Oracle® Communications Session Border Controller

Release Notes
Release S-CZ7.2.0

December 2016

ORACLE®

Contents

Preface

About this Guide

Overview

The Oracle Communications Session Border Controller Release Notes provides the following information when applicable:

- An overview of the new features available
- An overview of the interface enhancements
- A summary of known issues and caveats

If any of these sections does not appear in the document, then there were no changes to summarize in that category for that specific release.

Supported Platforms

Release Version S-CZ7.2.0 is supported on the Acme Packet 3820, 4500, 6100, and 6300 series platforms.

Related Documentation

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

Document Name	Document Description
Acme Packet 4500 Hardware Installation Guide	Contains information about the components and installation of the AP4500.
Acme Packet 3820 Hardware Installation Guide	Contains information about the components and installation of the AP 3800.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the AP 6300.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the AP 6100.
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 Oracle Communications Session Border Controller.

Document Name	Document Description
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 Oracle Communications Session Border Controller logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the Oracle Communications Session Border Controller's accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the Oracle Communications Session Border Controller's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the Oracle Communications Session Border Controller's support for its Administrative Security license.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the Oracle Communications Session Border Controller family of products.

Revision History

This section contains a revision history for this document.

Date	Description
June 2014	Initial release
July 2014	• Corrects MSRP Platform Support • Updates Rf Event ACR Generation description to include REGISTER messages • Updates TLS 1.1 and 1.2 Support section to exclude MSRP support • Updates Wildedcarded Public User Identity feature description • Updates Diameter Message Manipulation feature description to exclude Rf messaging
November 2014	• Details how to identify compatible ETCv1 cards • Clarifies when to upgrade QoS FPGA image on applicable NIUs
June 2014	• Updates NIU and Feature Group Requirements section to indicate IPv4-only support for QoS on certain platforms
April 2015	• Updates Known Issues section • Updates Platform Support section • Adds Behavioral Changes section • Adds a note that for an Acme Packet 3820/4500, if you have an NIU with transcoding, and you update to release S-CZ7.2.0 or higher, you must also have a high-speed fan module in the chassis

Date	Description
May 2015	• Adds CDR Record date format change
November 2015	• Adds Caveat and amends Known Issue to clarify that the Web GUI and SIP Monitor and Trace features are not supported in this release.
December 2015	• Adds note of Source routing deprecation to Caveats section.
March 2016	• Adds changes from S-CX6.4.0 to the section Application SNMP changes
June 2016	• Update Accounting-request-number AVP; it is compliant with RFC 3588 • Adds known issue on addressing that must not be used for HA deployments that include transcoding cards • Diameter and CDR in HA pair: upgrade of standby will not sync and thus will go out of service. Workaround available
December 2016	• Adds Session Router defect • Adds SSH output defect

1

Introduction to S-CZ7.2.0

The Oracle Communications Session Border Controller S-CZ7.2.0 Release Notes provide the following information about this product:

- Supported platforms and hardware requirements
- An overview of the new features available in this release
- An overview of previously-available features that are new to the GA of this major release
- A summary of changes the Oracle Communications Session Border Controller interfaces including the ACLI, MIB Support, and accounting interfaces.
- Caveats and Known Issues

Platform Support

The following platforms are supported by S-CZ7.2.0:

- Acme Packet 3820
- Acme Packet 4500
- Acme Packet 6100
- Acme Packet 6300

Acme Packet 3820 and 4500 CPU Support

- All versions of the 32-bit Acme Packet 3820 CPU are supported.
- Only the 64-bit CPU 2 on the Acme Packet 4500 is supported. The Acme Packet 4500's CPU revision must be MOD-0026-xx. Systems containing MOD-0008-xx are unsupported. You may query this with the **show prominfo cpu** command.

Acme Packet 3820 and 4500 Transcoding NIU Support

Acme Packet 3820/4500 chasses with a transcoding NIU upgrading to S-CZ7.2.0 and above must have a high-speed fan module to avoid overheating problems.

Image and Bootloader File Conventions

The AP4500, AP 6100, and AP6300 should be provisioned with the 64-bit Oracle Communications Session Border Controller image file in the boot parameters. 64-bit image files are recognized by the "64" between the image revision and file extension. e.g., nnSCZ720.64.bz . The AP3820 should be provisioned with a 32-bit Oracle Communications

Session Border Controller image file in the boot parameters. 32-bit image files are recognized by the "32" between the image revision and file extension. e.g., nnSCZ720.32.bz .

All platforms require that you install a stage 3 bootloader. The Stage 3 bootloader is identified by ending with a `.boot` extension. Stage 3 bootloaders and system image files have identical name portions of the filename, and are distributed together. For this software the GA system image and Stage 3 bootloader are `nnSCZ720.64.bz` and `nnSCZ720.boot` respectively.

Bootloader Requirements

AP3820 and AP4500 Bootloaders

The AP 3820 and AP 4500 require Stage 1, Stage 2, and Stage 3 bootloaders.

Stage 1 and Stage 2 bootloaders should be dated no earlier than July 3, 2013 (MOS patch # 18185632) . Use the **show version boot** command to view current bootloader version on your system.

Stage 1 and Stage 2 bootloader updates are available on My Oracle Support listed under the respective hardware.

The Stage 3 bootloader accompanies the OCSBC image file, as distributed. It should be installed according to the instructions found in the Maintenance and Troubleshooting Guide.

AP6100 and AP6300 Bootloaders

AP6100 and AP6300 require a Stage 3 bootloader that accompanies the OCSBC image file, as distributed. It should be installed according to the instructions found in the Maintenance and Troubleshooting Guide.

NIU and Feature Group Requirements

This section includes tables that list the feature groups that require specific NIUs for all hardware platforms.

Table 1: AP4500 NIU and Feature Group Support Matrix

S-CZ7.2.0 supports the NIUs listed in the left column on the AP4500. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA	SRTP	QoS	Transcoding	MSRP B2BUA
Clear (RJ45)	✗	✗	✗	✗	✗	✗
Clear (SFP)	✗	✗	✗	✗	✗	✗
ETCv1	✓	✓	✓	✓	✗	✓
ETCv2	✓	✓	✓	✓	✗	✓
Encryption	✗	✗	✗	✗	✗	✗
QoS	✗	✗	✗	✓ *	✗	✗
Encryption & QoS	✗	✗	✗	✓ *	✗	✗
Transcoding	✗	✗	✗	✓ *	✓	✗

* QoS Reporting is supported for IPv4 only.

Table 2: AP3820 NIU and Feature Group Support Matrix

S-CZ7.2.0 supports the NIUs listed in the left column on the AP3820. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA	SRTP	QoS	Transcoding	MSRP B2BUA (unsupported)
Clear (RJ45)	✗	✗	✗	✗	✗	✗
Clear (SFP)	✗	✗	✗	✗	✗	✗
ETCv1	✓	✓	✓	✓	✗	✗
ETCv2	✓	✓	✓	✓	✗	✗
Encryption	✗	✗	✗	✗	✗	✗
QoS	✗	✗	✗	✓ *	✗	✗
Encryption & QoS	✗	✗	✗	✓ *	✗	✗
Transcoding	✗	✗	✗	✓ *	✓	✗

* QoS Reporting is supported for IPv4 only.

