Oracle® Communications Session Border Controller & Session Router

Release Notes
Release S-CZ7.3.0

October 2017

ORACLE

Notices

Contents

Preface

About this Guide

Overview

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

- An introduction to the full release
- An overview of the new features available
- An overview of the interface enhancements
- A summary of known issues, caveats, and behavioral changes

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.

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 Acme Packet 4500.
Acme Packet 3820 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3820.
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.
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 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), 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 Oracle Communications Session Border Controller's accounting support, including details about RADIUS and Diameter 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.
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.

Revision History

This section contains a revision history for this document.

Date	Description
October, 2015	• Initial Release • Added Neighbor Release Patch Equivalency • Removed TSCF Known Issue that was inaccurate

Date	Description
November, 2015	• Moved SIP Monitor & Trace and WebGUI Known Issues to a consolidated Caveat
March, 2016	• Updates Known Issues for the SCZ730M1 release
March, 2016	• Adds 6300 HA issue to Known Issues list.
March, 2016	• 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. • Adds note of Source routing deprecation to Caveats section. • Removes Notice on IPSec/IKEv1 over IPv6
March, 2016	• Moves performance and MSRP defect content • Resolves Important Notices content
March, 2016	• Adds S-CZ7.3.0M1p1 Known Issues, per request
May, 2016	• Adds additional S-CZ7.3.0M1p1 Known Issues • Updates the section QoS NIU Version Requirement • Adds known issue on addressing that must not be used for HA deployments that include transcoding cards
August, 2016	• Adds S-CZ7.3.0M2 Known Issues • Corrects upgrade path information.
August, 2016	• Adds HA issue to Known Issues
September, 2016	• Adds software version source information to defects related to M2
January, 2017	• Adds Session Router defect
March, 2017	• Updates the supported FPGA version to 2.22 and removes the **show qos** command from the "QoS NIU Version Requirement for Acme Packet 3820 and Acme Packet 4500" section.
September 2017	• A limitation regarding the **packet-trace remote** command was added. • Adds reference to physical interface bug ACMECSBC-2625

Date	Description
October 2017	Adds the following Caveat • Interface Utilization Support

1

Introduction to S-CZ7.3.0

The Oracle Communications Session Border Controller S-CZ7.3.0 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.
- A summary of known issues, caveats, and behavioral changes

Platform Support

The following platforms are supported by S-CZ7.3.0:

- Acme Packet 3820
- Acme Packet 4500
- Acme Packet 4600
- 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 prom-info cpu** command.

Acme Packet 3820 and 4500 Transcoding NIU Support

Acme Packet 3820/4500 chasses with a transcoding NIU upgrading to S-CZ7.3.0 and above must have a high-speed fan module to ensure sufficient cooling.

Image and Bootloader File Conventions

The Acme Packet 4500, 4600, 6100, and 6300 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., nnSCZ730.64.bz . The Acme Packet 3820 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., nnSCZ730.32.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 `nnSCZ730.64.bz` and `nnSCZ730.boot` respectively.

Bootloader Requirements

Acme Packet 3820 and Acme Packet 4500 Bootloaders

The Acme Packet 3820 and 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 Installation Guide.

Acme Packet 4600, 6100, and 6300

The Acme Packet 4600, 6100, and 6300 require a Stage 3 bootloader that accompanies the OCSBC image file, as distributed. It should be installed according to the instructions found in the Installation Guide.

NIU and Feature Group Requirements

This section lists the feature groups that require specific NIUs for all hardware platforms.

Table 1: Acme Packet 4500 NIU and Feature Group Support Matrix

S-CZ7.3.0 supports the NIUs listed in the left column on the Acme Packet 4500. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA	SRTP	QoS	Transcoding	MSRP B2BUA	TSCF
Clear (RJ45)	✗	✗	✗	✗	✗	✗	✗
Clear (SFP)	✗	✗	✗	✗	✗	✗	✗
ETCv1 (8G)	✓	✓	✓	✓	✗	✓	✗
ETCv2	✓	✓	✓	✓	✗	✓	✗
Encryption	✓	✗	✓	✗	✗	✗	✗
QoS	✗	✗	✗	✓ *	✗	✗	✗
Encryption & QoS	✓	✗	✓	✓ *	✗	✗	✗
Transcoding	✗	✗	✗	✓ *	✓	✗	✗

* QoS Reporting is supported for IPv4 only.

Table 2: Acme Packet 3820 NIU and Feature Group Support Matrix

S-CZ7.3.0 supports the NIUs listed in the left column on the Acme Packet 3820. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA (unsupported)	SRTP	QoS	Transcoding	MSRP B2BUA (unsupported)	TSCF (unsupported)
Clear (RJ45)	✗	✗	✗	✗	✗	✗	✗
Clear (SFP)	✗	✗	✗	✗	✗	✗	✗
ETCv1 (8G)	✓	✗	✓	✓	✗	✗	✗
ETCv2	✓	✗	✓	✓	✗	✗	✗
Encryption	✓	✗	✓	✗	✗	✗	✗
QoS	✗	✗	✗	✓ *	✗	✗	✗
Encryption & QoS	✓	✗	✓	✓ *	✗	✗	✗
Transcoding	✗	✗	✗	✓ *	✓	✗	✗

* QoS Reporting is supported for IPv4 only.

- 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).

Table 3: Acme Packet 4600 NIU and Feature Group Support Matrix

S-CZ7.3.0 supports the NIUs listed in the left column on the Acme Packet 4600. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA	SRTP	QoS	Transcoding	MSRP B2BUA	TSCF
2x10Gig + Transcode NIU	✓	✓	✓	✓	✓ (Requires DSP Modules)	✓	✓

Table 4: Acme Packet 6100 NIU and Feature Group Support Matrix

S-CZ7.3.0 supports the NIUs listed in the left column on the Acme Packet 6100. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA	SRTP	QoS	Transcoding	MSRP B2BUA	TSCF
2x10Gig NIU	✓	✓	✓	✓	✗	✓	✓

Table 5: Acme Packet 6300 NIU and Feature Group Support Matrix

S-CZ7.3.0 supports the NIUs listed in the left column on the Acme Packet 6300. The matrix indicates the feature sets that require the supported NIUs.

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

*Requires transcode carrier unit and DSP module

Unsupported Hardware

This release does not support the 4G version of the ETCv1 interface card.

Supported Upgrade Paths

The following upgrade paths are supported:

- S-CX6.4.0 -> S-CZ7.3.0
- S-CZ7.1.2m5 -> S-CZ7.3.0
- S-CZ7.1.2m5p2 -> S-CZ7.3.0
- S-CZ7.2.0m5p3 -> S-CZ7.3.0

If you are upgrading from an S-CZ7.1.2 image to S-CZ7.3.0, please read the Oracle Communications Session Border Controller Release Notes for releases S-CZ7.2.0 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 Subscriber-Aware Load Balancer

With an Oracle Communications Subscriber-Aware Load Balancer running L-CX1.5.0 or S-CZ7.2.10 software, SBC cluster members may run S-CZ7.3.0 on the following hardware:

- Acme Packet 3820 (L-CX1.5.0 only)
- Acme Packet 4500
- Acme Packet 6100
- Acme Packet 6300

Please refer to the *Oracle Communications Subscriber-Aware Load Balancer Essentials Guide* for additional limitations.

