.33      33.33       -    33.33      33.33       -

Avg Latency=0.000 for 146
Max Latency=0.001
```

The SBC also captures these rates over SNMP. To capture these rates, the MIB includes 3 event codes within the apSipMethodStatsTable, under apSipMethodStatsEventCount (1.3.6.1.4.1.9148.3.15.1.2.10.1.4.*) in the ap-sip.mib file:

- eventSuccessRate (55)
- eventTimeoutRate (56)
- eventFailureRate (57)

> **Note:**
>
> For SNMP retrieval, the SBC only presents total client and server transaction values, and displays the data as using integers.

These three stats events are also available as ENUM values:

- SNMP_SIP_METHOD_STATS_SUCCESS_RATE
- SNMP_SIP_METHOD_STATS_TIMEOUT_RATE
- SNMP_SIP_METHOD_STATS_FAILURE_RATE

SIP Message Counters

SIP Message counters come in two forms, event-based and session-based. The Oracle Communications Session Border Controller maintains and presents both message counts on the ACLI through show commands.

Event-based messaging refers to short messages transported as SIP MESSAGEs. These statistics are retrieved by typing the **show sipd status** command, and viewing the row identified as "Standalone Messages".

Session-based messaging refers to short messages transported SIP INVITE messages. These statistics are retrieved by typing the **show sessions** command and viewing the row identified as "Messaging Sessions".

All Messaging Sessions counter rows are provided for the current Period (total and high), System lifetime (total, period maximum, and lifetime high), and finally the current active number. Message counters only show successful messages.

In order to label a SIP INVITE and/or SIP MESSAGE to be treated as a message for incrementing this message counters, you configure two parameters. If no values are configured, the SBC parses for a default IMS Communication Service Identifier (ICSI).

You will configure these parameters with the ICSI used for matching incoming message request.

Message Type	containing configuration elements	parameter	default
Session-based	**session-agent** **realm-config** **sip-interface**	**sm-icsi-match-for-invite**	`urn:rrn-7:3gpp-service.ims.icsi.oma.cpm.msg`
Event-based	**session-agent** **realm-config** **sip-interface**	**sm-icsi-match-for-message**	`urn:urn-7:3gpp-service.ims.icsi.oma.cpm.largemsg`

When the ICSI value is embedded within a tag, the SBC escapes the tag value for comparison against the configured value. For example, If the Accept-Contact: header contains the tag: `urn%3Aurn-7%3A3gpp-service.ims.icsi.oma.cpm.largemsg` it will be normalized to `urn:urn-7:3gpp-service.ims.icsi.oma.cpm.largemsg`.

Session-based Message Counter Logic

Session-based message counters, reflecting messages in SIP INVITEs, are incremented when a match is made between the configured (or default) value in**sm-icsi-match-for-invite** and in the content of one of the following headers, checked in the following order:

1. P-Asserted-Service
2. P-Preferred-Service
3. Feature-Caps
4. Accept-Contact
5. Contact

After a match is made, when the SBC receives the 200OK response for the forwarded INVITE, the counter is incremented.

Event-based (Standalone) Message Counter Logic

Event-based message counters, reflecting messages in SIP MESSAGEs, are incremented when a match is made between the configured (or default) value in **sm-icsi-match-for-message** and in the content of one of the following headers, checked in the following order:

1. P-Asserted-Service
2. P-Preferred-Service
3. Feature-Caps
4. Accept-Contact
5. Contact

After a match is made, when the SBC receives the 203 Accepted response for the forwarded MESSAGE and it does not contain an In-Reply-To header, the counter is incremented.

Alternatively, if a SIP MESSAGE's content-type matches: `application/vnd.3gpp.sms` the message counter is incremented when the SBC receives the 203 Accepted response for the forwarded MESSAGE and that response does not contain an In-Reply-To header.

H.323 Protocol Performance

This section describes the different statistics you can access for monitoring H.323 protocol performance.

Viewing the H.323 Performance Statistics

Display the H.323 performance statistics by using the **show h323d** command. The main **show h323d** command executed without arguments indicates the date and time the current period began and displays session statistics, status statistics, and stack statistics for functioning H.323 processes.

For example:

```
acmepacket# show h323d
18:22:24-84
Session Stats                        -- Period --  -------- Lifetime -------
                           Active    High   Total      Total  PerMax    High
```

```
Incoming Calls                135     176    1001      77258
785     196
Outgoing Calls                135     176    1001      77258
785     196
Connected Calls               135     172     977      74390
727     196
Incoming Channels             251     319    1953     148780
1454     358
Outgoing Channels             251     319    1953     148780
1454     358
Contexts                      135     179    1001      77258
785     197
H323D Status     Current   Lifetime
Queued Messages      238      16000
TPKT Channels        542       4004
UDP Channels           0          0
Stack                State    Type Mode       Registered Gatekeeper
external             enabled  H323 Gateway    No
```

internal enabled H323 Gateway No

The following table lists the session statistics along with a brief description.

Statistic	Description
Incoming Calls	Number of H.323 calls coming into the Oracle Communications Session Border Controller.
Outgoing Calls	Number of H.323 calls going out of the Oracle Communications Session Border Controller.
Connected Calls	Number of H.323 calls that are currently connected via the Oracle Communications Session Border Controller.
Incoming Channels	Number of incoming channels that have been established on the Oracle Communications Session Border Controller.
Outgoing Channels	Number of outgoing channels that have been established on the Oracle Communications Session Border Controller.
Contexts	Number of contexts (i.e., the number of calls traversing the Oracle Communications Session Border Controller) that have been established on the Oracle Communications Session Border Controller.

About Status Statistics

The following table lists the current H.323 process status statistics along with a brief description:

Statistic	Description
Queued Messages	Number of messages queued.
TPKT Channels	Number of Transport Packet (TPKT) channels open(ed).
UDP Channels	Number of User Datagram Protocol (UDP) channels open(ed).

Note:

The show h323d status command shows the same information available when the show h323d command is executed without any arguments.

About Stack Statistics

The stack statistics provide a summary of information about the H.323 stacks configured on the Oracle Communications Session Border Controller via the **h323 stack**. This information includes the following facts about each stack: its name, whether or not it is enabled, its type, its mode (either Gateway or Gatekeeper), and whether or not it is registered with a Gatekeeper.

Viewing Current Configuration

Display statistics for the H.323 configuration currently running on the Oracle Communications Session Border Controller by using the **show h323d** config command. Only information about the main configuration element is shown, not for any subelements.

```
ORACLE# show h323d config
h323-config
        state                          enabled
        log-level                      INFO
        response-tmo                   4
        connect-tmo                    32
        rfc2833-payload                101
        alternate-routing              proxy
        codec-fallback                 disabled
        last-modified-date             2006-07-07 07:49:57
```

Viewing Session Agent Stats

You can view statistics about the session agents.

Viewing Session Agent Stats

Display statistics about the session agent by using the **show h323d agentstats** command. For example:

```
ORACLE# show h323d agentstats 172.16.0.13
19:57:21-51
Session Agent 172.16.0.13(h323172) [In Service]
                             -- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Inbound Sessions        0       0       0          0       0       0
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Reg Rate Exceeded     -       -       0          0       0       -
Outbound Sessions     199     245     196      23583     164     256
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Reg Rate Exceeded     -       -       0          0       0       -
Out of Service          -       -       0          0       0       -
Trans Timeout           0       0       0         19       2       1
Requests Sent           -       -    2092     234608    1569       -
Requests Complete       -       -     196      23563     164       -
Seizure                 -       -     196      23583     164       -
Answer                  -       -     199      23563     164       -
  ASR Exceeded          -       -       0          0       0       -
Messages Received       -       -    2267     258308    1675       -
Latency=0.011; max=0.045
```

The following table lists and describes the inbound statistics.

Statistic	Description
Active	Number of active sessions sent to each session agent listed in the Session Agent column of this command’s output.
Rate	Average rate of session invitations (per second) sent to each session agent listed in the Session Agent column of this command’s output.
ConEx	Number of times that the constraints established in the constraints fields of the session-agent element have been exceeded. The constraints fields of the session-agent element include the following: max-sessions, max-outbound-sessions, max-burst-rate, max-sustain-rate, burst-rate-window, and sustain-rate-window.

The following table lists and describes the outbound statistics.

Statistic	Description
Active	Number of active sessions sent from each session agent listed in the Session Agent column of this command’s output.
Rate	Average rate of session invitations (per second) sent from each session agent listed in the Session Agent column of this command’s output.
ConEx	Number of times that the constraints established in the constraints fields of the session-agent element have been exceeded.

The following table lists and describes the latency statistics.

Statistic	Description
Avg	Average latency for packets traveling to and from each session agent listed in the Session Agent column of this command’s output.
Max	Maximum latency for packets traveling to and from each session agent listed in the Session Agent column of this command’s output.
Max Burst	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 of the session-agent element.

Viewing Specific Session Agent Statistics

Display the activity for the particular H.323 session agent specified in the <agent> argument by using the **show h323d agents <agent>** command.

```
ORACLE# show h323d agentstats 172.16.0.13
19:57:21-51
Session Agent 172.16.0.13(h323172) [In Service]
                             -- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Inbound Sessions        0       0       0          0       0       0
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Reg Rate Exceeded     -       -       0          0       0       -
Outbound Sessions     199     245     196      23583     164     256
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Reg Rate Exceeded     -       -       0          0       0       -
Out of Service          -       -       0          0       0       -
Trans Timeout           0       0       0         19       2       1
Requests Sent           -       -    2092     234608    1569       -
Requests Complete       -       -     196      23563     164       -
Seizure                 -       -     196      23583     164       -
Answer                  -       -     199      23563     164       -
  ASR Exceeded          -       -       0          0       0       -
Messages Received       -       -    2267     258308    1675       -
Latency=0.011; max=0.045
```

The following table lists the statistics and a brief description.

Statistic	Description
Rate Exceeded	Number of times the session or burst rate was exceeded for inbound sessions.
Num Exceeded	Number of times the time constraints were exceeded for inbound sessions.

Statistic	Description
Rate Exceeded	Number of times the session or burst rate was exceeded for outbound sessions.
Num Exceeded	Number of times the time constraints were exceeded for outbound sessions.
Burst	Number of times the 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 that timed out for this session agent.
Requests Sent	Number of messages sent via the 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.

Viewing Session Agent Group Stats

You can view statistics for session agent groups.

Viewing Session Agent Group Stats

Display session information for the session agent groups by using the **show h323d groupstats** command. Session information is compiled by totalling the session agent statistics for all session agents that make up a particular session agent group.

While the **show h323d groupstats** command accesses the subcommands that are described in this section, the main **show h323d groupstats** command (when executed without arguments) displays a list of all session agent groups for the Oracle Communications Session Border Controller.

All of the categories for these statistics are the same as those used in the displays produced by the **show h323d agent** command.

```
ORACLE# show h323d groupstats
19:38:59-30
          ---- Inbound ---- --- Outbound ---- -Latency- ---- Max ----
SAG       Active Rate ConEx Active Rate ConEx Avg   Max Burst  In Out
H323Group      0  0.0     0      0  0.0     0 0.0   0.0     0   0   0
```

Viewing Session Agent Details

You can list and show the 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 this level of detail.

```
ORACLE# show h323d groups -v
SAG:              SGTest
19:38:59-30
                ---- Inbound ---- --- Outbound ---- -Latency- --- Max
---
SAG             Active Rate ConEx Active Rate ConEx  Avg  Max Burst In
Out
H323Group            0  0.0     0      0  0.0     0  0.0  0.0     0
0   0
SAG:            SGTest
192.168.200.61     120  0.0     0    359  0.0     0  0.0  0.0    50
0   0

Totals:
SGTest          D  120  0.0     0    359  0.0     0  0.0  0.0    50
0   0
ORACLE#
```

Viewing Specific Session Group Statistics

Display statistics for the designated session agent group by using the **show h323d groups <group name>** command with the name of a specific session agent group.

```
ORACLE# show h323d groups testgroup
16:35:18-18
          ---- Inbound ---- --- Outbound ---- -Latency-  Max
SAG       Active Rate ConEx Active Rate ConEx Avg   Max  Burst
testgroup      0  0.0     0      0  0.0     0 0.0   0.0  0
ORACLE#
```

If this command is carried out, but the name of an existing session agent group is not available, the system will display a messaging saying that the group statistics are not available.

```
ORACLE# show h323d groups test
group statistics not available
ORACLE#
```

Viewing Stats for Each Configured Stack

Display information for each of the configured H.323 stacks by using the **show h323d h323stats** command.

```
ORACLE# show h323d h323stats
STACK : h323172
H.225 : Sent    585622  Recd    764844  maxCPU  0
H245  : Msg     976289  Ack     1171626 Rej     0       Rel     0
RAS   : Req     0       Ack     0       Rej     0       maxCPU  0
STACK : h323192
H.225 : Sent    586040  Recd    585622  maxCPU  0
H245  : Msg     976087  Ack     1171626 Rej     0       Rel     0
RAS   : Req     0       Ack     0       Rej     0       maxCPU  0
```

The display identifies the H.323 stack by its name and then provides the data described in the following table.

Statistic	Description
H.225	Number of H.225 messages sent and received by this H.323 stack
H245	Number of H.245 requests, acknowledgements, rejections, and releases sent and received by this H.323 stack
RAS	Number of RAS requests, acks, and rejects sent and received by this H.323 stack

Viewing Statistics for Specific Stacks

Display detailed statistics for the H.323 stack specified in the <stack name> argument by using the show **h323d h323stats <stack name>** command. This information is displayed according to the following categories: H.225, H.245, and RAS.

```
acmepacket# show h323d h323stats h323172
STACK : h323172
H.225 STATISTICS
MESSAGE TYPE         SENT       RECD
Setup                200118     0
Call Proceeding      0          0
Alerting             0          200112
Connect              0          200109
Progress             0          0
Facility             0          0
Release Complete     199906     191628
Status               0          0
Status Inquiry       0          0
Notify               0          0
Info                 0          0
H.245 STATISTICS (Total)
MESSAGE TYPE                   MSG        ACK        REJ        REL
Master Slave                   200110     400218     0          0
Terminal Capability            400218     400218     0          0
OpenLogical Channel            0          0          0          0
CloseLogical Channel           399812     399812     0          0
RAS STATISTICS FOR MESSAGES SENT
MESSAGE TYPE         REQ        CON        REJ
GK Discovery         0          0          0
Registration         0          0          0
Unregistration       0          0          0
Admission            0          0          0
Location             0          0          0
Bandwidth            0          0          0
Disengage            0          0          0
Info                 0          0
RAS STATISTICS FOR MESSAGES RECD
MESSAGE TYPE         REQ        CON        REJ
GK Discovery         0          0          0
Registration         0          0          0
Unregistration       0          0          0
Admission            0          0          0
Location             0          0          0
Bandwidth            0          0          0
Disengage            0          0          0
Info                 0          0
ORACLE#
```

The following table lists and describes the H.225 statistics.

Type	Description
MESSAGE TYPE	Type of messages sent and received by this H.323 stack.
SENT	For each type of message specified in the MESSAGE TYPE column, how many of the message types were sent by this H.323 stack.
RECD	For each type of message specified in the MESSAGE TYPE column, this statistic shows how many of the message types were received by this H.323 stack.

The following table lists and describes H.245 statistics.

Type	Description
MESSAGE TYPE	Type of H.245 messages sent and received by this H.323 stack.
MSG	For each type of H.245 message specified in the MESSAGE TYPE column, this statistic shows how many message requests were sent and received by this H.323 stack.
ACK	For each type of H.245 message specified in the MESSAGE TYPE column, this statistic shows how many acknowledgements were sent and received by this H.323 stack.
REJ	For each type of H.245 message specified in the MESSAGE TYPE column, this statistic shows how many rejections were sent and received by this H.323 stack.
REL	For each type of H.245 message specified in the MESSAGE TYPE column, this statistic shows how many releases were sent and received by this H.323 stack.

The following table lists and describes RAS statistics for messages. There are two sections of RAS statistics: one for SENT (or issued) and one for RECD (or received.

Type	Description
MESSAGE TYPE	Type of RAS messages sent and received by this H.323 stack.
REQ	For each type of RAS message specified in the MESSAGE TYPE column, this statistic shows how many requests were issued/received by this H.323 stack.
CON	For each type of RAS message specified in the MESSAGE TYPE column, this statistic shows how many confirmations were issued/received by this H.323 stack.
REJ	For each type of RAS message specified in the MESSAGE TYPE column, this statistic shows how many rejections were issued/received by this H.323 stack.

Viewing H.323 Registrations

Display the total number of H.323 endpoint registrations by using the **show h323d reg** command.

```
acmepacket# show h323d reg
Stack: external       Number of registrations: 256
Total Number of Registrations : 256
```

Viewing DNS ALG Message Rate Statistics

The Oracle Communications Session Border Controller provides message rate statistics for DNS ALG traffic. You must first enable extra method statistics generation in the dns config.

To enable full DNS ALG message rate statistics:

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

   ```
   ORACLE# configure terminal
   ```

2. Type **media-manager** and press Enter to access the media-manager path.

   ```
   ORACLE(configure)# media-manager
   ```

3. Type **dns-config** and **select** an existing configuration element.

   ```
   ACMESYSTEM(media-manager)# dns-config
   ACMESYSTEM(dns-config)# select
   <realm-id>:
   1: realm01
   selection: 1
   ```

4. **extra-dnsalg-stats**—Set this parameter to enabled for the Oracle Communications Session Border Controller to collect message rate statistics for DNS ALG objects.
5. Type **done** when finished.

   DNS ALG Message rate statistics are maintained system-wide, per realm, and per DNS Server. This command is entered as:

   ```
   ORACLE# show dnsalg rate [realm-id <realm-name> | server-ip-addr
   <server-ip-address>]
   ```

show dnsalg rate

The **show dnsalg rate** command displays request and response rates for DNS messages on a system-wide basis. The rates are calculated based on the time in the current monitoring window (100+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ORACLE# show dnsalg rate
17:31:21-15
Realm-id  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
              Rate      Rate      Rate      Rate       Rate       Rate
ALL            0.0       0.0       0.0       0.0        0.0        0.0
```

show dnsalg rate realm-id

The **show dnsalg rate realm-id** command displays request and response rates for DNS messages on a per-realm basis. If you add a realm-name to the query, that specific realm’s data will be returned. Entered without a realm name, all configured realms will be displayed. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ORACLE# show dnsalg rate realm-id peer
17:31:31-26
Realm-id  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp Sent
              Rate      Rate      Rate      Rate       Rate       Rate
peer           0.0       0.0       0.0       0.0        0.0        0.0
```

show dnsalg rate server-ip-addr

The **show dnsalg rate server-ip-addr** command displays request and response rates for DNS messages on a per-DNS server basis. If you add a DNS Server IP address to the query, that specific server’s data will be returned. Entered without a server IP address, all configured servers will be displayed. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ORACLE# show dnsalg rate server-ip-addr 172.16.10.5
17:32:19-44
DNS ALG Realm peer
Ip Address             Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv
Resp Sent
                           Rate      Rate      Rate      Rate
Rate       Rate
172.16.10.5                 0.0       0.0       0.0       0.0
0.0        0.0
```

SNMP Reporting of Message Rate Statistics pointer

Message Rate Statistics are available via SNMP. See the MIB Reference Guide, SNMP Reporting of Message Rate Statistics section for detailed information.

ENUM Server Message Rate Statistics

The Oracle Communications Session Border Controller provides message rate statistics for ENUM traffic. You must first enable extra method statistics generation in the sip config.

To enableENUM message rate statistics:

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

   ```
   ORACLE# configure terminal
   ```

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

   ```
   ORACLE(configure)# session-router
   ORACLE(session-router)#
   ```

3. Type **sip-config** and press Enter.

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

4. **extra-enum-stats**—Set this parameter to enabled for the Oracle Communications Session Border Controller to collect and track ENUM message statistics per second.
5. Save and activate your configuration.

   ENUM Message rate statistics are maintained system-wide, per realm, and per ENUM Server. This command is entered as:

   ```
   ORACLE# show enum rate [config-name <enum-server-name> | server-ip-
   addr <server-ip-address>]
   ```

show enum rate

The **show enum rate** command displays request and response rates for ENUM messages on a system-wide basis. The rates are calculated based on the time in the current monitoring window (100+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ORACLE# # show enum rate
17:22:28-23
Config Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp
Sent
                 Rate      Rate      Rate      Rate       Rate
Rate
ALL               0.0       0.0       0.0       0.0        0.0
0.0
```

show enum rate config-name

The **show enum rate config-name** command displays request and response rates for ENUM messages per ENUM configuration. If you add a an enum-config-name to the query, that specific configuration’s data will be returned. Entered without a name, all configured enum-configs will be displayed. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ORACLE# show enum rate config-name test1
17:22:53-48
Config Name  Msg Recv  Msg Sent  Req Recv  Req Sent  Resp Recv  Resp
Sent
```

```
                  Rate       Rate       Rate       Rate        Rate        Rate
test1              0.0        0.0        0.0        0.0         0.0         0.0
```

show enum rate server-ip-addr

The **enum rate server-ip-addr** command displays request and response rates for individual enum-servers. If you add an IP address to the query, that specific server's data will be returned. Entered without a server IP address, all configured servers will be displayed. If an IP address is present in more than one ENUM configuration then the message processing level is displayed separately for each configuration object. The rates are calculated based on the time in the current monitoring window (30+current period elapsed). The Message Received and the Messages sent columns are the sum of the corresponding Requests or responses. For example:

```
ORACLE# show enum rate server-ip-addr 192.168.201.5
17:24:00-55
ENUM Config Name enum
Ip Address        Msg Recv   Msg Sent   Req Recv   Req Sent   Resp Recv   Resp Sent
                      Rate       Rate       Rate       Rate        Rate        Rate
192.168.201.5          0.0        0.0        0.0        0.0         0.0         0.0
17:24:00-55
ENUM Config Name test1
Ip Address        Msg Recv   Msg Sent   Req Recv   Req Sent   Resp Recv   Resp Sent
                      Rate       Rate       Rate       Rate        Rate        Rate
192.168.201.5          0.0        0.0        0.0        0.0         0.0         0.0
```

SNMP Reporting of Message Rate Statistics pointer

Message Rate Statistics are available via SNMP. See the MIB Reference Guide, SNMP Reporting of Message Rate Statistics section for detailed information.

Viewing External Policy Server Statistics

show ext-band-mgr

The **show ext-band-mgr** command includes cumulative statistics for all configured ext-policy-server server objects. The display includes the following counts for Period and Lifetimes:

- socket connections established
- total active Diameter connections
- active Diameter server transaction
- active Diameter client transactions

Further the **show ext-band-mgr** command displays the event counts with respect to client transaction with recent and lifetime counts only:

- reserve requests sent
- update requests sent
- termination requests (STR) sent

- times requests are transmitted
- responses received to install flows
- request errors occurred
- deny/reject responses received from the server
- client transactions expired
- total application errors occurred

```
ORACLE# show ext-band-mgr
10:50:28-196
EBM Status                 -- Period -- -------- Lifetime --------
                 Active    High   Total      Total  PerMax    High
Client Trans          0       0       0          0       0       0
Server Trans          0       0       0          0       0       0
Sockets               0       0       0          0       0       0
Connections           0       0       0          0       0       0
                            ---- Lifetime ----
                    Recent      Total  PerMax
Reserve                  0          0       0
Modify                   0          0       0
Commit                   0          0       0
Remove                   0          0       0
EBM Requests             0          0       0
EBM Installs             0          0       0
EBM Req. Errors          0          0       0
EBM Rejects              0          0       0
EBM Expires              0          0       0
EBMD Errors              0          0       0
```

show policy-server

The **show policy-server** command displays each external policy server’s name and address, followed by the policy server's IP addresses that are resolved through DNS, its priority, state of the server, socket related errors and Diameter related failures. The command can also display cumulative statistics for policy-groups, as well as for specific policy-agents that are members of policy-groups. The command can restrict returned statistics to a specific Diameter message.

The display also includes the following external bandwidth manager counts for recent and lifetime periods.

- Total socket connections established
- Total Diameter connections established

Client transactions counts include:

- reserve type requests sent
- update requests sent
- termination requests (STR) sent
- responses received that installs the flow
- deny/rejected responses received from the server

- client transaction timeouts occurred
- client side related errors that occurred

Server transactions counts include:

- requests received from the client
- duplicate requests received
- responses sent successfully
- errors occurred while sending the response
- requests dropped

The command displays aforementioned statistics for all configured external policy server configuration elements. In addition, the command displays mutilhomed IPPort for SCTP configurations. Here is an example of **show policy-server connections**:

```
ORACLE# show policy-server connections

Local IPPort         Remote IPPort        Socket State
-------------------------------------------------------
168.192.42.204:8978  168.192.160.12:6002    CONNECTED
168.192.42.11:6001   168.192.160.13:6003
```

Here is an example of **show policy-server [name]**:

```
ORACLE# show policy-server server1
name = server1
-----------------------------------------
Server:port        Priority       State     SCTP-Failures  Diameter-Failures
192.168.42.13:1817    0           active      2261              0
168.192.42.24:8978
-----------------------------------------
18:47:36-183
Bandwidth Policy Server          --  Recent -- -------- Lifetime --------
                           Active    High   Total      Total  PerMax    High
Sockets                         1       1       0          1       1       1
Connections                     1       1       0          1       1       1
Client Transactions             0       1      12        738       7       1
  Reserve Requests Sent         -       -       0          0       0
  Update Requests Sent          -       -       0          0       0
  Remove Requests Sent          -       -       0          0       0
  Requests Re-Trans             -       -       0          0       0
  Install Resp Received         -       -       0          0       0
  Reject Resp Received          -       -       0          0       0
  Remove Resp Received          -       -       0          0       0
  Errors Received               -       -       0          0       0
  Transaction Timeouts          -       -       0          0       0
  Errors                        -       -       0          0       0
Server Transactions             0       0       0          3       3       3
  Requests Received             -       -       0          0       0
  Dup Req Received              -       -       0          0       0
  Success Resp Sent             -       -       0          3       3
  Error Resp Sent               -       -       0          0       0
  Requests Dropped              -       -       0          0       0
```

```
CER Sent                                        1          1       1
CEA Success                                     1          1       1
CEA Errors                                      0          0       0
AAR Sent                                        0          0       0
AAA Success                                     0          0       0
AAA Errors                                      0          0       0
STR Sent                                        0          0       0
STA Success                                     0          0       0
STA Errors                                      0          0       0
RAR Rcvd                                        0          0       0
RAA Rcvd Success                                0          0       0
RAA Rcvd Errors                                 0          0       0
DWR Sent                                      737        737     737
DWA Success                                   737        737     737
DWA Errors                                      0          0       0
DWR Rcvd                                        3          3       3
DWA Rcvd Success                                3          3       3
DWA Rcvd Errors                                 0          0       0
ASR Rcvd                                        0          0       0
ASA Rcvd Success                                0          0       0
ASA Rcvd Errors                                 0          0       0

-----------------------Summary Stats---------------------
18:47:36-183
Bandwidth Policy Server          --  Recent -- -------- Lifetime
--------
                           Active    High   Total      Total
PerMax    High
Sockets                         1       1       0          2
2       2
Connections                     1       1       0          1
1       1
Client Transactions             0       1      12        791
17       2
  Reserve Requests Sent         -       -       0          0       0
  Update Requests Sent          -       -       0          0       0
  Remove Requests Sent          -       -       0          0       0
  Requests Re-Trans             -       -       0          0       0
  Install Resp Received         -       -       0          0       0
  Reject Resp Received          -       -       0          0       0
  Remove Resp Received          -       -       0          0       0
  Errors Received               -       -       0          0       0
  Transaction Timeouts          -       -       0          0       0
  Errors                        -       -       0          0       0
Server Transactions             0       0       0          3
3       3
  Requests Received             -       -       0          0       0
  Dup Req Received              -       -       0          0       0
  Success Resp Sent             -       -       0          3       3
  Error Resp Sent               -       -       0          0       0
  Requests Dropped              -       -       0          0       0
CER Sent                                       54         54      54
CEA Success                                     1          1       1
CEA Errors                                     46         46      46
AAR Sent                                        0          0       0
```

```
AAA Success                                     0          0       0
AAA Errors                                      0          0       0
STR Sent                                        0          0       0
STA Success                                     0          0       0
STA Errors                                      0          0       0
RAR Rcvd                                        0          0       0
RAA Rcvd Success                                0          0       0
RAA Rcvd Errors                                 0          0       0
DWR Sent                                      737        737     737
DWA Success                                   737        737     737
DWA Errors                                      0          0       0
DWR Rcvd                                        3          3       3
DWA Rcvd Success                                3          3       3
DWA Rcvd Errors                                 0          0       0
ASR Rcvd                                        0          0       0
ASA Rcvd Success                                0          0       0
ASA Rcvd Errors                                 0          0       0
```

CLF Statistics

The **show ext-clf-srv** command is entered as follows:

```
show ext-clf-srv [<realm-name> | ext-policy-server <policy-server-name>]
```

The **show ext-clf-svr** command displays aggregate statistics for all CLF external policy servers active on the system. You can enter a realm-name to display only the given realm’s statistics. For example:

```
ORACLE# show ext-clf-svr
16:11:38-168
EBM Status                 -- Period -- -------- Lifetime --------
                  Active    High   Total      Total  PerMax    High
Client Trans      0         0      0          6      2         1
Server Trans      0         0      0          0      0         0
Sockets           1         1      0          1      1         1
Connections       1         1      0          2      1         1
                           ---- Lifetime ----
                    Recent      Total  PerMax
CLF Requests             0          4       1
CLF Admits               0          0       0
CLF Req. Errors          0          0       0
CLF Rejects              0          4       1
CLF Expires              0          0       0
CLFD Errors              0          0       0
```

Note the following application statistics:

- CLF Requests—This counter is incremented when new CLF request are sent.
- CLF Admits—This counter is incremented when the Oracle Communications Session Border Controller received RESP_STATUS_OK response from the external policy server (i.e. successful registration).