Table 3: AP6100 NIU and Feature Group Support Matrix

S-CZ7.2.0 supports the NIUs listed in the left column on the AP6100. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA	SRTP	QoS	Transcoding	MSRP B2BUA
2x10Gig NIU	✓	✓	✓	✓	✗	✓
Transcode NIU	N/A	N/A	N/A	N/A	N/A	N/A

Table 4: AP6300 NIU and Feature Group Support Matrix

S-CZ7.2.0 supports the NIUs listed in the left column on the AP6300. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA	SRTP	QoS	Transcoding	MSRP B2BUA
2x10Gig NIU	✓	✓	✓	✓	✓ (required)	✓
Transcode NIU	✗	✗	✗	✗	✓	✗

Unsupported Hardware

• ETCv1 Cards with 4GB RAM. These NIUs can be identified by a revision lower than 2.09 (use **show prom-info phy** and look to the ETC NIU's *Functionalrev* attribute to confirm compatibility).

Supported Upgrade Paths

The following upgrade paths are supported:

- S-CX6.3.7 -> S-CZ7.2.0
- S-CX6.3.3 -> S-CZ7.2.0
- S-CX6.4.0 -> S-CZ7.2.0
- S-CZ7.1.2 -> S-CZ7.2.0

If you are upgrading from an S-CX6.3.X image to S-CZ7.2.0, please read the Oracle Communications Session Border Controller Release Notes for releases S-CX6.4.0 and S-CZ7.1.2 for notification of changes.

If you are upgrading from an S-CX6.4.0 image to S-CZ7.2.0, please read the Oracle Communications Session Border Controller Release Notes for release S-CZ7.1.2 for notification of changes.

Coproduct Support

The products/features listed in this section run in concert with the Oracle Communications Session Border Controller for their respective solutions.

Oracle Communications Session Load Balancer

With an Oracle Communications Session Load Balancer running L-CX1.5.0 software, SBC cluster members may run S-CZ7.2.0 on the following hardware:

- AP3820
- AP4500
- AP6300

Pooled Transcoding

The pooled transcoding feature requires an access function Oracle Communications Session Border Controller (A-SBC/P-CSCF) using transcoding resources provided by Oracle Communications Session Border Controllers with transcoding hardware (T-SBC). When the A-SBC/P-CSCF function is based on S-CZ7.2.0 software, the following hardware/software combinations may be used as a T-SBC in a pooled transcoding scenario:

- AP3820, Transcoding NIU, S-CX6.3.7M2+ or S-CZ7.2.0+
- AP4500, Transcoding NIU, S-CX6.3.7M2+ or S-CZ7.2.0+
- AP6300, Transcoding NIU, S-CZ7.1.2+
- AP6300, Transcoding NIU, S-CZ7.2.0+

Oracle Communications Session Element Manager

Oracle Communications Session Element Manager versions 7.4M1 and later support this GA release of the Oracle Communications Session Border Controller

QoS NIU Version Requirement for Acme Packet 3820 and Acme Packet 4500

A Network Interface Unit (NIU) that supports the Quality of Service (QoS) feature group on the Acme Packet 3820 and the Acme Packet 4500, except the two Enhanced Traffic Control (ETC) cards, requires QoS Field Programmable Gate Array (FPGA) revision 2.19 for the S-CZ7.2.0 release. The 2.19 FPGA upgrade image is available at My Oracle Support, *https://support.oracle.com/*, with a customer account.

If the QoS FPGA Hardware Revision is lower than 1.109 (which corresponds to 2.19 FPGA image), you need to upgrade the QoS FPGA image. Use the **show qos revision** command (or **show datapath ppx info** in S/E-CZ7.x.x forward) from the ACLI to find the QoS FPGA Hardware Revision number, for example:

```
ACMEPACKET# show qos revision
QoS FPGA Hardware Revision is 1.109
ACMEPACKET#
```

Oracle Communications Session Router Platform Requirements

In addition to being supported by the AP3820, AP4500, AP6100, and AP6300, the OCSR may run on other platforms

As of release S-CZ7.2.0, the Sun Netra X3-2 and legacy Net-Net 7150 and Net-Net 7350 blade are supported for the Oracle Communications Session Router application.

Minimum requirements for Sun Netra X3-2 support are:

- 2 x Intel Xeon E5-2658 CPUs
- 300 GB HDD
- 16 GB (2 x 8 GB DIMMs) DDR3-1600

Access Control Endpoint Classification Capacity and DoS

The following capacities are for both IPv4 and IPv6 endpoints.

Platform	Denied	Trusted	Media	Untrusted	Dynamic Trusted	ARP	VLAN
AP3820	32000	8000	8000	2000	250000	4000	4000
AP4500	32000	8000	32000	2000	250000	4000	4000

Supported SPL Engines

The following SPL engine versions are supported by this software

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.2.0
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.1.0
- C3.1.1
- C3.1.2

2

New Features in Service Provider Release S-CZ7.2.0

Note: System session capacity and performance are subject to variations between various use cases (e.g. call models) and major software releases.

Accounting Features

The features listed in this section are related to the Oracle Communications Session Border Controller's suite of accounting-related functionality. Feature descriptions of the following items may be found in the Accounting Guide.

Rf Event ACR Generation

The Oracle Communications Session Border Controller generates Rf Event ACRs in the following cases:

- SIP Final/Redirection Response 3xx
- SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful session-unrelated procedure
- SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP session set-up

Rf Event ACRs are also generated for REGISTER messages, which represents the only session-unrelated message this feature supports.

Rf Event ACR Generation for Unsuccessful Session Attempts

When the Oracle Communications Session Border Controller receives a 4xx, 5xx or 6xx response to a SIP INVITE indicating unsuccessful session attempt, an EVENT ACR is generated. The cause-code AVP in the EVENT ACR are follows:

- 4xx Request failure— used when the SIP transaction is terminated due to an IMS node receiving a 4xx error response.
- 5xx Server failure code— used when the SIP transaction is terminated due to an IMS node receiving a 5xx error response.
- 6xx Global failure code— used when the SIP transaction is terminated due to an IMS node receiving a 6xx error response.

Configurable ACR Retries

When the Oracle Communications Session Border Controller has connectivity issues connecting to a CCF to send ACRs, the number of ACR retries, and the interval at which reconnections to the CCF are made are both configurable.

ACR Buffering while waiting for ACA

The Oracle Communications Session Border Controller does not send ACRs for a given session until the previously sent ACR is acknowledged with an ACA from the CCF. This will be done on a per-session basis, i.e. if an ACR for one session is postponed it will not cause a delay in sending other sessions ACRs.

Accounting-request-number AVP

A value that uniquely identifies this message in the session (i.e., a sequence number for this connection). The sequence number is assigned sequentially starting with 0 as described below. This is compliant with RFC 3588. The combination of the Accounting-Record-Number AVP and the Session-Id AVP (both of which are unique for the given session) are used to match accounting records with confirmations. This is done by assigning the noted values to the records listed below:

RCSe/MSRP Features

The features listed in this section are related to the Oracle Communications Session Border Controller's MSRP/RCSe support. Feature descriptions of the following items may be found in the RCS Services chapter in the ACLI Configuration Guide.

The Oracle Communications Session Border Controller supports Message Relay Protocol (MSRP) sessions initiated by Session Description Protocol (SDP) messages exchanged via the Session Initiation Protocol (SIP) offer/answer model. MSRP usage with SDP and SIP is described in Section 8 of RFC 4975, The Message Relay Protocol. The Session Director functions as a Back-to-Back User Agent (B2BUA) for MSRP sessions, terminating incoming MSRP, proxying for the MSRP session originator, initiating outgoing MSRP to the endpoint peer, and providing Network Address Translation (NAT) services. Both IPv4 and IPv6 (and interworking) MSRP sessions are supported.