Note: This release adds IMS-AKA support between an SLB running L-CX1.5.0 and an Acme Packet 4500. The prior release supported IMS-AKA traffic only between the SLB and SBC running on Acme Packet 6100 and 6300 platforms only.

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-CZ7.3.0 software, the following hardware/software combinations may be used as a T-SBC in a pooled transcoding scenario:

- Acme Packet 3820, Transcoding NIU: S-CX6.3.7M2+ or S-CZ7.2.0+, S-CZ7.3.0+

- Acme Packet 4500, Transcoding NIU: S-CX6.3.7M2+ or S-CZ7.2.0+, S-CZ7.3.0+
- Acme Packet 6300, Transcoding NIU: S-CZ7.1.2+, S-CZ7.2.0+, S-CZ7.3.0+

Oracle Communications Session Element Manager

Oracle Communications Session Element Manager versions 7.5 and later support this GA release of the Oracle Communications Session Border Controller .

QoS NIU Version Requirement for Acme Packet 4500

A Network Interface Unit (NIU) that supports the Quality of Service (QoS) feature group on the Acme Packet 4500, except the two Enhanced Traffic Control (ETC) cards, requires QoS Field Programmable Gate Array (FPGA) revision 2.22 or higher for the S-CZ7.3.0M1 release. he *Acme Packet 4500/3820 V2.22 QOS FPGA Upgrade 24369382* image is available at My Oracle Support, *https://support.oracle.com/*, with a customer account.

Oracle Communications Session Router Platform Requirements

In addition to being supported by the Acme Packet 3820, 4500, 4600, 6300, the Oracle Communications Session Router may run on other platforms

As of release S-CZ7.3.0, the Oracle Netra Server X3-2, X5-2 and legacy HP platforms are supported for the Oracle Communications Session Router application.

Oracle Platforms

Table 6: Minimum Hardware Requirements for Sun Platforms

Device	Processor	Memory	Hard Drive
Oracle Netra Server X3-2	2 x Intel Xeon E5-2658 CPUs	16 GB (2 x 8 GB DIMM) DDR3-1600	300 GB HDD
Oracle Netra Server X5-2	2 x Intel Xeon E5-2699 v3 CPUs	256 GB (16 x 16 GB DIMM) DDR4-2133	1.2 TB (2 x 600GB HDD)
Oracle Server X5-2	2 x Intel Xeon E5-2699 v3 CPUs	256 GB (16 x 16 GB DIMM) DDR4-2133	1.2 TB (2 x 600GB HDD)

HP Platforms

All supported HP platforms require SPP2015.06.

The correct SPP must be installed onto the host/blade at the time the software is upgraded or downgraded. Combinations with older firmware are unsupported.

See the *Oracle Communications Session Router Software Installation on HP Platforms - SPP2015.06 Release 1.0*guide for information on supported platforms and the minimum requirements.

System Capacities

To query the current system capacities for the platform you are using, execute the **show platform limit** command. System capacities vary across the full range of platforms which support the Oracle Communications Session Border Controller.

Neighbor Release Patch Equivalency

Patch equivalency indicates which patch content in neighbor releases is included in this release. This assures you that in upgrading, defect fixes in neighbor stream releases are included in this release.

Neighbor Release Patch Equivalency for S-CZ7.3.0 GA:

- S-CZ7.3.0P1

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
- C2.2.1
- 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
- C3.1.3

2

New Features in Service Provider Release S-CZ7.3.0

Please read the *Important Notices About This Release* in the Caveats and Known Issues chapter before considering this release for use.

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

System Features

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.

IPv6 Trap Receiver Transport Support

This feature supports configuring trap receivers with IPv6 address notation, and allows traps to be sent to IPv6 targets.

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

Link Redundancy

Link redundancy enables the Oracle Communications Session Border Controller to run a pair of media interfaces redundantly so that in the event of a network or link failure, the Oracle Communications Session Border Controller automatically fails over to the redundant physical link. The Oracle Communications Session Border Controller polls link state on a one-second basis, so the maximum outage time is one second. And if gateway heartbeats are enabled, then gateway timeout alarms will also cause failovers.

This feature is only supported on the Acme Packet 3820 and 4500 on the following NIUs:

- 4-port 10/100/1000 copper
- 4-port 1Gig SFP
- 4-port 10/100/1000 copper

4-port 1Gig SFP phy card with QoS

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

IPv6 NTP Server Support

The Oracle Communications Session Border Controller can be configured with IPv6 addresses of NTP servers. When multiple NTP servers are configured, they may be of mixed address family.

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

Interface Description in MIB Enhancement

The *ifDescr* object in the *ifEntry* object in *ifTable* is a string of up to 255 characters. It currently contains the name of the interface only. This change adds to the *ifDescr* string, separated from the first part by a space, a keyword that represents the internal interface type. The values can be {ETH, FE, GE, OC, XE, null}.

This feature description is found in the MIB Guide.

TCP and SCTP State Connection Counters

Systemwide counts of TCP and SCTP states are available by using **show ip tcp** and **show ip sctp** commands respectively, from the ACLI.

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.

AP6300/AP6100: 1 Million Trusted DDoS ACLs

The Acme Packet 6100 and 6300 can now support 1,000,000 trusted DDoS ACLs. Refer to the **show platform limits** command for the most up-to-date running capacities.

Remove All Default Passwords

The Oracle Communications Session Border Controller utilizes default or hard-coded passwords as shipped. These are predictable and pose a security risk if not changed promptly. Password setup must be completed through SSH or Console connections. Passwords need to be set when a particular privilege level is accessed and the system determines when the password is the default value.

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

TACACS+ Administrative Security

Oracle Communications Session Border Controllers use either the RADIUS (Remote Authentication Dial-In User Service) or the TACACS+ (Terminal Access Control Access Control System Plus) protocol for centralized access control administration; however, prior to this release, you could connect to the TACACS + server only from the system's media interfaces. This feature implements TACACS+ authorization (user permissions management on a command basis), authentication (user management), and accounting on management interfaces.

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

TACACS+ Authorization Command and Arguments Boundary

Each TACACS+ authorization entry on an ACLI command line comprises the command and its arguments. Currently everything typed as a TACACS+ authorization command by an authenticated admin user, including the arguments, is sent to the TACACS+ server in the command field of the TACACS+ message; the argument field in the TACACS+ message contains no arguments and is set to “cmd-

arg=<CR>". This feature adds the new parameter **tacacs-authorization-arg-mode** to the **authentication** configuration element, which enables the TACACS+ authorization command and its arguments to be sent to the TACACS+ server separately.