- CLF Req. Errors—This counter is incremented when the Oracle Communications Session Border Controller has protocol level based type of error returned back from the external policy server, i.e. a bad request.
- CLF rejects—This counter is incremented when the CLF returns a response code other than "RESP_STATUS_OK" or "RESP_STATUS_BAD"(i.e. Above mentioned CLF Req Errors)
- CLF Expires—This counter is incremented when the Oracle Communications Session Border Controller does not receive a response to a request it sent to the CLF.
- CLFD Errors—This counter is incremented when the encounters a general error in processing the received response from the external policy server (i.e. no socket for request, no agent for socket or no response in socket).

The **show ext-clf-svr ext-policy-server** command displays all ext-policy-servers Summarys. For example:

```
ORACLE# show ext-clf-svr ext-policy-server
15:41:22-1687
Ext Clf Server summary
Ext Clf Server           Recent      Total      PerMax
diameter_check_1           0           0           0
diameter_check_2           0           0           0
diameter_check_3           0           0           0
```

The **show ext-clf-svr ext-policy-server** with a supplied ext-policy-server configuration object **name** displays specific statistics for the named external policy server. For example:

```
ORACLE# show ext-clf-svr ext-policy-server diameter_check_1
15:41:43-1707
Ext Clf Svr Errors
                         -------- Lifetime --------
                         Recent      Total  PerMax
Errors                      0          0       0
```

HSS Statistics

The show home-subscriber command displays detailed information about HSS transactions. For example:

```
ORACLE## show home-subscriber-server
17:54:58-186
HSS Status                 -- Period -- -------- Lifetime --------
                 Active    High   Total      Total  PerMax    High
Client Trans          0       0       0         12       4       1
Server Trans          0       0       0          1       1       1
Sockets               1       1       0          1       1       1
Connections           1       1       0          1       1       1
                           ---- Lifetime ----
                    Recent      Total  PerMax
LIR                      0          0       0
Sent Req Accepted        0         11       3
Sent Req Rejected        0          0       0
Sent Req Expired         0          0       0
Sent Req Error           0          0       0
Internal Errors          0          0       0
```

Note the following statistics provided for Recent and Lifetime periods:

- LIR—Number of LIR requests sent
- Sent Req Accepted—Number of requests for which we got success response (2xxx)
- Sent Req Rejected—Number of permanent failures (5xxx)
- Sent Req Expired—Number of requests for which there was no response
- Sent Req Error—Number of protocol errors/bad requests (1xxx, 3xxx, 4xxx)

Viewing Accounting Data and Statistics

This section explains how to view accounting data and statistics. See Admission Control and Quality of Service Reporting in the Oracle Communications Session Border Controller ACLI Configuration Guide for additional details about Quality of Service (QoS). See the Oracle Communications Session Border Controller RADIUS Guide for additional details about Remote Authentication Dial-in User Service (RADIUS).

QoS Reporting

If you are using for the QoS functionality in collecting and calculating the jitter, latency, and loss statistics. QoS reporting provides you with real-time evaluation of network and route performance. It lets you contrast internal domain and external domain performance and facilitates SLA verification and traffic engineering.

QoS metrics are collected and reported on a per-session basis, per call-leg basis for completed calls. These metrics are reported through real-time RADIUS records along with call accounting data. These metrics are the result of the monitoring of the Real-Time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP) traffic for each flow that has QoS enabled.

The following statistics:

- lost packets for RTP and RTCP that indicates the count of packets lost based on comparing the sequence numbers since the beginning of the call or the last context memory flow
- jitter count for RTP and RTCP that indicates the incremental number of packets that have been used to generate total and max jitter since the beginning of the call or the last context memory poll
- jitter total for RTP and RTCP indicates the incremental accumulated jitter (ms) over all the packets received since the beginning of the call or the last context memory poll
- jitter max for RTP and RTCP that indicates the maximum single jitter value (ms) from all the packets since the beginning of the call or the last context memory poll
- latency count for RTCP only indicates the number of RTCP frames over which latency statistics have been accumulated since the beginning of the call or the last context memory poll

- latency total for RTCP only indicates the incremental total of latency values reported since the beginning of the call or the last context memory poll
- latency max for RTCP only indicates the highest single latency value measured since the beginning of the call or the last context memory poll

From these flow context statistics the QoS daemon derives the following statistics that are kept in host memory while the call is active:

- lost packets indicates the total number of RTP and RTCP lost packets for the call
- jitter count indicates the number of RTP and RTCP packets that make up a call
- jitter total indicated the accumulated jitter over all the packets received during the call
- jitter average indicates the total accumulated jitter divided by the total jitter count for the call
- jitter max indicates the maximum single jitter value from all the packets during the call
- latency count for RTCP indicates the number of RTCP frames of which latency statistics have been accumulated during the call
- latency total for RTCP only indicates the incremental total of latency values reported
- latency max for RTCP only indicates the highest latency value reported during the call
- latency average for RTCP only indicates the RTCP latency total divided by the latency count

You can access QoS statistics that provide information about four areas of call performance.

Viewing Network Management Control Statistics

You can use the new ACLI **show net-management-control** command to see the statistics that the Oracle Communications Session Border Controller collects. When you use the command, you specify the name of the network management control rule for which you want to display data or you can enter **all** to see the statistics for all control rules.

For each network management control rule, the Oracle Communications Session Border Controller gathers statistics for the number of:

- Incoming calls—Incoming calls that match the destination identifier
- Rejected calls—Calls that were rejected as a result of the control rule being applied
- Diverted calls—Incoming that were diverted as a result of the control rule being applied

The display you see when you execute this command shows statistics for the current period, lifetime, and maximum value in a period.

Displaying Network Management Control Statistics

To display network management control statistics:

- In either User or Superuser mode, type the **show net-management-control** command, a Space, and then the name of the control rule for which you want to see data. You can enter **all** if you want to see the data for all control rules. Then press Enter.

```
ORACLE# show net-management-control nmcpercent
14:45:15-63
Name: nmcpercent
Type: gap-percent             ------ Lifetime -----
                      Current      Total     PerMax
Incoming Calls              0          0          0
Rejected Calls              0          0          0
Diverted Calls              0          0          0
```

Resetting Network Management Control Statistics

To reset network management control statistics, you use the ACLI **reset net-management-control** command followed by the name of the control rule for which you want to reset statistics. This command resets the counters to zero (0).

To reset network management control statistics:

- In Superuser mode, type the ACLI **reset net-management-control** command, a Space, and then the name of the control rule for which you want to see data. Then press Enter.

```
ORACLE# reset net-management-control nmcpercent
```

Monitoring Your System in Real-Time

This section explains how to monitor your system in real-time by using the **monitor media** and **monitor sessions** commands.

- **monitor media:** real-time media statistics
- **monitor sessions:** real-time SIP statistics

> **Note:**
>
> The ACLI statistics displays use standard VT100 escape sequences to format the display. Therefore, your terminal emulator or terminal itself must support VT100.

Displaying the Statistics

The following information explains how to work with the statistics display.

Changing the Refresh Rate

At any point, you can press any numerical digit (**0-9**) to change the number of seconds for the refresh rate (the rate at which the display is updated). By default, the statistics refresh every second. For example, while viewing the statistics, you can press **6** to cause the system statistics to refresh every 6 seconds. While viewing the statistics via the ACLI, you can press any key to automatically refresh the statistics upon key press.

Quitting the Display

Pressing <q> or <Q> allows you to exit the statistics display and returns you to the ACLI system prompt (for example, ORACLE#). From that point, you can continue with any other task you choose.

Viewing Real-Time Media Statistics

Display real-time media statistics for your running system by using the **monitor media command.**

```
acmepacket# monitor media
17:31:00-160
MBCD Status                -- Period -- -------- Lifetime --------
                 Active    High   Total      Total  PerMax    High
Client Sessions     143     182    1930    1218332    4225     683
Client Trans          0      18    5744    2500196    8439     625
Contexts            144     182    1930     834745    2783    2001
Flows               296     372    3860    1669498    5566    3689
Flow-Port           286     362    3860    1669488    5566    3679
Flow-NAT            294     365    3788    1658668    5563    2051
Flow-RTCP             0       0       0          0       0       0
Flow-Hairpin          0       0       0          0       0       0
Flow-Released         0       0       0          0       0       0
MSM-Release           0       0       0          0       0       0
NAT Entries         295     365    3791    1658671    5563    2051
Free Ports         7430    7518    7828    3346410   11604    8002
Used Ports          572     724    7724    3338980   11132    8000
Port Sorts            -       -       0      14796    4156
MBC Trans          1141    1234    5748    2503147    8440    2974
MBC Ignored           -       -       0          0       0
```

ARP Trans 0 0 0 8 8 1

Real-time statistics for the following categories appear on the screen:

- Client Sessions
- Client Trans
- Contexts
- Flows
- Flow-Port
- Flow-NAT
- Flow-RTCP
- Flow-Hairpin
- Flow-Release
- MSM-Release

- NAT Entries
- Free Ports
- Used Ports
- Port Sorts
- MBC Trans
- MBC Ignored
- ARP Trans

By default, the statistics refresh every second. Press any numerical digit (**0-9**) to change the refresh rate. For example while viewing the statistics, you can press **6** to cause the system statistics to refresh every 6 seconds.

Pressing **q** or **Q** allows you to exit the statistics display and returns you to the ACLI system prompt.

Viewing Real-Time SIP Session Statistics

If you have Superuser access, display real-time monitoring of your running system for sessions. This table displays information similar to that which is displayed for the **show sipd** command, except that the information in the **monitor sessions** table is real-time and updates automatically.

```
ORACLE# show sipd
14:16:43-149
SIP Status                -- Period -- -------- Lifetime --------
                Active    High   Total      Total  PerMax    High
Sessions             0       0       0          0       0       0
Subscriptions        0       0       0          0       0       0
Dialogs              0       0       0          0       0       0
CallID Map           0       0       0          0       0       0
Rejections           -       -       0          0       0
ReINVITEs            -       -       0          0       0
Media Sessions       0       0       0          0       0       0
Media Pending        0       0       0          0       0       0
Client Trans         0       0       0          0       0       0
Server Trans         0       0       0          0       0       0
Resp Contexts        0       0       0          0       0       0
Saved Contexts       0       0       0          0       0       0
Sockets              0       0       0          0       0       0
Req Dropped          -       -       0          0       0
DNS Trans            0       0       0          0       0       0
DNS Sockets          0       0       0          0       0       0
DNS Results          0       0       0          0       0       0
Session Rate = 0.0
Load Rate = 0.0
```

Real-time statistics for the following categories appear on the screen:

- Dialogs
- Sessions
- CallID Map

- Rejections
- ReINVITES
- Media Sessions
- Media Pending
- Client Trans
- Server Trans
- Resp Contexts
- Sockets
- Reqs Dropped
- DNS Trans
- DNS Sockets
- DNS Results

By default, the statistics refresh every second. Press any numerical digit (**0-9**) to change the refresh rate. For example, while viewing the statistics, you can press **6** to cause the system statistics to refresh every 6 seconds.

Pressing **q** or **Q** allows you to exit the statistics display and returns you to the ACLI system prompt.

Thread Level Load Monitoring and Alarms

The Oracle Communications Session Border Controller provides a thread-level monitoring for CPU usage, specifically including three critical traffic processes: SIP, ATCP and MBCD.

Several mechanisms are available for monitoring CPU usage on a per-thread basis: ACLI commands, alarms, HDR, traps and MIBs. The thread usage table MIB object is found in **ap-usbcsys.mib**. It supports the output of process and thread utilization information. HDR information is produced as a comma separated value file whose data can be displayed in a formatted fashion via command line. The system sends SNMP traps when any of the SIP, ATCP worker threads or MBCD tasks exceed configured thresholds. Users can construct a Threshold Crossing Alarm (TCA) which issues minor, major and critical system alarms when the thread usage level exceeds pre-configured values. These Thread Overload Alarms follow the example in the *Configurable Alarm Thresholds and Traps* section.

ACLI

The following commands display thread-level load statistics:

- **show processes**: add sipd, atpcd and overload arguments
- **show queues atcpd**
- **show queues sipd**

Alarms

The user-configurable alarm may be created to notify the user of any problematic usage of CPU resources by specific processes at a thread-level basis.

To create alarms, the user sets the **alarm-threshold**, **type** with the following values to create the corresponding threshold crossing alarm.

- **cpu-sipd**
- **cpu-atcp**
- **cpu-mbcd**

When a thread alarm is active due to crossing a pre-configured threshold, the system sends the **apUsbcSysThreadUsageExceededTrap** trap.

When the thread's load falls below the threshold that triggered the alarm, the system sends the **apUsbcSysThreadUsageClearTrap** trap.

The user can get this information using the **display-alarms** command.

Historic Data Recording (HDR)

There are two HDR groups available to record Thread Level Load Monitoring information:

- **thread-event**: reports pending and dropped events per protocol as well as calculating latency
- **thread-usage**: reports CPU thread usage per protocol and an overload condition

The data captured by these two HDR groups corresponds to the **show queues atcpd** and **show queues sipd** ACLI command output.

SNMP MIBs and Traps

Thread Level Load Monitoring information can be retrieved via SNMP by from MIB objects in the `ap-usbcsys.mib`. In addition, traps are available to send off-system notifications.

There are two types of traps that provide process-level thread threshold indicators.

- Traps managed by the process-level thread alarm configurations, which use the alarm configuration as triggers. These traps include:
  - **apUsbcSysThreadUsageExceededTrap**
  - **apUsbcSysThreadUsageClearTrap**
- Traps managed by Symmetric Multi-processing (SMP)-aware task load limiting function's configurations, which use the use the SMP Transport, SIP and Media limiting configurations as triggers. These traps include:
  - **apUsbcSysThreadUsageOverloadEnableTrap**
  - **apUsbcSysThreadUsageOverloadDisableTrap**

Information in overload enable/disable traps include the threshold type, the overload alarm exceeded or cleared as well as the overload method activated or de-activated.

The system follows the SMP-Aware Task Load Limiting rules described in the *Oracle® Communications Session Border Controller Troubleshooting and Maintenance Guide* to determine the action(s) it takes when crossing these thresholds.

The system manages these traps by applying a function similar to CPU overloading limit to smooth the output and avoid issuing too many traps. Each trap contains the thread name. The usage exceeded trap also contains current thread usage.

For SIP, ACTP and MBCD, traps display the threshold type, the overload alarm exceeded or cleared, or the overload method activated or de-activated.

Viewing TLS Information

You can use the commands described in this section to obtain information about TLS and its associated Acme Packet SSM hardware module.

Clearing the Entire TLS Session Cache

To clear the entire TLS session cache:

- Enter the ACLI **clear-cache tls** command.

```
ORACLE# clear-cache tls
```

Viewing TLS Session Cache State and Statistics

You can view TLS information for session traffic using the command **show security tls <session-cache | stats>**.

1. Use the **show security tls session-cache** command to confirm whether TLS session caching is enabled and to view the number of entries.

```
ORACLE# show security tls session-cache
TLS Session Caching enabled.
Current TLS Session Cache Entries: 3
```

2. Use the **show security tls stats** command to view TLS statistics for session traffic.

```
ORACLE# show security tls stats

-------------------------  TLS Stats -----------------------------

active connections                        : 0
successful connects                       : 0
successful accepts                        : 0
connection close                          : 0
```

> **Note:**
>
> This command only reports TLS statistics for session traffic and not TLS statistics for other administrative functions like STIR/SHAKEN or the REST API interface.

Viewing Certificates in PEM Form

The ACLI **show certificates** command has been enhanced to provide a **pem** argument that you can use to retrieve the Privacy Enhanced Mail Security Certificate (PEM) portion of the certificate after it the Oracle Communications Session Border Controller has imported it.

You enter this command with the name of the certificate you want to see in PEM form.

To see a certificate in PEM form:

- Enter the command **show security certificates pem** followed by a Space, the name of the certificate, and then press Enter.

```
ORACLE# show security certificates pem client1a
certificate-record:client1a
-----BEGIN PKCS7-----
MIIDRwYJKoZIhvcNAQcCoIIDODCCAzQCAQExADADBgEAoIIDJDCCAyAwggKJoAMC
AQICCAITAlAAhACeMA0GCSqGSIb3DQEBBQUAMHAxCzAJBgNVBAYTAlVTMRMwEQYD
VQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEOMAwGA1UEChMFc2lw
aXQxKTAnBgNVBAsTIFNpcGl0IFRlc3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTA2MDgxMDE1NDQ0OVoXDTA5MDgwOTE1NDQ0OVowVzELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk1BMRMwEQYDVQQHEwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVl
cmluZzEQMA4GA1UEAxMHcnlhbmVuZDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAshgHLBsuBe6HhyxDsv+6hB53a7rTWRNju10QkOhitAEhVswgyj3wCHnd5o62
LVAi3esKJfnRJI/gleHZ7uhVlL3juMhDTcF/XT+Dzb+ZBMmgJQzrkokseRgL2aLl
FBbnnG3DoUugyk/Jp3J6CBz+ZGUf85WQri1JuDREJ9fVCM0CAwEAAaOB2zCB2DAP
BgNVHREECDAGggRyeWFuMAkGA1UdEwQCMAAwHQYDVR0OBBYEFAphhPV97obtLICT
9mn1yOVU2yduMIGaBgNVHSMEgZIwgY+AFGtGFxTqlHYlgFRuE1TaoeNUFKG2oXSk
cjBwMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMI
U2FuIEpvc2UxDjAMBgNVBAoTBXNpcGl0MSkwJwYDVQQLEyBTaXBpdCBUZXN0IENl
cnRpZmljYXRlIEF1dGhvcml0eYIBADANBgkqhkiG9w0BAQUFAAOBgQAzSuW+sYI2
I/K/8Fo8Pj6T8qDWh3qcEoqJkPylFXHSWCdQPdKr0iiYAgnV3wE8dhRRZWWRb30T
yIQzfc2YTJStJ/XveX/Hwt4X1yRwcBL32Rr4XjiDpeUWWRfwwqAH5RfjS4X/kHw4
agrTDzKbE03+kSr2dPb42ko+TaiSDoLI8jEA
-----END PKCS7-----
ORACLE#
```

Viewing SSM Status

For TLS support, you must have an Oracle SSM hardware module installed in the system chassis. Without this module, TLS functions will not work.

The Oracle Communications Session Border Controller tells you whether or not the SSM installed on boot-up, but now you can check the module’s status from the command line.

To view the status of the SSM installed in your Oracle Communications Session Border Controller chassis:

- Enter the command **show security ssm-accelerator**, and press Enter. The system will tell you if an SSM is installed.

```
ORACLE# show security ssm-accelerator
SSM (Security Service Module) present.
ORACLE#
```

Viewing IPSec Statistics

The following section explains the commands used to obtain IPSec statistics which can be helpful for debugging purposes.

Security Association Entries

The ACLI **show security ipsec sad** command displays the security association database entries which are programmed into the security processor. In the case of manual keying, the entries should match that of the running configuration. Network-interface is entered as a network interface configuration element name, selectors are entered as the selector term, a <space>, and a search term for that selector. You can enter multiple selector in one command. The command's syntax follows:

```
show security ipsec sad [network-interface] <brief | detail>
[selectors]
```

Entering no selectors returns all entries for that network interface. Valid values for the selectors argument are as follows:

- direction—Direction (IN | OUT | BOTH), Default: BOTH
- dst-addr-prefix—Destination address prefix, Default: match any
- dst-port—Destination port, Default: match any
- ipsec-protocol—IPSec protocol (AH | ESP | ALL), Default: ALL
- spi—security-policy-index, Default: match any
- src-addr-prefix—Source address prefix, Default: match any
- src-port—Source port, Default: match any
- trans-proto—Transport protocol (UDP | TCP | ICMP | ALL), Default: ALL

Security Policy Entries

The **show security ipsec spd** command shows the security policy database entries which are programmed into the security processor. Network-interface is entered as a network interface configuration element name. The command's syntax follows:

```
show security ipsec spd [network-interface]
```

IPSec Statistics

The ACLI **show** commands for IPSec statistics are used to display statistical values as reported directly from the IPSec hardware. There are two versions of this command:

- The **show security ipsec statistics sad** command queries a selected IPSec processor for statistics about the SAs configured on it, as located in the security association database (SAD).
- The s**how security ipsec statistics gmac** command queries the GMAC side of the security processor for Ethernet statistics.

Viewing Statistics for a Specific SA

The **show security ipsec statistics sad** command shows statistical values for a particular SA entry on the IPSec security processor. You enter a network interface configuration name, selectors by the selector term, a Space, and a search term for that selector. You can enter multiple selector in one command. The command's syntax follows:

```
show security ipsec statistics [network-interface] sad <selectors>
```

Entering no selectors returns all entries for that network interface. Valid values for the selectors argument are as follows:

- direction—Direction (IN | OUT | BOTH), Default: BOTH
- dst-addr-prefix—Destination address prefix, Default: match any
- dst-port—Destination port, Default: match any
- ipsec-protocol—IPSec protocol (AH | ESP | ALL), Default: ALL
- spi—security-policy-index, Default: match any
- src-addr-prefix—Source address prefix, Default: match any
- src-port—Source port, Default: match any
- trans-proto—Transport protocol (UDP | TCP | ICMP | ALL), Default: ALL

Viewing Statistic for Traffic to from the GMAC Interface and the Security Processor

The **show security ipsec statistics gmac** command displays statistics on traffic that moves between the GMAC interface and the security processor on a specified network interface. Network-interface is entered as a network interface configuration element name. You can display either errors, transmit statistics, receive statistics, or all statistics per HW accelerator / gmac interface . The command's syntax follows:

```
show security ipsec statistics [network-interface] gmac <enter | error | rx
| tx>
```

Viewing IPSec Interface Status

The **show security ipsec status** command displays whether a particular interface on Oracle Communications Session Border Controller is IPSec enabled, and the hardware status of the security processor. Network-interface is entered as a network interface configuration element name. The **show security ipsec status** command usage is as follows:

```
show security ipsec status [network-interface]
```

Viewing SSH Security Information

The following section explains the commands used to obtain SSH statistics which can be helpful for debugging purposes.

View Keys

Use the **show security <key type>** command to view keys imported into the SBC.

Viewing Authorized Keys

Use the **show security authorized-keys** command to view keys imported into the SBC's authorized_keys file.

The command syntax:

```
show security authorized-key <brief | detail> [name]
```

1. Run the command without the `name` parameter to view all the authorized keys.

   ```
   ORACLE# show security authorized-key brief
   key-type:      authorized-key
   key-encr:      rsa
   key-size:      4096
   key-name:      client1
   user-class:    admin

   finger-print:
       22:b4:6b:6c:9f:47:33:31:14:e1:78:65:d4:2e:73:6c
   finger-print-raw:
       ca:ee:1c:fc:4b:65:7b:5e:b7:18:db:68:14:25:f9:46

   key-type:      authorized-key
   key-encr:      rsa
   key-size:      4096
   key-name:      admin
   user-class:    admin

   finger-print:
       b2:be:69:18:6e:32:d3:9f:5a:5a:d1:24:38:91:c8:9c
   finger-print-raw:
       4e:cc:6c:e5:8a:20:39:58:fd:4e:e9:5f:01:56:14:4d
   ORACLE#
   ```

2. Run the command with the `name` parameter to view the details of a specific authorized key.

   For example:

   ```
   ORACLE# show security authorized-key brief client1
   key-type:      authorized-key
   key-encr:      rsa
   key-size:      4096
   key-name:      client1
   user-class:    admin

   finger-print:
       22:b4:6b:6c:9f:47:33:31:14:e1:78:65:d4:2e:73:6c
   finger-print-raw:
       ca:ee:1c:fc:4b:65:7b:5e:b7:18:db:68:14:25:f9:46
   ```

Viewing Known Host Keys

Use the **show security known-host** command to view the public keys in the SBC's known_hosts file.

The command syntax:

```
show security known-host <brief | detail> [name]
```

1. Run the command without the `name` parameter to view all the known host keys.

```
ORACLE# show security known-host brief
key-type:     known-host
key-encr:     rsa
key-size:     4096
key-name:     10.0.0.10
user-class:   userfinger-print:
    22:b4:6b:6c:9f:47:33:31:14:e1:78:65:d4:2e:73:6c
finger-print-raw:
    ca:ee:1c:fc:4b:65:7b:5e:b7:18:db:68:14:25:f9:46

key-type:     known-host
key-encr:     rsa
key-size:     2048
key-name:     10.0.0.20
user-class:   userfinger-print:
    f7:e0:50:39:0b:54:fa:cd:e1:ac:de:dd:a9:42:e5:9f
finger-print-raw:
    16:5e:44:e8:2a:a6:f8:86:e5:67:1e:48:b7:34:63:c9
```

2. Run the command with the `name` parameter to view the details of a specific known host key.

```
ORACLE# show security known-host brief 10.0.0.20
key-type:     known-host
key-encr:     rsa
key-size:     2048
key-name:     10.0.0.20
user-class:   user

finger-print:
    f7:e0:50:39:0b:54:fa:cd:e1:ac:de:dd:a9:42:e5:9f
finger-print-raw:
    16:5e:44:e8:2a:a6:f8:86:e5:67:1e:48:b7:34:63:c9
```

Viewing CA Keys

Use the **show security ca-key** command to view the certificate authority keys imported into the SBC.

The command syntax:

```
show security ca-key <brief | detail> [name]
```

1. Run the command without the `name` parameter to view all the CA keys.

    ```
    ORACLE# show security ca-key brief
    key-type:      ca-key
    key-encr:      rsa
    key-size:      4096
    key-name:      rootCA
    user-class:    userfinger-print:
        3e:7a:54:22:d7:5d:51:a7:05:93:21:af:7a:f2:fd:89
    finger-print-raw:
        fe:87:18:d1:ec:a5:e8:aa:e9:7e:93:86:fa:1a:0d:9a
    ```

2. Run the command with the `name` parameter to view the details of a specific CA key.

    ```
    ORACLE# show security ca-key brief rootCA
    key-type:      ca-key
    key-encr:      rsa
    key-size:      4096
    key-name:      rootCA
    user-class:    admin

    finger-print:
        3e:7a:54:22:d7:5d:51:a7:05:93:21:af:7a:f2:fd:89
    finger-print-raw:
        fe:87:18:d1:ec:a5:e8:aa:e9:7e:93:86:fa:1a:0d:9a
    ORACLE#
    ```

Viewing ETC NIU Statistics

The following ACLI commands are NOT supported by the ETC NIU; they continue to be supported on the HiFN-based NIU.

- show sec srtp spd
- show security srtp status
- show security srtp statistics

The following ACLI commands have been modified when used in conjunction with the ETC NIU; these commands continue to operate as described in previous documentation releases when used in conjunction with the HiFN-based NIU.

- show sa stats
  The **srtp** option (**show sa stats srtp**) is not available for the ETC NIU; the option continues to be supported on the HiFN NIU.