Feature Description Location: ACLI Configuration Guide, RCS Services Chapter

MSRP Platform Requirements

MSRP is supported on the following platforms:

* AP4500
* AP6100
* AP6300

The AP3820 does not support MSRP.

Users with AP4500 systems must have an ETCv1 or ETCv2 NIU card installed in their systems. The AP6100 and AP6300 have the requisite hardware in their systems by default.

The Oracle Communications Session Border Controller now supports MSRP over IPv6 and IPv4/IPv6 interworking for MSRP.

IMS/VoLTE Features

The features listed in this section are related to the Oracle Communications Session Border Controller suite of IMS features functionality. These features are often used within VoLTE deployments. Feature descriptions of the following items may be found in the ACLI Configuration Guide, IMS Chapter unless noted otherwise.

Emergency Calls from Unregistered Users

Version S-CZ7.2.0 provides compliance with Section 5.1.6.2 of 3GPP TS24.229. This section mandates that unregistered, or roaming User Endpoints (UE) must perform an emergency registration before sending any SIP request (for example, an INVITE) related to the emergency situation.

Recording Session Refresh

The Oracle Communications Session Border Controller provides for periodic in-dialog OPTIONS request/response exchanges to test the availability of the recording session dialog.

Wildcarded Public User Identity

The Oracle Communications Session Border Controller supports wildcard Public User Identies (PUI). This capability is most often used to streamline processing of REGISTER and INVITE messages between a PBX and an IMS core. This feature is also supported as part of P-CSCF reg event package (i.e. NOTIFY messages).

Rx Interface Reason Header Usage

The Oracle Communications Session Border Controller has increased capability to map network events to a configurable SIP Reason header. The extended capability provides for the mapping of specific disconnect events on the Rx Interface.

Feature Description Location: ACLI Configuration Guide, External Policy Servers Chapter

Network Provided Location Information enhancement

Enhanced Phase 2 NPLI support is provided by Version S-CZ7.2.0, and later releases. Phase 2 provides for an explicit subscription to NPLI changes resulting in the dynamic update of NPLI as opposed to the single static transaction provided by the initial Phase 1.

Feature Description Location: ACLI Configuration Guide, External Policy Servers Chapter

TS 24.237 Proposed Changes

The Oracle Communications Session Border Controller implements a proposed change in the processing of failed or cancelled SRVCC sessions. The new processing model has been presented to the 3GPP for inclusion in TS 24.237, IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) service continuity; Stage 3.

IR.94 Loss of Voice Bearer

The Oracle Communications Session Border Controller provides compliance with an IMS Profile for Conversational Video Service (IR.94) requirement that specifies the termination of a multi-media session (voice and video) if the voice bearer is lost.

STR On Successful SRVCC Handover

The Oracle Communications Session Border Controller provides support for the IR-94 (IMS Profile for Conversational Video Service) requirement that a P-CSCF send a Session Termination Request (STR) message after a successful SRVCC handover.

P-Early-Media Header Support

Version S-CZ7.2.0 provides support for the SIP P-Early-Media that can be used in SIP INVITES, PRACKS, and UPDATES to request and authorize the use of early media. It offers an alternative to policy-based early media support.

Media-Component-Number AVP Enhancement

The values assigned to the Media-Component-Number and Flow-Number AVPs are not derived in compliance with 3GPP standards. Version S-CZ7.2.0 provides the capability to derive compliant values.

Feature Description Location: ACLI Configuration Guide, External Policy Servers Chapter

Sec-agree Support

Version S-CZ7.2.0 introduces support for RFC 3329, Security Mechanism Agreement for the Session Initiation Protocol, commonly referred to as Sec-Agree. The RFC defines three SIP headers, Security-Client, Security-Server, and Security-Verify that provide the ability for SIP UAs and other SIP entities (servers, proxies, and registrars) to negotiate next-hop security mechanisms. Note that this initial implementation does not provide support for server-initiated security negotiation, nor does it support media-plane security. That is, support is limited to client-initiated negotiation during initial registration, and to signalling security.

Supported-Features AVP

The Oracle Communications Session Border Controller supports the Supported Features AVP as defined in 3GPP TS 29.229.

Security Features

The features listed in this section are related to the Oracle Communications Session Border Controller's suite of security features for both traffic transport and system hardening. Feature descriptions of the following items may be found in the Security chapter of the ACLI Configuration Guide, except where otherwise noted

4096 bit RSA Key Support

The Oracle Communications Session Border Controller supports 4096 bit RSA keys for SIP TLS on AP platforms with SSMv3 hardware. Systems supporting the SSMv3 include the AP6100 and AP6300.

TLS 1.1 and 1.2 Support

The Oracle Communications Session Border Controller supports TLS 1.1 and 1.2. In order to support TLS version 1.2, additional cipher suites have been added.

TLS 1.2 is supported only for SIP messaging.

Signaling Application and Monitoring Features

The features listed in this section are related to the Oracle Communications Session Border Controller's VoIP application functions. New functionality listed in this section may include protocol features, application-oriented network entity features, and application monitoring features. Locations of the features descriptions within the Oracle Communications Session Border Controller documentation set are noted.

SIP Instance ID in Registration Cache

As defined in RFC 5626, Managing Client-Initiated Connections in the Session Initiation Protocol (SIP), the +sip.instance uniquely identifies a specific user agent instance. The instance-id does not change even when the User Agent is rebooted or power cycled. Using the instance-id from the +sip-instance parameter allows the SBC to locate a registered contact even when the IP address of the UA has changed.

This feature description is found in the ACLI Configuration Guide, SIP Signaling Services Chapter.

SIPREC Recording Session Liveliness

The Oracle Communications Session Border Controller provides for periodic in-dialog OPTIONS request/response exchanges to test the availability of the recording session dialog.

This feature description is found in the ACLI Configuration Guide, Call Traffic Monitoring Chapter.

CAC Utilization Statistics via SNMP

The Oracle Communications Session Border Controller allows you to retrieve information on current session utilization and burst rate as a percentage of their configured maximums on per session-agent and/or realm basis. The Oracle Communications Session Border Controller uses the configured max-session and max-burst-rate settings in conjunction with a percentage formula to calculate this value. The system also uses an ACLI configuration setting to establish the threshold at which trap and trap clear messages are sent from the SNMP agent to the configured manager(s).

This feature description is found in the ACLI Configuration Guide, Admission Control and QoS Chapter.

SNMP Reporting of Message Rate Statistics

The message rate statistics feature was introduced in S-CX6.4.0. It enables the system to provide message rate statistics for SIP, DNS, and ENUM traffic via ACLI and HDR output. This feature has been enhanced to offer the same statistics via SNMP.

Pointers for this feature description are found in the Maintenance and Troubleshooting Guide, Performance Management Chapter, Message Rate Statistics for SIP, DNS, and ENUM sections.

The full feature description is found in the MIB Reference Guide, Enterprise MIBs chapter.

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.

This feature description is found in the Maintenance and Troubleshooting Guide, Fault Management Chapter.