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

IMS 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.

AAR Message Optimization

The Oracle Communications Session Border Controller, acting as a P-CSCF, already supports AAR message optimization (the suppression of unnecessary AARs). This feature reduces the number of AAR transactions to the minimum to assure that the end-to end session set-up and dedicated bearer creation works seamlessly. For more information, see the ACLI Configuration Guide, External Policy Servers Chapter.

ATCF ICSI Invite Matching

The Oracle Communications Session Border Controller can check, on reception of an INVITE on an ingress sip interface that has a configured ATCF and before applying any of the already implemented logic, whether the incoming INVITE includes the ICSI (Instantaneous Channel-State Information) of the requested service. The ATCF will be involved in the call flow when the configured ICSI value matches the ICSI value in the original INVITE; otherwise the handoff call will be rejected with code 480 (Temporarily Unavailable).

IR.92 Multiple Emergency Numbers

The Oracle Communications Session Border Controller expands compliance with the IR.92 standard by including an alternative service and message for emergency traffic.

Network Provided Location Information During Register

For most cases, location information is relevant at the time of the session request. However, Network Provided Location Information (NPLI) upon REGISTER is required for some Authorization-Authentication Requests (AAR) and Authorization-Authentication Answers (AAA).

Network Provided Location Information for SMS

For most cases, location information is relevant at the time of the session request. Network Provided Location Information (NPLI) for SIP is delivered by DIAMETER in Authentication-Authorization Answers (AAA) and Reauthentication- Authorization Requests (RAR). In certain countries, it is a regulatory requirement to provide location information also for the Short Message Service (SMS), which in LTE networks is implemented using the SIP MESSAGE method to carry the text.

SIP Surrogate Agent Registration Re-initialization

Surrogate agents in the IMS network integrate IP Private Branch Exchange (PBX) that cannot register itself to the registrar. The Oracle Communications Session Border Controller supports registration retry attempts to the IMS core up to the configured maximum register attempts before failing. When the Oracle Communications Session Border Controller identifies an unregistered surrogate agent, the registration cache can cleared as a normal SIP user and the registration process re-started.

SRVCC Handover Support in Alerting Phase

Oracle now supports handovers between Packet-Switched (PS) and Circuit-Switched(CS) networks for calls in an alerting phase; that is, a 180 ringing response for the initial INVITE has been sent or received and the SIP final response has not been sent or received.

Subscription for Notification of Signaling Path Status

The Oracle Communications Session Border Controllercan explicitly open a flow for the signaling and through a subscription to this flow, provide status change notifications.

Surrogate Agent Reregistration to SAG Member Handling

In a round-robin environment sometimes requests need to go to the same server as the initial request. The Oracle Communications Session Border Controller will direct the reREGISTER request to a 401/407 response for a surrogate agent to the same Proxy Call Session Control Function(P-CSCF) as the prior REGISTER request for security purposes.

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.

SBC Graceful Shutdown Procedure

In its simplest form, this is the graceful shutdown procedure. Details and exceptions to this procedure when there are active calls or registrations are discussed in later paragraphs. The first six actions are performed whether or not the Oracle Communications Session Border Controller (SBC) is part of an Oracle Communications Session Border Controller (SLB) Cluster

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

SIP Recursion Policy

Session Agents (and Session agent groups) can utilize a SIP Recursion policy to customize the Oracle Communications Session Border Controller behavior when recursing through a list of target SIP peers. These policies are useful for networks with large numbers of SIP peers that wish to customize recursive routing behavior for individual session agents or session agent groups, based on number of recursion attempts or the returned SIP response code.

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

Timer to Tear Down Long Duration Calls

The Oracle Communications Session Border Controller currently provides the “flow-time-limit” timer to terminate long duration calls. However, this timer is reset whenever the Oracle Communications Session Border Controller receives a Re-INVITE or UPDATE message, even when it is provided for the session timer. This feature adds a non-resettable timer that, when enabled and upon expiration, tears down long duration calls.

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

Mapping of Diversion Information Between Diversion and History-Info Headers

History-Info and Diversion are the two headers in SIP signaling used to convey information related to call transfer and call diversion. Although both provide call diversion information, they have different syntaxes,

the main difference being that the chronology of events is reversed between the two headers. To date, Oracle Communications Session Border Controllers have provided mapping and interworking of the History-Info and Diversion headers through the use of an SPL plug-in. This feature implements this interworking functionality within the software by adding a new parameter to the **sip-interface** configuration element.

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

TSCF Features

The features in this section are related to Tunneled Services Control Function or TSCF support. Feature descriptions of the following items may be found in the Tunneled Services Control Function chapter in the ACLI Configuration Guide.

This release of the Oracle Communications Session Border Controller includes the Tunneled Services Control Function (TSCF) feature set, also called Tunnel Session Management (TSM). This technology improves firewall traversal for over-the-top (OTT) Voice-over-IP (VoIP) applications, and reduces the dependency on SIP/TLS and SRTP by encrypting access-side VoIP within standardized Virtual Private Network (VPN) tunnels. As calls or sessions traverse a TSM tunnel, the TSCF forwards all SIP and RTP traffic from within the TSM tunnel to appropriate servers or gateways within the secure network core. Operating in a TSM topology, the Oracle Communications Session Border Controller provides exceptional tunnel performance and capacity, as well as optional high availability (HA), DoS protection and tunnel redundancy that improves audio quality in lossy networks.

Refer to the ACLI Configuration Guide's Tunneled Service Control Function chapter for a detailed explanation of the licensing requirement for TSCF.

Prior to this release, the TSCF feature set was available as the Oracle Communications Tunneled Session Controller. That functionality is now available as an Oracle Communications Session Border Controller feature on the Acme Packet 4600 and Acme Packet 6000 series platforms.

Transcoding 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.

Opus Codec Transcoding Support

Opus is an audio codec developed by the IETF that supports constant and variable bitrate encoding from 6 kbit/s to 510 kbit/s and sampling rates from 8 kHz (with 4 kHz bandwidth) to 48 kHz (with 20 kHz bandwidth, where the entire hearing range of the human auditory system can be reproduced). It incorporates technology from both Skype's speech-oriented SILK codec and Xiph.Org's low-latency CELT codec. This feature adds the Opus codec as well as support for transrating, transcoding, and pooled transcoding to the 4600 and 6300 platforms.

SILK Codec Transcoding Support

SILK is an audio codec developed by Skype Limited that supports bit rates from 6 kbit/s to 40 kbit/s and sampling rates of 8, 12, 16, or 24 kHz. It can also use a low algorithmic delay of 25 ms (20 ms frame size + 5 ms look-ahead). This feature adds the SILK codec as well as support for transrating, transcoding, and pooled transcoding to the 4600 and 6300 platforms.