- show security srtp sad
  Only the **brief** option (**show security srtp sad intName brief**) is supported for the ETC NIU; the **sal-index** and **sad-index**, which are HiFN-specific values, along the **ssrc** (session source) values are not available.

```
ORACLE# show security srtp sad M00:33 brief
WARNING: This action might affect system performance and take a long time to
finish.
Are you sure [y/n]?: y
SRTP security-association-database for interface 'M00:33':
Displaying SA's that match the following criteria -
        direction                  : both
        src-addr-prefix            : any
        src-port                   : any
        dst-addr-prefix            : any
        dst-port                   : any
        trans-proto                : ALL

Inbound:
        destination-address        : 192.168.203.51
        destination-port           : 10022
        vlan-id                    : 33
        mode                       : srtp
        encr-algo                  : aes-128-ctr
        auth-algo                  : hmac-sha1
        auth-tag-length            : 80
        mki                        : 0
        mki length                 : 0
        roll over count            : 0

Outbound:
        destination-address        : 192.168.200.254
        destination-port           : 10000
        vlan-id                    : 33
        mode                       : srtp
        encr-algo                  : aes-128-ctr
        auth-algo                  : hmac-sha1
        auth-tag-length            : 80
        mki                        : 0
ORACLE#
```

The following ACLI commands have been augmented for use with the ETC HIU.

show nat flow-info all

The **show nat flow-info all** ACLI command provides two new fields that identify the encryption/decryption protocol applied by the ETC NIU to inbound and outbound SRTP packets.

```
ORACLE# show nat flow-info all
SA_flow_key       : 172.16.28.1          SA_prefix : 32
DA_flow_key       : 172.16.28.2          DA_prefix : 32
SP_flow_key       : 0                    SP_prefix : 0
DP_flow_key       : 10034                DP_prefix : 16
```

```
VLAN_flow_key     : 0
Protocol_flow_key : 17
Ingress_flow_key  : 1
Ingress Slot      : 1
Ingress Port      : 0
NAT IP Flow Type  : IPv4 to IPv4
XSA_data_entry    : 192.168.28.2
XDA_data_entry    : 192.168.28.1
XSP_data_entry    : 12034
XDP_data_entry    : 8000
Egress_data_entry : 0
Egress Slot       : 0
Egress Port       : 0
flow_action       : 0X41
optional_data     : 0
FPGA_handle       : 0x00000045
assoc_FPGA_handle : 0x00000000
VLAN_data_entry   : 0
host_table_index  : 7
Switch ID         : 0x00000005
average-rate      : 0
weight            : 0x0
init_flow_guard   : 300
inact_flow_guard  : 300
max_flow_guard    : 86400
payload_type_2833 : 0
index_2833        : 0
pt_2833_egress    : 0
qos_vq_enabled    : 0
codec_type        : 0
HMU_handle        : 0
SRTP Crypto In    : AES_CM_128_HMAC_SHA1_80
SRTP Crypto Out   : AES_CM_128_HMAC_SHA1_32
---------------------------------------------

    Input Link Parameters -  IFD Index: 0x5
    ---------------------------------------------
                IFD Byte Enable: false
                EPD Mode Enable: true
                         Retain: false
                       ABJ Mode: true
                  Disable Empty: false
                Ignore On Empty: false
                           TGID: 0x6
                          WRGID: 0x0
                      TG Enable: true
                     WRG Enable: false

    Output Link Parameters -  OFD Index: 0x5
    ---------------------------------------------
                    shaped_flow: false
              latency_sensitive: false
                       pkt_mode: Packet Mode
           zero_min_credit_flow: false
                parent_pipe_num: 0x1
```

```
                          delta: 0x1
            flow_credit_min_exp: 0x0
            flow_credit_min_man: 0x0

IFD 0x00000005:       dropCount = 0x00000000


IFD 0x00000005:       acceptCount = 0x00000028

----------------------------------------------

q - quit, return - next page, space - through to the end :
...
...
```

Supported values for SRTP Crypto In/Out are as follows:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- ARIA_CM_192_HMAC_SHA1_80
- ARIA_CM_192_HMAC_SHA1_32
- NONE

show nat flow-info srtp statistics

The **show nat flow-info srtp statistics** ACLI command displays global statistics for all SRTP flows.

```
ORACLE# show nat flow-info srtp statistics
PPM_ID_SRTP_E:
PPX Global Statistics
---------------------
        alloc_count               : 34768
        dealloc_count             : 34732
        input-packets             : 0
        output-packets            : 0
        sessions-count            : 602
        init-requests             : 1798
        init-success              : 1798
        init-fail                 : 0
        modify-requests           : 600
        modify-success            : 600
        modify-fail               : 0
        delete-requests           : 1796
        delete-success            : 1796
        delete-fail               : 0
        query-requests            : 2
        query-success             : 2
        query-fail                : 0
        resources-error           : 0
        protect-fail              : 0
        unprotect-fail            : 0
        status-err                : 0
        bad-param                 : 0
        alloc-fail                : 0
        dealloc-fail              : 0
        terminus                  : 0
        auth-fail                 : 0
        cipher-fail               : 0
        replay-fail               : 0
        replay-old                : 0
        algo-fail                 : 0
        no-such-op                : 0
        no-ctx                    : 0
        cant-check                : 0
        key-expired               : 0
        nonce-bad                 : 0
        read-failed               : 0
        write-failed              : 0
        parse-err                 : 0
        encode-err                : 0
        pfkey-err                 : 0
        mki-changed               : 0
        srtp-pkt-too-small        : 0
        srtcp-pkt-too-small       : 0
PPM_ID_SRTP_D:
PPX Global Statistics
---------------------
        alloc_count               : 34768
        dealloc_count             : 34732
        input-packets             : 0
        output-packets            : 0
        sessions-count            : 602
        init-requests             : 2398
        init-success              : 2398
        init-fail                 : 0
        modify-requests           : 600
        modify-success            : 600
        modify-fail               : 0
        delete-requests           : 2396
        delete-success            : 2396
        delete-fail               : 0
        query-requests            : 2
        query-success             : 2
        query-fail                : 0
        resources-error           : 0
        protect-fail              : 0
        unprotect-fail            : 0
        status-err                : 0
        bad-param                 : 0
        alloc-fail                : 0
        dealloc-fail              : 0
        terminus                  : 0
        auth-fail                 : 0
        cipher-fail               : 0
        replay-fail               : 0
        replay-old                : 0
        algo-fail                 : 0
        no-such-op                : 0
        no-ctx                    : 0
        cant-check                : 0
        key-expired               : 0
        nonce-bad                 : 0
        read-failed               : 0
        write-failed              : 0
        parse-err                 : 0
        encode-err                : 0
        pfkey-err                 : 0
        mki-changed               : 0
        srtp-pkt-too-small        : 0
        srtcp-pkt-too-small       : 0
ORACLE#
```

show nat flow-info srtp by-addr

The **show nat flow-info srtp by-addr** ACLI command displays cryptographic details for a specific SRTP data flow, as identified by an IPv4 address specifying the data flow source.

Alternatively, you can use the **all** argument in place of a specific IP address to display cryptographic details for all SRTP data flows.

```
ORACLE# show nat flow-info srtp by-addr 172.16.28.1
Crypto Parameters 172.16.28.1:7000 -> 172.16.28.3:8000
=================

        Collapsed                 : true
        SRTCP Only                : false
Crypto In
------------------
        destination-address       : 172.16.28.2
        destination-port          : 10036
        vlan-id                   : 0
        encr-algo                 : aes-128-ctr
        auth-algo                 : hmac-sha1
        auth-tag-length           : 80
                key index                 : 0
                mki                       : none
                roll-over-count           : 0

Crypto Out
------------------
        destination-address       : 172.16.28.3
        destination-port          : 8000
        vlan-id                   : 0
        encr-algo                 : aes-128-ctr
        auth-algo                 : hmac-sha1
        auth-tag-length           : 80
                key index                 : 0
                mki                       : none
                roll-over-count           : 0
```

```
PPM_ID_SRTP_E:
PPX Statistics
--------------
Stream #1
        ssrc                      : 3735928559
        rtp-cipher-id             : AES-128-ICM
        rtp-auth-id               : HMAC-SHA1
        rtp-security-level        : Crypto + Auth
        rtp-total-packets         : 9
        rtp-total-bytes           : 178
        rtp-cipher-bytes          : 70
        rtp-auth-bytes            : 178
        rtcp-cipher-id            : AES-128-ICM
        rtcp-auth-id              : HMAC-SHA1
rtcp-security-level       : Crypto + Auth
        rtcp-total-packets        : 0
        rtcp-total-bytes          : 0
        rtcp-cipher-bytes         : 0
        rtcp-auth-bytes           : 0
        key-lifetime              : 4294967295
        direction                 : Sender
PPM_ID_SRTP_D:
PPX Statistics
--------------
Stream #1
        ssrc                      : 3735928559
        rtp-cipher-id             : AES-128-ICM
        rtp-auth-id               : HMAC-SHA1
        rtp-security-level        : Crypto + Auth
        rtp-total-packets         : 8
        rtp-total-bytes           : 240
        rtp-cipher-bytes          : 64
        rtp-auth-bytes            : 160
        rtcp-cipher-id            : AES-128-ICM
        rtcp-auth-id              : HMAC-SHA1
        rtcp-security-level       : Crypto + Auth
        rtcp-total-packets        : 0
        rtcp-total-bytes          : 0
        rtcp-cipher-bytes         : 0
        rtcp-auth-bytes           : 0
        key-lifetime              : 4294967295
        direction                 : Receiver
ORACLE#
```

show mbcd errors

The **show mbcd statistics** ACLI command provides new counters tracking SRTP error conditions.

```
ORACLE# show mbcd errors
18:05:10-142
MBC Errors/Events              ---- Lifetime ----
                        Recent       Total  PerMax
Client Errors                0          0       0
Client IPC Errors            0          0       0
Open Streams Failed          0          0       0
Drop Streams Failed          0          0       0
Exp Flow Events              0         22       2
Exp Flow Not Found           0          0       0
Transaction Timeouts         0          0       0

Server Errors                0          0       0
Server IPC Errors            0          0       0
Flow Add Failed              0          0       0
Flow Delete Failed           0          0       0
Flow Update Failed           0          0       0
Flow Latch Failed            0          0       0
Pending Flow Expired         0          0       0
ARP Wait Errors              0          0       0
Exp CAM Not Found            0          0       0
Drop Unknown Exp Flow        0          0       0
Drop/Exp Flow Missing        0          0       0
Exp Notify Failed            0          0       0
Unacknowledged Notify        0          0       0
Invalid Realm                0          0       0
No Ports Available           0          0       0
Insufficient Bandwidth       0          0       0
Stale Ports Reclaimed        0          0       0
Stale Flows Replaced         0          0       0
Telephone Events Gen         0          0       0
Pipe Alloc Errors            0          0       0
Pipe Write Errors            0          0       0
Not Found In Flows           0          0       0
SRTP Flow Add Failed         0          0       0
SRTP Flow Delete Failed      0          0       0
SRTP Flow Update Failed      0          0       0
SRTP Capacity Exceeded       0          0       0
ORACLE#
```

show mbcd statistics

The **show mbcd statistics** ACLI command displays additional counters enumerating the number of active SRTP/SRTCP flows, as well as the number of SRTP sessions.

The SRTP flow count indicates the number of flows that require either SRTP encryption or decryption on either side of the flow.

The SRTP session count indicates the number of concurrent SRTP/SRTCP sessions on the Oracle Communications Session Border Controller. An SRTP session is counted as a full SRTP plus SRTCP crypto context, including both an encryption and decryption context. Note that a collapsed flow containing SRTP and SRTCP will count as one SRTP Session, and two uncollapsed flows for SRTP and the corresponding SRTCP will also count as one SRTP session.

Note that a hairpin connection counts as two SRTP sessions, one for each SRTP/SRTCP pair on each call leg, and two SRTP collapsed flows.

```
ORACLE# show mbcd statistics
18:13:14-126
```

```
MBCD Status                -- Period -- -------- Lifetime --------
                 Active    High   Total      Total  PerMax    High
Client Sessions       1       1       0         18       3       4
Client Trans          0       0       0         75       6       3
Contexts              2       2       0         19       3       5
Flows                 4       4       0         38       6      10
Flow-Port             2       2       0         36       6       8
Flow-NAT              4       4       0         74      12      10
Flow-RTCP             0       0       0          0       0       0
Flow-Hairpin          0       0       0          0       0       0
Flow-Released         0       0       0          0       0       0
MSM-Release           0       0       0          0       0       0
Rel-Port              0       0       0          0       0       0
Rel-Hairpin           0       0       0          0       0       0
NAT Entries           4       4       0         74      12      10
Free Ports         1998    1998       0       2070    2002    2002
Used Ports            4       4       0         72      12      16
Port Sorts            -       -       0          0       0       0
Queued Notify         0       0       0          0       0       0
MBC Trans             0       0       0         75       6       5
MBC Ignored           -       -       0          0       0       0
ARP Trans             0       0       0          0       0       0
Relatch NAT           0       0       0          0       0       0
Relatch RTCP          0       0       0          0       0       0
SRTP Only Flows       0       0       0          0       0       0
SRTCP Only Flows      0       0       0          0       0       0
SRTP Collapsed Flows  0       0       0          2       2       2
SRTP Sessions         0       0       0          2       2       2


Flow Rate = 0.0
Load Rate = 0.0
ORACLE#
```

show mbcd all

The show mbcd all ACLI command provides new counters tracking SRTP data flow additions, updates, and deletions.

```
ORACLE# show mbcd statistics
18:18:14-111
MBCD Status                -- Period -- -------- Lifetime --------
                 Active    High   Total      Total  PerMax    High
Client Sessions       0       0       0          0       0       0
Client Trans          0       0       0          0       0       0
Contexts              1       1       0          1       1       1
Flows                 2       2       0          2       2       2
Flow-Port             0       0       0          0       0       0
Flow-NAT              2       2       0          2       2       2
Flow-RTCP             0       0       0          0       0       0
Flow-Hairpin          0       0       0          0       0       0
Flow-Released         0       0       0          0       0       0
MSM-Release           0       0       0          0       0       0
Rel-Port              0       0       0          0       0       0
```

```
Rel-Hairpin           0       0       0          0       0       0
NAT Entries           2       2       0          2       2       2
Free Ports         2002    2002       0       2002    2002    2002
Used Ports            0       0       0          0       0       0
Port Sorts            -       -       0          0       0
Queued Notify         0       0       0          0       0       0
MBC Trans             0       0       0          0       0       0
MBC Ignored           -       -       0          0       0
ARP Trans             0       0       0          0       0       0
Relatch NAT           0       0       0          0       0       0
Relatch RTCP          0       0       0          0       0       0
SRTP Only Flows       0       0       0          0       0       0
SRTCP Only Flows      0       0       0          0       0       0
SRTP Collapsed Flows  0       0       0          2       2       2
SRTP Sesssions        0       0       0          2       2       2


Flow Rate = 0.0
Load Rate = 0.0

18:18:14-111
NAT Entries             ---- Lifetime ----
                 Recent      Total  PerMax
Adds                  0          2       2
Deletes               0          0       0
Updates               0          0       0
Non-Starts            0          0       0
Stops                 0          0       0
Timeouts              0          0       0

18:18:14-111
ACL Entries                -- Period -- -------- Lifetime --------
                 Active    High   Total      Total  PerMax    High
Static Trusted        0       0       0          0       0       0
Static Blocked        0       0       0          0       0       0
Dynamic Trusted       0       0       0          0       0       0
Dynamic Blocked       0       0       0          0       0       0

ACL Operations          ---- Lifetime ----
                 Recent      Total  PerMax
App Requests          0          0       0
Added                 0          0       0
Removed               0          0       0
Dropped               0          0       0

18:18:14-111
MBC Errors/Events              ---- Lifetime ----
                        Recent      Total  PerMax
Client Errors                0          0       0
Client IPC Errors            0          0       0
Open Streams Failed          0          0       0
Drop Streams Failed          0          0       0
Exp Flow Events              0          0       0
Exp Flow Not Found           0          0       0
Transaction Timeouts         0          0       0
```

```
Server Errors                0          0       0
Server IPC Errors            0          0       0
Flow Add Failed              0          0       0
Flow Delete Failed           0          0       0
Flow Update Failed           0          0       0
Flow Latch Failed            0          0       0
Pending Flow Expired         0          0       0
ARP Wait Errors              0          0       0
Exp CAM Not Found            0          0       0
Drop Unknown Exp Flow        0          0       0
Drop/Exp Flow Missing        0          0       0
Exp Notify Failed            0          0       0
Unacknowledged Notify        0          0       0
Invalid Realm                0          0       0
No Ports Available           0          0       0
Insufficient Bandwidth       0          0       0
Stale Ports Reclaimed        0          0       0
Stale Flows Replaced         0          0       0
Telephone Events Gen         0          0       0
Pipe Alloc Errors            0          0       0
Pipe Write Errors            0          0       0
Not Found In Flows           0          0       0
SRTP Flow Add Failed         0          0       0
SRTP Flow Delete Failed      0          0       0
SRTP Flow Update Failed      0          0       0
SRTP Capacity Exceeded       0          0       0


SRTP Flows              ---- Lifetime ----
                 Recent      Total  PerMax
Adds                  0          2       2
Deletes               0          0       0
Updates               0          0       0
ORACLE#
```

show sipd errors

The **show sipd errors** ACLI command provides a counter tracking the number of SIP sessions that failed because of SRTP signaling problems.

```
ORACLE# show sipd errors
16:56:32-110
SIP Errors/Events             ---- Lifetime ----
                       Recent      Total  PerMax
SDP Offer Errors            0          0       0
SDP Answer Errors           0          0       0
Drop Media Errors           0          0       0
Transaction Errors          0          0       0
Application Errors          0          0       0
Media Exp Events            0          2       1
Early Media Exps            0          0       0
Exp Media Drops             0          0       0
Expired Sessions            0          1       1
```

```
Multiple OK Drops           0          0       0
Multiple OK Terms           0          0       0
Media Failure Drops         0          0       0
Non-ACK 2xx Drops           0          0       0
Invalid Requests            0          0       0
Invalid Responses           0          0       0
Invalid Messages            0          0       0
CAC Session Drop            0          0       0
Nsep User Exceeded          0          0       0
Nsep SA   Exceeded          0          0       0
CAC BW Drop                 0          0       0
SRTP Errors                 0          0       0
ORACLE# show sipd errors
```

show security srtp sessions

The **show security srtp sessions** ACLI command displays summary information for currently active SRTP sessions.

```
ORACLE# show security srtp sessions

16:31:52-199 Capacity=10000
SRTP Session Statistics       -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
SRTP Sessions          100      55     100      17264     100      75
ORACLE#
```

4 System Management

User Privilege Levels and Passwords Without Data Storage Security

User and Superuser Modes

There are two modes available in the ACLI: User mode and Superuser mode. User mode provides only limited system access and allows no system configuration. It simply enables you to view configuration files, logs, and all show commands. Superuser mode provides more complete system access and it allows you to configure your Oracle Communications Session Border Controller.

When you log in to a SBC from the console you are initially in User mode. To indicate this, the system uses a `>` as the final character of the ACLI prompt. To enter Superuser mode, you type **enable** followed by Enter at the ACLI prompt. The system prompts you to enter the Superuser password. After you enter the correct password, the prompt changes to a `#` to indicate Superuser mode.

```
User Access Verification
Password:
ORACLE> enable
Password:
ORACLE#
```

To exit to User mode from Superuser mode, type **exit** at the top-level ACLI prompt.

```
ORACLE# exit
ORACLE>
```

All local accounts in the user class have `>` as the final character in the prompt, while all local accounts in the admin class have `#` as the final character in the prompt.

Setting Passwords

The Oracle Communications Session Border Controller forces you to set a new password when you first login. However, you may also change the password with the **secret** command.

To set new ACLI passwords:

1. Type **secret login** and press Enter to set the User password.

   ```
   ORACLE# secret login
   Enter new password  :
   ```

If you do not enter a password in the required format, the following error message appears:

```
% Password must be 6-8 characters with at least one non-alpha
```

2. Type **secret enable** to set the Superuser password.

```
ORACLE# secret enable
Enter new password  :
```

3. To change the password of a local account, see the "Manage Local Accounts" section in the Getting Started chapter of the *ACLI Configuration Guide*.

SSH RADIUS Authentication VSA Support

The SBC supports the use of the Cisco Systems Inc.™ Cisco-AVPair vendor specific attribute (VSA). This attribute allows for successful administrator login to servers that do not support the Oracle authorization VSA. While using RADIUS-based authentication, the SBC authorizes you to enter Superuser mode locally even when your RADIUS server does not return the lowercase ACME_USER_CLASS VSA (`admin` or `user`) or the Cisco-AVPair VSA.

For this VSA, the Vendor-ID is 1 and the Vendor-Type is 9. The list below shows the values this attribute can return, and the result of each:

- shell:priv-lvl=15—User automatically logged in as an administrator
- shell:priv-lvl=1—User logged in at the user level, and not allowed to become an administrator
- Any other value—User rejected

Expanded Privileges

Commands available to the User level user now include:

- All show commands
- All display commands
- All monitor commands

See the Oracle Communications Session Border Controller ACLI Reference Guide Command Summary Chapter for a list of privileges for each ACLI command.

User Sessions

The Oracle Communications Session Border Controller provides a way to manually terminate an existing user session on your system. Sessions are terminated by issuing the kill command to a specifically chosen session. You first identify the session you wish to kill and then issue the command.

1. Display the current user sessions with the **show users** command.

```
ORACLE# show users
Index     remote-address           IdNum  duration  type
state        User
```

```
--------------------------------------------------------------------------
----------
    1 10.0.0.7:53581                3386  00:00:25      ssh       priv
*       admin
    0 127.0.0.1                     2777  00:42:10  console
login          user
    1 10.0.0.8:53586                3393  00:00:05     sftp
admin         admin
ORACLE#
```

The current session is noted by the asterisk to the right of the entry in the state column. In the above example, the current session has an index number of 1.

Identify the session you wish to kill by the IPv4 address listed in the remote-address column of the show users display.

2. Kill the user session. The **kill** command has two arguments: the session type and the index number. The index number is listed when you issue the **show users** command.

   The kill command syntax:

   ```
   kill <ssh | sftp | web> <index>
   ```

   For example:

   ```
   ORACLE# kill sftp 1
   Killing sftp session [1]
   Successfully killed session [sftp-admin@10.0.0.8] at index[1]
   ```

   > **Note:**
   >
   > You must be in Superuser mode to issue the kill command, but you only need to be in User mode to issue the **show users** command .

Concurrent Sessions

The Oracle Communications Session Border Controller allows a maximum number of 5 concurrent SSH sessions. The SSH allowance is shared between SSH and SFTP sessions.

Data Storage Security

In Acme Packet Release C5.0, the Oracle Communications Session Border Controller supports more secure storage of the various passwords used for system functions and using certain system features. These include: administration, certificate private key information, and manual IPSec security association key information. In addition, the Oracle Communications Session Border Controller now stores passwords in a more secure manner when you enable password-secure mode.

> **Note:**
>
> Before enabling the features described in this section, you should be certain that you want to upgrade to Acme Packet OS Release C5.0.

Considerations When Enabling Data Storage Security

The features in this group make your system more secure, and in doing so they correspondingly make it difficult for an outsider to tamper both with sensitive information used for IPSec, TLS, and HDR and with your passwords in secure-password mode.

If you use these security measures, you should be careful to:

- Guard against losing your secure data password.
- Enable secure-password mode in Upgrade to Acme Packet Release C5.0 and when you are certain you will not need to fall back to an earlier software image.

Note that the password-secure mode feature does not default to enabled on your system. This is for backward compatibility, so you need to enable password-secure mode if you want to use it and you should exercise caution when you enable it.

About Oracle Communications Session Border Controller Password Features

This section describes the multiple ways that password support has been expanded and improved to provide your system with a greater degree of security. It contains information about new password support for configurations, configuration migration, new password requirements and backwards compatibility.

Protected Configuration Password for TLS IPSec and HDR

You can now set a password for your configuration to guard sensitive information for TLS, IPSec, and HDR configurations.

Once you set the protected configuration password, the older configuration can become unusable unless you set the password back to the old value when creating the backup configuration. During the verification and activation of a configuration, the Oracle Communications Session Border Controller checks these values. If there is a conflict and the Oracle Communications Session Border Controller cannot access encrypted data using the password information you set, it displays a message notifying you of the fact.

Note that for HA nodes, the Oracle Communications Session Border Controller requires you to update the new password manually both on the active and on the standby systems.

Configuration Migration

If you want to move a configuration file from one Oracle Communications Session Border Controller to another, the Oracle Communications Session Border Controller checks passwords during the verification and activation processes. If there is a conflict and the Oracle Communications Session Border Controller cannot access encrypted data using the password information you set, it displays a message notifying you of the fact.

However, you can still reuse this configuration. Simply enter the correct protected configuration password information, and then verify and activate the configuration again.

Password Requirements

Since we are inclined to select passwords that are easy for us to remember, the Oracle Communications Session Border Controller has several requirements for passwords that make them more difficult to tamper with. The passwords you enter on the Oracle Communications Session Border Controller must be:

- Between 8 and 20 characters in length
- Comprised of both alphabetical and numeric characters, where your password must have at least one non-alphabetical character
- Comprised of both upper and lower case letters, where your password must have at least one upper case character and one lower case character
- Void of any of the passwords commonly used as default on the Oracle Communications Session Border Controller: default, password, acme, packet, user, admin

Note on Backwards Compatibility

Since the password requirements for previous releases of the Acme Packet OS clearly do not meet with the new criteria that have been defined for Acme Packet Release C5.0, the password-secure mode is disabled by default. Once you are certain that you want to run Acme Packet Release C5.0, you can enable the new password feature.

When you enable the password-secure mode, all old passwords become invalid. These old passwords are rendered useless in order to close any possible holes in security.

Password Reset and Recovery

The enhancements to password protection on the Oracle Communications Session Border Controller have been intentionally implemented so that password recovery and reset are not accessible through the ACLI. Acme Packet strongly recommends that you treat this password information with care and take all precautions against losing it.

For both password secure mode and the protected configuration password, the process for recovery and reset involves loading a diagnostics image on your system. For information about loading and running diagnostics, contact Acme Packet Customer Support.

Password Policy

When you use password secure mode on your Oracle Communications Session Border Controller, you can now configure the minimum acceptable length for a secure password if you have Superuser (administrative) privileges. The maximum password length is 64 characters.

In password secure mode, your password requires three out of four of the following:

- Upper case letters
- Lower case letters

- Numbers
- Punctuation marks

However, secure mode password cannot contain any of the following strings in any variations of case: default, password, acme, user, admin, packet.

Any change you make to the password length requirement does not go into effect until you configure a new password (and are in password secure mode). Pre-existing passwords can continue to be used until you go to change them.

Upgrade to ACP

Another measure Acme Packet Release C5.0 takes to provide enhanced security is upgrading the version of the Acme Control Protocol (ACP) from version 1.0 to version 1.1. Version 1.0 uses normal digest authentication, but version 1.1 uses advanced digest authentication. Advanced digest authentication does not require that credentials be stored using reversible format; it uses a pre-calculated hash to construct the digest value. In ACP version 1.1, there is an additional directive (user credentials hash algorithm) in the Authentication header so that the server (such as the Acme Packet EMS) can calculate the proper digest.

SSH Password Considerations

Your existing SSH password will still work after you upgrade to Acme Packet Release C5.0. However, because this password is no longer stored in the **/code/ssh** directory, a warning will appear every time the SSH server accesses the file for user authentication:

```
ORACLE# Cannot check the integrity of SSH password storage.
Should consider reset the SSH password.
```

As of Acme Packet Release C5.0, the hash of the password is saved. The file with the password also contains information that guards integrity to prevent tampering.

Resetting your password will prevent the warning messages and make your SSH sessions more secure. The procedure for setting your SSH password is the same as in prior releases.

Password Administration

This section shows you how to set a password policy.

Setting a Protected Configuration Password Matching Configurations

You set a protected configuration password using the ACLI **secret** command. As the system warning indicates when you start this process, changing the password makes backup and archived configurations unusable and requires you to change the password on the standby system in an HA node (if applicable).

When your saved and active configurations match, the process will proceed as in the sample below. However, when the saved and active configuration are out of sync, the Oracle Communications Session Border Controller requires you to correct the condition by activating the configuration (using the ACLI **activate-config** command).

To set a protected configuration password when configuration data is in synch:

1. In Superuser mode, type **secret config** at the system prompt and press Enter.

   ```
   ORACLE# secret config
   ```

2. The Oracle Communications Session Border Controller issues a warning for the change you are about to make, and asks you to confirm whether or not you want to proceed. Type a **y** and press Enter to continue; type an n and press Enter to abort the process.

   ```
   --------------------------------------------------
   WARNING:
   Proceed with caution!
   Changing the configuration password will result in any
   previous backup/archive configuration unusable.
   You also need to change the password on any stand-by
   SDs when you have changed the password successfully
   --------------------------------------------------
   Are you sure [y/n]?: y
   ```

3. Then the system asks for the old configuration password.

   ```
   Enter old password  : [your entry will not echo]
   ```

   If your entry does not match the old password, the system displays an error message: % Password mismatch - aborted.

   If your entry matches, you will be asked for the new password.

4. Enter the new configuration password. Your entry must confirm to the Password Requirements for Acme Packet Release C5.0.

   ```
   Enter new password  : [your entry will not echo]
   ```

5. Confirm the new configuration password and press Enter. The Oracle Communications Session Border Controller first displays a message letting you know that it is changing the password, and then another message confirming the change. It also prompts you to save and activate your configuration.

   ```
   Enter password again: [your entry will not echo]
   Changing the configuration password...
   Be patient. It might take a while...
   Preparing backup...
   Creating backup...
   Done
   Removing backup...
   Done
   Configuration password changed
   ORACLE#
   ```

Setting a Protected Configuration Password Mismatched Configurations

When the saved and active configuration are out of sync, the Oracle Communications Session Border Controller requires you to correct the condition by activating the configuration (using the ACLI **activate-config** command). Once this is complete, you can carry out the process for setting a protected configuration password.

To set a protected configuration password when the saved and active configurations are different:

1. In Superuser mode, type **secret config** at the system prompt and press Enter.

   ```
   ORACLE# secret config
   ```

2. The Oracle Communications Session Border Controller issues a warning for the change you are about to make, and asks you to confirm whether or not you want to proceed. Type a **y** and press Enter to continue; type an n and press Enter to abort the process.

   ```
   --------------------------------------------------
   WARNING:
   Proceed with caution!
   Changing the configuration password will result in any
   previous backup/archive configuration unusable.
   You also need to change the password on any stand-by
   SDs when you have changed the password successfully
   --------------------------------------------------
   Are you sure [y/n]?: y
   Currently active (137) and saved configurations (138) do not match!
   To sync & activate, run 'activate-config' or 'reboot activate'.
   ORACLE#
   ```

3. Use the **activate-config** command to synchronize the saved and active configurations.

   ```
   *ORACLE# activate-config
   Activate-Config received, processing.
   waiting 120000 for request to finish
   Request to 'ACTIVATE-CONFIG' has Finished,
   Activate Complete
   ```

4. Continue with the process described in Setting a Protected Configuration Password: Matching Configuration.

Setting a Protected Configuration Password Committing Changes

This section describes the process of committing the changes you have made by saving and activating configurations when both the configuration data and password have been updated. Committing the changes means saving and activating your configuration.

To commit your protected configuration password changes:

1. Carry out the process described in Setting a Protected Configuration Password: Matching Configuration.

2. After you have finished and the system is done creating a backup, the system reminds you that you need to save and activate.

   ```
   Preparing backup...
   Creating backup...
   Done
   updating cert-record name: end
   updating cert-record name: ca
   updating security-association name: sa1
   Removing backup...
   Done
   ----------------------------------------------
   WARNING:
   Configuration changed, run 'save-config' and
   'activate-config' commands to commit the changes.
   ----------------------------------------------
   ```

3. Save your configuration using the save-config command.

   ```
   ORACLE# save-config
   Save-Config received, processing.
   waiting 1200 for request to finish
   Copy OK: 8516 bytes copied
   Copy OK: 8517 bytes copied
   Request to 'SAVE-CONFIG' has Finished,
   Save complete
   ```

4. Activate your configuration using the activate-config command.

   ```
   *ORACLE# activate-config
   Activate-Config received, processing.
   waiting 120000 for request to finish
   Request to 'ACTIVATE-CONFIG' has Finished,
   Activate Complete
   ```

Changing Protected Configuration Password on a Standby System in an HA Node

When changing the protected configuration password for an HA node, you carrying out the Setting a Protected Configuration Password: Matching Configuration process (or one of the related processes) on the active system, and then must manually change it on the standby. However, changing the protected configuration password on the standby is an abbreviated process.

To change the protected configuration password on a standby system in an HA node:

1. On the stand-by system, delete the configuration using the delete-config command.

   ```
   ORACLE2# delete-config
   ```

2. On the active system, update the configuration password.

   ```
   ORACLE1# secret config
   ```

   Carry out all of the subsequent confirmations, paying close attention to the warnings.