Diameter Message Manipulation

The Oracle Communications Session Border Controller can perform manipulations on all grouped and non-grouped AVPs. This is referred to as Diameter Manipulation Rules (DMR). A message manipulation is the ability to search for a predefined string within an AVP and then replace it with another value. This is similar to the Oracle Communications Session Border Controller's header manipulation rules functionality. This feature does not apply to Rf based accounting.

This feature description is found in the ACLI Configuration Guide, External Policy Servers Chapter.

System Feature

The features listed in this section are related to the Oracle Communications Session Border Controller's internal systems functionality. These features are used for every day integration and maintenance within in your network. Locations of the features descriptions are noted.

Tuning HA Synchronization Channels

The Oracle Communications Session Border Controller queues HA data for transfer from the primary to the backup system using one or more HA transaction channels. The use of multiple channels increases the speed of HA synchronization because it increases the number of HA transactions the system can processes simultaneously. The Oracle Communications Session Border Controller configures an optimum number of channels automatically on Acme Packet 6000 and virtual systems; the user can configure this manually on the Acme Packet 4500.

traceroute

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.

This feature description is found in the Maintenance and Troubleshooting Guide, Fault Management Chapter

Debug mode

The **debug-enable** command is used to enable access to the **shell**, **control**, and **lshell** commands by setting a single password that provides authorization to executing them. Accessing debug level commands should only be performed at the direction of Oracle engineering or support.

This feature description is found in the ACLI Reference Guide, The ACLI Chapter

IPv6 Support for Management and Telemetry

Several management-oriented parameters on the Oracle Communications Session Border Controller may be configured with IPv6 addresses to be used within IPv6 networks.

This feature description is found in the ACLI Configuration Guide, System Configuration Chapter

Entitlements-based licensing

The majority of the Oracle Communications Session Border Controller's capacities and features are self provisioned at the ACLI. Initial system configuration consists of setting the system type and available features. These choices determine the feature groups that are available for use and the maximum session capacities available for certain features. The system provisions a set of default entitlements based on the software version, the hardware on which the software runs, and the product type that you choose.

This feature description is found in the ACLI Configuration Guide, Getting Started Chapter

Transcoding and DTMF Transfer Features

The features listed in this section are related to the Oracle Communications Session Border Controller's suite of Transcoding and DTMF Interworking functions. Feature descriptions of the following items may be found in the Transcoding and DTMF Transfer sections of the ACLI Configuration Guide, except where otherwise noted.

Locally Generated RTCP for Transcoded Calls

The Oracle Communications Session Border Controller is capable of creating and sending RTCP reports using Transcoding resources. This produces RFC 3550 compliant RTCP report information on media traffic for active sessions. The system calculates these statistics using measurements on traffic between a target end station and itself. With respect to a given media session, the system does not produce end-to-end reports. In addition, the system can drop RTCP reports generated upstream so target stations don't receive RTCP reports that are redundant to its own.

SNMP Retrieval of Transcoding Statistics

Several global transcoding statistics are available via SNMP. This feature presents current and high counts of transcoding resources by system capacity percentage and number of sessions. In addition, a table indicating in-use sessions listed by in- and out- codec pairs is also available via SNMP GET.

Active and Period Statistics for EVRC and other Codecs

Codec use per-realm statistics include more detail by breaking out the EVRC codecs into their specific variants. That is, the system keeps track of EVRC0, EVRC1, EVRCB, EVRCB0, and EVRCB1 codec use per-realm on an explicit basis. These 5 counts are also available for SNMP query and are added to the ap-codec.mib file. Additionally, The Oracle Communications Session Border Controller now maintains counts for all codecs that appear in the **show sipd codecs <realm>** command for Active, Recent High, and Lifetime High periods.

Transcoding Support for Asymmetric Dynamic Payload Types

Transcoding Support for Asymmetric Dynamic Payload Types supports the case when asymmetric payload types such that the RTP offered with one payload type and answered with another payload type will be acceptable to the Oracle Communications Session Border Controller when performing transcoding.

DTMF Indication over HD Audio Codecs

When performing DTMF transcoding while HD Audio codecs are present, Oracle Communications Session Border Controller accounts for telephone-event tone indication at clock rates that match those of the HD audio codecs.

RFC2833 and KPML Interworking

Keypad Markup Language (KPML) is used to indicate DTMF tones in SIP messaging. KPML is used by the Key Press Stimulus Package as a SIP Event Notification Package. Endpoints will send DTMF tone indications via NOTIFY messages. The Oracle Communications Session Border Controller can engage in the Event Notification with an endpoint on one call leg and perform digit translation to RFC 2833 telephone-events on the other call leg.

Asymmetric Payload Type Support for RFC2833 Interworking

RFC3264 describes when an endpoint sends a different payload-type value that what it receives for a given codec as is asymmetric behavior. Otherwise, when an endpoint can only send the same payload-type value for what it receives, the behavior is symmetric. The Oracle Communications Session Border Controller can be configured to behave in an RFC compliant manner which is to support asymmetric cases. Symmetric cases are covered by baseline functionality. For asymmetric cases, the Oracle Communications Session Border Controller can receive the a different payload-type that was offered.

Conditional Codec Policy Enhancements

The Oracle Communications Session Border Controller now supports using conditional codec policy syntax in the **codec-policy**'s **order-codecs** parameter.

AP6300 NIU Hotswap Guidelines

The AP6300 Session Border Controller provides a 3-slot chassis. Each chassis is monitored by a dedicated Hot-Swap sensor that maintains state information for the resident Network Interface Units.

3

Inherited Features

Feature descriptions found in this chapter are inherited (forward merged) from Oracle Communications Session Border Controller releases S-CX6.3.0M3, S-CX6.3.0M4, S-CX6.4.0M1, S-CX6.4.0M2, S-CX6.4.0M3, S-CZ7.1.2M1, S-CZ7.1.2M2. These features were not included in S-CZ7.1.2 GA docset.

S-C6.3.0 Maintenance Release Features

The following features appear in the this major release documentation set for the first time.

SDP Version Change without SDP Body Change

When an SRTP call is made through the Oracle Communications Session Border Controller and a UE sends a reINVITE, there may be no change in the SDP contents. When the other UE responds, some devices will increment the o= line's session version, despite no SDP change. Normally the change in SDP version indicates that the SDP has changed, which would otherwise require the Oracle Communications Session Border Controller to modify the media flow set-up. In order to leave the media flows unchanged when session version changes but the rest of the SDP does not, an option is configured in the media-manager-config.

This feature description is found in the ACLI Configuration Guide, SIP Signaling Services Chapter.

IPv6 Link Local Addresses

The Oracle Communications Session Border Controller supports IPv6 Link Local addresses configured for a network interface's gateway.

This feature description is found in the ACLI Configuration Guide, System Configuration Chapter.

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.

This feature description is found in the Maintenance and Troubleshooting Guide, System Management Chapter.