T.140 to Baudot Relay

The T.140 to Baudot Relay feature uses the Oracle Communications Session Border Controller's transcoding resources to relay T.140 text messages to Baudot tones and vice versa. The T.140 Protocol is used for multimedia text conversation over IP and is designed as a replacement for TDD devices. Baudot tones are a common protocol in the US in Telecommunications Device for the Deaf (TDD). Details of the protocol implementation are available in TIA/EIA-825-A. The T.140-Baudot relay is a regulatory requirement, and is specified for both emergency and non-emergency traffic. This feature is only available on Acme Packet 4600 and 6300 with transcoding hardware.

Session Router Features

The features listed in this section are related to the Oracle Communications Session Router. Refer to the Oracle Communications Session Router installation guide for more information.

For applicable platforms, boot media options have been enhanced:

- .iso installation media is available for this release on Oracle Netra platforms. Some installation locations may prohibit the use of read/write USB Flash drives. The .iso distribution media may be used for burning the image to DVD for a DVD-ROM installation.
- For USB Flash drive media created with the Boot Media Creator, once the system has been successfully booted, the user may remove the USB Flash media from the server.

Please see the Oracle Communications Session Router Installation Guide for system provisioning and installation.

New Platforms - Acme Packet 4600

For the first time appearing at a major release GA, Oracle Communications introduces the Acme Packet 4600 hardware platform.

The Acme Packet 4600 supports the Oracle Communications Session Border Controller and Session Router software. This platform is based on the Acme Packet 6300 architecture and features encryption and transcoding in a single system. Transcoding functionality can utilize up to 1 through 12 transcoding modules on the NIU. The encryption feature set relies on the SSM3 encryption module. The Acme Packet 4600 platform runs the 64-bit software image exclusively.

The NIU provides six media ports (i.e., 4 x GbE and 2 x 10GbE) on a single NIU card. Simultaneous operations of the GbE and 10GbE media ports is unsupported.

The Acme Packet 4600 has an internally mounted SSD memory drive (80GB or 400GB). The system employs the same file system as the Acme Packet 6300/6100 platform that runs the S-Cz Series software. The mounted partitions include the /boot partition (2GB), the /code partition (2GB) and the /opt partition. The /opt partition is intended for core dumps, log files, and CDRs.

The Acme Packet 4600 has 5 cooling fans mounted of the front on the chassis to maintain proper operating temperature. The chassis contains 1:1 fully redundant AC or DC power supplies and load share when both are powered on. The two power supplies also have integrated fans.

The Acme Packet 4600 FRU list consists of the following

- Acme Packet 4600 Chassis w/Mainboard
- Acme Packet 4600 NIU
- Transcoding Module
- Signaling Security Module (aka Encryption SSM3)
- Solid State Drive (80GB SSD or 400GB SSD)
- AC-input 1100-watt Power Supply w/cabling
- DC-input 1100-watt Power Supply w/cabling

- Fan Pod
- System Air Filter
- SFP Module (1 GbE)
- SFP+ Module (10GbE)

3

Inherited Features

Feature descriptions found in this chapter are inherited (forward merged) from Oracle Communications Session Border Controller releases:

- S-CX6.4.0 M4, M5, M6
- S-CZ7.1.2 M3, M4, M5
- S-CZ7.2.0 M1, M2, M3, M4, M5

These features were not included in S-CZ7.2.0 GA docset.

S-CX6.4.0 Maintenance Release Features

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

Configurable DNS Response Size

When a realm is used for DNS queries, the Oracle Communications Session Border Controller can accept UDP DNS responses configurable up to 65535 bytes.

This feature description is found in the ACLI Configuration Guide, Session Routing chapter.

DNS SRV Session Agent Recursion Error Handling

When a session request is sent from the Oracle Communications Session Border Controller to a session agent, and an error response is received (or a transport failure occurs), the Oracle Communications Session Border Controller attempts to reroute the message through the list of dynamically resolved IP addresses. The SBC can be configured to resend session requests through the list of IP addresses under more failure conditions.

This feature description is found in the ACLI Configuration Guide, Session Routing chapter.

LMSD Offerless INVITE Handling

To enhance LMSD interworking, the Oracle Communications Session Border Controller does not remove SDP from a 180 response sent back to the UAC when the initial request did not contain SDP. The Oracle Communications Session Border Controller also forwards UAS-side UPDATE requests to the UAC; it does not respond locally. These represent behavioral changes and require no configuration.

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

S-CZ7.1.2 Maintenance Release Features

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

Multipart Message Body Encoding Support

SIP messages and responses may arrive at the Oracle Communications Session Border Controller with encoded multipart message bodies, such that the content of the body is unreadable. This information may be encoded for the purpose of compressing the data. Normally, the Oracle Communications Session Border Controller would consider the body invalid and reject the entire message, replying to the sender with a 400 Invalid Body error response. The user, however, can configure the **sip-config** option, **proxy-content-type-encodings**, allowing the Oracle Communications Session Border Controller to accept, process and forward messages containing these encoded parts. This configuration causes the Oracle Communications Session Border Controller to ignore the encoding, identify the end of the message via content length, and pass the message towards its intended recipient with the multipart body fully encoded.

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

S-CZ7.2.0 Maintenance Release Features

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

DSCP Marking for MSRP and Media over TCP

The Oracle Communications Session Border Controller supports Differentiated Services Code Point (DSCP) marking of MSRP and Media over TCP traffic. This feature may be used for MSRP traffic in both B2BUA and non-B2BUA modes.

This feature description is found in the ACLI Configuration Guide, Realms chapter.

SIP REFER Call Transfer UUI Relay

The SIP REFER Call Transfer *User to User Information (UUI)* Relay option assists in the transfer of caller details through using the information in the "Refer-To" header in a new "User to User" header in the INVITE to the Referred-to party. This feature only works when the **refer-call-transfer** option is enabled on the realm or session agent where the REFER is received. This behavior change is enabled by default. This option can be used by a Call Center application to transfer a call with user information to an agent.

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

SLB Client Support of IPsec traffic within L3 Tunnels

The Oracle Communications Session Border Controller, acting as a Subscriber-aware Load Balancer (SLB) client can exchange IPSec traffic within the L3 tunnels between itself and the SLB server. One application of this feature is using an SLB to balance and re-balance IMS-AKA traffic among an SLB cluster.

This feature description is found in the Oracle Communications Session Load Balancer Essentials Guide.

SRTP Re-keying

Initialization of SRTP re-keying is supported by the Oracle Communications Session Border Controller.

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

SRTP and Transcoding

Secure Real Time Transport Protocol (SRTP) allows secure media transmission. Transcoding is the ability to convert between media streams that are based upon different codecs. The Oracle Communications Session

Border Controller supports IP-to-IP transcoding for SIP sessions and can connect two voice streams that use different coding algorithms with one another. Both SRTP and transcoding are available in the same call. This feature is not available on the Acme Packet 3820 or Acme Packet 4500 platforms.