3. On the stand-by system, update the configuration password. Ensure that the password you set on the stand-by matches the password you set on the active system

   ```
   ORACLE2# secret config
   ```

   Carry out all of the subsequent confirmations, paying close attention to the warnings.

4. On the stand-by system, acquire the configuration from the activate system using the **acquire-config** command.

   ```
   ORACLE2# acquire-config
   ```

5. Reboot the stand-by system.

   ```
   ORACLE2# reboot
   ```

Confirming Synchronous Protected Configuration Password and Configuration

To confirm that your protected configuration password and configuration are synchronized:

- In Superuser mode, type **verify-config** at the system prompt and press Enter.

  ```
  ORACLE2# verify-config
  Checking configuration data...
  OK: configuration password is in sync with the configuration data
  ```

Configuration Migration

This section provides with instructions for how to move your configuration file from one Oracle Communications Session Border Controller to another. Additional checking has been added to the verification and activation processes.

When copying a configuration between different physical platforms or between virtual and physical platforms, keep in mind that some configuration elements or attributes may be configured on the source device but not be configurable on the destination device. For example, if copying a configuration from a VM to an Acme Packet 3900, first remove any references in the **system-config** element to forwarding-cores, dos-cores, and transcoding-cores, because these are not used (or even configurable) on the Acme Packet 3900.

To migrate a configuration from SBC1 (where the password configuration has been set) to SBC2:

1. Ensure that the protected configuration password on SBC1 and SBC2 are the same.

2. On SBC1, back up a well-working configuration that you also want to use on SBC2. Use the **backup-config** command. The ACLI tells you when the back up has been saved.

   ```
   ORACLE1# backup-config copyConfig1
   task done
   ```

3. On SBC2, update the protected configuration password if necessary.
4. On SBC2, delete the configuration using the **delete-config** command.

   ```
   ORACLE2# delete-config
   ```

5. On SBC2, use the **restore-backup-config** command with the appropriate file name for the backup from SBC1. Save the configuration once the backup is restored.

   ```
   ORACLE2# restore-backup-config copyConfig1
   Need to perform save-config and activate/reboot activate for changes to
   take effect...
   task done
   ORACLE2# save-config
   Save-Config received, processing.
   waiting 1200 for request to finish
   Request to 'SAVE-CONFIG' has Finished,
   Save complete
   Currently active and saved configurations do not match!
   To sync & activate, run 'activate-config' or 'reboot activate'.
   ```

6. Before activating the configuration, verify it.

   ```
   ORACLE2# verify-config
   …
   Checking configuration password...
   OK: configuration password is in sync with the configuration data
   …
   ```

7. Activate the configuration on SBC2.

   ```
   ORACLE2# activate-config
   Activate-Config received, processing.
   waiting 120000 for request to finish
   Request to 'ACTIVATE-CONFIG' has Finished,
   Activate Complete
   ```

Setting the Password Policy

In the security ACLI path, you will find the **password-policy** configuration. It contains the **min-secure-pwd-len** parameter where you set the length requirement—between 8 and 64 characters—to use for passwords when password secure mode is enabled. For example, if you set this value to 15, then your password must be a minimum of 15 characters in length.

To set the minimum password length to use for password secure mode:

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

   ```
   ORACLE# configure terminal
   ORACLE(configure)#
   ```

2. Type **security** and press Enter.

   ```
   ORACLE(configure)# security
   ORACLE(security)#
   ```

3. Type **password-policy** and press Enter.

   ```
   ORACLE(system-config)# password-policy
   ORACLE(password-policy)#
   ```

4. **min-secure-pwd-len**—Enter a value between 8 and 64 characters that defines the minimum password length to use when in password secure mode. This parameter defaults to 8.
5. Save and activate your configuration.

Admin Security and Admin Security ACP Licenses

The Admin Security and Admin Security ACP licenses both work to increase the security of the Oracle Communications Session Border Controller (SBC). If a device already has an Admin Security license installed, you can add an Admin Security ACP license later if you need to reopen access to ACP ports. Both licenses may co-exist on a single device, or either license may be on the device alone. An Admin Security ACP license performs the same functions as an Admin Security license, but also enhances password strength requirements and allows access to the ACP (Acme Control Protocol) ports blocked by an Admin Security license.

As with any other license, an **activate-config** command must be executed after license installation for all changes to take effect. Certain ACLI aspects, such as login and password change prompts, change immediately after installation of the Admin Security license.

> **Note:**
>
> Once the Admin Security or the Admin Security with ACP entitlement is provisioned, it can not be removed from the system in the field; your chassis must be returned to Oracle for replacement.

> **Note:**
>
> The Admin Security or the Admin Security ACP feature sets are not intended for all customer use. Consult your Oracle representative to understand the ramifications of enabling these features.

License Requirements

Support for enhanced password strength requires two licenses: the previously existing Admin Security license and the newly available Admin Security ACP license.

Password Policy

The Admin Security feature set supports the creation of password policies that enhance the authentication process by imposing requirements for:

- password length
- password strength
- password history and re-use
- password expiration and grace period

  The Admin Security feature set restricts access to the ACP ports and mandates the following password length/strength requirements.

  - user password must contain at least 9 characters (Admin Security only)
  - admin password must contain at least 15 characters
  - passwords must contain at least 2 lower case alphabetic characters
  - passwords must contain at least 2 upper case alphabetic characters
  - passwords must contain at least 2 numeric characters
  - passwords must contain at least 2 special characters (such as !, ", #, $, %, &, ' , (,), *, +, , , -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~)
  - passwords must differ from the prior password by at least 4 characters
  - characters in password must differ from the prior password in at least 8 positions
  - passwords cannot contain, repeat, or reverse the entire user name
  - passwords cannot contain three consecutive identical characters

The Admin Security ACP add-on feature imposes the same password length/strength requirements as above except for the minimum length requirement, and also provides access to the ACP ports.

When you set the **password-policy**, **password-policy-strength** config property to **enabled** as part of the Admin Security ACP feature, you impose the following requirements in addition to those enforced with the Admin Security feature:

- passwords cannot contain two or more sequential characters from the user ID. This rule is not case sensitive. For example, if the username is "admin," the password cannot contain "ad" nor "AD."
- passwords cannot contain a sequence of three or more characters from any password contained in the password history cache
- passwords cannot contain a sequence of two or more characters more than once
- passwords cannot contain either sequential numbers or characters

In the absence of the Admin Security ACP feature, you may safely ignore the **password-policy-strength** config property and retain the default value (**disabled**). For more information, see *Configuring the Admin Security with ACP Password Rules*.

Some specific password policy properties, specifically those regarding password lifetime and expiration procedures, are also applicable to SSH public keys used to authenticate client users.

Configuring Password Policy Properties

The single instance **password-policy** configuration element defines the password policy.

1. From superuser mode, use the following command path to access password-policy configuration mode.

   ```
   ORACLE# configure terminal
   ORACLE(configure)# security
   ORACLE(security)# password-policy
   ORACLE(password-policy)#
   ```

   The **password-policy** configuration element properties (with the introduction of the Admin Security or JITC feature) are shown below with their default values.

   ```
   min-secure-pwd-length       8
   expiry-interval             90
   expiry-notify-period        30
   grace-period                30
   grace-logins                3
   password-history-count      3
   password-change-interval    24
   password-policy-strength    disabled
   ```

2. The **min-secure-pwd-length** command is ignored when the Admin Security with ACP feature is installed and the **password-policy-strength** configuration element is set to **enabled**.
3. Use the **expiry-interval** command to specify the password lifetime in days. Password lifetime tracking begins when a password is changed.

   Allowable values are integers within the range 0 through 65535, with a default value of 90 (days).

   > **Note:**
   >
   > The minimum **expiry-interval** is 0 with a provisioned JITC feature only and remains 1 when only an Admin Security feature is provisioned.

   ```
   ORACLE(password-policy)# expiry-interval 60
   ORACLE(password-policy)#
   ```

4. Use the **password-change-interval** command to specify the minimum password lifetime (the minimum time that must elapse between password changes.)

Allowable values are integers within the range 1 through 24, with a default value of 24 (hours).

```
ORACLE(password-policy)# password-change-interval 18
ORACLE(password-policy)#
```

5. Use the **expiry-notify-period** to specify the number of days prior to expiration that users begin to receive password expiration notifications.

   Allowable values are integers within the range 1 through 90, with a default value of 30 (days).

   During the notification period, users are reminded of impending password expiration at both Session Director login and logout.

   ```
   ORACLE(password-policy)# expiry-notify-period 10
   ORACLE(password-policy)#
   ```

6. Use the **grace-period** command in conjunction with the **grace-logins** command, to police user access after password expiration.

   After password expiration, users are granted some number of logins (specified by the **grace-logins** command) for some number of days (specified by the **grace-period** command). Once the number of logins has been exceeded, or once the grace period has expired, the user is forced to change his or her password.

   Allowable values for **grace-period** are integers within the range 1 through 90, with a default value of 30 (days).

   Allowable values for **grace-logins** are integers within the range 1 through 10, with a default value of 3 (logins).

   ```
   ORACLE(password-policy)# grace-period 1
   ORACLE(password-policy)# grace-logins 1
   ORACLE(password-policy)#
   ```

7. Use the **password-history-count** command to specify the number of previously used passwords retained in encrypted format in the password history cache.

   Allowable values are integers within the range 1 through 24, with a default value of 3 (retained passwords).

   > **Note:**
   >
   > The maximum **password-history-count** is 24 with a provisioned JITC feature only and remains 10 when only an Admin Security feature is provisioned.

   By default, a user’s three most recently expired passwords are retained in the password history. As the user’s current password is changed, that password is added to the history, replacing the oldest password entry.

New, proposed passwords are evaluated against the contents of the password cache, to prevent password re-use, and guard against minimal password changes.

```
ORACLE(password-policy)# password-history-count 10
ORACLE(password-policy)#
```

8. (Optional) Use the **password-policy-strength** command to enable the enhanced password strength requirements.

   In the absence of the Admin Security ACP feature set, this command can be safely ignored.

   password-policy-strength may be enabled when the Admin Security with ACP feature is enabled. This feature includes all of the password security features contained in the Admin Security feature set and also adds password strength requirements beyond those imposed by Admin Security. Specific new requirements are as follows:

   - passwords cannot contain two or more characters from the user ID
     For example, given a user ID of administrator, the password thispasswordistragic is not allowed because istra is a substring of administrator
   - passwords cannot contain a sequence of three or more characters from any password contained in the password history cache
   - passwords cannot contain a sequence of two or more characters more than once
     For example, ...w29W29... is legal; ...w29W29&&29... is not.
   - passwords cannot contain either sequential numbers or characters, or repeated characters more than once
     For example, ‘66666’, ‘aaaa’, ‘abcd’, ‘fedc’, ‘1234’, ‘7654'.

     For example, 666, aaa abcd, fedc, 1234, and 7654 all render a password illegal.

   In the absence of the Admin Security ACP feature, retain the default value (**disabled**). With the Admin Security with ACP feature installed, use **enabled** to add the new password requirements as listed above; use **disabled** to retain only the password requirements defined by Admin Security.

```
ORACLE(password-policy)# password-policy-strength enabled
ORACLE(password-policy)#
```

9. Use **done**, **exit** and **verify-config** to complete password policy.

Licensing Issues

The Admin Security license key enables the various security enhancements described in the Admin Security Essentials guide.

As with any other license, an activate-config command must be executed after license installation for all changes to take effect. Certain ACLI aspects, such as login and password change prompts, change immediately after installation of the Admin Security license.

These two licenses relate as follows:

1. An Oracle Communications Session Border Controller (OCSBC) with an Admin Security license also requires the Admin Sec-Shell license for operating system access.
2. An SBC that has never had an Admin Security license install will have shell access enabled.
3. Removal of the Admin Security license does not re-enable operating system access (such access requires the Admin Sec-Shell license to be present). This ensures that a system cannot be compromised via the operating system by simple removing the Admin Security license.

   A bit is permanently set in the NVRAM of an SBC to denote that it currently has, or has previously had an Admin Security license. This bit will is checked even if the license is removed, to determine if the SBC should enforce the added security features.

   Should the Admin Security license be removed the following restrictions are imposed, resulting in a severely compromised SBC:

   - EMS (Element Management System) access is not available
   - audit log deletion is not allowed
   - ACP (Acme Control Protocol) is disabled
   - operating system access is not allowed

     When an Admin Security APC license is in place, however, removal of the Admin Security license produces near-normal SBC operations.

   - EMS access is available
   - a static and inaccessible audit long remains
   - ACP (Acme Control Protocol) is enabled
   - operating system access is allowed

System Time

There are several reasons why your Oracle Communications Session Border Controller needs to keep an accurate reference to the system time. These include, but are not limited to, the need for accurate billing, logging, and the need to stay synchronized with other network equipment.

Setting Time

To manually set the system-time on your Oracle Communications Session Border Controller:

- In the ACLI at the superuser prompt, enter the **systime-set** command and press Enter. Enter the Date and Time in the exact format shown on the screen. Remember to use 24-hour time when entering the time. You will be given a chance to confirm your change. Type **Y** followed by <enter> to confirm.

```
ORACLE# systime-set
Date YYYY MM DD: 2005 01 26
Time HH MM: 16 05
WARNING: Changing the time can have an adverse
         effect on session processing
Do you want to continue [y/n]?: y
```

```
Setting time to: WED JAN 26 16:05:00 2000
ORACLE#
```

Setting Timezone

The timezone on the Acme Packet ESD must be set manually via the ACLI using one of two methods:

- using the **timezone-set** command at the root prompt. This commands starts a timezone wizard that allows you to answer prompts specifically related to timezone settings. You can set your timezone location and the wizard automatically sets the daylight savings time for the location you select.
- at the path **system**, **timezone**. This parameter allows you to create a timezone name and apply specific instructions for daylight savings time (DST) and specify the number of minutes from Coordinated Universal Time (UTC). If you initiated the timezone-set wizard previous to accessing this parameter, the settings for **system**, **timezone** are already populated. You can change them if required.

It is recommended you set the timezone after first boot of the system.

About UTC Timezones

Coordinated Universal Time (UTC) is used as the official world reference for time. Coordinated Universal Time replaced the use of Greenwich Mean Time (GMT) in 1972. Sometimes time zones are represented similar to UTC - 5h or GMT - 5h. In this example, the (-5h) refers to that time zone being five hours behind UTC or GMT and so forth for the other time zones. UTC +5h or GMT +5h would refer to that time zone being five hours ahead of UTC of GMT and so forth for the other time zones.

The usage of UTC and GMT is based upon a twenty four hour clock, similar to military time, and is based upon the 0° longitude meridian, referred to as the Greenwich meridian in Greenwich, England.

UTC is based on cesium-beam atomic clocks, with leap seconds added to match earth-motion time, where as Greenwich Mean Time is based upon the Earth's rotation and celestial measurements. UTC is also known as Zulu Time or Z time.

In areas of the United States that observe Daylight Saving Time, local residents move their clocks ahead one hour when Daylight Saving Time begins. As a result, their UTC or GMT offset would change from UTC -5h or GMT - 5h to UTC -4h or GMT - 4h. In places not observing Daylight Saving Time the local UTC or GMT offset will remain the same year round. Arizona, Puerto Rico, Hawaii, U.S. Virgin Islands and American Samoa do not observe Daylight Saving Time.

In the United States Daylight Saving Time begins at 2:00 a.m. local time on the second Sunday in March. On the first Sunday in November areas on Daylight Saving Time return to Standard Time at 2:00 a.m. The names in each time zone change along with Daylight Saving Time. Eastern Standard Time (EST) becomes Eastern Daylight Time (EDT), and so forth. A new federal law took effect in March 2007 which extends Daylight Saving Time by four weeks.

The United States uses nine standard time zones. From east to west they are Atlantic Standard Time (AST), Eastern Standard Time (EST), Central Standard Time (CST), Mountain Standard Time (MST), Pacific Standard Time (PST), Alaskan Standard Time (AKST), Hawaii-Aleutian Standard Time (HST), Samoa standard time (UTC-11) and Chamorro Standard Time (UTC+10).

The following tables identify the standard time zone boundaries and the offsets.

Coordinated Universal Time (UTC)	Greenwich Mean Time (GMT)
UTC/GMT +0	UTC/GMT +0

The following table identifies the United States GMT/UTC offsets.

Time Zone in United States	Examples of Places in the United States in These Time Zones	UTC Offset Standard Time	UTC Offset Daylight Saving Time
Atlantic	Puerto Rico, US Virgin Islands	UTC - 4h	N/A
Eastern	Connecticut, Delaware, Florida, Georgia, part of Indiana, part of Kentucky, Maine, Maryland, Massachusetts, Michigan, New Hampshire, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Rhode Island, South Carolina, part of Tennessee, Vermont Virginia, and West Virginia	UTC - 5h	UTC - 4h
Central	Alabama, Arkansas, Florida, Illinois, part of Indiana, Iowa, part of Kansas, part of Kentucky, Louisiana, part of Michigan, Minnesota, Mississippi, Missouri, Nebraska, North Dakota, Oklahoma, part of South Dakota, part of Tennessee, most of Texas, and Wisconsin	UTC - 6h	UTC - 5h
Mountain	Arizona*, Colorado, part of Idaho, part of Kansas, Montana, part of Nebraska, New Mexico, part of North Dakota, part of Oregon, part of South Dakota, part of Texas, Utah, and Wyoming	UTC - 7h	UTC - 6h *n/a for Arizona
Pacific	California, part of Idaho, Nevada, most of Oregon, Washington	UTC - 8h	UTC - 7h

Time Zone in United States	Examples of Places in the United States in These Time Zones	UTC Offset Standard Time	UTC Offset Daylight Saving Time
Alaska	Alaska and a portion of the Aleutian Islands that is east of 169 degrees 30 minutes west longitude observes the Alaska Time Zone	UTC - 9h	UTC - 8h
Hawaii-Aleutian	Hawaii and a portion of the Aleutian Islands that is west of 169 degrees 30 minutes west longitude observes the Hawaii-Aleutian Standard Time Zone. ALthough Hawaii does not observe daylight savings time, the Aleutian Islands do observe daylight saving time.	UTC - 10h	UTC - 9h Hawaii does not observe daylight saving time

Using the Timezone-Set Wizard

You can configure the timezone on the Acme Packet ESD by running a **timezone-set** wizard from the root location via the ACLI. Use the following procedure to configure the Acme Packet ESD timezone. If you need to exit the **timezone-set** command before completing it, use the key sequence **Ctrl-D**.

> **Note:**
>
> The procedure described below may display different prompts depending on whether your system is running on VXWorks or LINUX.

To configure the timezone:

1. At the root prompt, enter **timezone-set** and press Enter.

   ```
   ORACLE# timezone-set
   ```

   The following displays.

   ```
   ===============================================

   Calling tzselect. Use ^D to cancel without save
   Please identify a location so that time zone rules can be set
   correctly.
   Please select a continent or ocean.
   1) Africa
   2) Americas
   3) Antarctica
   4) Arctic Ocean
   ```

```
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#?

===============================================
```

2. Enter **the number corresponding to the continent or ocean you want to select,** and press Enter. Or enter **none** to specify the time zone using the Portable Operating System Interface (POSIX) timezone format.

   > **Note:**
   >
   > For a procedure to configure timezones using POSIX format, see Configuring Timezone using POSIX Format.

   ```
   #? 2
   ```

   The following displays.

   ```
   ===============================================

   Please select a country.
   1) Anguilla
   2) Antigua & Barbuda
   3) Argentina
   4) Aruba
   5) Bahamas
   6) Barbados
   7) Belize
   8) Bolivia
   9) Bonaire Sint Eustatius & Saba
   10) Brazil
   11) Canada
   12) Cayman Islands
   13) Chile
   14) Colombia
   15) Costa Rica
   16) Cuba
   17) Curacao
   18) Dominica
   19) Dominican Republic
   20) Ecuador
   21) El Salvador
   22) French Guiana
   23) Greenland
   24) Grenada
   25) Guadeloupe
   ```

```
26) Guatemala
27) Guyana
28) Haiti
29) Honduras
30) Jamaica
31) Martinique
32) Mexico
33) Montserrat
34) Nicaragua
35) Panama
36) Paraguay
37) Peru
38) Puerto Rico
39) Sint Maarten
40) St Barthelemy
41) St Kitts & Nevis
42) St Lucia
43) St Martin (French part)
44) St Pierre & Miquelon
45) St Vincent
46) Suriname
47) Trinidad & Tobago
48) Turks & Caicos Is
49) United States
50) Uruguay
51) Venezuela
52) Virgin Islands (UK)
53) Virgin Islands (US)
#?

===============================================
```

3. Enter **the number corresponding to the country you want to select,** and press Enter.

   ```
   #? 49
   ```

   The following displays.

   ```
   ===============================================

   Please select one of the following time zone regions.
   1) Eastern Time
   2) Eastern Time - Michigan - most locations
   3) Eastern Time - Kentucky - Louisville area
   4) Eastern Time - Kentucky - Wayne County
   5) Eastern Time - Indiana - most locations
   6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
   7) Eastern Time - Indiana - Pulaski County
   8) Eastern Time - Indiana - Crawford County
   9) Eastern Time - Indiana - Pike County
   10) Eastern Time - Indiana - Switzerland County
   11) Central Time
   12) Central Time - Indiana - Perry County
   13) Central Time - Indiana - Starke County
   ```

```
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee
Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Time - Navajo
21) Mountain Standard Time - Arizona
22) Pacific Time
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Metlakatla Time - Annette Island
30) Hawaii
#?

===============================================
```

4. Enter **the number corresponding to the time zone region you want to select,** and press Enter.

   ```
   #? 1
   ```

   The following displays.

   ```
   ===============================================

   The following information has been given:
           United States
           Eastern Time
   Therefore TZ='America/New_York' will be used.
   Local time is now:      Wed Mar 13 11:18:52 EDT 2013.
   Universal Time is now:  Wed Mar 13 15:18:52 UTC 2013.
   Is the above information OK?
   1) Yes
   2) No
   #?

   ===============================================
   ```

5. Enter **1 (Yes),** and press Enter. Or enter **2** (No) to go back to Step 2 and enter the correct timezone information.

   ```
   #? 1
   ```

   The following displays.

```
===============================================

Timezone=America/New_York
ORACLE#


===============================================
```

You have completed the **timezone-set** wizard.

Configuring Timezone using POSIX Format

If you want to configure the timezone using POSIX format, you can select the option **none - I want to specify the time zone using the Posix TZ format** in Step 2 of the timezone-set wizard. If you need to exit the **timezone-set** command before completing it, use the key sequence **Ctrl-D**.

To set the timezone using POSIX format:

1. At the root prompt, enter **timezone-set** and press Enter.

   ```
   ORACLE# timezone-set
   ```

   The following displays.

   ```
   ===============================================

   Calling tzselect. Use ^D to cancel without save
   Please identify a location so that time zone rules can be set
   correctly.
   Please select a continent or ocean.
   1) Africa
   2) Americas
   3) Antarctica
   4) Arctic Ocean
   5) Asia
   6) Atlantic Ocean
   7) Australia
   8) Europe
   9) Indian Ocean
   10) Pacific Ocean
   11) none - I want to specify the time zone using the Posix TZ
   format.
   #?

   ===============================================
   ```

2. Enter **11,** and press Enter.

   ```
   #? 11
   ```

   The following displays.

```
===============================================

Please enter the desired value of the TZ environment variable.
For example, GST-10 is a zone named GST that is 10 hours ahead (east) of
UTC.

===============================================
```

3. Enter **the UTC/GMT** value for your location. For valid UTC/GMT values, see the Timezone Offsets Table.

   ```
   #? UTC-10
   ```

   The following displays.

   ```
   ===============================================

   The following information has been given:
           TZ='UTC-10'
   Therefore TZ='UTC-10' will be used.
   Local time is now:      Thu Apr 11 02:50:18 UTC 2013.
   Universal Time is now:  Wed Apr 10 16:50:18 UTC 2013.
   Is the above information OK?
   1) Yes
   2) No
   #?

   ===============================================
   ```

4. Enter **1 (Yes),** and press Enter. Or enter **2** (No) to go back to Step 2 and enter the correct timezone information.

   ```
   #? 1
   ```

   The following displays. If you specified a value that does not relate to your Acme Packet ESD location, a warning displays.

   ```
   ===============================================

   Timezone=UTC-10
   WARNING: custom timezone will apply to application only.
   ORACLE#

   ===============================================
   ```

   You have completed the **timezone-set** wizard.

Displaying the System Timezone

You can display the timezone configured for your Oracle Communications Session Border Controller using the ACLI **show timezone** command from the root prompt.

```
ORACLE# show timezone
America/New_York
ORACLE#
```

To show more specific information about timezone settings, such as daylight savings time, navigate to the timezone parameter at the path **system**, **timezone**, and initiate the **show** command. The following example shows the results from the show command.

```
ORACLE(timezone)# show
timezone
        name     TimezoneA
        minutes-from-utc     240
        dst-start-month                         1
        dst-start-day                           1
        dst-start-weekday                       sunday
        dst-start-hour                          1
        dst-start-rule                          disabled
        dst-end-month                           1
        dst-end-day                             1
        dst-end-weekday                         sunday
        dst-end-hour                            1
        dst-end-rule                            disabled
```

NTP Synchronization

This section provides information about how to set and monitor NTP on your Oracle Communications Session Border Controller.

When an NTP server is unreachable or when NTP service goes down, the Oracle Communications Session Border Controller generates traps for those conditions. Likewise, the Oracle Communications Session Border Controller clears those traps when the conditions have been rectified. The Oracle Communications Session Border Controller considers a configured NTP server to be unreachable when its reach number (whether or not the NTP server could be reached at the last polling interval; successful completion augments the number) is 0. You can see this value for a server when you use the ACLI **show ntp server** command.

- The traps for when a server is unreachable and then again reachable are: **apSysMgmtNTPServerUnreachableTrap** and **apSysMgmtNTPServerUnreachableClearTrap**
- The traps for when NTP service goes down and then again returns are: **apSysMgmtNTPServiceDownTrap** and **apSysMgmtNTPServiceDownClearTrap**

Note:

The Oracle Communications Session Border Controller does not support NTP service over wancom0 when that interface is configured for a VLAN.

Setting NTP Synchronization

When the Oracle Communications Session Border Controller requires time-critical processing, you can set NTP for time synchronization. Setting NTP synchronizes both the hardware and the software clocks with the reference time from an NTP server that you specify. NTP is most useful for synchronizing multiple devices located on one network, or across many networks, to a reference time standard.

To guard against NTP server failure, NTP is restarted periodically to support the dynamic recovery of an NTP server.

Note that **ntp-sync** works only by way of the management interface and only on wancom0. Do not configure **ntp-sync** by way of the media interface or any other port.

To set NTP synchronization:

1. In the ACLI's configure terminal section, type **ntp-sync** and then press Enter to access the NTP configuration.

   ```
   ORACLE# configure terminal
   ORACLE(configure)# ntp-sync
   ORACLE(ntp-config)#
   ```

2. To add an NTP server, type **add-server**, the Space bar, the IPv4 or IPv6 address of the server and then press the Enter key.

   For example, this entry adds the NTP server at the Massachusetts Institute of Technology in Cambridge, MA:

   ```
   ORACLE(ntp-config)# add-server 18.26.4.105
   ```

3. To delete an NTP server, type **delete-server**, the Space bar, and the IPv4 or IPv6 address of the server you want to delete and then press the Enter key.

   ```
   ORACLE(ntp-config)# del-server 18.26.4.105
   ```

Authenticated NTP

The Oracle Communications Session Border Controller can authenticate NTP server requests using MD5. The configured MD5 keys are encrypted and obscured in the ACLI. You configure an authenticated NTP server with its IP address, authentication key, and the key ID. Corresponding key and key IDs are provided by the NTP server administrator.

To configure an authenticated NTP server:

1. Access the ntp-config configuration element.

   ```
   ORACLE# configure terminal
   ORACLE(configure)# ntp-sync
   ACMEPACKET(ntp-config)#
   ```

2. Type select.

   ```
   ORACLE(ntp-config)# select
   ```

3. Access the auth-servers configuration element

   ```
   ORACLE(ntp-config)# auth-servers
   ORACLE(auth-servers)#
   ```

4. ip-address — Enter the IPv4 or IPv6 address of the NTP server that supports authentication.
5. key-id — Enter the key ID of the key you enter in the next step. This value's range is 1 - 999999999.
6. key — Enter the key used to secure the NTP requests. The key is a string 1 - 31 characters in length.
7. Type **done** to save your work.
8. Type **exit** to return to the previous configuration level.
9. Type **done** to save the parent configuration element.

Monitoring NTP from the ACLI

NTP server information that you can view with the **show ntp server** command tell you about the quality of the time being used in terms of offset and delays measurements. You can also see the maximum error bounds.

When you use this command, information for all configured servers is displayed. Data appears in columns that are defined in the table below:

Display Column	Definition
server	Lists the NTP servers configured on the Oracle Communications Session Border Controller by IP address. Entries are accompanied by characters: Plus sign (+)—Symmetric active server Dash (-)—Symmetric passive server Equal sign (=)—Remote server being polled in client mode Caret (^)—Server is broadcasting to this address Tilde (~)—Remote peer is sending broadcast to * Asterisk (*)—The peer to which the server is synchronizing
st	Stratum level—Calculated from the number of computers in the NTP hierarchy to the time reference. The time reference has a fixed value of 0, and all subsequent computers in the hierarchy are n+1.
poll	Maximum interval between successive polling messages sent to the remote host, measured in seconds.

Display Column	Definition
reach	Measurement of successful queries to this server; the value is an 8-bit shift register. A new server starts at 0, and its reach augments for every successful query by shifting one in from the right: 0, 1, 3, 7, 17, 37, 77, 177, 377. A value of 377 means that there have been eight successful queries.
delay	Amount of time a reply packet takes to return to the server (in milliseconds) in response.
offset	Time difference (in milliseconds) between the client’s clock and the server’s.
disp	Difference between two offset samples; error-bound estimate for measuring service quality.