ACLI Parameter Long String Length

The following parameters may be configured as strings, 128 characters in length. These parameters may also start with a number character.

system path:

- **system** > **network-interface** > **name**
- **system** > **phy-interface** > **name**
- **system** > **snmp-user -entry** > **user-name**
- **system** > **redundancy** > **name** > **peer**

media-manager path:

- **codec-policy** > **name**
- **dns-config** > **client-name**
- **dns-config** > **server-dns-attributes** > **server-realm**
- **ext-policy-server** > **name**
- **ext-policy-server** > **realm**
- **media-policy** > **name**
- **realm-config** > **identifier**
- **realm-config** > **parent-realm**
- **realm-config** > **dns-realm**
- **realm-config** > **media-policy**
- **realm-config** > **media-sec-policy**
- **realm-config** > **class-profile**
- **realm-config** > **enforcement-profile**
- **static-flow** > **in-realm-id**
- **static-flow** > **out-realm-id**
- **steering-pool** > **realm-id**
- **vbg-config** > **realm-id**

security path:

- **certificate-recorder** > **name**
- **ike** > **data-flow** > **name**
- **ike** > **data-flow** > **realm-id**
- **ike** > **dpd-params** > **name**
- **ike** > **ike-interface** > **dpd-params-name**
- **ike** > **ike-sainfo** > **name**
- **ike** > **local-address-pool** > **name**
- **ike** > **local-address-pool** > **dns-realm-id**
- **ike** > **local-address-pool** > **data-flow**
- **ike** > **tunnel-orig-params** > **name**
- **ims-aka-profile** > **name**
- **media-sec-policy** > **name**
- **media-mikey-policy** > **name**
- **media-sdec-policy** > **name**
- **public-key** > **name**
- **tls-profile** > **name**

session-router path

- **access-control** > **realm-id**
- **call-recording-server** > **primary-realm**
- **call-recording-server** > **secondary-realm**

- **class-profile** > **media-policy**
- **class-profile** > **policy** > **profile-name**
- **enforcement-profile** > **name**
- **enum-config** > **name**
- **enum-config** > **realm-id**
- **enum-config** > **service-type**
- **enum-config** > **health-query-number**
- **enum-config** > **failover-to**
- **h248-config** > **h248-mgc-config** > **realm-id**
- **h248-config** > **h248-mg-config** > **realm-id**
- **h323** > **h3232-stack** > **name**
- **h323** > **h3232-stack** > **realm-id**
- **h323** > **h3232-stack** > **assoc-stack**
- **h323** > **h3232-stack** > **gk-identifier**
- **h323** > **h3232-stack** > **filename**
- **local-routing-config** > **name**
- **local-routing-config** > **file-name**
- **media-profile** > **name**
- **media-profile** > **subname**
- **mgcp-config** > **private-realm**
- **mgcp-config** > **public-realm**
- **net-management-control** > **name**
- **net-management-control** > **next-hop**
- **net-management-control** > **rph-profile**
- **qos-constraints** > **name**
- **rph-policy** > **name**
- **rph-profile** > **name**
- **rph-profile** > **media-policy**
- **session-constraints** > **name**
- **session-router** > **sr-primary-name**
- **session-router** > **sr-secondary-name**
- **session-agent** > **realm-id**
- **session-agent** > **egress-realm-id**
- **session-agent** > **response-map**
- **session-agent** > **local-response-map**
- **session-agent** > **enforcement-profile**
- **session-agent** > **sip-profile**
- **session-agent** > **sip-isup-profile**
- **session-group** > **group-name**
- **sip-config** > **home-realm-id**
- **sip-config** > **egress-realm-id**
- **sip-config** > **enforcement-profile**
- **sip-interface** > **realm-id**
- **sip-interface** > **operator-identifier**
- **sip-interface** > **ext-policy-server**
- **sip-interface** > **constraint-name**
- **sip-interface** > **response-map**
- **sip-interface** > **local-response-map**
- **sip-interface** > **enforcement-profile**
- **sip-interface** > **sip-profile**

- **sip-interface** > **sip-isup-profile**
- **sip-interface** > **tunnel-name**
- **sip-manipulations** > **name**
- **sip-nat** > **realm-id**
- **sip-profile** > **name**
- **sip-response-map** > **name**
- **sip-isup-profile** > **name**
- **surrogate-agent** > **realm-id**

S-CX6.4.0 Maintenance Release Features

The following features appear in the this major release documentation set for the first time.

IPv6 Support for Static Flows

The Oracle Communications Session Border Controller supports IPv6-IPv6, IPv4-IPv6, and IPv6-IPv6 static flows.

This feature description is found in the ACLI Configuration Guide, Static Flows Chapter.

SDP Alternate Connectivity

The Oracle Communications Session Border Controller can create an egress-side SDP offer containing both IPv4 and IPv6 media addresses via a mechanism which allows multiple IP addresses, of different address families (i.e., IPv4 & IPv6) in the same SDP offer. Our implementation is based on the RFC draft "draft-boucadair-mmusic-altc-09".

This feature description is found in the ACLI Configuration Guide, Realms and Nested Realms Chapter.

AF-Application-Identifier AVP Generation

By default, the Oracle Communications Session Border Controller populates the AF-Application-Identifier AVP with the hostname parameter of the external policy server object that receive's the AAR for the call.

The Oracle Communications Session Border Controller can populate the AF-Application-Identifier AVP with the IMS Communication Service Identifier (ICSI).

This feature description is found in the ACLI Configuration Guide, External Policy Servers Chapter.

DDoS Protection from Devices Behind a NAT

A DDoS attack could be crafted such that multiple devices from behind a single NAT could overwhelm the Oracle Communications Session Border Controller. The Oracle Communications Session Border Controller would not detect this as a DDoS attack because each endpoint would have the same source IP but multiple source ports. Because the Oracle Communications Session Border Controller allocates a different CAM entry for each source IP:Port combination, this attack will not be detected. This feature remedies such a possibility.

This feature description is found in the ACLI Configuration Guide, Security Chapter.

Authenticated NTP

The Oracle Communications Session Border Controller supported authenticated NTP.

This feature description is found in the Maintenance and Troubleshooting Guide, System Management Chapter.

Local Route Table Performance

Capabilities

- Loads approximately 500 LRT tables during boot time
- Loads 100,000 entries per LRT file

- Loads 2,000,000 LRT entries total per system

Constraints

- You cannot configure the

  Oracle Communications Session Border Controller with 500 LRT files each with 100,000 entries.
- Actual performance that affects the interaction among the three performance attributes varies with system memory and configuration.

This feature description is found in the ACLI Configuration Guide, Session Routing and Load Balancing Chapter.

RCSe TLS/TCP Re-Use Connections

In an RCSe environment the sip-interface reuse-connections option is used to make the Oracle Communications Session Border Controller retain the TCP/TLS connection established by the endpoint during the registration for all subsequent messages to that endpoint, essentially providing for a persistent connection between the Oracle Communications Session Border Controller and the user equipment (UE).

This feature description is found in the ACLI Configuration Guide, RCS Services Chapter.

Differentiated Services for DNS and ENUM

The Oracle Communications Session Border Controller can mark DNS/ENUM packets with a configurable differentiated services code point (DSCP).

This feature description is found in the ACLI Configuration Guide, Realms and Nested Realms Chapter.

S-CZ7.1.2 Maintenance Release Features

The following features appear in the this major release documentation set for the first time.

IMS-AKA Change Client Port

The Oracle Communications Session Border Controller is now in compliance with 3GPP TS 33.203, *Access Security for IP-Based Services*.

This feature description is found in the ACLI Configuration Guide, IMS Chapter.

☞ **Note:** This feature removes the client-protected-port parameter from the ims-aka-profile.

4

Interface Changes

This chapter summarizes ACLI, SNMP, and RADIUS changes (where applicable) for S-CZ7.2.0. Additions, removals, and changes appearing in this chapter are since the release of S-CZ7.1.2 GA.