This feature description is found in the ACLI Configuration Guide, Transcoding and RCS Services chapter.

Minimum Advertised SSL/TLS Version

The sslmin option is available to set a minimum advertised security level to mitigate using older, more vulnerable versions of SSL. One such problem is the poodle attack(CVE-2014-3566).

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

4

Interface Changes

This chapter summarizes ACLI, SNMP, HDR, Alarms, and RADIUS changes (where applicable) for S-CZ7.3.0. Additions, removals, and changes appearing in this chapter are since the previous major release of the Oracle Communications Session Border Controller.

ACLI Command Changes

This section summarizes the ACLI command changes that first appear in the Oracle Communications Session Border Controllerrelease S-CZ7.3.0

Command	Description
show sipd codecs	Adds counts for newly supported SILK and opus codecs
show registration sipd surrogate-agent <realm-id/ unregistered>	Adds **surrogate-agent** field to the **show registration sipd** command to display all surrogate agents and their state to support the SIP Surrogate Agent Registration Re-initialization feature
clear-cache registration sip	Enhances command to restart the registration process for all address of record for surrogate agents to support the SIP Surrogate Agent Registration Re-initialization feature
show ip tcp ; **show ip sctp**	Adds options to display systemwide counts for TCP and SCTP State Connection Counters

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 Oracle Communications Session Border ControllerS-CZ7.3.0

System Features

New Parameters	Description
ntp-sync > **add-server**	Accepts IPv6 addresses for configured NTP time servers for IPv6 NTP Server Support feature.
system > **trap-receiver** > **ip-address**	Accepts IPv6 addresses for configured trap receiver for IPv6 Trap Receiver Transport Support feature.
session-router > **sip-config** > **retry-after-upon-offline**	Adds parameter to support load balancing restart for when Oracle Communications Session Border Controller is configured as a cluster member in conjunction with the Oracle Communications Session-aware Load Balancer.

Accounting Features

There are no new configuration elements, nor new parameters for Accounting features in this release.

IMS/VoLTE Features

New Parameters	Description
media-manager > **ext-policy-server** > **specific-action-sig-flow-subscription**	Adds subscription to track signaling path status change information for Subscription for Notification of SIgnaling Path Status feature
session-router > **sip-config** > **npli-upon-register**	Adds ability to capture Network Provided Location Information during Registration for the NPLI During Register feature.
session router > **net-management-control** > **sip-380-reason**	Adds configurable reason for IR.92 Multiple Emergency Numbers feature
session-router > **sip-config** > **msg-hold-for-loc-info**; **cache-loc-info-expire**; **keep-cached-loc-info-after-timeout**	Adds parameters to manage Network Provided Location Information and its cache for the Short Message Service
session router > **sip-config** > **atcf-isci-match**	Adds ATCF ISCI matching rule for the ATCF ISCI Invite Matching feature.

New Configuration Elements	New Parameters and Description
session router > **sip-feature-caps**	Adds new sip-feature-caps configuration element with the following parameters to support SRVCC handover and other ATCF functionality: • **state** • **atcf-management-uri** • **atcf-alerting**

Signaling Features

New Parameters	Description
media-manager > **realm-config** > **session-max-life-limit**	Adds parameter to set maximum interval before the system terminates long-duration calls for the Timer to Tear Down Long Duration Calls feature.
session-router > **sip-interface** > **diversion-info-mapping-mode**	Adds mode to enable the Mapping of Diversion Information Between Diversion and History-Info Headers

New Configuration Elements	New Parameters and Description
session-router > **sip-recursion-policy**	Adds the following parameters to terminate recursion on received responses to support the SIP Recursion Policy: • **name** • **description** • **global-count** • **mode** • **sip-response-code**
session-router > **sip-recursion-policy** > **sip-response-code**	Adds the following parameters for refined SIP Recursion Policy configuration: • **response-code** • **attempts**

Transcoding Features

New Parameters	Description
media-manager > **codec-policy** > **allow-codecs**	Parameter now allows **`text:no`** value which strips "m=text" occurrence in the outbound INVITE and enables T.140 to Baudot transcoding.
session router > **media profile** > **name**	Adds **SILK** and **OPUS** values

TSCF Features

TSCF Functionality includes a new top level menu, **tscf**, that appears within the security path.

New Configuration Elements	New Parameters and Description
security > **tscf** > **tscf-address-pool**	This configuration element defines local address pools for the TSCF application. Supported parameters are: • **name** • **address-range** • **dns-realm-id** • **data-flow** • **protocol-policy**

New Configuration Elements	New Parameters and Description
security > **tscf** > **tscf-address-pool** > **address-range**	This configuration element defines the address ranges for the TSCF application. The following parameters are supported: • **network-address** • **subnet-mask**
security > **tscf** > **tscf-config**	Global parameters for tunneled services control function. Supported parameters are: • **keepalive-timer** • **keepalive-timer-datagram** • **tunnel-persistence-time** • **red-port** • **red-max-trans** • **red-sync-start-time** • **red-sync-comp-time** • **element-id**
security > **tscf** > **tscf-data-flow**	Configures the data flow name for managing data traffic within an address pool. The following parameters are supported: • **name** • **realm-id** • **group-size** • **upstream-rate** • **downstream-rate**
security > **tscf** > **tscf-interface**	Used to configure interfaces for the TSCF application. The following parameters are supported: • **state** • **realm-id** • **max-tunnels** • **local-address-pools** • **nagle-state** • **assigned-services** • **tscf-ports**
security > **tscf** > **tscf-interface** > **tscf-port**	Used to configure TSCF ports on TSCF interfaces. Supported parameters are: • **address** • **port** • **transport-protocol** • **tls-profile**
security > **tscf** > **tscf-protocol-policy**	Configures the protocol policy to enable policy-based forwarding. The following parameters are supported: • **name**

New Configuration Elements	New Parameters and Description
	• **ip-address** • **port** • **transport-type** • **realm-id** • **remote-ip-address**

Security Features

New Parameters	Description
security > **authentication** > **tacacs-authorization-arg-mode**	Adds **tacacs-authorization-arg-mode** parameter for enabling TACACS+ Authorization Command and Arguments Boundary feature.

Inherited Features

The following table summarizes the ACLI configuration element changes that first appeared in a release prior to Oracle Communications Session Border ControllerS-CZ7.3.0, but are new to this major release.

New Parameters	Description
media-manager > **realm-config** > **dns-max-response-size**	Adds parameter to set maximium size of DNS response to queries for Configurable DNS Response Size
security > **media-security** > **sdes-profile** > **srtp-rekey-on-reinvite**	Adds parameter to enable re-key upon the receipt of a SIP reINVITE that contains SDP for the SRTP Re-keying.