View Statistics

To view statistics for NTP servers:

- At the command line, type **show ntp server** and press Enter.

```
ORACLE# show ntp server
NTP Status                                    FRI APR 11:09:50 UTC 2007
 server                   st  poll  reach   delay    offset      disp
----------------------- -- ----  ------  -------  --------    ---------
*64.46.24.66              3    64     377  0.00018  0.000329    0.00255
=61.26.45.88              3    64     377  0.00017  0.002122    0.00342
```

You can the see the status of NTP on your system by using the **show ntp status** command. Depending on the status of NTP on your system, one of the following messages will appear:

- NTP not configured
- NTP Daemon synchronized to server at [the IP address of the specific server]
- NTP synchronization in process
- NTP down, all configured servers are unreachable

View Status

To view the status of NTP on your Oracle Communications Session Border Controller:

- At the command line, type **show ntp status** and press Enter.

```
ORACLE# show ntp status
```

Automated Daylight Savings Time (DST) Updates

In addition to configuring DST at the command prompt, the Oracle Communications Session Border Controller provides a mechanism to create static or rules-based time updates to reflect your location’s seasonal Daylight Savings Time changes. This configuration offsets the Oracle Communications Session Border Controller ’s internal time, obtained via NTP or from ACLI configuration. When DST is configured as a configuration element, it is persistent across reboots.

When the DST start date/time is reached, 1 hour is added to the system clock. When the DST end date/time is reached, 1 hour is subtracted from the system clock.

Baseline Configuration

To complete automated DST configuration, you must give a name to the time zone that this system adheres to and the minutes from UTC (offset) from UTC, entered as +/-720.

Static DST Updates

You can configure the Oracle Communications Session Border Controller to enact and rescind DST offset on a predefined start and stop date. This is set with the following parameters:

dst start/end rule — This parameter is set to static when configuring static DST start and end times.

dst start/end month — The month when DST offset begins or ends, entered as 1-12.

dst start/end day — The day of the month when DST offset begins or ends, entered as 1-31.

dst start/end hour — The hour on the chosen day when DST offset starts or ends, entered as 0-23.

Rules-based DST Updates

You can configure the Oracle Communications Session Border Controller to enact and rescind DST offset based on rules that correspond to relative dates in a month. That is, start and stop dates can be the Nth (or last) day-name, in a calendar month, as opposed to a day-number of the month.

dst start/end rule — This parameter is set to ordinal number of the start/stop weekday when configuring rules-based DST start and end times. This parameter is entered as: first | second | third | fourth | last.

dst start/end month — The month when DST offset begins or ends, entered as 1-12.

dst start/end weekday — The named day when DST offset begins or ends, entered as: sunday | monday | tuesday | wednesday | thursday | friday | saturday.

dst start/end hour — The hour on the chosen day when DST offset starts or ends, entered as 0-23.

dst start/end day is not configured when entering rules based DST updates.

DST Update Examples

The current DST rule for North America is that daylight savings starts on the second Sunday in March at 2:00am and ends on the first Sunday in November at 2:00am. Thus the settings for the Eastern Time Zone would be as follows:

```
name                =  EST
minutes-from-utc    =  300
dst-start-month       =  3
dst-start-day         =  1
```

```
dst-start-weekday   =  sunday
dst-start-hour       =  2
dst-start-rule     =  second
dst-end-month       =  11
dst-end-day         =  1
dst-end-weekday       =  sunday
dst-end-hour       =  2
dst-end-rule         =  first
```

Note:

The dst-start-day and dst-end-day values are ignored.

The European Union directive states that DST starts on the last Sunday in March at 1:00am UTC and ends on the last Sunday in October at 1:00am UTC. Therefore the timezone settings for the UK would be:

```
name                =  GMT
minutes-from-utc    =  0
dst-start-month       =  3
dst-start-day         =  1
dst-start-weekday   =  sunday
dst-start-hour       =  1
dst-start-rule     =  last
dst-end-month       =  10
dst-end-day         =  1
dst-end-weekday       =  sunday
dst-end-hour       =  2
dst-end-rule         =  last
```

Note the dst-end-hour is 2 because this is the local time and 2am BST is 1am UTC.

System Task Management

It is useful to directly control the tasks and processes that are running on your system. For example, you might need to terminate a hung task.

The Oracle Communications Session Border Controller also offers several debugging features such as: viewing stack traces and task control blocks, and configuring task-specific logs.

Setting Task Log Levels

Logging tasks is essential for debugging problem configurations on your Oracle Communications Session Border Controller.

The log setting changes made via the ACLI’s **log-level** commands are not persistent after a system reboot. Upon reboot, you need to change the log settings in the system-config element in order for them to be persistent. See the Oracle Communications Session Border Controller ACLI Reference Guide for the default log levels associated with each configuration element.

You can set log levels globally for all tasks or on a task-by-task basis.

To set log levels globally:

- In the ACLI at the Superuser prompt, enter the **log-level all** command, followed by the logging severity level the system should set all processes to. Refer to the following table for an explanation of logging levels, which can be entered in either numerical or English format.

  ```
  ORACLE# log-level all 4
  ```

  To set log levels for a specified task:

- In the ACLI at the superuser prompt, enter the **log-level** command followed by a specific task name and then the logging severity level to set this process to. Refer to the following table for an explanation of logging levels. Log levels can be entered in either numerical or English format.

  ```
  ORACLE# log-level mbcd minor
  ```

The following table defines the syslog levels by severity and number against the log enumeration. For more information regarding the syslog severities, refer to IETF RFC 3164, “The BSD syslog Protocol.“

syslog Level (numerical code)	syslog Severity Level (number) From RFC 3164	Code Description
Emergency (1)	Emergency (0)	The EMERGENCY syslog level signifies the utmost severity. These situations require immediate attention. If you do not attend to these types of conditions immediately, there will be physical, permanent, and irreparable damage to your system.
Critical (2)	Alert (1)	The CRITICAL syslog level signifies a serious condition within the system. These situations require attention as soon as they are noted. If you do not attend to these conditions immediately, there may be physical, permanent, and irreparable damage to your system.
Major (3)	Critical (2)	The MAJOR syslog level signifies that functionality has been seriously compromised. As a result, these situations may cause loss of functionality, hanging applications, and dropped packets. If you do not attend to these situations, your system will suffer no physical harm, but it will cease to function.
Minor (4)	Error (3)	The MINOR syslog level signifies that functionality has been impaired to a certain degree. As a result, you may experience compromised functionality. There will be no physical harm to your system. However, you should attend to these types of conditions as soon as possible in order to keep your system operating properly.

syslog Level (numerical code)	syslog Severity Level (number) From RFC 3164	Code Description
Warning (5)	Warning (4)	The WARNING syslog level signifies those conditions that signal that the system has noted some irregularities in performance. This condition is used to describe situations that are noteworthy. However, you should attend to these conditions in order to keep your system operating properly.
Notice (6)	Notice (5)	These log levels are used for Oracle support purposes.
Info (7)	Informational (6)	These log levels are used for Oracle support purposes.
Trace (8) Debug (9)	Debug (7)	These log levels are used for Oracle support purposes.

Stopping a Task

The stop-task command shuts down a specified task. You can obtain the identification number of the task you wish to end by using the tcb command. Follow the procedure below to stop a task.

To stop a task:

- In the ACLI at the superuser prompt, enter the **stop-task** command followed by the name or ID of the task you wish to terminate.

```
ORACLE# stop-task tRadd
ORACLE#
```

Notifying Tasks

The notify command sends a notification to a specific task. Notify commands have different applications and are used as a general method of telling tasks to perform a given action. Several notify applications are presented below. The generalized syntax for using the notify command is:

```
notify <task_name> <action> [<arguments>...]
```

Tracing Sockets

The notify command is used for runtime protocol tracing for UDP/TCP sockets. This use of the command provides for all protocol messages for ServiceSocket sockets to be written in a log file or sent out of the system to a UDP port. This mechanism allows for tracing to be enabled for any socket, provided that the class has a logical method for displaying and formatting the protocol message. All ACP classes and SIP supports this. Tracing can be enabled for all processes, specific sockets, all sockets, or specific processes. Tracing for specific sockets is specified by the local IPv4 address and port on which the socket is connected.

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

The <socket-address> is the IPv4 or IPv6 address and the port on which the socket is connected. The <out-udp-port> is the UDP IPv4 or IPv6 address and port to which the log messages are sent. If the <out-udp-port> is not specified, the logs are written to the <filename>.

Notify Subcommands

The tables below list and define the subcommands and additional capabilities that are included in the **notify** command.

notify Subcommand	Description
notify berpd force	This command is used to perform a manual switchover between systems in HA architectures, regardless of the system on which the command is executed (active or standby). This command forces the active system into the Standby state and forces the standby system into the Active state.

This table lists and defines the MBCD **notify** subcommands.

notify Subcommand	Description
notify mbcd nolog	This command disables MIBOCO logging.
notify mbcd log	This command enables MIBOCO logging in the miboco.log.
notify mbcd debug	This command sets the log level for MBCD for debugging purposes. Unless a specific log type is specified, this command will use its defaults: FLOW and MEDIA.
notify mbcd nodebug	This command disables setting the log level for MBCD. This command is used for debugging purposes.

The following table lists and defines the RADD **notify** subcommands.

notify Subcommand	Description
notify radd reload	This command changes the configurations for RADIUS dynamically by reloading the configuration data in the account-config.

The following table lists and defines the SIPD **notify** subcommands.

notify Subcommand	Description
notify sipd reload	This command allows you to reload SIPd and thereby update its running state with the latest configuration changes. This command cannot tear down any in-progress sessions, and it cannot tear down any listening sockets. For example, if the previously configured SIP port is 5060 and you edit the configuration and change the port to 5061, both 5060 and 5061 will be listening ports. This command only adds the new listening port to the SIP functionality and does not overwrite the previous one. Calls in progress remain up.
notify sipd nosiplog	This command disables logging SIP and MIBOCO messages, including SIP messages as seen from the system SIP proxy’s perspective (i.e., all messages are seen coming from and going to home realm addresses) and MIBOCO messages exchanged with the MBCD to manage flows.
notify sipd siplog	This command enables the logging of SIP and MIBOCO messages in the sipmsg.log.
notify sipd report	This command writes all SIP process statistics to the log file.
notify sipd dump limit	This command writes CPU limit information to the log file.
notify sipd debug	This command sets the log level for the SIP protocol for some SIP activity. This command is used for debugging purposes. Unless a specific log type is specified, this command uses its defaults: SIP, SESSION, TRANS, SIPNAT, and MEDIA.
notify sipd nodebug	This command disables setting the log level for the SIP protocol for some SIP activity. This command is used for debugging purposes.

Viewing Power Supply and RAMdrive Status

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.

```
ORACLE# show power
Power Supply A (right): Present \ On
Power Supply B (left): Present \ Off or Fail
```

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

```
ORACLE# show ramdrv
---------------  ---------  -------------  ---------  -------
/opt Directory      #Files          Bytes     Blocks  Percent
---------------  ---------  -------------  ---------  -------
collect                 35           1400         35        0
H323CfgFile              1            394          1        0
spl                      0              0          0        0
logs                    64       46646727      11430        8
crash                    0              0          0        0
./                       2           2036          2        0
---------------  ---------  -------------  ---------  -------
Total                  108       46652937      11474        8
Free                            490078208          -       91
  log-min-free=161061270(30%)
```

```
log-min-check=268435450(50%)
log-max-usage=268435450(50%)
```

Rebooting the SBC

The **reboot** command is used to reboot the Oracle Communications Session Border Controller system. There are three modes you can use to reboot your Oracle Communications Session Border Controller. Different modes determine which configurations are used to boot your system.

reboot activate

The **reboot activate** command reboots the system with the last saved current configuration. This command is useful if changes have been made and saved to the system configuration but that configuration has not yet been activated and the system goes out of service.

In terms of making the current configuration into the running configuration, using this command is the same as using the **activate-config** command.

reboot fast

On VM/server-based platforms, the **fast** argument has been added to the reboot command. The **reboot fast** (VM only) command reboots the system using the last running configuration and does not reinvoke the bootloader.

reboot force

The **reboot force** command reboots the system using the last running configuration. This command does not require you confirm the reboot directive. The boot sequence begins immediately after issuing this command.

reboot force activate

The **reboot force activate** command reboots the system using the last saved current configuration. This command does not require you confirm the reboot directive. The boot sequence begins immediately after issuing this command.

Like the **reboot activate** command, **reboot force activate** allows you to activate the current configuration that has been saved but not previously activated. Reboot **force activate** is the same as issuing the **activate-config** command and then a **reboot force**.

reboot Subcommand	Description
reboot activate	This subcommand reboots the Oracle Communications Session Border Controller and activates the newly saved configuration.
reboot force	This subcommand reboots the Oracle Communications Session Border Controller and loads the last running configuration without confirmation.
reboot force activate	This subcommand reboots the Oracle Communications Session Border Controller and activates the newly saved configuration without confirmation.

Reboot Safeguards

The ACLI's reboot command has safeguards to prevent it from being executed in one ACLI session when certain key processes are in progress in another ACLI session.

Attempting to reboot the Oracle Communications Session Border Controller while a key process is in progress in another ACLI session will result in a warning and notification message that appears on the console. The message informs you that another ACLI session is manipulating the system configuration if any of the following commands/processes are executed:

- save-config
- backup-config
- restore-backup-config
- delete-backup-config
- delete-config

Reboot Status File

The **delete-status-file** command removes the taskcheckdump.dat and statsDump.dat files on the Oracle Communications Session Border Controller. These files contains information from Oracle Communications Session Border Controller system failures.

The system writes status information to the statsDump.dat file before the system reboots itself. Oracle uses the status file to gather information about why a system rebooted itself for debugging and/or technical service purposes. To carry out this command, type **delete-status-file** into the command line and press Enter.

Warning on Reboot

The Oracle Communications Session Border Controller issues a warning when you attempt to reboot the system without having saved configuration changes. If you encounter this warning, you can simply save your configuration (using the ACLI **save-config** command), and then proceed with the reboot. If you want to reboot without saving changes, you can confirm to the reboot but any changes to the configuration (made since the last save) will be lost).

System Watchdog Timer

The Oracle Communications Session Border Controller's watchdog timer ensures that the system will reset itself if it becomes unstable. If a set period of time elapses before the timer is reset by another process, the system will initiate a hardware reset. The watchdog timer expires after 31 seconds. This period is not configurable.

The watchdog process runs at a very high priority so that it is always active. As long as other essential processes are running, the watchdog timer will be reset before it expires. If an essential system process encounters a problem, forcing the system software to hang or enter into an unstable state, the watchdog timer will not be reset. As a consequence, the watchdog timer will expire, and the system will reboot.

Watchdog Timer Configuration

The watchdog timer has the following five configuration features:

1. The watchdog state is persistent across reboot.
2. The watchdog timer is disabled by default.
3. Changes to the watchdog timer state are activated in real time.
4. The watchdog timer state can only be changed from ACLI Superuser mode.
5. The watchdog timer state can be viewed from ACLI Superuser and User modes.

ACLI Example

The following template shows the usage of the watchdog command.

```
ORACLE# watchdog [enable | disable | fetch]
```

- enable—enables the watchdog timer
- disable—disables the watchdog timer
- fetch—prints the current state of the watchdog timer to the screen
  To enable the watchdog timer on your Oracle Communications Session Border Controller:

1. Enter the Superuser mode in the ACLI.

   ```
   ORACLE#
   ```

2. Type **watchdog** <space> **enable** and press Enter to enable the watchdog timer.

   ```
   ORACLE# watchdog enable
   Watchdog timer started
   ORACLE#
   ```

3. Type **watchdog** <space> **fetch** and press Enter to confirm that the watchdog timer has been enabled.

   ```
   ORACLE# watchdog fetch
   Watchdog timer is enabled
   ORACLE#
   ```

ARP Information

The ACLI’s ARP commands are used to associated IPv4 addresses (Layer 3) with Ethernet MAC addresses (Layer 2). You can view the ARP table, add or remove an entry, or test an entry.

show arp

The **show arp** command is one of the many **show** commands available to you on the Oracle Communications Session Border Controller. It displays the Link Level ARP table, ARP entries, and ARP table statistics. An example output is shown below.

```
ORACLE# show arp
IP address    HW type  Flags  HW address         Mask  Device
169.254.2.2   0x1      0x2    00:08:25:05:a2:e2  *     wancom2
172.41.0.244  0x1      0x2    00:04:96:52:6d:07  *     wancom0
172.41.0.248  0x1      0x2    00:04:96:34:96:f4  *     wancom0
169.254.1.2   0x1      0x2    00:08:25:05:a2:e1  *     wancom1
172.41.0.223  0x1      0x2    00:04:96:51:f1:ad  *     wancom0
              Total ARP Entries = 1
              -----------------------
Intf VLAN IP-Address MAC               time-stamp          type    active-
count
1/1  0    12.12.10.1 02:04:96:51:C1:4C 2013-07-23 10:45:36 dynamic 1
Gateway Status:
Intf VLAN IP-Address MAC               time-stamp          hb status
1/1  0    12.12.10.1 02:04:96:51:C1:4C 2013-07-23 09:45:34 *  reachable
-------------- L2 Table Info ----------------
Host Database:  size          : 4008
Host Database:  used entries  : 5
--------- Network Interface Table Info ------
Host Database:  size          : 4008
Host Database:  used entries  : 5
ORACLE#
```

arp-add

The **arp-add** command allows you to add ARP entries into the ARP table. Since some network devices do not support ARP, static ARP entries sometimes need to be added to the ARP table manually. The syntax for using the **arp-add** command is:

```
arp-add <slot> <port> <vlan-id> <IP address> <MAC address>
```

If there is no VLAN tagging on this interface, set vlan-id to 0.

arp-delete

The **arp-delete** command allows you to remove ARP entries from the ARP table. You only need to identify the IPv4 address, VLAN tag, and slot and port pair to be removed. The syntax for using the **arp-delete** command is:

```
arp-delete <slot> <port> <vlan-id> <IP address>
```

arp-check

The arp-check command allows you to test a particular address resolution. When this command is carried out, a test message is sent. The test is successful when an OK is returned. If there is no VLAN identifier to be entered, then enter a value of 0. The syntax for using the **arp-check** command is:

```
arp-check <slot> <port> <vlan-id> <IP address>
```

SCTP Information

Monitoring SCTP Operations

The ACLI **show ip sctp** command provides basic SCTP information as shown below.

```
ORACLE# show ip sctp
SCTP Statistics
        0 input packets
                0 datagrams
                0 packets that had data
                0 input SACK chunks
                0 input DATA chunks
                0 duplicate DATA chunks
                0 input HB chunks
                0 HB-ACK chunks
                0 input ECNE chunks
                0 input AUTH chunks
                0 chunks missing AUTH
                0 invalid HMAC ids received
                0 invalid secret ids received
                0 auth failed
                0 fast path receives all one chunk
                0 fast path multi-part data
        0 output packets
                0 output SACKs
                0 output DATA chunks
                0 retransmitted DATA chunks
                0 fast retransmitted DATA chunks
                0 FR's that happened more than once to same chunk
                0 output HB chunks
                0 output ECNE chunks
                0 output AUTH chunks
                0 ip_output error counter
        Packet drop statistics:
                0 from middle box
                0 from end host
                0 with data
                0 non-data, non-endhost
                0 non-endhost, bandwidth rep only
                0 not enough for chunk header
                0 not enough data to confirm
                0 where process_chunk_drop said break
                0 failed to find TSN
                0 attempt reverse TSN lookup
                0 e-host confirms zero-rwnd
                0 midbox confirms no space
                0 data did not match TSN
                0 TSN's marked for Fast Retran
        Timeouts:
                0 iterator timers fired
                0 T3 data time outs
                0 window probe (T3) timers fired
                0 INIT timers fired
                0 sack timers fired
                0 shutdown timers fired
                0 heartbeat timers fired
                0 a cookie timeout fired
                0 an endpoint changed its cookiesecret
                0 PMTU timers fired
                0 shutdown ack timers fired
                0 shutdown guard timers fired
                0 stream reset timers fired
                0 early FR timers fired
                0 an asconf timer fired
                0 auto close timer fired
                0 asoc free timers expired
                0 inp free timers expired
        0 packet shorter than header
        0 checksum error
        0 no endpoint for port
        0 bad v-tag
        0 bad SID
        0 no memory
        0 number of multiple FR in a RTT window
        0 RFC813 allowed sending
        0 RFC813 does not allow sending
        0 times max burst prohibited sending
        0 look ahead tells us no memory in interface
        0 numbers of window probes sent
        0 times an output error to clamp down on next user send
        0 times sctp_senderrors were caused from a user
        0 number of in data drops due to chunk limit reached
        0 number of in data drops due to rwnd limit reached
        0 times a ECN reduced the cwnd
        0 used express lookup via vtag
        0 collision in express lookup
        0 times the sender ran dry of user data on primary
        0 same for above
        0 sacks the slow way
        0 window update only sacks sent
        0 sends with sinfo_flags !=0
        0 unordered sends
        0 sends with EOF flag set
        0 sends with ABORT flag set
        0 times protocol drain called
        0 times we did a protocol drain
```

```
    0 times recv was called with peek
    0 cached chunks used
    0 cached stream oq's used
    0 unread messages abandonded by close
    0 send burst avoidance, already max burst inflight to net
    0 send cwnd full avoidance, already max burst inflight to net
    0 number of map array over-runs via fwd-tsn's


asctpd task Statistics

Control:(from app)
    0 bad messages from app
    0 listen (0 errors)
        0 listen4
        0 listen6
    0 close (0 errors)
    0 connect (0 errors)
        0 connect4
        0 connect6
    0 setsockopt
Control:(to app)
    0 accept (0 errors)
        0 accept4
        0 accept6
    0 connected (0 errors)
        0 connected4
        0 connected6
    0 disconnected
    0 control replies
    0 Tx retries
Data:
    0 send requests from app (0 errors)
    0 data to app (0 errors)
    0 data dropped due to sendQ full
Debug:
    Socket Allocs: 0  Frees: 0
    Mblk alloc errors (0 data, 0 ctrl)

IPv6 Miscellaneous
    0 IPv4 Packet
    0 IPv6 Easy Packet
    0 IPv6 Jumbo Discarded
    0 IPv6 Bad Packet
    0 IPv6 Reassembled Packet
    0 IPv6 Hard Packet
    0 IPv6 Deleted Frag Stream
    0 IPv6 Bad Fragment
    0 IPv6 Single Fragment
    0 IPv6 Can't Create Frag Stream
    0 IPv6 Won't Create Frag Stream
    0 IPv6 Current Number Frag Streams
    0 IPv6 Total Frag Streams
    0 IPv6 Reassemble no Mblk
    0 IPv6 Reassemble Too Big
```

```
ORACLE#
```

The ACLI **show ip asctp** command provides active SCTP state information as shown below.

```
ORACLE# show ip connections asctp

A-SCTP Internet Connections
Active ASCTP associations (including servers)
Socket       Proto     Type     Local Address        Foreign Address
State
2b2d1a84     SCTP      1to1     10.1.209.50:8192     10.1.209.47:5050    pri
ESTAB
                                10.1.210.50:8192     10.1.210.47:5050    sec

2b2d238C     SCTP      1to1     2.2.2.2:5060
LISTEN
                                1.1.1.1:5060

2b2d2730     SCTP      1to1     10.1.210.50:5060
LISTEN
                                10.1.209.50:5060

ORACLE#
```

NAT Information

The ACLI can display NAT table information and the NAT table itself in a variety of formats: by entry range, by table entry range in tabular form, by matching source and destination addresses. This information is used primarily for debugging purposes.

NAT information is displayed using the **show nat** command with the appropriate arguments.

show nat info

The **show nat info** command allows displays general NAT table information. The output is used for quick viewing of the system’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.

```
ORACLE# show nat info
-- NAT table info --
Maximum number of entries  : 7768
Number of used entries     : 0
Length of search key       : 2 (x 64 bits)
First search entry address : 0x0
length of data entry       : 4 (x 64 bits)
First data entry address   : 0x0
Enable aging               : 1
Enable policing            : 0
ORACLE#
```

show nat by-addr

The **show nat by-addr** command displays NAT table information that matches source and destination addresses. When using this command, you can specify the entries to display according to source address (SA) and/or destination address (DA) values.

The system matches these values to the NAT table entries and shows the pertinent information. If no addresses are entered, the system 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>
```

The table below explains the output of the **show nat by-addr** command.

Parameter	Description
SA_flow_key	Source IPv4 or !Pv6 address key used for matching in the look-up process.
DA_flow_key	Destination IPv4 or IPv6 address key used for matching in the look-up process.
SP_flow_key	UDP source port used for matching in the look-up process.
DP_flow_key	UDP destination port used for matching in the look-up process.
VLAN_flow_key	If this is a non-zero value, then there is an associated VLAN. If this value is zero, then there is no associated VLAN.
SA_prefix	This value determines how many bits in the key are considered in the look-up process for a match, where SA is the source IPv4 address.
DA_prefix	This value determines how many bits in the key are considered in the look-up process for a match, where DA is the destination IPv4 address.
SP_prefix	This value determines how many bits in the key are considered in the look-up process for a match, where SP is the UDP source port.
DP_prefix	This value determines how many bits in the key are considered in the look-up process for a match, where DP is the UDP destination port.
Protocol_flow_key	This value stands for the protocol used, where the following values and protocols correspond: • 1 = ICMP • 6 = IP • 17 = UDP
Ingress_flow_key	This value uniquely identifies from where the packet came, and it is a combination of the Ingress Slot and Ingress Port values.
Ingress Slot	Together with the Ingress Port, this value makes up the Ingress_flow_key.
Ingress Port	Together with the Ingress Slot, this value makes up the Ingress_flow_key.
XSA_data_entry	This is the translated (i.e., post-lookup) source IPv4 or IPv6 address value.
XDA_data_entry	This is the translated (i.e., post-lookup) destination IPv4 or IPv6 address value.
XSP_data_entry	This is the translated (i.e., post-lookup) source port value.
XDP_data_entry	This is the translated (i.e., post-lookup) destination port value.
Egress_data_entry	This value uniquely identifies the outbound interface for the packet, and it is a combination of the Egress Slot and Egress Port values. This is the functional equivalent to the Ingress_flow_key.

Parameter	Description
Egress Slot	Together with the Egress Port, this value makes up the Egress_data_entry.
Egress Port	Together with the Egress Slot, this value makes up the Egress_data_entry.
flow_action	This value displays the defined flow_action (i.e., flag) bits. The flow action bit mask includes the following bit options: • bit 1 - 1=MPLS strip • bit 2 - 1=Diffserv clear • bit 5 - 1=Latch source address • bit 6 - 1=Collapse flow • bit 7 - 1=Slow Path • bit 8 - 1=QoS Requirement • bit 9 - 1=RTCP, 0=RTP is bit 8 is set • bit 10 - 1=packet capture if bit 8 is set • bit 11 - 1=full packet capture, 0=header packet capture, if bit 9 is set Bits 8 through 11 only apply to QOS.
optional_data	This value is related to the flow_action value. If the flow_action Slow Path bit (bit 7) is set, then the optional_data value is the UDP destination port for delivery to the host. The optional_data value may also contain DSCP markings.
VLAN_data_entry	This value refers to the outbound VLAN look-up process. A non-zero value means that there is an associated VLAN, while a zero value means that there is no associated VLAN.
host_table_index	This value refers to the virtual index for the host management of CAM processing.
init_flow_guard	This timer is used to age the entries in the CAM.
inact_flow_guard	This timer is used to age the entries in the CAM.
max_flow_guard	This timer is used to age the entries in the CAM.

In the above table, the following values are equivalent:

- SA = Source IPv4 or IPv6 Address
- DA = Destination IPv4 or IPv6 Address
- SP = UDP Source Port
- DP = UDP Destination Port
- X = Translated

Using a zero in the source address location of the command execution line is a wildcard value. This is used for displaying NAT information by destination address only.

show nat by-index

The **show nat by-index** command displays a specified range of entries in the NAT table, with a maximum of 5024 entries. The syntax for using the show nat by-index command is:

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

To view lines 10 through 50 of the NAT table, you would enter the following:

```
show nat by-index 10 50
```

If you do not specify a range, the system uses the default range of 1 through 200. The range you enter corresponds to line numbers in the table, and not to the number of the entry itself.

show nat in-tabular

The **show nat in-tabular** command displays a specified range of entries in the NAT table display in table form, with a maximum of 5024 entries. This tabular output allows for ease in viewing the sometimes lengthy NAT table information. The syntax is modeled on the show nat by-index command:

```
show nat in-tabular 10 50
```

In this abbreviated display, the fields that are shown for each NAT entry are:

- SA_key—equivalent to SA_flow_key in other **show nat** commands. Displayed in hexadecimal format.
- DA_key—equivalent to DA_flow_key in other **show nat** commands. Displayed in hexadecimal format.
- SP_key—equivalent to SP_flow_key in other **show nat** commands. Displayed in hexadecimal format.
- DP_key—equivalent to DP_flow_key in other **show nat** commands. Displayed in hexadecimal format.
- VLAN_key—equivalent to VLAN_data_entry in other **show nat** commands.
- ING—equivalent to Ingress_flow_key in other **show nat** commands.
- PROTO—equivalent to Protocol_flow_key in other **show nat** commands.
- WEIGHT—Flow weight.

The display of the show nat in-tabular requires a 132-column display. Please adjust your terminal program appropriately.

SNMP Community and Trap Receiver Management

You can view and reset the counters for SNMP community table and SNMP trap receivers using the ACLI commands described in this section.

SNMP Community Table

The SNMP community table stores information about the SNMP servers that you configure. These configurations set the community name and define what kind of information that server can access.

show snmp-community-table

The **show snmp-community-table** command displays all of the configuration information for the SNMP community. It also shows the total responses in and total responses out. Type **show snmp-community-table** followed by pressing Enter in the ACLI to use this command. For example:

```
ORACLE# show snmp-community-table
community-name : public
access-mode         : READ-ONLY
ip-addresses        : 10.0.200.61
172.30.0.13
total requests  in  : 111
total responses out : 111
community-name : test
access-mode         : READ-ONLY
ip-addresses        : 172.30.0.13
10.0.200.61
total requests  in  : 21
total responses out : 21
community-name : test1
access-mode         : READ-ONLY
ip-addresses        : 10.0.200.61
172.30.0.13
total requests  in  : 101
total responses out : 101
community-name : testipv6
access-mode         : READ-ONLY
ip-addresses        : [fe80::221:f6ff:fe69:224]:162
total requests  in  : 121
total responses out : 121
```

reset snmp-community-table

You can specifically reset the counters on SNMP community table statistics by using the ACLI **reset snmp-community-table** command. This set of statistics also resets when you use the ACLI **reset all** command.