ACLI Command Changes

This section summarizes the ACLI command changes that first appear in release Version S-CZ7.2.0

Command	Description
show sipd agents <session-agent-name>#<destination-ip-address>	Adds functionality to show sipd agents command to retrieve statistics when more than one address is obtained for a session agent obtained via FQDN.
traceroute <destination-address> <options>	Adds standard **traceroute** command to ACLI.
show xcode	Adds **codecs** argument that displays current and maximum count codec pairs in use.
show sipd codecs	Modifies **show sipd codecs** command to displays EVRC0, EVRC1, EVRCB, EVRCB0, and EVRCB1 counts.
debug-enable debug-disable	Adds **debug-enable** and **debug-disable** commands for creating and removing a password for access to debug level commands.
show platform hotswap	Adds command to show AP6300 hotswap status.
setup product setup entitlements show entitlements	Adds commands to support Provisioned Entitlements method of licensing the Oracle Communications Session Border Controller.

The following table summarizes ACLI Command changes that have appeared in earlier versions of the Oracle Communications Session Border Controller software

Command	Description
show neighbor-table	Adds link level neighbor table output to show neighbor-table command to support IPv6 Link Local Addresses feature.
show timezone	Updates command to display the timezone and DST settings.
show sipd acl	Updates display to include counts of blocked NAT devices.

The following commands are no longer supported in this version of the Oracle Communications Session Border Controller.

• stack
• check-stack

The following commands are no longer supported in this and higher versions of OC- SBC

• show qos revision

ACLI Configuration Element Changes

This section summarizes the ACLI configuration element changes that first appear in release Version S-CZ7.2.0.

Accounting Features

New Parameter	Description
session-router > **account-config** > **acr-retry-interval** **session-router** > **account-config** > **max-acr-retries**	Parameters added to support Rf Accounting, Configurable ACR Retries feature.

IMS/VoLTE Features

New Parameters	Description
session-router > **sip-interface** > **p-early-media-header** **session-router** > **sip-interface** > **p-early-media-direction**	Parameters added for P-early-media header support
session-router > **sip-interface** > **sec-agree-feature** **session-router** > **sip-interface** > **sec-agree-pref**	Parameters added to support Sec-Agree.
session-router > **sip-config** > **rx-sip-reason-mapping**	Parameter added to support Rx Interface Reason Header Usage/mapping feature.
session-router > **local-response-map** > **local-response-map-entry** > **local-error**	Enumerated values added to accept Rx message Reasons Header values for Rx Interface Reason Header Usage/mapping feature.
session-router > **sip-config** > **add-ue-location-in-pani** **session-router** > **sip-config** > **hold-emergency-calls-for-loc-info** **media-manager** > **ext-policy-server** > **specific-action-subscription**	Parameters added or modified to support populating the P-Access-Network-Info header from 3GPP Network Provided Location Information specification.

MSRP/RCSE Features

MSRP Confirguration first appeared in S-CX6.4.0.

Signaling Features

New Parameters	Description
session-router > **sip-config** > **match-sip-instance** **session-router** > **sip-config** > **match-sip-instance**	Parameter added to support the SIP Instance ID feature.
session-router > **diameter-manipulation** > **name** **session-router** > **diameter-manipulation** > **description** **session-router** > **diameter-manipulation** > **diameter-manip-rules** subelement **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **name** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **avp-code** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **descr-avp-code** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **avp-type** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **action** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **msg-type** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **msg-cmd-code** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **comparison-type** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **match-value** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **new-value** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **avp-header-rule** subelement **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **move** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **avp-header-rule** > **name** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **avp-header-rule** > **header-type** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **avp-header-rule** > **action** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **avp-header-rule** > **match-value** **session-router** > **diameter-manipulation** > **diameter-manip-rules** > **avp-header-rule** > **new-value**	Configuration element and parameters added to support Diameter Message Manipulations feature

System Features

New Parameters	Description
session-router > **session-agent** > **cac-trap-threshold**	Parameters added to support Call Access Control Utilization Statistics trap via SNMP.

Interface Changes

New Parameters	Description
session-router > **session-constraints** > **cac-trap-threshold**	
session-router > **session-recording-server** > **refresh-interval**	Parameter added to support SIPREC Recording Session Liveliness feature.
session-router > **sip-config** > **sa-routes-stats**	Parameter added to support FQDN-resolved Session Agent Statistics feature.
bootparams > **inet on ethernet** **bootparams** > **gateway inet** **system** > **system-config** > **syslog-servers** > **address** **system** > **system-access-list** > **source-address** **system** > **system-access-list** > **netmask** **security** > **authentication** > **radius-servers** > **address**	IPv6 for Management and Telemetry update certain parameters to use IPv6 addresses, in addition to IPv4 addresses.

Transcoding Features

New Parameters	Description
media-manager > **codec-policy** > **order-codecs**	Parameter now accepts conditional codec policy syntax.
media-manager > **rtcp-policy** **media-manager** > **rtcp-policy** > **rtcp-generate**	Configuration element and parameter added to enable Local RTCP Generation feature

Security Features

New Parameters	Description
security > **tls-profile** > **tls-version** **security** > **tls-profile** > **cipher-list**	Values added to these parameters to enable TLS 1.1 and 1.2 support.
security > **certificate-record** > **key-size**	Value added to accommodate 4096-bit keys. This is only visible when valid hardware is installed in the system.

Inherited Features

The following table summarizes the ACLI configuration element changes that first appeared in release prior to Version S-CZ7.2.0, but are new to this major release.

New Parameters	Description
system > **timezone-config** > **name** **system** > **timezone-config** > **minutes-from-utc** **system** > **timezone-config** > **dst-start-rule** **system** > **timezone-config** > **dst-start-month** **system** > **timezone-config** > **dst-start-day** **system** > **timezone-config** > **dst-start-weekday**	Configuration element and parameter added to enable Automated Daylight Savings Time Updates feature.

New Parameters	Description
system > **timezone-config** > **dst-start-hour** **system** > **timezone-config** > **dst-end-rule** **system** > **timezone-config** > **dst-end-month** **system** > **timezone-config** > **dst-end-day** **system** > **timezone-config** > **dst-end-weekday** **system** > **timezone-config** > **dst-end-hour**	
Various.	See: *RN - S-C6.3.0 Maintenance Release Features*, ACLI Parameter Long String Length feature
media-manager > **static-flow** > **in-source** **media-manager** > **static-flow** > **in-destination** **media-manager** > **static-flow** > **out-source** **media-manager** > **static-flow** > **out-destination**	Parameters modified to accept IPv6 values in addition to existing IPv4 values.
session-router > **access-control** > **max-endpoints-per-nat** **session-router** > **access-control** > **nat-invalid-message-threshold** **media-manager** > **realm-config** > **max-endpoints-per-nat** **media-manager** > **realm-config** > **nat-invalid-message-threshold** **media-manager** > **realm-config** > **wait-time-for-invalid-register**	Parameters added to support DDoS protection from devices behind a NAT feature.
media-manager > **realm-config** > **alt-realm-family** **media-manager** > **realm-config** > **pref-address-type**	Parameters added to support SDP Alternate Connectivity feature.
ntp-sync > **auth-servers** **ntp-sync** > **auth-servers** > **ip-address** **ntp-sync** > **auth-servers** > **key-id** **ntp-sync** > **auth-servers** > **key**	Configuration element and parameters added to support authenticated NTP servers.
media-manager > **media-policy** > **tos-settings** > **media-type**	Parameter can accept **message/dns** value for Differentiated services for DNS/ENUM feature.
security > **ims-aka-profile** > **start-protected-client-port** **security** > **ims-aka-profile** > **end-protected-client-port**	Parameters added to support IMS-AKA Change Client Port feature. The **protected-client-port** parameter value, upon upgrade is copied to the **start-protected-client-port** parameter. The **protected-client-port** parameter is removed from version S-CZ7.2.0.