Alarms

This section summarizes the Alarm changes that appear in the Oracle Communications Session Border Controller version S-CZ7.3.0. The two alarms work in conjunction with the Opus and SILK Transcoding features.

- Licensed Opus Transcoding Capacity Threshold Alarm/131159 — A warning alarm is triggered if the Opus transcoding capacity exceeds a high threshold of 95% of licensed sessions in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm does not effect health.
- Licensed SILK Transcoding Capacity Threshold Alarm/131159 — A warning alarm is triggered if the SILK transcoding capacity exceeds a high threshold of 95% of licensed sessions in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm does not effect health.

Application SNMP/MIB Changes

This section summarizes the Application SNMP/MIB changes that appear in the Oracle Communications Session Border Controller version S-CZ7.3.0.

ap-codec.mib

Object Name/OID	Description
apCodecRealmCountOpus 1.3.6.1.4.1.9148.3.7.1.1.1.25	The count of SDP media streams received in the realm which negotiated to the Opus codec.
apCodecRealmCountSILK 1.3.6.1.4.1.9148.3.7.1.1.1.26	The count of SDP media streams received in the realm which negotiated to the SILK codec.
apCodecRealmCountT140 1.3.6.1.4.1.9148.3.7.1.1.1.27	The count of SDP media streams received in the realm which negotiated to the T140 codec.
apCodecRealmCountBAUDOT 1.3.6.1.4.1.9148.3.7.1.1.1.28	The count of SDP media streams received in the realm which negotiated to the BAUDOT codec.
apCodecRealmCountH264 1.3.6.1.4.1.9148.3.7.1.1.1.29	The count of SDP media streams received in the realm which negotiated to the H264 codec .
apCodecRealmStatsObjectsGroup5 1.3.6.1.4.1.9148.3.7.5.2.7	A collection of objects providing additional realm codec statistics, including Opus and SILK.
apCodecRealmStatsObjectsGroup6 1.3.6.1.4.1.9148.3.7.5.2.8	A collection of objects providing additional realm codec statistics, including T.140.
apCodecRealmStatsObjectsGroup7 1.3.6.1.4.1.9148.3.7.5.2.9	A collection of objects providing additional realm codec statistics, including BAUDOT.
apCodecRealmStatsObjectsGroup8 1.3.6.1.4.1.9148.3.7.5.2.10	A collection of objects providing additional realm codec statistics, including H.264.

ap-smgmt.mib

Table 7: New MIB Objects

Object Name/OID	Description
apSysCPULoadAvgOneMinute 1.3.6.1.4.1.9148.3.2.1.1.43	The percentage of CPU Load across all cores measured over 1 minute.
apSysCPULoadAvgFiveMinute 1.3.6.1.4.1.9148.3.2.1.1.44	The percentage of CPU Load across all cores measured over 5 minutes.
apSysCPULoadAvgFiftnMinute	The percentage of CPU Load across all cores measured over 15 minutes.

Object Name/OID	Description
1.3.6.1.4.1.9148.3.2.1.1.45	
apSysXCodeOpusCapacity 1.3.6.1.4.1.9148.3.2.1.1.46	The percentage of licensed Opus transcoding utilization (non pollable).
apSysXCodeSILKCapacity 1.3.6.1.4.1.9148.3.2.1.1.47	The percentage of licensed SILK transcoding utilization (non pollable).
apSysMgmtCPULoadAvgGroup 1.3.6.1.4.1.9148.3.2.4.2.31	Object to monitor CPU Load Average across all CPU cores for 1, 5, and 15 minutes.
apSysMgmtXCodeOpusUtilGroup 1.3.6.1.4.1.9148.3.2.4.2.32	Object to monitor licensed Opus transcoding utilization .
apSysMgmtXCodeSILKUtilGroup 1.3.6.1.4.1.9148.3.2.4.2.33	Object to monitor licensed SILK transcoding utilization.

Table 8: New Traps

Trap Name (clear trap)	Description
apSysMgmtCPULoadAvgTrap (apSysMgmtCPULoadAvgClearTrap)	The trap will be generated when CPU Load Average Alarm exceeds its minor alarm threshold. The clear trap will be sent when the CPU load average recedes to the minor alarm level.

capability MIBs

Table 9: New Capability MIBs

Object Name/OID	MIB file
apSmgmtCPULoadAvgCap 1.3.6.1.4.1.9148.2.1.8.55	ap-smgmt.mib
apSmgmtXCodeOpusUtilCap 1.3.6.1.4.1.9148.2.1.8.56	ap-smgmt.mib
apSmgmtXCodeSILKUtilCap 1.3.6.1.4.1.9148.2.1.8.57	ap-smgmt.mib
apCodecRealmCodecCap5 1.3.6.1.4.1.9148.2.1.13.7	ap-codec.mib
apCodecRealmCodecCap6 1.3.6.1.4.1.9148.2.1.13.8	ap-codec.mib
apCodecRealmCodecCap7	ap-codec.mib

Object Name/OID	MIB file
1.3.6.1.4.1.9148.2.1.13.9	
apCodecRealmCodecCap8 1.3.6.1.4.1.9148.2.1.13.10	ap-codec.mib

MIB Changes

apSipRecNotificationGroup (1.3.6.1.4.1.9148.3.15.3.2.4) has changed to apSipRecNotificationsGroup (1.3.6.1.4.1.9148.3.15.3.2.4).

Note: An "s" has been added to the end of "Notifications" in the MIB Object name.

Other Traps

When either Opus or SILK session utilitization exceeds 90%, an apSysMgmtGroupTrap is sent that includes the non-pollable apSysXCodeOPUSCapacity or apSysXCodeSILKWBCapacity OIDs, respectively. When utilization falls below 85%, the apSysMgmtGroupClearTrap is sent.

Unsupported MIBs

The following MIB objects are new this release, but are not supported for this product.