```
ORACLE# reset snmp-community-table
```

Trap Receiver

The trap receiver is a network management system (NMS) to which the Oracle Communications Session Border Controller sends SNMP traps to report system events. The SNMP agent uses trap receiver information that you configure to send traps to NMSs.

When you use the ACLI **show trap-receiver** table command, the system displays all of the configuration information for the SNMP community and the total number of traps sent to it.

show trap-receiver

The **show trap-receiver** command displays all of the configuration information for the SNMP community and the total number of traps sent to it. For example:

```
ORACLE# show trap-receiver
community-name : public
filter-level    : All
ip-address      : 10.0.0.43
total traps out : 3
community-name : test
filter-level    : All
ip-address      : 10.0.200.61
total traps out : 3
community-name : testipv6
filter-level    : All
ip-address      : fe80::221:f6ff:fe69:224
total traps out : 103
```

reset trap-receiver

You can specifically reset the counters for trap receiver statistics by using the ACLI **reset trap-receiver** command. This set of statistics also resets when you use the ACLI **reset all** command.

```
ORACLE# reset trap-receiver
```

Login Banner

You can customize the displayed text banner, visible at the start of each ACLI session on your Oracle Communications Session Border Controller. This feature lets you tailor the appearance of the ACLI's initial login screen to make it more company- or customer-specific. This file is stored in the /code/banners/ directory, which the system will creates for you if it does not exist when you upload the file (called banner.txt).

ACLI Audit Trail

You can configure your Oracle Communications Session Border Controller to send a history of all user-entered commands to a common audit log file. When you enable this feature, all commands entered from any ACLI session are written to the cli.audit.log file. You can also display the log file using the **show logfile cli.audit.log** command. In addition, the system records what configuration a user selects when using the **select** command. Prompted passwords are not saved, but the requests for changes to them are.

The cli.audit.log file is stored in the log directory, and it is lost when you reboot your system; this file is not available off-box. The ACLI audit trail is enabled by default, but you can turn it off by changing the system configuration's **cli-audit-trail** parameter to disabled.

SBC Processing Language (SPL)

SPL provides a means for Acme Packet to craft solutions and features to unique problems and deploy them in a portable plugin-type software package. SPL plugins are uploaded to the Oracle Communications Session Border Controller, marked to be executed, and then perform a feature-like function as expected. SPL only works for SIP messaging. You may only run signed SPL files on your Oracle Communications Session Border Controller available directly from Acme Packet.

Upon boot, the Oracle Communications Session Border Controller compiles all scripts in the /code/spl directory that are configured in the spl config configuration element. If there is an error during parsing tile SPL files, it is written to the log.sipd and the script is not loaded. Scripts are loaded in the order in which they are configured in the spl plugins configuration element.

SPL Packages act identically to SPL plugins but contain multiple plugins in one file. When a package file is configured in the **name** parameter of the spl plugins configuration element, the Oracle Communications Session Border Controller will load all SPL plugins contained in that package. You may also configure the Oracle Communications Session Border Controller to execute a single plugin contained within the package with the syntax package-name:plugin-name. You may omit the .pkg extension when configuring the Oracle Communications Session Border Controller to load one plugin from a package.

Enabling SPL Plugins

Enabling SPL plugins is a three step process.

1. Copy the SPL plugins to a Oracle Communications Session Border Controller.
2. Configure the Oracle Communications Session Border Controller to recognize and run the plugins.
3. Command the Oracle Communications Session Border Controller to execute the plugins.

Uploading SPL Plugins

SPL plugins must be manually transferred to the Oracle Communications Session Border Controller's /code/spl directory. The Oracle Communications Session Border Controller's SFTP server, if enabled may be reached from the system's wancom or eth0 management physical interface.

Configuring SPL Plugins

All SPL plugin files that you intend to run must be configured in the spl plugins configuration element. The Oracle Communications Session Border Controller executes the plugin files in the order in which they were configured.

To add an SPL Plugin or SPL Package to the configuration:

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

```
ORACLE# configure terminal
```

2. Type **system** and press Enter to access the system-level configuration elements.

   ```
   ORACLE(configure)# system
   ORACLE(system)#
   ```

3. Type **spl-config** and press Enter.

   ```
   ORACLE(system)# spl-config
   ORACLE(spl-config)#
   ```

4. Type **plugins** and press Enter. The system prompt changes to let you know that you can begin configuring individual parameters.

   ```
   ACMESYSTEM(spl-config)# plugins
   ACMESYSTEM(spl-plugins)#
   ```

5. **name**—Enter the name of a plugin file in the /code/spl directory that you wish the Oracle Communications Session Border Controller to execute.
   - You can enter the name of the SPL Package file in the name parameter.

     ```
     ACMESYSTEM(spl-plugins)#name SPL_PACKAGE.PKG
     ```

   - You can enter a single SPL Plugin that exists in a package file as follows:

     ```
     ACMESYSTEM(spl-plugins)#name SPL_PACKAGE:MODIFY_HEADER
     ```

6. Type **done** to save your work.

SPL Parameter Configuration

SPL Plugins may create the **spl-options** parameter in either the session-agent, sip-interface, realm-config, or spl-config configuration elements. The **spl-options** parameter appears in the ACLI after an SPL plugin that creates the parameter is executed. The **spl-options** parameter will not necessarily appear in all four (or any) configuration elements. Where and when to configure the **spl-options** parameter is discussed in each plugin's specific documentation.

Executing SPL Files

There are three ways to execute SPL files:

1. Perform a **save-config** and **activate-config** after exiting the configuration menu.
2. Reboot the system (after a **save-config**)
3. Execute the **reset spl** command—all configured SPL files are refreshed by with the **reset spl** command. You can also refresh a specific file by typing **reset spl <spl-file>.**

> **Note:**
>
> Acme Packet suggests that scripts are only refreshed during system downtime.

If an SPL file exists in the /code/spl directory, but is not configured in the **spl-files** parameter, it will be ignored when the Oracle Communications Session Border Controller loads all SPL plugins. You may still manually load an SPL file directly with the **reset** command. For example:

```
ORACLE#reset spl HelloWorld.spl
```

In this case, the operator must remember that HelloWorld.spl will no be loaded on the next reboot.

Synchronizing SPL Files

When running in an HA configuration, both the active and the standby system must have the same version of the running SPL plugins installed. To facilitate configuring the standby system, the **synchronize spl** ACLI command has been developed. Executing this command without any arguments copies all files in the /code/spl directory from the active system to the to the standby Oracle Communications Session Border Controller overwriting any existing files with the same name.

By adding the specific filename as an argument to the **synchronize spl** command, the individual, specified scripts are copied between systems. For example:

```
ORACLE#synchronize spl HelloWorld.spl
```

The **synchronize spl** command can only be executed from the active system in a HA pair. There is no means to automatically synchronization SPL files during a save and activate of the SBC.

Maintenance and Troubleshooting

show spl

Typing **show spl** displays the following items:

- 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.

For example:

```
ORACLE# show spl
SPL Version: C1.0.0
[acliConsole] File: signed_valid_lower_version.spl version: 1 signature:
signed and valid
```

```
[acliConsole] File: signed_valid.spl version: 1 signature: signed and
valid
[sipd] File: signed_valid_lower_version.spl version: 1 signature:
signed and valid
[sipd] File: signed_valid.spl version: 1 signature: signed and valid
```

Adding the task to the end of the show spl command displays only the plugin information for the specified task. For example:

```
ORACLE# show spl sipd
SPL Version: C1.0.0
[sipd] File: signed_valid_lower_version.spl version: 1 signature:
signed and valid
[sipd] File: signed_valid.spl version: 1 signature: signed and valid
```

SPL Signature State

Upon executing **show spl <task>** , the ACLI displays SPL file information including the signature which will be in one of three states:

1. not signed
2. signed and valid
3. signed but invalid

Deleting SPL Plugin Files

Deleting files from /code/spl must be performed via SFTP.

SPL Log Types

The SPL log messages can often be found in the respective task's log file when that task is set to DEBUG level.

5

Inventory Management

This chapter explains how to access Oracle Communications Session Border Controller inventory management statistics to review the hardware components and licenses installed on the system, as well as active and stored configurations, and configuration information for specific elements or realms.

Accessing Inventory Management Data

You can access inventory management statistics by using the ACLI show command with different subcommands. You can access all show commands at the User level, you do not need Superuser privileges.

Hardware Inventory

This section describes the information you can view about the hardware components installed in Acme Packet platforms.

Components

You can view hard-coded, programmable read-only memory (PROM) information about the following Oracle Communications Session Border Controller hardware components:

- mainboard (chassis)
- CPU
- PHY cards
- Management card
- Transcoding modules
- Motherboard
- Security modules
- Power supply information

show prom-info mainboard

Display the mainboard PROM information by using the **show prom-info** mainboard command. For example:

```
ORACLE# show prom-info mainboard

Contents of Main Board IDPROM
        Assy, NetNet4600
        Oracle System Serial Number:    091132009670
        Oracle Part Number:             002-0610-50
        Oracle Rev:                     07
        Oracle FRU Part Number:         0000000
        Acme Packet Part Number:        002-0850-50-05
        Serial Number:                  181550000576
        Acme Packet FunctionalRev:      1.03
        BoardRev:                       05.00
        PCB Family Type:                Main Board
        ID:                             NetNet 4600 Main Board
        Options:                        0
        Manufacturer:                   MiTAC China - MSL
        Week/Year:                      32/2017
        Sequence Number:                000576
        Number of MAC Addresses:        32
        Starting MAC Address:           00 08 25 22 81 a0
```

show prom-info CPU

Display the host CPU PROM information by using the **show prom-info CPU** command. For example:

```
ORACLE# show prom-info CPU
Contents of CPU IDPROM
        Part Number:                    MOD-0026-62
        Manufacturer:                   RadiSys
```

show prom-info PHY0

Display PROM information for the left physical interface card by using the **show prom-info** PHY0 command. For example:

```
ORACLE# show prom-info PHY0
Contents of PHY0 IDPROM
        Assy, 4 Port SFP
        Part Number:                    002-0611-58
        Serial Number:                  091138058055
        FunctionalRev:                  3.04
        BoardRev:                       03.00
        PCB Family Type:                Quad port GigE SFP PHY
        ID:                             4 Port GigE SFP
        Options:                        0
        Manufacturer:                   Benchmark Electronics
        Week/Year:                      38/2011
        Sequence Number:                058055
```

show sfps

The **show sfps** command displays the EEPROM contents of the SFP modules in the system (Small Form-factor Pluggable (optical transceiver module)). This command is only applicable to the Acme Packet 4600, 6100, 6300.

```
ORACLE# show sfps
PHY0 SFP0 EEPROM
Identifier: Unknown or unspecified
```

```
Extended Identifier: 0x0
Connector: Unknown or unspecified
SONET Compliance Codes: 0x0
Gigabit Ethernet Compliance Codes: 0x0
Fibre Channel Link Length: 0x0
Fibre Channel Transmitter Technology: 0x0
Fibre Channel Transmission Media: 0x0
Fibre Channel Speed: 0x0
Encoding: Unspecified
Nominal Bit Rate (100MBits/sec): 0
Link Length Supported 9/125mm fiber (km): 0
Link Length Supported 9/125mm fiber (100m): 0
Link Length Supported 50/125mm fiber (10m): 0
Link Length Supported 62.5/125mm fiber (10m): 0
Link Length Supported copper (m): 0
Vendor Name: AVAGO
Vendor OUI: j
Vendor Part Number: AFBR-703SDZ
Vendor Rev Number: G2.3
PHY0 SFP1 EEPROM:
Identifier: Unknown or unspecified
Extended Identifier: 0x0
Connector: Unknown or unspecified
SONET Compliance Codes: 0x0
Gigabit Ethernet Compliance Codes: 0x0
Fibre Channel Link Length: 0x0
Fibre Channel Transmitter Technology: 0x0
Fibre Channel Transmission Media: 0x0
Fibre Channel Speed: 0x0
Encoding: Unspecified
Nominal Bit Rate (100MBits/sec): 0
Link Length Supported 9/125mm fiber (km): 0
Link Length Supported 9/125mm fiber (100m): 0
Link Length Supported 50/125mm fiber (10m): 0
Link Length Supported 62.5/125mm fiber (10m): 0
Link Length Supported copper (m): 0
Vendor Name: AVAGO
Vendor OUI: j
Vendor Part Number: AFBR-703SDZ
Vendor Rev Number: G2.3
```

Software Inventory

This section explains how to access information about the system image used for booting.

System image

You can display the name the system image currently booting on your system by using the following commands:

- **show version**
- **bootparam** (if you have Superuser privileges)

Image Filename Acme Packet 4500

The output from both commands includes the image filename. If that filename starts with either of the following, the system is booting from flash memory:

- For the Acme Packet 4500, you can use **/boot**.
- /tffs1/ (referring to /code)

For example, /tffs1/sd200b1.gz.

If the filename starts with /tftpboot/, the system is booting from an external device. For example, /tftpboot/sd200b1.gz.

Location

The output from both commands also includes a code that signals the system from where to boot. The code also signals the system about which file to use in the booting process. This sequence always starts with 0x (these flags are hexadecimal). For example, 0x8.

bootparam

Display information about the system image being booted on your system by using the **bootparam** command. After you issue the bootparam command, you need to press Enter to scroll down the list of boot configuration parameters.

In the following example, the system image is identified as sd201b37.gz and the location from where the system should boot is identified by the flag’s value, 0x8.

For example:

```
ORACLE(configure)# bootparam
'.' = clear field;  '-' = go to previous field;  q = quit
boot device              : wancom0
processor number         : 0
host name                : goose
file name                : sd201b37.gz
inet on ethernet (e)     : 172.30.55.127:ffff0000
inet on backplane (b)    :
host inet (h)            : 172.30.0.125
gateway inet (g)         : 172.30.0.1
user (u)                 : vxftp
ftp password (pw) (blank = use rsh)     : vxftp
flags (f)                : 0x8
target name (tn)         : ACMEPACKET
startup script (s)       :
other (o)                :
```

> **Note:**
>
> These changed parameters will not go into effect until reboot. Also, be aware that some boot parameters may also be changed through PHY and Network Interface Configurations.

Version

You can view operating system (OS) information, including the OS version number and the date that the current copy of the OS was made, by using the **show version** command. For example:

show version

```
ACMESYSTEM# show version
ACME PACKET 4500 Firmware SCX6.3.0 GA (WS Build 299)
Build Date=04/14/12
```

Configuration Information

This section explains how to access information about the system current and running configurations. It also explains how to view configuration information for a specific element or for all elements associated with a specific realm.

Overview

You can display information about your system's configuration by using the following commands:

- **show running-config** displays the configuration currently active and running on the Oracle Communications Session Border Controller.
  You can also use subcommands with show running-config to specify the element configuration you want to view. See the table in the following section for a list.
- **show configuration** displays the new configuration or configuration that you are modifying.
  You can also use subcommands with show configuration to specify the element configuration you want to view. See the table in the following section for a list.
- **display-running-cfg-version** displays the running configuration's version number.
- **display-current-cfg-version** displays the current configuration's version number.
- **realm-specifics <realm ID>** displays realm-specific configuration based on the input realm ID.

Configuration Show Subcommands

The following table lists the subcommands you can use to specify the configuration element whose configuration you want to view. You use these subcommands with the **show running-config** or **show configuration** commands.

Subcommand	Description
to-file	Send output from this command to a file located on the local flash system file system.
account-config	Account configuration
h323-config	H323 configuration
h323-stack	All h323 stacks
iwf-stack	SIP/H.323 IWF stack
host-route	All host routes
local-policy	All local policies
media-profile	All media profiles
media-manager	Media manager
dns-config	All DNS configurations
network-interface	All network interfaces
ntp-config	NTP configuration
phys-interface	All physical interfaces
realm	All realms
MediaPolicy	All media policies
ClassPolicy	All class policies
redundancy-config	Redundancy configuration
ResponseMap	All response maps
session-agent	All session agents
session-group	All session groups
session-translation	All session translations
translation-rules	All translation rules
session-router	Session router
sip-config	All SIP configurations
sip-feature	All SIP features
sip-interface	All SIP interfaces
sip-nat	All SIP NATs
snmp-community	All SNMP communities
static-flow	All static flows
steering-pool	All steering pools
system-config	System configuration
TrapReceiver	All trap receivers
call-recording-server	All IP call recording servers
capture-receiver	All capture receivers
rph-profile	All RPH profiles
rph-policy	All RPHP policies
password-policy	Password policy
enforcement-profile	All enforcement profiles
realm-group	All realm groups
inventory	Displays an inventory of all configured elements

Running Configuration Commands

You can display the entire running configuration or specify the element for which you want to view configuration information. The information in this section includes an example of one of the available show subcommands, media-manager.

show running-config

Display the configuration currently running on the Oracle Communications Session Border Controller by using the **show running-config** command. A sample of the **show running-config** output is included at the end of this section.

show running-configuration media-manager

Display configuration information for media manager only. For example:

```
ORACLE# show running-config media-manager
media-manager
        state                           enabled
        latching                        enabled
        flow-time-limit                 86400
        initial-guard-timer             300
        subsq-guard-timer               300
        tcp-flow-time-limit             86400
        tcp-initial-guard-timer         300
        tcp-subsq-guard-timer           300
        tcp-number-of-ports-per-flow    2
        hnt-rtcp                        disabled
        mbcd-log-level                  NOTICE
        max-signaling-bandwidth         10000000
        max-untrusted-signaling         100
        min-untrusted-signaling         30
        app-signaling-bandwidth         0
        tolerance-window                30
        rtcp-rate-limit                 0
        min-media-allocation            32000
        min-trusted-allocation          1000
        deny-allocation                 1000
        anonymous-sdp                   disabled
        arp-msg-bandwidth               32000
        last-modified-date              2007-04-05 09:27:20
task done
```

display-running-cfg-version

Display the saved version number of the configuration currently running on the Oracle Communications Session Border Controller by using the **display-running-cfg-version** command. For example:

```
ORACLE# display-running-cfg-version
Running configuration version is 3
```

The version number value is incremented by one for each new configuration version.

Configuration Commands

You can display the entire new or modified configuration or you can specify the element for which you want to view configuration information. The information in this section includes an example of one of the available show subcommands, **media-manager**.

show configuration

Display the new or modified configuration that will become the running configuration after you execute the save-config and activate-config commands. The output for this command is similar to the output for the show running-config command. A sample of the show running-config output is included at the end of this section.

show configuration media-manager

Display configuration information for media manager only. For example:

```
ORACLE# show configuration media-manager
media-manager
        state                          enabled
        latching                       enabled
        flow-time-limit                86400
        initial-guard-timer            300
        subsq-guard-timer              300
        tcp-flow-time-limit            86400
        tcp-initial-guard-timer        300
        tcp-subsq-guard-timer          300
        tcp-number-of-ports-per-flow   2
        hnt-rtcp                       disabled
        algd-log-level                 NOTICE
        mbcd-log-level                 NOTICE
        red-flow-port                  1985
        red-mgcp-port                  1986
        red-max-trans                  10000
        red-sync-start-time            5000
        red-sync-comp-time             1000
        max-signaling-bandwidth        10000000
        max-untrusted-signaling        100
        min-untrusted-signaling        30
        app-signaling-bandwidth        0
        tolerance-window               30
        rtcp-rate-limit                0
        min-media-allocation           32000
        min-trusted-allocation         1000
        deny-allocation                1000
        anonymous-sdp                  disabled
        arp-msg-bandwidth              32000
        last-modified-date             2007-04-05 09:27:20
task done
```

display-current-cfg-version

Display the saved version number of the current configuration by using the **display-current-cfg-version** command. For example:

```
ORACLE# display-current-cfg-version
Current configuration version is 4
```

The version number value is incremented by one for each new configuration version.

Realm Specific

You can display configuration information for elements associated with a specific realm.

realm-specifics realm ID

Display realm-specific configuration based on the input realm ID by using the **realm-specifics <realm ID>** command. The information displayed includes the following:

- realm configuration
- steering pool
- session agent
- session translation
- class policy
- local policy (if the source realm or destination realm is defined)

For example:

```
ORACLE# realm-specifics testrealm
realm-config
        identifier                     testrealm
        addr-prefix                    0.0.0.0
        network-interfaces
        mm-in-realm                    disabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   disabled
        msm-release                    disabled
        qos-enable                     disabled
        max-bandwidth                  0
        ext-policy-svr                 boffo.com
        max-latency                    0
        max-jitter                     0
        max-packet-loss                0
        observ-window-size             0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
```

```
out-manipulationid
class-profile
average-rate-limit             0
access-control-trust-level     low
invalid-signal-threshold       0
maximum-signal-threshold       0
untrusted-signal-threshold     758
deny-period                    30
symmetric-latching             disabled
pai-strip                      disabled
trunk-context
early-media-allow              reverse
additional-prefixes            10.0.0.0/24
                               172.16.0.0
restricted-latching            peer-ip
restriction-mask               17
accounting-enable              enabled
last-modified-date             2006-07-06 12:43:39
```

6

Working with Configurations

Configuration Overview

The Oracle Communications Session Border Controller uses three configuration spaces: the current configuration, last-saved configuration, and the running configuration. The current configuration is a temporary workspace where changes to the configuration are initially stored before they go “live.” Once you are satisfied with your edits, they are saved to the last-saved configuration space, as a backup configuration that is persistent across reboot. Finally, when you execute the **activate-config** command the system goes live using this configuration and makes a copy of the configuration. The copy is also stored on the file system and is called the running configuration, reflecting the running state of the Oracle Communications Session Border Controller.

The following table lists the three configuration spaces along with the creation command and location of configuration.

Configuration Name	ACLI Command to create	Location of Configuration
Current Configuration	done	/opt/data
Last-saved Configuration	save-config	/code/config
Running Configuration	activate-config	/opt/running

Configuration Process

To make configuration changes, set a current configuration, create a last-saved configuration, and finally enact your changes by making a running configuration:

1. Set all the necessary parameters on the Oracle Communications Session Border Controller. Each time you complete configuring a full configuration element, type **done** to set that element and update the current configuration. When all configuration elements are set, back out of configuration tree to the topmost ACLI level at the superuser prompt. The following example sets an arbitrary configuration element and backs you out to the superuser prompt.

```
ORACLE(host-route)# dest-network 10.0.0.0
ORACLE(host-route)# netmask 255.255.0.0
ORACLE(host-route)# gateway 172.30.0.1
ORACLE(host-route)# done
host-routes
        dest-network                   10.0.0.0
        netmask                        255.255.0.0
        gateway                        172.30.0.1
ORACLE(host-route)# exit
ORACLE(system)# exit
ORACLE(configure)# exit
```

2. Save all configurations to the last-saved configuration by using the **save-config** command. This step is mandatory.

   ```
   ORACLE# save-config
   Save-Config received, processing.
   waiting 1200 for request to finish
   Request to 'SAVE-CONFIG' has Finished,
   Save complete
   Currently active and saved configurations do not match!
   To sync & activate, run 'activate-config' or 'reboot activate'.
   ORACLE#
   ```

3. Set the Oracle Communications Session Border Controller to enact the last-saved configuration into the running state by using the **activate-config** command. This will make the last-saved configuration the running configuration and write it to the local file system.

   ```
   ORACLE# activate-config
   Activate-Config received, processing.
   waiting 120000 for request to finish
   H323 Active Stack Cnt:  0
   Request to 'ACTIVATE-CONFIG' has Finished,
   Activate Complete
   ORACLE#
   ```

Verifying & Regenerating Configurations

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.

When the **verify-config** command is run, anything configured that is inconsistent produces either an error or a warning message. An error message lets the user know that there is something wrong in the configuration that will affect the way Oracle Communications Session Border Controller runs. A warning message lets the user know that there is something wrong in the configuration, but it will not affect the way the Oracle Communications Session Border Controller runs. The following is an example of the verify-config output:

```
ORACLE# verify-config
-----------------------------------------------------------------------
---------
ERROR: realm-config [r172] is missing entry for network-interface
ERROR: sip-nat [nat172] is missing ext-address entry
ERROR: sip-nat [nat172] is missing ext-proxy-address entry
ERROR: sip-nat [nat172] is missing domain-suffix entry
WARNING: sip-nat [nat172] has ext-address [5.6.7.8] which is different
from sip-interface [sip172] sip-port address [1.2.3.4]
-----------------------------------------------------------------------
---------
Total:
4 errors
1 warning
```

Every time a user executes the **save-config** command, **verify-config** is automatically run. If any configuration problems are found, you receive a message pointing to the number of errors found during the saving, along with a recommendation to run the **verify-config** command to view the errors fully. The following is an example of the **save-config** verification output:

```
ORACLE# save-config
-------------------------------------------------------------------
Results of config verification:
   4 configuration errors
   2 configuration warnings
Run verify-config for more details
-------------------------------------------------------------------
Save-Config received, processing.
waiting 1200 for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
```

Verifying Address Duplication

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

The following tables display the entire list of addresses which are checked for duplication, the network-interface or realm which they are checked against, and the port range:

Network-Interface

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
pri-utility-addr	Primary	itself	0	0
sec-utility-addr	Secondary	itself	0	0
ip-address	Unknown	itself	0	0
ftp-address	Unknown	itself	0	0
snmp-address	Unknown	itself	0	0
telnet-address	Unknown	itself	0	0
dns-ip-primary	Unknown	itself	0	0
dns-ip-backup1	Unknown	itself	0	0
dns-ip-backup2	Unknown	itself	0	0
hip-ip-address	Unknown	itself	0	0
icmp-address	Unknown	itself	0	0

Steering-Pool

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
ip-address	UDP	network-interface or realm-id	start-port	end-port

SIP-Interface

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
sip-port address	transport-protocol (UDP or TCP)	realm-id	sip-port port	0
sip-port address	UDP if transport-protocol is UDP	realm-id	port-map-start	port-map-end

SIP-NAT

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
ext-proxy-address	Unknown	realm-id	0	0
home-proxy-address	Unknown	realm-id	0	0
home-address	Unknown	realm-id	0	0
ext-address	Unknown	realm-id	0	0

* The **home-address value** must be unique across all network interfaces configured on the Oracle Communications Session Border Controller.

H323-Stack

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
local-ip	TCP	realm-id	q031-port	0
local-ip	TCP	realm-id	q931-start-port	q931-start-port + q931-number-ports - 1
local-ip	TCP	realm-id	dynamic-start-port	dynamic-start-port + dynamic-number-port - 1
local-ip	UDP	realm-id	ras-port	0
gatekeeper	Unknown	realm-id	0	0
alternate-protocol	UDP	realm-id	it's port	0

* If an **h323-stack**'s **q931-port** (TCP) parameter is configured with **a** value of 1720, there is an address duplication exception. This configured port can exist within two port map ranges; the value of **q931-start-port** and its entire port range, and the value of **dynamic-start-port** and its entire port range.

Local-Policy Local-Policy-Attributes

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
next-hop	Unknown	realm	0	0

Session-Agent

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
ip-address	UDP or TCP	realm-id	port	0
host-name (If different from ip-address)	UDP or TCP	realm-id	port	0
ip-address	UDP or TCP	egress-realm-id if no realm-id or different from it	port	0
host-name (If different from ip-address)	UDP or TCP	egress-realm-id if no realm-id or different from it	port	0

Static-Flow

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
in-source/32	Unknown	in-realm-id	0	0
in-destination/32	UDP or TCP if ALG is TFTP or otherwise unknown	in-realm-id	start-port	end-port
out-source/32	UDP or TCP if ALG is TFTP or NAPT otherwise unknown	out-realm-id	start-port	end-port
out-destination/32	Unknown	out-realm-id	0	0

Capture-Receiver

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
address	Unknown	network-interface	0	0

Realm-Config

Parameter Name	Address Type	Network Interface or Realm	Port Start	Port End
stun-server-ip	UDP	network-interfaces	stun-server-port	0
stun-server-ip	UDP	network-interfaces	stun-changed-port	0
stun-changed-ip	UDP	network-interfaces	stun-server-port	0
stun-changed-ip	UDP	network-interfaces	stun-changed-port	0

Verify-Config Errors and Warnings

The following tables list every error and warning the **verify-config** command produces for each configuration element:

Access-Control

Error Text	Reason for Error
WARNING: access-control [id] has unsupported application-protocol [x]	Unsupported protocols [x]
WARNING: access-control [x] has trust-level set to [y], while none of the attributes `invalid-signal-threshold[0], maximum-signal-threshold[0], nat-trust-threshold[0], max-endpoints-per-nat[0], nat-invalid-message-threshold[0], cac-failure-threshold[0]` are set	When DDoS is configured in media-manager, the access-control element [x] needs to have additional attributes set.
ERROR: access-control [id] has reference to realm-id [xyz] which does not exist	Realm was not found in realm table

Account-Config

Error Text	Reason for Error
ERROR: account-config is enabled, but there are no account servers configured	State is enabled, file-output is disabled and there are not servers
WARNING: account-config is enabled, there are no account-servers configured, but ftp-push is disabled	State and file-output are enabled, there are not account servers and ftp-push is disabled
WARNING: account-config is enabled, account-servers are configured, file-output is disabled, but ftp-push is enabled	State and ftp-push are enabled, account servers are configured, file-output is disabled
ERROR : account-config is enabled, ftp-push is enabled, but there is no ftp-address entered or push-receiver configured	State and ftp-push are enabled, but there is no ftp-address or push-receiver configured
ERROR: account-config has reference to push-receiver [xyz] which can not get password	Password failed decryption

Error Text	Reason for Error
ERROR: account-config has reference to push-receiver [xyz] which does not have remote-path set	Push-receiver has no remote-path set
ERROR: account-config has reference to push-receiver [xyz] which does not have username set	Push-receiver has no username set
ERROR: account-config has reference to push-receiver [xyz] which does not have password set for protocol FTP	Push-receiver has no password set for FTP
WARNING: account-config has reference to push-receiver [xyz] with a public key set, but protocol is set to FTP	Push-receiver has set public key, but protocol is FTP
ERROR: account-config has push-receiver [xyz] with reference to public-key [zyx] which does not exist	Public key was not found in public key table
ERROR: account-config has account-server [IP:Port] with empty secret	Account-server [IP:Port] has empty secret field

Authentication

Error Text	Reason for Error
ERROR: authentication has specified unsupported protocol [x] for type [y]	Unsupported protocols for given type
ERROR: authentication has no configured active radius servers for authentication type [x]	No configured active radius for given type

Call-Recording-Server

Error Text	Reason for Error
ERROR: call-recording-server must have a name	Name is missing
ERROR: call-recording-server [id] must have a primary-signaling-addr or primary-media-addr	There has to be either primary signaling or media address
ERROR: call-recording-server [id] is missing primary-realm	Realm name is missing
ERROR: call-recording-server [id] has reference to the primary-realm [xyz] which does not exist	Primary-realm [xyz] was not found in realm-config table
ERROR: call-recording-server [id] has reference to the secondary-realm [xyz] which does not exist	Secondary-realm [xyz] was not found in realm-config table

Capture-Receiver

Error Text	Reason for Error
ERROR: capture-receiver [id] has reference to network-interface [xyz] which does not exist	Network-interface was not found in network-interface table

Certificate-Record

Error Text	Reason for Error
ERROR: certificate-record [id] is not trusted and will not be loaded	Certificate record is not trusted
ERROR: certificate-record [id] cannot extract private key	Certificate record failed to extract the private key
ERROR: certificate-record [id] cannot convert PKCS7 string to structure	Failure to convert PKCS7 record to the structure

Class-Policy

Error Text	Reason for Error
ERROR: class-policy [id]] has reference to the media-policy [xyz] which does not exist	Media-policy [xyz] was not found in the media-policy table

DNS-Config

Error Text	Reason for Error
ERROR: dns-config [id] is missing client-realm entry	Missing client realm
ERROR: dns-config [id] has reference to client-realm [xyz] which does not exist	Realm was not found in the realm-config table
ERROR: dns-config [id] does not have any server-dns-attributes	Server-dns-attributes are missing
ERROR: dns-config [id] is missing server-realm entry	Realm entry is missing (source address is empty)
ERROR: dns-config [id] is missing server-realm entry for source-address [x]	Realm entry is missing (source address is not empty)
ERROR: dns-config [id] has reference to server-realm [xyz] which does not exist	Realm was not found in the realm-config table

ENUM-Config

Error Text	Reason for Error
ERROR: enum-config [id] is missing realm-id entry	Missing realm
ERROR: enum-config [id] has reference to the realm-id [xyz] which does not exist	Realm [xyz] was not found in realm-config table
ERROR: enum-config [id] has no enum-servers	List of ENUM servers is empty

Ext-Policy-Server

Error Text	Reason for Error
ERROR: ext-policy-server [id] is missing realm entry	Missing realm
ERROR: ext-policy-server [id] address is not valid	Invalid address entry

Error Text	Reason for Error
ERROR: ext-policy-server [id] has reference to protocol [xyz] which is not valid	Invalid protocol entry
ERROR: ext-policy-server [id] has reference to realm [xyz] which does not exist	Realm was not found in the realm-config table

H323-Stack

Error Text	Reason for Error
ERROR: h323-stack [id] has no realm-id	Missing realm entry
ERROR: h323-stack [id] has reference to the realm-id [xyz] which does not exist	Realm was not found in the realm-config table
WARNING: h323-stack [id] is missing local-ip address entry	Missing address entry
WARNING : h323-stack [id] has reference to media-profile [xyz] which does not exist	Media profile was not found in media profile table
ERROR: h323-stack [id] has reference to the assoc-stack [xyz] which does not exist	Stack name was not found in the h323-stack table

Host-Route

Error Text	Reason for Error
WARNING: host-route [id] has reference to gateway [xyz] which does not exist in any network-interface	gateway entry was not found in any network-interface object

IWF-Config

Error Text	Reason for Error
WARNING: iwf-config has reference to media-profile [xyz] which does not exist	media profile was not found in media profile table

Local-Policy

Error Text	Reason for Error
ERROR: local-policy [id] has reference to source-realm [xyz] which does not exist	Source-realm [xyz] was not found in realm-config table
WARNING: local-policy [id] has no policy-attributes set	No policy-attributes set
ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to realm [xyz] which does not exist	Realm [xyz] was not found in realm-config table
ERROR: local-policy-attribute [id1] from local-policy [id2] is missing next-hop entry	Next-hop is missing for given attribute
ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which is invalid	Invalid value for the next-hop
ERROR: local-policy-attribute [id1] from local-policy [id2] has reference to next-hop [xyz] which does not exist	Value for the next-hop was not found (either from enum-config, or lrt-config, or session-group)

Error Text	Reason for Error
WARNING: local-policy-attribute [id] from local-policy [di] has reference to media-policy [xyz] which does not exist	Media-policy [xyz] was not found in media-policy table
WARNING: local-policy [id] local-policy-attribute [id1] has duplicate address with sip-port [xyz] sip-interface has duplicate address with sip-port	Policy attribute next-hop is the same as the sip-port

Local-Routing-Config

Error Text	Reason for Error
ERROR: local-routing-config [id] has reference to the file-name [xyz] which does not exist	specified file is missing from /boot/code/lrt folder

Network-Interface

Error Text	Reason for Error
ERROR: network-interface [id] has reference to phy-interface [xyz] which does not exist	Phy-interface [xyz] was not found in phy-interface table
ERROR: network-interface [id] is missing pri-utility-addr entry	If redundancy is enabled pri-utility-addr entry has to be entered
ERROR: network-interface [id] is missing sec-utility-addr entry	If redundancy is enabled sec-utility-addr entry has to be entered
ERROR: network-interface [id] has reference to DNS address, but dns-domain is empty	Dns-domain is empty. Word “address” will be plural addresses if there are more DNS addresses entered
ERROR: network-interface [id] has reference to DNS address, but ip-address is empty	Ip-address is empty. Word “address” will be plural addresses if there are more DNS addresses entered

Phy-Interface

Error Text	Reason for Error
ERROR: phy-interface [id] has invalid operation-type value [x]	Operation-type value is invalid
ERROR: phy-interface [id] of type [x] with port [y] and slot [z] has invalid name	If type is MAINTENANCE or CONTROL name has to start with either “eth” or wancom
ERROR: phy-interface [id] of type [x] has duplicated port [y] and slot [z] values with phy-interface [di]	Port and slot values are duplicated with another phy-interface

Public-Key

Error Text	Reason for Error
ERROR: public-key [id] has no public/private key pair generated for public-key [x]	No public/private key generated
ERROR: public-key [id] cannot extract private key	Cannot extract private key

Realm-Config

Error Text	Reason for Error
ERROR: realm-config [id] has reference to ext-policy-svr [xyz] which doe not exist	Missing external BW manager
ERROR: realm-config [id] is missing entry for network-interface	Missing Network Interface
ERROR: realm-config [id] has reference to network-interface [xyz] which does not exist	Network interface was not found in network-interface table
ERROR: realm-config [id] has reference to media-policy [xyz] which does not exist	Media-policy was not found in media-policy table
ERROR: realm-config [id] has reference to class-profile [xyz] which does not exist	Class-profile was not found in class-profile table
ERROR: realm-config [id] has reference to in-translationid [xyz] which does not exist	In-translationid was not found in session translation table
ERROR: realm-config [id] has reference to out-translationid [xyz] which does not exist	Out-translationid was not found in session translation table
ERROR: realm-config [id] has reference to in-manipulationid [xyz] which does not exist	In-manipulationid was not found in manipulation table
ERROR: realm-config [id] has reference to out-manipulationid [xyz] which does not exist	Out-manipulationid was not found in manipulation table
ERROR: realm-config [id] has reference to enforcement-profile [xyz] which does not exist	Enforcement-profile was not found in enforcement-profile table
ERROR: realm-config [id] has reference to call-recording-server-id [xyz] which does not exist	Call-recording-server-id was not found in call-recording-server-table
ERROR: realm-config [id] has reference to codec-policy [xyz] which does not exist	Codec-policy was not found in codec-policy table
ERROR: realm-config [id] has reference to constraint-name [xyz] which does not exist	Constraint-name was not found in session constraint table
ERROR: realm-config [id] has reference to qos-constraint [xyz] which does not exist	Qos-constraint was not found in qos constraint table
ERROR: realm-config [id] with parent-realm [xyz] are part of circular nested realms	Realm and its parent realm are part of the closed loop where they referring back to themselves
ERROR: realm-config [id] has reference to dns-realm [xyz] which does not exist	Dns-realm doesn’t exist in the realm table
WARNING: realm-config [id] has reference to itself as a parent (parent-realm value ignored)	Realm name and parent name are the same
ERROR: realm-config [id] has reference to parent-realm [xyz] which does not exist	Parent realm doesn’t exist in the realm table
ERROR: realm-config [id] has identical stun-server-port and stun-changed port [x]	Stun-server-ip is identical to stun-changed-ip, when stun is enabled
ERROR: realm-config [id] has identical stun-server-ip and stun-changed-ip [x]	Stun-server-port is identical to stun-changed-port, when stun is enabled

Realm-Group

Error Text	Reason for Error
ERROR: realm-group [id] has reference to source-realm [xyz] which does not exist	Realm was not found in realm-config table

Error Text	Reason for Error
ERROR: realm-group [id] has reference to destination-realm [xyz] which does not exist	Realm was not found in realm-config table

Redundancy

Error Text	Reason for Error
ERROR: redundancy-config peer [id] has Address [x] which does not match pri-utility-addr from network-interface [y]	If redundancy is enabled, peer IP addresses have to match Primary Utility addresses from specified network-interface (pri-utility-addr is missing here)
ERROR: redundancy-config peer [id] has Address [x] which does not match pri-utility-addr [z] from network-interface [y]	If redundancy is enabled, peer IP addresses have to match Primary Utility addresses from specified network-interface
ERROR: redundancy-config peer [id] has Address [x] which does not match sec-utility-addr from network-interface [y]	If redundancy is enabled, peer IP addresses have to match Secondary Utility addresses from specified network-interface (sec-utility-addr is missing here)
ERROR: redundancy-config peer [id] has IP Address [x] which does not match sec-utility-addr [z] from network-interface [y]	If redundancy is enabled, peer IP addresses have to match Secondary Utility addresses from specified network-interface
ERROR: redundancy-config peer [id] has reference to network-interface [xyz] which does not exist	Network-interface [xyz] was not found in network-interface table
ERROR: redundancy-config peer [id] is missing destination object	Destination object is missing
ERROR: redundancy-config is missing Primary peer object	Primary peer object is missing
ERROR: redundancy-config is missing Secondary peer object	Secondary peer object is missing
ERROR: redundancy-config is missing both Primary and Secondary peer objects	Primary and Secondary peer objects are missing

Security-Association

Error Text	Reason for Error
ERROR: security-association [id] is missing network-interface entry	Missing network-interface entry
ERROR: security-association [id] has reference to network-interface [xyz] which does not exist	Network-interface was not found in network-interface table
ERROR: security-association [id] has invalid local-ip-addr	Invalid local-ip-addr entry
ERROR: security-association [id] has invalid remote-ip-addr	Invalid remote-ip-addr entry
ERROR: security-association [id] has reference to network-interface [xyz] which is not valid IPSEC enabled media interface	Network-interface is not valid IPSEC media interface

Error Text	Reason for Error
ERROR: security-association [id] Unable to decrypt auth-key from configuration. This configuration may not have been saved using this systems configuration password	Failed to decrypt auth-key
ERROR: security-association [id] has auth-algo [hmac-md5] with an auth-key of invalid length, must be 32 hex characters long	Invalid length of the auth-key for auth-algo [hmac-md5]
ERROR: security-association [id] has auth-algo [hmac-sha1] with an auth-key of invalid length, must be 40 hex characters long	Invalid length of the auth-key for auth-algo [hmac-sha1]
ERROR: security-association [id] Unable to decrypt encr-key from configuration. This configuration may not have been saved using this systems configuration password	Failed to decrypt encr-key
ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 64 bits (odd parity in hex)	Invalid encr-key length for given algorithm
ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 192 bits (odd parity in hex)	Invalid encr-key length for given algorithm
ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 128 bits (odd parity in hex)	Invalid encr-key length for given algorithm
ERROR: security-association [id] has encr-algo [xyz] with and encr-key of invalid length, must be 256 bits (odd parity in hex)	Invalid encr-key length for given algorithm
ERROR: security-association [id] has invalid aes-ctr-nonce (must be non-zero value) for encr-algo [xyz]	Has invalid aes-ctr-nonce for given algorithm
ERROR: security-association [id] has invalid tunnel-mode local-ip-addr (will be set to inner local-ip-address)	Invalid tunnel-mode local-ip-addr
ERROR: security-association [id] has invalid tunnel-mode remote-ip-addr (will be set to inner remote-ip-address)	Invalid tunnel-mode remote-ip-addr
ERROR: security-association [id] has invalid espudp local-ip-addr (must be non-zero)	Invalid espudp local-ip-addr
ERROR: security-association [id] has invalid espudp remote-ip-addr (must be non-zero)	Invalid espudp remote-ip-addr
ERROR: security-association [id] has invalid espudp local-port (must be non-zero)	Invalid espudp local-port
ERROR: security-association [id] has invalid espudp remote-port (must be non-zero)	Invalid espudp remote-port

Security-Policy

Error Text	Reason for Error
ERROR: security-policy [id] has invalid local-ip-addr-match	Empty local-ip-addr-match
ERROR: security-policy [id] has invalid local-ip-addr-match [x]	Invalid local-ip-addr-match

Error Text	Reason for Error
ERROR: security-policy [id] has invalid remote-ip-addr-match	Empty remote-ip-addr-match
ERROR: security-policy [id] has invalid remote-ip-addr-match [x]	Invalid remote-ip-addr-match
ERROR: security-policy [id] is missing network-interface entry	Missing network-interface entry
ERROR: security-policy [id] priority [x] is identical to security-policy [id2]	Duplication of the priorities
ERROR: security-policy [id] has reference to network-interface [xyz] which does not exist	Network-interface was not found in network-interface table
ERROR: security-policy [id] has reference to network-interface [xyz] which is not valid IPSEC enabled media interface	Network-interface is not valid IPSEC media interface

Session-Agent

Error Text	Reason for Error
ERROR: session-agent [id] has reference to realm-id [xyz] which does not exist	Realm was not found in realm table
ERROR: session-agent [id] has reference to egress-realm-id [xyz] which does not exist	Realm was not found in realm table
ERROR: session-agent [id] has reference to in-translationid [xyz] which does not exist	Translation id was not found in translation table
ERROR: session-agent [id] has reference to out-translationid [xyz] which does not exist	Translation id was not found in translation table
ERROR: session-agent [id] has reference to in-manipulationid [xyz] which does not exist	Manipulation id was not found in manipulation table
ERROR: session-agent [id] has reference to out-manipulationid [xyz] which does not exist	Manipulation id was not found in manipulation table
ERROR: session-agent [id] has reference to enforcement-profile [xyz] which does not exist	Enforcement-profile was not found in enforcement-profile table
ERROR: session-agent [id] has reference to code-policy [xyz] which does not exist	Codec-policy was not found in codec-policy table
ERROR: session-agent [id] has reference to response-map [xyz] which does not exist	Response-map was not found in response map table
ERROR: session-agent [id] has reference to local-response-map [xyz] which does not exist	Response-map was not found in response map table

Session-Group

Error Text	Reason for Error
ERROR: session-group [id] has reference to session-agent [xyz] which does not exist	Session agent was not found in the session agent table

Session-Translation

Error Text	Reason for Error
ERROR: session-translation [id] has reference to rules [xyz] which does not exist	Translation rule was not found in the translation rule table

SIP-Config

Error Text	Reason for Error
ERROR: sip-config has reference to home-realm-id [xyz] which does not exist	Realm was not found in the realm-config table
ERROR: sip-config has reference to egress-realm-id [xyz] which does not exist	Realm was not found in the realm-config table
ERROR: sip-config has reference to enforcement-profile [xyz] which does not exist	Enforcement profile was not found in enforcement profile table
WARNING: sip-config is missing home-realm-id for SIP-NAT, defaults to [sip-internal-realm]	Missing home-realm-id, defaulted to sip-internal-realm
WARNING: sip-config home-realm-id [xyz] does not have a sip-interface	Sip-interface missing for the home realm
WARNING: sip-config has nat-mode set to [None], but there are configured sip-nat objects	Nat-mode needs to be set to either Public or Private if there are sip-nat objects in the configuration
ERROR: sip-config object is disabled	Sip-config is disabled, but there are configured sip-interface objects

SIP-Interface

Error Text	Reason for Error
ERROR: sip-interface [id] is missing realm-id entry	missing realm
ERROR: sip-interface [id] has reference to realm-id [xyz] which does not exist	realm was not found in realm-config table
ERROR: sip-interface [id] has reference to in-manipulationid [xyz] which does not exist	in-manipulationid was not found in manipulation table
ERROR: sip-interface [id] has reference to out-manipulationid [xyz] which does not exist	out-manipulationid was not found in manipulation table
ERROR: sip-interface [id] has reference to enforcement-profile [xyz] which does not exist	enforcement profile was not found in enforcement profile table
ERROR: sip-interface [id] has reference to response-map [xyz] which does not exist	response-map was not found in response-map table
ERROR: sip-interface [id] has reference to local-response-map [xyz] which does not exist	local-response-map was not found in response-map table
ERROR: sip-interface [id] has reference to constraint-name [xyz] which does not exist	constraint-name was not found in session constraint table
ERROR: sip-interface [id] has no sip-ports	sip-ports are missing
ERROR: sip-interface [id] with sip-port [id2] has reference to tls-profile [xyz] which does not exist	tls-profile was not found in TLS profile table (only valid for protocols TLS or DTLS)
ERROR: sip-interface [id] with sip-port [id2] has reference to ims-aka-profile [xyz] which does not exist	ims-aka-profile was not found in Ims-Aka-Profile table (valid for protocols other than TLS or DTLS)

Error Text	Reason for Error
WARNING: sip-interface [id] has no sip-ports, using SIP-NAT external-address	no sip-ports so SIP-NAT external-address is used
WARNING: sip-interface [id] has no valid sip-ports, using SIP-NAT external-address	no valid sip-ports so SIP-NAT external-address is used

SIP-Manipulation

Error Text	Reason for Error
ERROR: sip-manipulation [id] has no header-rules defined	Missing header rules
ERROR: sip-manipulation [id] with header-rule [xyz] is missing new-value entry	Missing new-value entry (checked only for action type sip-manip)
ERROR: sip-manipulation [id] with header-rule [xyz] has reference to new-value [zxy] which does not exist	New-value entry missing from the sip-manipulation table
ERROR: sip-manipulation [id] with header-rule [xyz] has new-value that refers to itself from sip-manipulation [di]	Looping reference between two objects

SIP-NAT

Error Text	Reason for Error
ERROR: sip-nat [id] is missing home-address entry	Missing home-address
ERROR: sip-nat [id] has invalid home-address [x] entry	Invalid home-address entry
ERROR: sip-nat [id] is missing ext-address entry	Missing ext-address
ERROR: sip-nat [id] has invalid ext-address [x] entry	Invalid ext-address entry
ERROR: sip-nat [id] is missing ext-proxy-address entry	Missing ext-proxy-address
ERROR: sip-nat [id] has invalid ext-proxy-address [x] entry	Invalid ext-proxy-address entry
ERROR: sip-nat [id] is missing user-nat-tag entry	Missing user-nat-tag
ERROR: sip-nat [id] is missing host-nat-tag entry	Missing host-nat-tag
ERROR: sip-nat [id] is missing domain-suffix entry	Missing domain-suffix
ERROR: sip-nat [id] is missing realm-id entry	Missing realm entry
ERROR: sip-nat [id] does not match sip-interface realm [xyz]	Sip-interface name was not found in realm table
ERROR: sip-nat [id] does not have a sip-interface	Sip-interface is missing
WARNING: sip-nat [id] has same user-nat-tag as sip-nat [di]	Duplicated user-nat-tag
WARNING: sip-nat [id] has same host-nat-tag as sip-nat [di]	Duplicated host-nat-tag
WARNING: sip-nat [id] has ext-address [x] which is different from sip-interface [di] sip-port address [y]	Sip-nat ext-address needs to be the same as sip-port address
ERROR: sip-nat [id] has same home-address [x] as sip-nat [di]	Duplicated home-address

Static-Flow

Error Text	Reason for Error
ERROR: static-flow [id] is missing in-realm-id entry	Missing in-realm-id
ERROR: static-flow [id] has reference to in-realm-id [xyz] which does not exist	Realm was not found in the realm-config table
ERROR: static-flow [id] is missing out-realm-id entry	Missing out-realm-id
ERROR: static-flow [id] has reference to out-realm-id [xyz] which does not exist	Realm was not found in the realm-config table
ERROR: ext-policy-server [id] has illegal protocol value [xyz]	Invalid protocol entry

Steering-Pool

Error Text	Reason for Error
ERROR: steering-pool [id] has invalid start-port [x]	Invalid start-port value (smaller than 1025)
ERROR: steering-pool [id] has start-port [x] greater than end-port [y]	Start-port value is greater than end-port value
ERROR: steering-pool [id] is missing realm entry	Missing realm entry
ERROR: steering-pool [id] has reference to realm [xyz] which does not exist	Realm [xyz] was not found in realm-config table
ERROR: steering-pool [id] has reference to network-interface [xyz] which does not exist	Network-interface [xyz] was not found in network-interface table

Surrogate-Agent

Error Text	Reason for Error
ERROR: surrogate-agent [id] is missing realm entry	Missing realm entry
ERROR: surrogate-agent [id] has reference to realm [xyz] which does not exist	Realm was not found in the realm-config table
ERROR: surrogate-agent [id] is missing customer-next-hop entry	Missing customer-next-hop entry
ERROR: surrogate-agent [id] is missing register-contact-user entry	Missing register-contact-user entry
ERROR: surrogate-agent [id] is missing register-contact-host entry	Missing register-contact-host entry

System-Config

Error Text	Reason for Error
ERROR: system-config has reference to default-gateway [xyz] which does not exist	gateway was not found in the network-interface table or boot parameters
ERROR: system-config collect has sample-interval [x] greater than push-interval	sample-interval greater than push-interval
ERROR: system-config collect has start-time [x] greater than end-time [y]	Start-time greater than end-time

Error Text	Reason for Error
ERROR: system-config collect has group [xyz] with sample-interval [x] greater than collection push-interval [y]	Group [xyz] has incorrect sample interval
ERROR: system-config collect has group [xyz] with start-time [x] greater than end-time [y]	Group [xyz] has incorrect sample interval
ERROR: system-config collect has no push-receivers defined	No push-receivers defined
ERROR: system-config collect has reference to push-receiver [xyz] which does not have user-name set	No user-name set
ERROR: system-config collect has reference to push-receiver [xyz] which does not have password set	No password set
ERROR: system-config collect has reference to push-receiver [xyz] which does not have address set	No address set
ERROR: system-config collect has reference to push-receiver [xyz] which does not have data-store set	No data-store set

TLS-Profile

Error Text	Reason for Error
ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not have any certificates	End-entity-certificate entry missing certificate or certificate-record is part of config, but record was not imported to the SD
ERROR: tls-profile [id] has end-entity-certificate [xyz] which has an end entry certificate, but the private key is invalid.	Bad private key for the cert-record
ERROR: tls-profile [id] has reference to end-entity-certificate [xyz] which does not exist	Certificate record was not found in cert-record table
ERROR: tls-profile [id] has an end-entity-certificate records without any end entity certificate	End certificate missing from all end-entity-certificate records or none of them where imported to the SD
ERROR: tls-profile [id] found an entry in the trusted-ca-certificates with zero length	Found an empty trusted-ca-record in the list
ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] which does not have any certificates	Trusted-ca-records entry missing certificate
ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] with PKCS7 structure which does not have any certificates	Trusted-ca-records entry with PKCS7 structure missing certificate
ERROR: tls-profile [id] has reference to trusted-ca-certificates [xyz] which does not exist	Certificate record was not found in cert-record table
ERROR: tls-profile [id] has no trusted-ca- certificates, but mutual-authentication is enabled	No trusted certificates, but enabled mutual-authentication

Other Verify Config Errors and Warnings

Error Text	Reason for Error
WARNING: [x] and [y] should not be run simultaneously as they may interfere with each other and lead to undefined behavior.	Two or more of these conflicting items have been activated: comm-monitor, packet-trace, call-trace and SIP Monitoring & Trace. Only one may be enabled at a time.

Viewing Configurations

While configuration archives describe a full Oracle Communications Session Border Controller configuration, you can not display them on the screen for quick reference. To view configurations through a local connection, there are two options.

1. To display the current configuration on the screen, type **show configuration** at a command prompt. You can add a specific configuration element after the show configuration command to display only that element on the screen.

   ```
   ORACLE> show configuration host-route
   host-routes
           dest-network                   10.0.0.0
           netmask                        255.255.0.0
           gateway                        172.30.0.1
   task done
   ORACLE>
   ```

2. To display the running configuration on the screen, type **show running-configuration** at a command prompt.

Checking Configuration Versions

The Oracle Communications Session Border Controller maintains a running count of the version of both the running configuration and current configuration. It can be helpful to know when the running and current configurations are out of sync.

While they can differ, the current configuration and the running configuration should generally be the same. After a configuration is modified, saved and activated, the current and running configuration versions should be the same.

To check the version of each configuration:

1. Type **display-current-cfg-version** at a command prompt to display the version number of the current configuration.

   ```
   ORACLE> display-current-cfg-version
   Current configuration version is 3
   ORACLE>
   ```

2. Type **display-running-cfg-version** at a command prompt to display the version number of the running configuration.

   ```
   ORACLE> display-running-cfg-version
   Running configuration version is 3
   ORACLE>
   ```

Deleting Configurations

You can completely delete the data in the last-saved configuration with one command. This can be useful if you want to reconfigure your Oracle Communications Session Border Controller starting with a blank configuration. You must reboot your Oracle Communications Session Border Controller after issuing the **delete-config** command to complete this task.

To delete the running and current configuration:

1. Type **delete-config** at a superuser command prompt. You will be prompted to confirm that you want to complete this task.

   ```
   ORACLE# delete-config
   ******************************************************
   Do you really want to ERASE the current config:? [y/n]?: y
   Deleting configuration
   NOTE: need to reboot for changes to take effect
   task done
   ```

2. Reboot the Oracle Communications Session Border Controller using the **reboot** command.

Configuration Checkpointing

In an HA configuration, configuration checkpointing copies all configuration activity and changes on one Oracle Communications Session Border Controllerto the other Oracle Communications Session Border Controller. Checkpointed transactions copy added, deleted, or modified configurations from the active system to the standby system. You only need to perform configuration tasks on the active Oracle Communications Session Border Controller because the standby SD will go through the checkpointing process and synchronize its configuration to the active Oracle Communications Session Border Controller to reflect activity and changes.

The **acquire-config** command is used to manually invoke configuration checkpointing between two Oracle Communications Session Border Controllers in an HA node.

To synchronize the systems in an HA node:

1. On either the active or standby Oracle Communications Session Border Controller, type **acquire-config** <IP address of other SD in HA pair>.

   - The IPv4 or IPv6 address for the Oracle Communications Session Border Controller from which to acquire the configuration.

   - For **acquire-config** to work, one rear interface on each SD must be named wancom1, and one rear interface on each SD must be named wancom2.

     ```
     ORACLE# acquire-config 10.0.1.8
     ```

2. Following the procedure defined directly above, confirm that the HA node now has synchronized configurations.

   ```
   ORACLE-1# display-current-cfg-version
   Current configuration version is 30
   ORACLE-1# display-running-cfg-version
   Running configuration version is 30
   ORACLE-2# display-current-cfg-version
   Current configuration version is 30
   ORACLE-2# display-running-cfg-version
   Running configuration version is 30
   ```

Realm-Specific Delete Command

The ACLI provides a way to delete a specific realm and the configurations (objects) associated with that realm. You use the **delete realm-specifics** command with the name of the realm you want to delete. Not only does the Oracle Communications Session Border Controller delete that realm, it also deletes the configurations where that realm is also used as a primary or foreign key—such as steering pools, session agents, and SIP interfaces. A complete list of configurations subject to deletion appears below.

The Oracle Communications Session Border Controller safeguards against unintentionally deleting configurations by showing you a complete list of the configurations it is about to delete, warns you that you are about to the delete the realm, and then asks you for confirmation. The list of candidates for deletion appears each with its key identifier so that you can more easily recognize it. You must type in a **y** for **yes** or **n** for **no** to move forward.

Despite these safeguards, you should use the **delete realm-specifics** command with the utmost care. Oracle recommends that only advanced users work with this command. In fact, the command appears in the configuration menu, to which only Superusers have access.

Deleted Configurations

This section provides a list of the configuration that use the name of realm either as a primary or as a foreign key. These are the configuration that you can remove from your configuration when you delete a specific realm.

ACLI Configuration Name	ACLI Parameter Value
access-control	realm-id
call-recording-server	primary-realm secondary-realm
dns-config	client-realm
enum-config	realm-id
ext-policy-server	realm
h323, h323-stack	realm-id
lawful-intercept	(associated parameters; specified in Oracle LI support documentation)
local-policy	source-realm
realm-config	identifier
session-agent	realm-id
sip-features	realm
sip-interface	realm-id
sip-nat	realm-id
static-flow	in-realm-id out-realm-id
steering-pool	realm-id
surrogate-agent	realm-id

There are configurations (objects) that use realms but do not reference them directly either as a primary or foreign key. The Oracle Communications Session Border Controller does not delete these configurations when you use the **delete realm-specifics** command:

- media-policy

- class-policy
- translation-rules
- sip-manipulation

> **Note:**
>
> This command cannot delete realms associated with network management control configurations.

Deleted Parameter Values

For other configurations that reference realms, only the parameters containing realm identifiers are cleared while the object as a whole remains. By confirming you want to delete the realm, the Oracle Communications Session Border Controller clears the parameters set out in this section, the Oracle Communications Session Border Controller informs you of the configuration object and the parameter within it that will be affected.

The following table shows you which parameters are cleared.

ACLI Configuration Name	ACLI Parameter Value(s)
dns-config	server-realm
local-policy	source-realm next-hop realm
media-manager	home-realm-id
realm-config	parent-realm dns-realm ext-policy-svr
realm-group	source-realm destination-realm
session-agent	egress-realm
session-group	dest
sip-config	egress-realm-id home-realm-id

Deleted Parameter Configuration

This section shows you how to use the **delete realm-specifics** command. Remember that you need to be in Superuser mode to use it.

To use the **delete realm-specifics** command, you need to know the identifier for the realm (and the other configurations associated with the realm) that you want to delete.

These instructions and examples do not include information for parameters that will be emptied for configurations that will otherwise be left intact. This information will appear in the following form: <attribute> <attribute value> removed from <object name/configuration name> with key <key value>.

To delete a specific realm and its associated configurations:

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

```
ORACLE# configure terminal
ORACLE(configure)#
```

2. Type delete realm-specifics, a Space, and the name of the realm you want deleted. The press Enter.

   After you press Enter, the system displays a list of all configurations on which the deletion will have an impact. It also warns you that you are about to delete the realm.