Application SNMP Changes

This section summarizes the Application SNMP/MIB changes that appear inOracle Communications Session Border Controller Version S-CZ7.2.0.

New table name	MIB file location	Description
apSIPRateIntfStatsTable	Ap-sip.mib	This table provides a listing of SIP message rate statistics per SIP interface.
apSipInterface	Ap-sip.mib	This table creates a mapping between an index and SIP interface configuration name.
ApSipMethod	Ap-tc.mib	This table creates a mapping between an index and one of 15 methods as used in the apSIPRateIntfStatsTable and apSIPRateAgentStatsTable tables.
apSIPRateAgentStatsTable	Ap-sip.mib	This table provides a listing of SIP message rate statistics per SIP session agent.
apSipAgent	Ap-sip.mib	This table creates a mapping between an index and SIP session agent configuration name.
apDnsAlgServerTable	Ap-dnsalg.mib	• This table creates a mapping between an index and configured DNS ALG realm. • Table can now accommodate multiple IP addresses as Session agent when using FQDN to retrieve session agent addresses.
apDnsAlgConfigTable	Ap-dnsalg.mib	This table creates a mapping between an index and DNS ALG configuration name.
apEnumServerRateStatsTable	Ap-dnsalg.mib	This table provides a listing of ENUM message rate statistics per configured ENUM server element.
apDnsAlgServerRateStatsTable	Ap-apps.mib	This table provides a listing of message rate statistics for per configured DNS Alg Server element.
apSigRealmCacStatsTable apSipSaCacStatsTable	Ap-sip.mib	These tables provide a listing of CAC Utilization by Realm or Session Agent as described in the CAC Utilization Statistics via SNMP feature.

Changes from S-CX 6.4.0

The apEnvMonTemperatureStatusTable in ap-env-monitor.mib reports component order differently from S-CX6.4.0. The new order for the Object identifiers (OIDs) in 7.2.0 is :

```
SNMPv2-SMI::enterprises.9148.3.3.1.3.1.1.3.1 = STRING: "MAIN TEMP0"
SNMPv2-SMI::enterprises.9148.3.3.1.3.1.1.3.2 = STRING: "MAIN TEMP1"
SNMPv2-SMI::enterprises.9148.3.3.1.3.1.1.3.3 = STRING: "CPU TEMP0"
SNMPv2-SMI::enterprises.9148.3.3.1.3.1.1.3.4 = STRING: "PHY TEMP0"
```

```
SNMPv2-SMI::enterprises.9148.3.3.1.3.1.1.3.5 = STRING: "PHY TEMP1"
SNMPv2-SMI::enterprises.9148.3.3.1.3.1.1.3.6 = STRING: "PHY FPGA TEMP0"
```

System Provisioning

The majority of the Oracle Communications Session Border Controller's capacities and features are self provisioned at the ACLI. Initial system configuration consists of setting the system type and available features. These choices determine the feature groups that are available for use and the maximum session capacities available for certain features. The system provisions a set of default entitlements based on the software version, the hardware on which the software runs, and the product type that you choose.

Provisioning a New System

An uninitialized system does not have the product type set, nor does it have any features installed. A system that has legacy keyed licenses installed is considered an uninitialized system.

You may not enable features until the product type has been set. Use the **setup product** command to set the system product type and use the **setup entitlements** command to enable features.

Controlled Features

Certain features are enabled only by entering a license key in the **system** > **license** configuration element, and not through the **setup entitlements** command. Contact your sales representative for more information on purchasing these features.

The following controlled features are available:

☞   **Note:** Not all of the controlled features above are available on all platforms.

Provisioning a System with Existing Keyed Licenses

When changing the Oracle Communications Session Border Controller licensing technique from the legacy keyed licenses method to the self-provisioned method, be aware of the following:

- After running **setup product** and **setup entitlements**, the system will be seeded with the existing licenses' functionality.
- When the system is seeded with its previous functionality to the provisioned entitlements system, functionality may be changed with the **setup entitlements** command.
- You may notice that there are fewer entitlements than there were keyed licenses. This is normal.
- After setting up provisioned features, the **show features** command will still function to display the previously installed keyed entitlements.

Product Type Provisioning

1. Type **setup product** at the ACLI. If this is the first time running the command on this hardware, the product will show as Uninitialized.
2. Type **1 <Enter>** to modify the uninitialized product.
3. Type the number followed by **<Enter>** for the product type you wish to initialize.
4. Type **s <Enter>** to commit your choice as the product type of this platform.

☞   **Note:** When configuring an HA pair, you must provision the same product type and features on each system.

Feature Provisioning

1. Type **setup entitlements** at the ACLI. Currently provisioned features are printed on the screen.

2. Type the number of the feature you wish to configure followed by pressing the **<Enter>** Key. Some features are set as enabled/disabled (provisionable feature), and some features are provisioned with a maximum capacity value (provisionable capacity feature). The command will let you provision these values as appropriate.

3. Type **enabled** or **disabled** to set a provisionable feature , or type an integer value for a provisionable capacity feature. Both input types are followed by pressing the **<Enter>** key.

4. Repeat steps 2 and 3 to configure additional entitlements.

5. Type **d** followed by the **<Enter>** key to review the full range of your choices. Note that disabled entitlements display their state as blank.

6. Type **s** followed by the **<Enter>** key to commit your choice as an entitlement for your system. After saving the value succeeds you will be returned to the ACLI.

7. Reboot your Oracle Communications Session Border Controller.

☞ **Note:** When configuring an HA pair, you must provision the same product type and features on each system.

Editing and Viewing Features

If you are not changing the product type, and you are changing only the features, you can edit the existing feature with the **setup entitlements** command. Executing this command will display existing features before giving you the option to modify their settings.

The **show entitlements** command displays the currently provisioned features and controlled features. You may also use the **setup entitlements** command and type **d** to display the current features. Upon first executing the **setup entitlements** command, all features (excluding controlled features) are displayed on the screen.

Keyed Licenses and Provisioned Entitlements Compatibility

The Oracle Communications Session Border Controller supports keyed licenses and the provisioned entitlements process for provisioning features on the system. Know the following about how licensing mechanisms work with each other.

• You are not required to begin using the provisioned entitlement system as of this release.
• You may continue to obtain keyed licenses and install them as necessary.
• Upon migrating to the provisioned entitlements system, the current range of your installed, keyed licenses will be seeded to the provisioned entitlements system. The system's functionality will remain identical.
• If you upgrade to the provisioned entitlements system, then downgrade the software to a version without the provisioned entitlements system, the pre-existing keyed licenses will still function.
• If you upgrade to the provisioned entitlements system, then change the functionality (such as, adding more SIP sessions or removing a feature set), upon downgrade to a pre-provisioned entitlements image, the new functionality will not be present.

5

Caveats and Known Issues

Caveats

Transcoding - general

Only SIP signaling is supported with transcoding.