- apSecurityDhcpInterfaceCap 1.3.6.1.4.1.9148.2.1.14.14
- apUsbcSysDPDKMibCapabilities 1.3.6.1.4.1.9148.2.1.25
- apUsbcSysDPDKCap 1.3.6.1.4.1.9148.2.1.25.1
- apUsbcSysScalingMibCapabilities 1.3.6.1.4.1.9148.2.1.26
- apUsbcSysScalingCap 1.3.6.1.4.1.9148.2.1.26.1
- apNNCTrapRelayNotAliveNotification 1.3.6.1.4.1.9148.3.8.5.3.1.0.3
- apNNCTrapRelayAliveNotification 1.3.6.1.4.1.9148.3.8.5.3.1.0.4
- apSecurityDhcpInterfaceStatsTable 1.3.6.1.4.1.9148.3.9.1.11
- apSecurityDhcpInterfaceStatsEntry 1.3.6.1.4.1.9148.3.9.1.11.1
- apSecurityDhcpInterfaceType 1.3.6.1.4.1.9148.3.9.1.11.1.1
- apSecurityDhcpInterfaceAddress 1.3.6.1.4.1.9148.3.9.1.11.1.2
- apSecurityDhcpInterfaceDisRcvd 1.3.6.1.4.1.9148.3.9.1.11.1.3
- apSecurityDhcpInterfaceOfferSent 1.3.6.1.4.1.9148.3.9.1.11.1.4
- apSecurityDhcpInterfaceReqRcvd 1.3.6.1.4.1.9148.3.9.1.11.1.5
- apSecurityDhcpInterfaceAckSent 1.3.6.1.4.1.9148.3.9.1.11.1.6
- apSecurityDhcpInterfaceNAckSent 1.3.6.1.4.1.9148.3.9.1.11.1.7
- apSecurityDhcpInterfaceFailures 1.3.6.1.4.1.9148.3.9.1.11.1.8
- apSecurityDhcpInterfaceRelRcvd 1.3.6.1.4.1.9148.3.9.1.11.1.9
- apSecurityDhcpInterfaceOfferTimeouts 1.3.6.1.4.1.9148.3.9.1.11.1.10
- apSecurityDhcpInterfaceLeaseTimeouts 1.3.6.1.4.1.9148.3.9.1.11.1.11
- apSecurityDhcpInterfaceCurrentSessions 1.3.6.1.4.1.9148.3.9.1.11.1.12
- apSecurityDhcpInterfaceMaxSessions 1.3.6.1.4.1.9148.3.9.1.11.1.13
- apSecurityDhcpInterfaceTotalSessions 1.3.6.1.4.1.9148.3.9.1.11.1.14
- apUsbcSysScalingObjects 1.3.6.1.4.1.9148.3.17.1.1.12
- apUsbcSysEstSessions 1.3.6.1.4.1.9148.3.17.1.1.12.1
- apUsbcSysEstG711G729Trans 1.3.6.1.4.1.9148.3.17.1.1.12.2
- apUsbcSysEstSigTPS 1.3.6.1.4.1.9148.3.17.1.1.12.3
- apUsbcSysEstACLs 1.3.6.1.4.1.9148.3.17.1.1.12.4

- apUsbcSysEstTCP 1.3.6.1.4.1.9148.3.17.1.1.12.5
- apUsbcSysEstTL 1.3.6.1.4.1.9148.3.17.1.1.12.6
- apUsbcSysEstVLANs 1.3.6.1.4.1.9148.3.17.1.1.12.7
- apUsbcSysDPDKObjects 1.3.6.1.4.1.9148.3.17.1.1.13
- apUsbcSysDPDKFwdPurpose 1.3.6.1.4.1.9148.3.17.1.1.13.1
- apUsbcSysDPDKDOSPurpose 1.3.6.1.4.1.9148.3.17.1.1.13.2
- apUsbcSysDPDKSigPurpose 1.3.6.1.4.1.9148.3.17.1.1.13.3
- apUsbcSysDPDKTransPurpose 1.3.6.1.4.1.9148.3.17.1.1.13.4
- apUsbcSysDPDKCmdLine 1.3.6.1.4.1.9148.3.17.1.1.13.5
- apUsbcSysDPDKFileMem 1.3.6.1.4.1.9148.3.17.1.1.13.6
- apUsbcSysDPDKSysMem 1.3.6.1.4.1.9148.3.17.1.1.13.7
- apUsbcSysDPDKNum1G 1.3.6.1.4.1.9148.3.17.1.1.13.8
- apUsbcSysDPDKNum2MB 1.3.6.1.4.1.9148.3.17.1.1.13.9
- apUsbcSysDPDKHypervisorType 1.3.6.1.4.1.9148.3.17.1.1.13.10
- apUsbcSysDPDKAddFwdCores 1.3.6.1.4.1.9148.3.17.1.1.13.11
- apUsbcSysDPDKAddSigCores 1.3.6.1.4.1.9148.3.17.1.1.13.12
- apUsbcSysDPDKAddTransCores 1.3.6.1.4.1.9148.3.17.1.1.13.13
- apUsbcSysScalingGroup 1.3.6.1.4.1.9148.3.17.3.1.3
- apUsbcSysDPDKGroup 1.3.6.1.4.1.9148.3.17.3.1.4

Documentation Updates and Changes

In addition to updates that correspond with new feature functionality, the S-CZ7.3.0 documentation library contains the following substantive changes:

- The MIB Reference Guide has been updated and reformatted into an easier to use format.
- A new Oracle Communications Session Border Controller installation Guide has been created. Existing upgrade information has been removed from the Maintenance and Troubleshooting Guide and Configuration Guide and centralized.
- A new Oracle Communications Session Router installation Guide has been created. Existing upgrade information has been removed from the Maintenance and Troubleshooting Guide and Configuration Guide and centralized.
- A new Oracle Communications Session Router installation Guide for supported HP platforms has been created.
- A new Oracle Communications Call Traffic Monitoring Guide has been created. This guide pulls together chapters that existed in previous release's ACLI Configuration Guide on the topic of call traffic monitoring which includes packet trace, SIP Monitor and Trace (and the WebGUI), and the Oracle Communications Session Monitor.

5

Caveats and Known Issues

This chapter lists the caveats, known issues, and behavioral changes for this release. Please ensure you're using the latest revision of this guide to stay informed about these issues.

Important Notices About This Release

Users must not deploy this initial release into a production network if using the following features:

- MSRP B2BUA
- TSCF
- IPSec / IKEv1 over IPv6

Note: Release S-CZ730M1 resolves these issues, allowing device deployment into production environments supporting all of the above.

Caveats

Interface Utilization Support

The Interface Utilization: Graceful Call Control, Monitoring, and Fault Management feature is unsupported for this release.

Transcoding - general

Only SIP signaling is supported with transcoding.

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

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.

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 Acme Packet 3820 and Acme Packet 4500 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 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.

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.

IMS-AKA

IMS-AKA is not supported on the Acme Packet 3820.

MSRP

The Acme Packet 6300 does not support forwarding MSRP over TSM's TLS /DTLS tunnels.

The Acme Packet 6300 doesn't forward MSRP over TCP into TLS/DTLS tunnels

Note: This issue is resolved as of SCZ730M1.

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

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.

packet-trace remote Command Limitation

The **packet-trace remote** command does not work with IPv6. This defect was found in release SCZ740.

- **Defect ID**—26338219

RFC2833 to UII Interworking

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

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.

H.323

HA Redundancy is not supported for H.323 calls.

Accounting

RADIUS stop records for IWF calls may display inaccurate values.

Configuration Verification

Executing **verify-config** on a system will report a non-existent, non-affecting TSCF error.

Note: This issue is resolved as of SCZ730M1.