```
ORACLE(configure)# delete realm-specifics peer_1
RealmConfig with key identifier=peer_1 will be deleted
SteeringPool with key ip-address=192.168.0.11 start-port=21000 realm-
id=peer_1 w
ill be deleted
SessionAgent with key hostname=127.0.0.11 will be deleted
SipInterface with key realm-id=peer_1 will be deleted
SipNatConfig with key realm-id=peer_1 will be deleted
WARNING: you are about to delete the realm!
Delete the realm? [y/n]?:
```

3. At the end of the display, the system asks you to confirm (by typing a **y**) or abort (by typing an **n**) the deletion.

```
Delete the realm? [y/n]?: y
```

   If you confirm the deletion, the system will list all of the configurations that have been removed.

```
RealmConfig with key identifier=peer_1 deleted
SteeringPool with key ip-address=192.168.0.11 start-port=21000 realm-
id=peer_1 d
deleted
SessionAgent with key hostname=127.0.0.11 deleted
SipInterface with key realm-id=peer_1 deleted
SipNatConfig with key realm-id=peer_1 deleted
ORACLE(configure)#
```

   When you abort the deletion, the Oracle Communications Session Border Controller will return you to the ORACLE(configure)# system prompt.

System Prompt Indicator

Using the **prompt-enabled** command, you can enable a system prompt indicator to show you when a configuration requires saving and activation.

The system informs you should a configuration has been changed and you have 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 prompted prefixes one asterisk (*). This command allows you to decide whether or not you want the system to give this prompt. To clarify:

- **—Requires save and activate

- *—Configuration saved, but requires activate

This feature is disabled by default.

Configuration File Format

The functionality described in this section is of interest only to those users running a 6.3x software version which pre-dates S-C630F1 who want to downgrade to an earlier release. Other users can safely ignore this section.

Configuration files, referred to as config files, are stored in XML format. Releases prior to C630F1 saved certain special characters in a non-standard XML format. From release C630F1 and forward, these characters are saved in formats compliant with current W3C XML standards. Character formats are shown below.

Character	Standard XML C63F1 (and after)	Non-Standard XML Pre C63F1
ASCII hard tab	&#xp;	value 0x9
ASCII line feed	&#xA;	value 0xA
ASCII carriage return	&#xD;	value 0xD
Ampersand	&amp;	&
Less than	&lt;	<
Greater than	&gt;	>
Double quote	&quote;	"
Single quote	&apos;	'

By default config files are now saved using standard XML coding. Consequently pre-C630F1 software images are unable to parse such config files, complicating the software downgrade process.

To address these complications, the **save-config** and **backup-config** ACLI commands has been enhanced to allow the saving of config files and backup configuration files in either standard XML or legacy, non-standard XML format.

save-config ACLI Command

By default, config files are saved in standard XML format that is non-parsable by a pre-C63F1 software image.

```
ORACLE# save-config
checking configuration
-------------------------------------------------------------------
Results of config verification:
2 configuration warnings
Run 'verify-config' for more details
--------------------------------------------------------------------
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
ORACLE# verify-config
```

```
---------------------------------------------------------------------
WARNING: security-policy [SP] local-ip-addr-match has 0.0.0.0. This is an
acceptable configuration if intended.
WARNING: security-policy [SP] remote-ip-addr-match has 0.0.0.0. This is an
acceptable configuration if intended.
---------------------------------------------------------------------
Total:
2 warnings
ORACLE#
```

save-config, when used in conjunction with a newly supported argument, **standard**, also saves config files in standard XML format that is non-parsable by a pre-C63F1 software image.

```
ORACLE# save-config standard
checking configuration
--------------------------------------------------------------------
Results of config verification:
2 configuration warnings
Run 'verify-config' for more details
---------------------------------------------------------------------
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
ORACLE# verify-config
---------------------------------------------------------------------
WARNING: security-policy [SP] local-ip-addr-match has 0.0.0.0. This is an
acceptable configuration if intended.
WARNING: security-policy [SP] remote-ip-addr-match has 0.0.0.0. This is an
acceptable configuration if intended.
---------------------------------------------------------------------
Total:
2 warnings
ORACLE#
```

save-config, when used in conjunction with a newly supported argument, **non-standard**, saves config files in legacy XML format that is parsable by a pre-C63F1 software image.

```
ORACLE# save-config non-standard
checking configuration
--------------------------------------------------------------------
Results of config verification:
2 configuration warnings
Run 'verify-config' for more details
---------------------------------------------------------------------
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
```

```
ORACLE# verify-config
---------------------------------------------------------------------
WARNING: security-policy [SP] local-ip-addr-match has 0.0.0.0. This is
an acceptable configuration if intended.
WARNING: security-policy [SP] remote-ip-addr-match has 0.0.0.0. This
is an acceptable configuration if intended.
---------------------------------------------------------------------
Total:
2 warnings
ORACLE#
```

backup-config ACLI Command

By default, backup config files are saved in standard XML format that is non-parsable by a pre-C63F1 software image.

```
ORACLE# backup-config testBU
task done
ORACLE#
```

backup-config <filename> standard also saves backup config files in standard XML format that is non-parsable by a pre-C630F1 software image.

```
ORACLE# backup-config standardBU standard
task done
ORACLE#
```

backup-config <filename> non-standard saves backup config files in legacy XML format that is parsable by a pre-C63F1 software image.

```
ORACLE# backup-config nonStandardBU non-standard
task done
ORACLE#
```

> **Note:**
>
> The standard and non-standard optional arguments are not supported by the backup-config <filename> saved command, which takes the last saved version of config (whatever the XML format), and saves a copy of that file as the backup.

Moving a Configuration

This section outlines a process for moving an existing Oracle Communications Session Border Controller configuration to a new system. Process summary:

1. Create a backup configuration file on the source Oracle Communications Session Border Controller.

2. Using SFTP, copy the source backup from the source to the destination Oracle Communications Session Border Controller .
3. Restore the newly-transferred backup on the target Oracle Communications Session Border Controller.

Backup Commands

The Oracle Communications Session Border Controller software includes a set of commands for easily working with backup configurations. These commands are **backup-config**, **display-backups**, **delete-backup-config**, **restore-backup-config**.

To back up a configuration, use the **backup-config** command. You can confirm that your backup has been created with the **display-backups** command. When the **backup-config** command is executed, the system checks for sufficient resources to complete the operation. If resources are sufficient, the system creates the backup. If resources are insufficient, the task is not completed and the system displays the limiting resources and recommends completing the task at another time.

Backups are created as gzipped files in a .gz format. They are stored in the /code/bkups directory.

Backing up the current configuration

To create a backup:

- In superuser mode, use the **backup-config** command followed by a descriptive filename for the backup you are creating.

```
ORACLE#backup-config 02_Feb_2008
task done
ORACLE#
```

Listing Backups

You can view the backups available on your system using the **display-backups** command.

To list available backup configurations:

- In Superuser mode, enter the **display-backups** command. A list of available backup files from the `/code/bkups` directory is displayed on the screen.

```
ORACLE# display-backups
test_config.gz
test-config.gz
runningcfgtest.gz
runningtest_one.gz
BACK_UP_CONFIG.gz
02_Feb_2008.gz
01_Feb_2008.gz
ORACLE#
```

Copy the Backup to the destination

Send the backup configuration file by way of SFTP from the source to destination Oracle Communications Session Border Controller.

To copy a backup configuration from the source to destination Oracle Communications Session Border Controller:

1. Use an SFTP client to connect to the SBC. The management IP address is configured in the bootparams.
2. Change directory to where you want to upload a file.
   - cd /code/bkups for backup configurations
3. Type bin and press Enter to force the SFTP program into binary mode.
4. Upload the file you want to transfer by typing the filename and pressing Enter.

```
C:\Documents and Settings>sftp 172.30.55.127
Connected to 172.30.55.127.
220 VxWorks (1.0) FTP server ready
User (172.30.55.127:(none)): user
331 Password required
Password:
230 User logged in
sftp> cd /code/bkups
250 Changed directory to "/code/bkups"
sftp> bin
200 Type set to I, binary mode
sftp> put 02_Feb_2008.gz
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
sftp: 9587350 bytes sent in 51.64Seconds 185.65Kbytes/sec.
sftp>
```

Restoring Backups

To restore a backup configuration on the Oracle Communications Session Border Controller:

1. In Superuser mode, enter the **restore-backup-config** command followed by the backup filename you want to restore to the current configuration. You must explicitly name the backup file you want to restore, including the file extension

```
ORACLE# restore-backup-config 02_Feb_2008.gz
Need to perform save-config and activate/reboot activate for
changes to take effect...
task done
ORACLE#
```

2. Correct the Virtual MAC address configuration established on the former device to be suitable for the new device.

Establish the base MAC needed for HA operation by, first, determining the base MAC by way of the ethernet address value of the show media physical command.

```
ORACLE#show media physical
s0p0 (media slot 0, port 0)
     Flags: UP BROADCAST MULTICAST ARP RUNNING
     Type: ETHERNET_CSMACD
     Admin State: enabled
     Auto Negotiation: enabled
…
     Ethernet address is 00:08:25:01:08:44
```

Apply the formula for calculating virtual MAC addressing to the MAC addressing used for this system. This formula is described in the ACLI Configuration Guide.

Configure the physical interfaces with the computed virtual MAC addressing. Refer to the following command line sequence as an example of this procedure.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# phy-interface
ORACLE(phy-interface)# select
<name>:
1: s0p0
2: s1p0
selection: 1
ORACLE(phy-interface)# virtual-mac 00:08:25:01:08:48
ORACLE(phy-interface)# done
phy-interface
        name                           s0p0
        operation-type                 Media
        port                           0
        slot                           0
        virtual-mac                    00:08:25:01:08:48
```

3. Save the configuration.

```
ORACLE# save-config
```

4. Activate the configuration.

```
ORACLE# activate-config
```

7

Managing Backups and Archives

Introduction

The Oracle Communications Session Border Controller can concatenate the full system configuration into a single backup file and also archive log files. You can perform a set of actions on backup files or archived log files, such as saving, backing up, listing, and deleting the files.

To save disk space, the Oracle Communications Session Border Controller has archiving features that use the standard tar and gzip utilities. Archiving lets you easily change, move, store, and back up the system's log files. After a log file has been archived, it can be transferred to a remote host. The Oracle Communications Session Border Controller has a set of file manipulation commands that you can apply only to archive files.

Using the **backup** command enables you to successfully save and restore an existing configuration. The major difference between backup and archive files is that backup commands are used for configurations and log archive commands are used with log files.

Backup Commands

The Oracle Communications Session Border Controller includes a set of commands for easily working with backup configurations. These commands are **backup-config**, **display-backups**, **delete-backup-config**, **restore-backup-config**.

Oracle suggests that you back up properly functioning configurations on your system before making any new major configuration changes. The backup configurations are crucial to have when configuration changes do not function as anticipated and a rollback must be applied immediately.

To back up the system configuration, use the **backup-config** command. You can confirm your backup has been created with the **display-backups** command. When the **backup-config** command is executed, the system checks if sufficient resources exist to complete the operation. If resources are sufficient, the system creates the backup. If resources are insufficient, the task is not completed and the Oracle Communications Session Border Controller instead displays the limiting resources, recommending that the task be completed at another time.

Backups are created as gzipped files in a .gz format. They are stored in the /code/bkups directory on the Oracle Communications Session Border Controller.

Creating Backups

To create a backup :

- In the ACLI at the superuser prompt, enter the **backup-config <filename> [editing | running]** command. Enter **backup-config** followed by a descriptive filename for the backup you are creating. You can also enter an optional argument to specify whether you want to create a backup from the editing configuration cache or the running configuration cache.

```
ORACLE# backup-config 01_Feb_2005_Test running
task done
ORACLE#
```

Listing Backups

To list available backup configurations:

- In the ACLI at the superuser prompt, enter the **display-backups** command. A list of available backup files from the /code/bkups directory is displayed on the screen.

  ```
  ORACLE# display-backups
  test_config.gz
  test-config.gz
  runningcfgtest.gz
  runningtest_one.gz
  BACK_UP_CONFIG.gz
  02_Feb_2005.gz
  01_Feb_2005_Test.gz
  ORACLE#
  ```

Restoring Backups

To restore a backup configuration:

- In the ACLI at the superuser prompt, enter the **restore-backup-config <filename> [running | saved]** command. Enter **restore-backup-config** followed by the backup filename you wish to restore to the current configuration. You must explicitly name the backup file you wish to restore, including the file extension. You can also enter an optional argument to specify whether you want to restore the last running configuration or the last saved configuration on the Oracle Communications Session Border Controller.

  ```
  ORACLE# restore-backup-config backup_file.gz saved
  Need to perform save-config and activate/reboot activate for
  changes to take effect...
  task done
  ORACLE#
  ```

  You can restore files from either .tar.gz format or just .gz. All backup files are gzipped in the .gz format.

  You must still save and activate the configuration or reboot the Oracle Communications Session Border Controller to apply the backup configuration.

Deleting Backups

The **delete-backup-config** command deletes the backup configurations from the /code/bkups directory on your system.

- In the ACLI at the superuser prompt, enter the **delete-backup-config** command, followed by the backup file you wish to delete.

```
ORACLE# delete-backup-config FEB_BACKUP.gz
task done
ORACLE#
```

Viewing Backup Configurations

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

- In the ACLI at the superuser prompt, enter the show backup-config command followed by the backup configuration filename you want to view.

```
ORACLE# show backup-config
```

The configuration of the backup file you specify is displayed on the screen. The contents of this output are in the same format as the **show configuration** command. For example:

```
ORACLE# show backup-config
Possible configuration files are:
0606_HMRSIPNAT_Overlay.gz
0606_HMRSIPPeering.gz
0605_SingleSIPNATH_in_access.gz
0605_SingleSIPNATHTN_ABBN.gz
0605_SNB_ABBN.gz
HMR_OAI_config.gz
0619_HMR_OAI.gz
```

Archive Commands

Creating Archives

You can create archives of log files. Creating log archives requires a unique procedure described below.

File Locations

The following table lists source and destination directories used with archive functions.

Configuration Type	Source Directory	Destination Directory
Log	/opt/logs	/opt/archives

Log File Archives

To create an archive that contains all log files on the Oracle Communications Session Border Controller:

1. Enter the archives shell by typing **archives** at the topmost ACLI level while in superuser mode.

```
ORACLE# archives
ORACLE(archives)#
```

2. Type **create LOGS,** followed by a name for the archive file. The Oracle Communications Session Border Controller will pause while it completes the task and alert you when the task has completed.

```
ORACLE(archives)# create LOGS All_Logs_27_Feb
task done
ORACLE(archives)#
```

Listing Archives

To display a list of the archived log files:

1. Enter the archives shell by typing **archives** at the topmost ACLI level while in superuser mode.

```
ORACLE# archives
ORACLE(archives)#
```

2. Type **display LOGS** to view the available log files.

```
ORACLE(archives)# display LOGS
testlogs1.tar
log.algdd.tar
bluff1.tar
log.mbcd.tar
log.lemd.tar
log.sipd.tar.gz
log.NOTTESTING.sipd.tar
sipd.log.tar.gz
ORACLE(archives)#
```

Deleting Archives

To delete archived log files:

1. Enter the archives shell by typing **archives** at the topmost ACLI level while in superuser mode.

```
ORACLE# archives
ORACLE(archives)#
```

2. Type **delete LOGS,** followed by the filename of the log file to delete.

```
ORACLE(archives)# delete LOGS sipd.log.tar.gz
ORACLE(archives)#
```

Renaming Archives

To rename archived log files:

1. Enter the archives shell by typing **archives** at the topmost ACLI level while in superuser mode.

   ```
   ORACLE# archives
   ORACLE(archives)#
   ```

2. Type **rename LOGS**, followed by the full filename of the old log file, and then the new filename without an extension.

   ```
   ORACLE(archives)# display LOGS
   log.sipd.tar.gz
   ORACLE(archives)# rename LOGS log.sipd.tar.gz backup_log.sipd
   ORACLE(archives)# display LOGS
   backup_log.sipd.tar.gz
   ORACLE(archives)#
   ```

   The newly renamed file remains in the same directory.

Viewing Free Space

The **check-space-remaining** command checks the free space in the boot directory, code (flash memory), and other devices. Type a ? at the command to see all valid values. This command displays the total number of bytes free and total number of bytes available on the specified device. Each volume is used in the following way:

- /boot—A flash memory partition used primarily for system boot images and the bootloader image.
- /code—A flash memory partition used to store archives and data that needs to be persistent across reboot.

- In the ACLI at the superuser prompt, enter the **check-space-remaining** command followed by the device you want to check the space on. Valid devices are **boot**, **code**, **opt**. All examples of this command are shown below.

  ```
  ORACLE# check-space-remaining boot
  boot: 29759488/29760512 bytes (99%) remaining
  ```

8

File System Maintenance

Local File System

The file system consists of 2 essential volumes and 1 or more user-defined volumes.

Acme Packet engineered systems maintain `/boot` and `/code` partitions that are each 2 GB. These volumes are located on the same internal 4GB flash drives. Once a storage device is installed in the system, the `/opt` and `/opt/crash` volumes are moved there.

With SFTP, only the local admin account can read, write, and list the contents of the `/boot` directory. If other supplementary administrators need to upload boot images with SFTP, they can upload to the `/code/images` directory.

- `/opt` is located on the first system partition and is always 8 GB. Although it can be used for many purposes, it is primarily intended for core dumps, log files, CDRs, and HDR data.
- `/opt/crash` is located on the second system partition. It appears as just `/crash`. It is the remainder of the storage device with an 8GB minimum. `/opt/crash` is used for crash files.

Default Paths

The **show platform paths** command displays the default paths for system files. For example:

```
ORACLE# show platform paths
Filesystem paths
----------------
boot            : /boot/
code            : /code/
base            : /opt/
crash           : /opt/crash
logs            : /opt/logs/
tar config      : /code/config/
gz config       : /code/gzConfig/
backups         : /code/bkups/
import          : /code/imports/
temp            : /opt/tmp/
collect         : /opt/collect/
running ver     : /code/runVer.dat
config ver      : /code/configVer.dat
running data    : /opt/running/
editing data    : /opt/data/
SPL files       : /code/spl/
SPL bytecode    : /opt/spl/
```

File System Management

The Oracle Communications Session Border Controller provides you with tools to manage the file system.

Identifying File System Volumes

You can identify partitions on the file system with the **show space** command. In addition, free and used space are reported. This command is entered as follows:

```
show space < boot | code | system-disk | data-disk | hard-disk >
```

Where

- boot - the /boot partition
- code - the /code partition
- system-disk - all system partitions, including /opt and /opt/crash
- data-disk - all user partitions that mount under /mnt
- hard-disk - all partitions

Formatting the File System

The storage device format scheme is dependent on the drive’s size. With a large storage device, you can accept the file system’s default partition configuration, or you can create your own scheme. The formatting plan differs based on the internal storage device being less than or equal to 40 GB or greater than 40 GB.

40GB or Less Format Plan

When formatting a 40 GB or smaller storage device, no data partitions are created. The default partitioning scheme is as follows:

Table 8-1 System Default Format Plan (40 GB max):

Location	Volume Name	Volume Size
system partition	/opt	8 GB
system partition	/opt/crash	32 GB

40GB or More Default Format Plan

When formatting a storage device larger than 40 GB, /mnt/sys and /mnt/app volumes are created in the data partition. Their relative sizes are based on the drive’s size.

Table 8-2 System Format Plan (40 GB +):

Volume Number	Volume Name	Volume Size
system partition	/opt	8 GB

Table 8-2 (Cont.) System Format Plan (40 GB +):

Volume Number	Volume Name	Volume Size
system partition	/opt/crash	2 x RAM size (not less than 8 GB)
data partition	/mnt/sys	20% remaining space
data partition	/mnt/app	80% remaining space

40GB or More Custom Format Plan

You can customize the format plan when a storage device larger than 40 GB is installed in your system. Before formatting the storage device, plan the number of volumes, volume names, and relative percentage of storage device disk space. A maximum of 4 volumes in the data partition are allowed.

Table 8-3 Custom System Format Plan (40 GB +):

Volume Number	Volume Name	Volume Size
systempartition	/opt	8 GB
system partition	/opt/crash	2 x RAM size (not less than 8 GB)
data partitions	/mnt/<user-label>	user-defined percentage of remaining space

Note:

Oracle recommends creating a single mount point for data partitions, such as `/mnt/app`, and then using subfolders for specific purposes, such as `/mnt/app/HDR` or `/mnt/app/CDR`.

Caution:

Creating a folder directly under `/mnt` without first formatting a partition is not supported and likely to result in data loss. Use the `format` command to create mount points.

Formatting Procedure

Formatting a hard drive should always be an offline activity. Prior to formatting the hard drive, back-up the configuration, delete the configuration, and reboot. Additionally, no external network connections should be active as the format procedure is executed.

The **format** command requires one of the following arguments:

- system-disk — formats and creates the 2 system partitions: /opt and /opt/crash
- data-disk — formats and creates 1 or more data partitions with the default (/mnt/sys and /mnt/app) or user-defined volumes

- hard-disk — formats and creates both the system partition and data partition

After the drive(s) are formatted, the system mounts the newly created partitions.

Note:

Ensure that no application traffic flows over the Oracle Communications Session Border Controller when you format the disk.

Note:

The format command may only be executed if certain tasks like local CDR and HDR generation are not active. Remove any boot time configuration for these features and reboot the system before attempting to format the hard-disk.

The following example shows the format command process.

```
ORACLE# format hard-disk
WARNING: Please ensure device is not currently in use by any
applications before proceeding
Continue [y/n]?: y
The following system partitions will now be created:
1: /opt             8000000 bytes
2: /crash           16218284032 bytes
Create the system partitions and filesystems as configured above [y/
n]?: y
******************************************************
WARNING: All system logs and data on the disk will be
permanently erased and unrecoverable.
Are you sure [y/n]?: y
The format process will take a few minutes. Once
the format process begins, it cannot be stopped.
Please do not power down or reboot the system until
the format process is complete.
Continue [y/n]?: y
Suspending logging to hard disk
Stopping tLogCleaner task
Relocating logging onto RAM drive
Initializing /opt/ Cleaner
Starting tLogCleaner task
*** Removing previous system partitions - please wait ***
*** Creating new system partitions - please wait ***
*** Formatting partition /opt. Please wait... ***
[...]
This filesystem will be automatically checked every 23 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
*** Formatting completed successfully ***
*** Formatting partition /crash. Please wait... ***
[...]
This filesystem will be automatically checked every 31 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

```
*** Formatting completed successfully ***
e2fsck 1.41.14 (22-Dec-2010)
opt: clean, 11/1960 files, 1323/7812 blocks
e2fsck 1.41.14 (22-Dec-2010)
crash: clean, 11/991232 files, 104681/3959542 blocks
```

This section of the format hard-drive walk-through shows the data partition creation. The following system output shows that the user has chosen to define a custom data partition scheme by typing n at the **Use factory default data partitions [y/n]?:** prompt.

```
Suspending logging to RAM drive
Stopping tLogCleaner task
Relocating logging onto hard disk
Initializing /opt/ Cleaner
Starting tLogCleaner task
Disk space used by system:
        16226317824 bytes
Use factory default data partitions [y/n]?: n
Enter the number of data partitions to create: 3
Total unallocated space = 100 %
Enter the name of volume 1 (or 'q' to quit): VOLUME1
Enter the size of the volume (in %): 20
Total unallocated space = 80 %
Enter the name of volume 2 (or 'q' to quit): VOLUME2
Enter the size of the volume (in %): 40
Total unallocated space = 40 %
Enter the name of volume 3 (or 'q' to quit): VOLUME3
Enter the size of the volume (in %): 40
The following data partitions will now be created:
/VOLUME1  96776308838 bytes
/VOLUME2  193552617676 bytes
/VOLUME3  193552617676 bytes
Create the data partitions and filesystems as configured above [y/n]?: y
******************************************************
WARNING: All non-system data on the disk will be
permanently erased and unrecoverable.
Are you sure [y/n]?: y
The format process will take a few minutes. Once
the format process begins, it cannot be stopped.
Please do not power down or reboot the system until
the format process is complete.
Continue [y/n]?: y
*** Beginning format process ***
*** Removing previous data partitions - please wait ***
*** Creating new data partitions - please wait ***
*** Formatting partition /VOLUME1. Please wait... ***
mke2fs 1.41.14 (22-Dec-2010)
[...]
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
This filesystem will be automatically checked every 37 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
*** Formatting completed successfully ***
*** Formatting partition /VOLUME2. Please wait... ***
mke2fs 1.41.14 (22-Dec-2010)
[...]
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
This filesystem will be automatically checked every 23 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
*** Formatting completed successfully ***
*** Formatting partition /VOLUME3. Please wait... ***
mke2fs 1.41.14 (22-Dec-2010)
[...]
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
This filesystem will be automatically checked every 31 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
*** Formatting completed successfully ***
*** Format finished successfully
New partitions have been created ***
*** Mounting partitions ***
e2fsck 1.41.14 (22-Dec-2010)
VOLUME1: clean, 11/5914624 files, 418265/23626953 blocks
/VOLUME1 mounted
e2fsck 1.41.14 (22-Dec-2010)
VOLUME2: clean, 11/11821056 files, 789884/47254150 blocks
/VOLUME2 mounted
e2fsck 1.41.14 (22-Dec-2010)
VOLUME3: clean, 11/11821056 files, 789884/47253628 blocks
/VOLUME3 mounted
```

Mounting and Unmounting Filesystems

You may unmount and stop the file system with the **unmount** command. Unmounting a file system is required to resize user partitions or replace a storage device. Prior to issuing this command you must disable user-initiated tasks that access the target volume. An example of a task which writes to disk is local CDR creation. Task log files generation is automatically halted. The **unmount** command is entered as follows:

```
unmount <data-disk | system-disk | hard-disk>
```

Where each of the arguments corresponds to the format command.

- system-disk — unmount 2 system partitions: /opt and /opt/crash
- data-disk — unmount the 1 or more data partitions containing the default (/mnt/sys and /mnt/app) or user-defined volumes
- hard-disk — unmounts both the system partition and data partition

For example:

```
ORACLE# unmount data-disk
WARNING: Please ensure device is not currently in use by any
applications before proceeding
```

```
Continue [y/n]?: y
/VOLUME1 unmounted
/VOLUME2 unmounted
/VOLUME3 unmounted
ORACLE# show space hard-disk
ORACLE# unmount system-disk
WARNING: Please ensure device is not currently in use by any applications
before proceeding
Continue [y/n]?: y
Suspending logging to hard disk
Stopping tLogCleaner task
Relocating logging onto RAM drive
Initializing /opt/ Cleaner
Starting tLogCleaner task
ORACLE#
```

You may mount and start the file system with the **mount** command. Mounting the file system is required to bring the storage device volumes back online after they have been unmounted. The **mount** command is entered as follows:

```
mount <data-disk | system-disk | hard-disk>
```

Where each of the arguments corresponds to those used in the format command.

- system-disk — mount 2 system partitions: /opt and /opt/crash
- data-disk — mount the 1 or more data partitions containing the default (/mnt/sys and /mnt/app) or user-defined volumes
- hard-disk — mounts both the system partition and data partition

For example:

```
ORACLE# mount system-disk
Suspending logging to ramdrive
Stopping tLogCleaner task
Relocating logging onto hard disk
e2fsck 1.41.14 (22-Dec-2010)
opt: clean, 60/488640 files, 67799/1953125 blocks
Initializing /opt/ Cleaner
Starting tLogCleaner task
e2fsck 1.41.14 (22-Dec-2010)
crash: clean, 11/991232 files, 104681/3960320 blocks
ORACLE#
```

Setting Storage to Read-Only

If SBC storage becomes inaccessible during operation, such as during a host to NAS connection fault, the SBC may mark the file systems as read-only to prevent data loss and journal corruption. Restart the affected virtual machine after you have corrected the host fault so that the SBC can return the file system to read/write mode.