Codec policies can only be used with realms associated with SIP signaling.

Transcoding is not available in conjunction with SRTP.

☞ **Note:** This Caveat has been removed as of S-CZ7.2.0M2

QoS is not supported for transcoded calls.

SIPREC may not be performed on a transcoded call.

T.38 Fax Transcoding

T.38 Fax transcoding available for G711 only at 10ms, 20ms, 30ms ptimes.

Fax codec policy based on D7.0 fax transcoding policy.

Pooled Transcoding for Fax is unsupported.

DTMF Interworking

RFC 2833 interworking with H.323 is unsupported.

SIP-KPML to RFC2833 conversion is not supported for transcoded calls.

High Availability

When the AP6300 experiences call rates over 650 CPS, SIP and/or MBCD may fail to synchronize.

H.248

The Border Gateway and H.248 functionality are unsupported.

H.323 Signaling Support

If H.323 and SIP traffic are run in system, each protocol (SIP, H.323) should be configured in its own separate realm.

Media Hairpinning

Media hairpinning is not supported for hair-pin/spiral call flows involving both H.323 and SIP protocols.

Archive Logs

Archiving log files is unsupported on AP3820 and AP4500 platforms without a HDD installed.

HMR action on Call-ID

HMR operations on the Call-ID: header are deprecated.

Lawful Intercept

Lawful Intercept is supported for the X123 and PCOM (post-GA release) protocols only.

FTP Support

The Oracle Communications Session Border Controller's FTP Server is deprecated. Only SFTP server services are supported.

FTP Client access for features such as HDR/CDR push remains.

Fragmented Ping Support

The Oracle Communications Session Border Controller does not respond to inbound fragmented ping packets.

Physical Interface RTC Support

After changing any Physical Interface configuration, a system reboot is required.

SRTP Caveats

MIKEY key negotiation is not supported.

The ARIA cipher is not supported.

Linksys SRTP is not supported.

For hold and resume SRTP calls, if the rollover counter increments, upon a subsequent hold and resume action without an SRTP rekey or SSRC change an SRTP rekey, the media portion of the call will be lost. This Caveat only applies to systems running Encryption or QoS & Encryption NIUs.

Packet Trace

Output from the packet trace local feature on hardware platforms running this software version may display invalid MAC addresses for signaling packets.

Phy Link Redundancy

Phy link redundancy is not supported in this release.

MGCP Signaling Support

MGCP Signaling is not supported in this release.

Session Replication for Recording

Session Replication for Recording is not supported in this release.

RTCP Generation

Video flows are not supported in realms where RTCP generation is enabled.

SCTP

SCTP Multihoming does not support dynamic and static ACLs configured in a realm.

SCTP must be configured to use different ports than configured TCP ports for a given interface.

SIP Monitor and Trace / WebGUI

The SIP Monitor & Trace and WebGUI features are unsupported. Ensure that the **system** > **web-server-config** > **state** parameter is set to **disabled**.

Source-based Routing

The source routing feature as configured by **system-config** > **source-routing** is deprecated. Please review the HIP information in the Network Interface section in the System Configuration chapter of the ACLI Configuration guide for background of accessing SBC Administrative Applications over media Interfaces.

Known Issues

Supported Hardware

Acme Packet 3820 and 4500 hardware with BoardRev: 3.00 will not load the licenses that are expected to appear. As a workaround, reinstall licenses manually after reboot with the original key. Use the **show version boot** command and look to the Mainboard Info section, BoardRev: attribute.

This known issue is fixed as of S-CZ7.2.0M1.

IPSec

When the security-association configuration element is configured as an IPv6 SA, it is not RTC enabled.

The **transport-protocols** parameter in **security-policy** configuration element is set to the default of all, regardless of configuration.

Session Router

When the session-router is configured with a operation-mode of session, it is failing to correctly clear sessions.

File Systems

For users with Acme Packet 3820 and 4500 systems with a hard-disk, an upgrade from pre-S-CZ7.1.2 software to this version will not change the hard drive's filesystem from FAT-32 to ext3 to preserve any existing data. This results in the SFTP application not providing the expected filesystem user security. To rectify this, reformat the system's hard-disk.

☞ **Note:** By reformatting the hard-disk, you will lose the contents of /opt and any other user-created partitions located under /mnt.

Encryption Hardware Support

On the Acme Packet 3820 and 4500, IPSec and SRTP are supported on with ETCv1 and ETCv2 NIUs only.

TCP Ports

Maximum TCP Ports supported

RFC2833 to UII Interworking

SIP-H323 hairpin calls with DTMF tone indication interworking is not supported

IMS AKA

Inbound and outbound SA counts can lose synchronization when an IMS-AKA protected port pool is enabled.

After failover, Security Parameter Index (SPI) values are not properly synchronized when the IMS-AKA protected port pool is enabled.

SBC Running as an SLB Cluster Member

Rebalancing is unavailable on the Oracle Communications Session Load Balancer when running an Acme Packet 6300 as a cluster member. Set the SLB's **cluster-config** > **auto-rebalance** parameter to **disabled** to use an Acme Packet 6300 as a cluster member from that SLB.

Web-GUI

See the SIP Monitor & Trace and WebGUI entry in the Caveats section of this chapter.

Uploading LRT files via the Web-GUI does not function as expected on the Acme Packet 4500. You may SFTP LRT files directly to the system instead.

H.323

HA Redundancy is not supported for H.323 calls.

SIP over TCP

No more than 500 SIP Interfaces with SIP over TCP are supported.

RADIUS and TACACS+ Authentication

When the Oracle Communications Session Border Controller performs user authentication through via RADIUS or TACACS+, all logins are provisioned with user-level access.

Redundancy Configuration

Do not use the 169.254.16.x or 169.254.21.x networks in the redundancy-config of the Oracle SBC (including the network-interface configuration for the wancom1 and wancom2 interfaces) when installed on an Acme Packet platform that includes a transcoding card. The system uses these networks to provide software to transcoding DSPs. When the user configures the redundancy configuration with these networks, the system fails to route this software properly.

Workaround: Choose any available network for redundancy other than 169.254.16.x or 169.254.21.x. Note that user documentation describes redundancy configuration using the 169.254.1.x/16 network, which works properly with transcoding cards.

Diameter, CDR and High Availability

If you use Diameter as the protocol in **account-config** and have the default **cdr-output-redundancy** setting in a HA pair, the upgrade of a standby will not sync and thus will go out of service.

Workaround: Set **cdr-output-redundancy** to **enabled** before the upgrade. Once both units in the HA pair have been upgraded, you may then set **cdr-output-redundancy** to **disabled** if needed.

System Tools

When an SSH session closes, the tSSHoutput task may fail while trying to send an operational message to the ACLI and begin to send error messages to the ACLI instead. The SBC continues to provide service, but may require rebooting to eliminate the error messages.

Fixed in: SCZ720m6p2

Behavioral Changes

Please review the following sections prior to using this software release.

Filesystem Security

The user-level account now has read-only access on the filesystem. In order to SFTP files onto an Oracle Communications Session Border Controller's filesystem, you must log in with a superuser-level (admin) account.

☞ **Note:** If you load this release and then downgrade to an earlier S-CZ release, these permission changes persist; the default permissions from previous releases will not be honored.

Accounting

For users upgrading from S-CX6.x.x or prior, all timestamp values in CDR records (RADIUS and local CDRs) are now created in mixed-case.