Session Router

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

Session Router on HP Platforms

If after upgrading to a S-CZ7.3.0 OCSR software image and its corresponding 7.3 stage3 bootloader, you decide to downgrade to a pre- S-CZ7.3.0 product release, you MUST install the corresponding 7.2 stage3 bootloader before reboot with the older image.

TSCF

Do not execute the **show tscf tunnel all** command while media traffic is running. Doing so will make the Oracle Communications Session Border Controller non-functional.

Note: This issue is resolved as of SCZ730M1.

HA redundancy fails if a second failover occurs.

Note: This issue is resolved as of SCZ730M1.

When configured with a large number of DTLS tunnels (~400k), running **`show tscf`** commands can cause a datapath failure. The user can verify this issue via ACLI error output after running the command, and via the dump.datapath file.

The user must reboot the system to resume normal operation.

This issue was introduced in SCZ730M1p1.

When running TSCF in HA mode, DTLS tunnel information is not synchronized when the standby reboots. The user can verify this by running the **`sh tscf tunnel all`** command on the standby after the reboot.

The standby will display new tunnels as they are established.

This issue was introduced in SCZ730M1p1.

When configured with TSCF and IMS-AKA, the OC-SBC limits the number of IMS-AKA endpoints it supports to 10k. Do not configure TSCF in conjunction with IMS-AKA if you intend to support more than 10k endpoints.

This issue was identified in SCZ730M2.

When configured with TSCF and MSRP, the OC-SBC cannot support any MRSP B2BUA Sessions. The user can verify this using the show entitlements command. Do not configure MSRP in conjunction with TSCF.

This issue was identified in SCZ730M2.

When running TSM, the OC-SBC crashes after setting up approximately 2500 TLS tunnels/calls.

This issue was identified in SCZ730M2.

Online Upgrade for HA Systems

When running S-CZ7.3.0 in an HA configuration, the secondary SBC may go out of service (OOS) during upgrades, failovers, and other HA processes while transitioning from its "Becoming Standby" state. This event has been observed in approximately 25% of these conditions. The user can verify this issue via log.berpd, which would indicate that the media has failed to synchronize.

Workaround: Reboot the secondary until it successfully reaches its "Standby" state.

When running software prior to S-Cz7.3.0m2 in an HA configuration, the active Oracle SBC goes out of service (OOS) when failing over to a secondary that has been upgraded to S-Cz7.3.0m2 if the active's SIPREC license is enabled, but the SIPREC feature is not configured. The secondary successfully becomes Active.

To prevent this, either configure SIPREC or disable the license on the Active prior to running the notify berpd force command. You can also upgrade the Active to S-Cz7.3.0m2 and reboot it, temporarily disabling high availability.

This issue has been resolved in S-Cz7.3.0M2.

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.

System Tools

Ping is not supported from the ACLI for IPv6 targets from media interfaces.

Note: This issue is resolved as of SCZ730M1.

Executing the **notify all rotate-logs** command crashes and reboots the system.

IKEv1 and IPv6 Support

IPv6 IPSec tunnels configured with IKEv1 do not get established.

Note: This issue is resolved as of SCZ730M1.

MSRP

MSRP file transfer over TLS is not functional.

Note: This issue is resolved as of SCZ730M1.

When configured for MSRP with IPv6, and running on the Acme Packet 6300, the Oracle Communications Session Border Controller may experience inordinate packet loss errors and chunked file transfer may fail. This issue was introduced in the SCZ730 release.

When running MSRP over TLS with infinite call hold times, the OC-SBC terminates sessions by sending a BYE

When running MSRP over TLS load tests, the OC-SBC intermittently sends inappropriate 503 responses to SIP requests.

This issue was identified in SCZ730M2.

IMS-AKA

For IMS-AKA endpoints that registered over UDP and are re-registering over TCP before half-time expiry, the Oracle Communications Session Border Controller forwards re-registration messages to the core instead of replying with 200OK. This issue was introduced in the SCZ730 release.

Note: This issue is resolved as of SCZ730M1.

SRTP

On the Acme Packet 3820, the OC-SBC inappropriately begins to send 503 responses to requests over SRTP when it reaches approximately 1600 sessions.

This issue was identified in SCZ730M2.

On the Acme Packet 4500, the OC-SBC begins to send 503 responses to messages over SRTP when it reaches approximately 1600 sessions. It then crashes, producing a DPWD error.

This issue was identified in SCZ730M2.

P-CSCF

If a UE successfully registers two contacts on the OC-SBC's P-CSCF, and the S-CSCF is out of service, the OC-SBC sends a 504 for a session on the first contact and a 403 for a session on the second contact.

This issue was identified in SCZ730M2.

High Availability

After a HA switchover, the new standby OC-SBC retains some TCP sockets of IMS-AKA subscribers. The user can clear these sockets by rebooting the OC-SBC.

This issue was identified in SCZ730M2.

Physical Interface

The system feature provided by the **phy-interfaces**'s **overload-protection** parameter and **overload-alarm-threshold** sub-element is not functional. Specifically, enabling the protection and setting the thresholds does not result in trap and trap-clear events based on the interface's traffic load.

The applicable ap-smgmt.mib SNMP objects include:

- apSysMgmtPhyUtilThresholdTrap
- apSysMgmtPhyUtilThresholdClearTrap

This issue was identified in SCZ720.

Behavioral Changes

The following behavioral changes from the previous GA release appear in this release. These changes reflect new behaviors that occur without any user intervention. If you are upgrading to this release from S-CZ7.1.2, ensure that you read the behavioral changes section in the S-CZ7.2.0 Release Notes.

SFTP Security Behavior

The user-level account now has read-only access on the filesystem for all platforms. In order to SFTP files onto an Oracle Communications Session Border Controller's filesystem, you must log in with a superuser-level (admin) account. This behavior only existed on certain platforms in the S-CZ7.2.0 GA release.

Default Password Removal

Upon starting the system, if default passwords exist, the user will be required to change them.

Minimum Advertised SSL/TLS Version

The default acceptable SSL/TLS version for clients connecting to the Oracle Communications Session Border Controller is TLS1.0. Prior to this release, SSLv3 was accepted. The legacy behavior may be enabled by configuration. More information is found in the ACLI Configuration Guide's Security chapter, Transport Layer Security section.

TLS1.2 Preferred Cyphers

When using TLS1.2, the advertised cypher suites order has changed to prioritize AES_GCM ciphers. The new order is:

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA

TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA
TLS_RSA_WITH_NULL_MD5

MIB changes

See *Interface Description in MIB Enhancement* feature.

media-profile subtype Configuration Restrictions

media-profiles are subject to stringent configuration restrictions. You must avoid creating a **media-profile** with configured **subtype** parameter that does not substantively differ (in all additional parameters) from the default (unconfigured) media profile. An example of an invalid configuration is **media-profile** > **name** of g729, and a **media-profile** > **subname** of g729, with no additional parameter configurations other than the default values. Such configuration can cause unexpected behaviors and must be avoided.