Oracle® Communications Session Border Controller & Session Router

Release Notes

Release S-CZ7.4.0

October 2018

Oracle Communications Session Border Controller & Session Router Release Notes, Release S-CZ7.4.0

Contents

List of Tables

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.
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.

Document Name	Document Description
MIB Reference Guide	Contains information about Management Information Base (MIBs), Oracle Communication's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the 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
November 2016	• Initial Release
December 2016	• Updated for S-Cz7.4.0p1, including marking resolved defects
December 2016	• Corrects 'Found In' for TSCF known issue • Corrects OC-SR platform support
January 2017	• Adds IMS-AKA DDoS upgrade note
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	• Adds M1 content • Removes Aria Cipher caveat
October 2017	Adds the following Caveat • Interface Utilization Support
June 2018	• Adds the High Availability Configuration Caveat. • Adds Pooled Transcoding Caveats • Adds Pooled Transcoding known issues

Date	Description
August 2018	• Moves QoS for transcoded calls caveat to "Older Caveats Fixed in This Release" • Adds M2 Appendix • Updates known issues table with defect fixes
September 2018	• Adds the SIP Known Issue.
October 2018	• Corrects information in M2 copy directing user to locate .XSD files on MOS

1
Introduction to S-CZ7.4.0

The Oracle Communications Session Border Controller S-CZ7.4.0 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 the S-CZ7.4.0 version of the SBC:

- Acme Packet 3820
- Acme Packet 4500
- Acme Packet 4600
- Acme Packet 6100
- Acme Packet 6300

The following platforms are supported by the S-CZ7.4.0 version of the SR:

- Acme Packet 4500
- Acme Packet 4600
- Acme Packet 6100
- Acme Packet 6300
- Bare-Metal Platforms, including Netra X5-2

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-CZ7.4.0 and above must have a high-speed fan module to ensure sufficient cooling.

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 1-1 Acme Packet 4500 NIU and Feature Group Support Matrix

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 1-2 Acme Packet 3820 NIU and Feature Group Support Matrix

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

Table 1-2 (Cont.) Acme Packet 3820 NIU and Feature Group Support Matrix

NIU	IPSec	IMS-AKA (unsupported)	SRTP	QoS	Transcoding	MSRP B2BUA (unsupported)	TSCF (unsupported)
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 1-3 Acme Packet 4600 NIU and Feature Group Support Matrix

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

Table 1-4 Acme Packet 6100 NIU and Feature Group Support Matrix

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

Table 1-5 Acme Packet 6300 NIU and Feature Group Support Matrix

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.

Upgrade Information

This section provides key information about upgrading to this software version.

Supported Upgrade Paths

The following upgrade paths are supported:

- S-CX6.4.0m7p3 -> S-CZ7.4.0
- S-CZ7.1.2m5p11 -> S-CZ7.4.0
- S-CZ7.2.0m6p7 -> S-CZ7.4.0
- S-CZ7.3.0m2 -> S-CZ7.4.0
- S-CZ7.3.0m2p1 -> S-CZ7.4.0

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

Upgrading Systems Running IMS-AKA DDoS

When upgrading an SBC running IMS-AKA DDoS and HA from S-CZ7.3.0M1 and later to S-CZ7.4.0, the user must upgrade and simultaneously reboot both the active and secondary nodes. This properly clears ACLs built by the earlier version, allowing the system to instantiate new, operational ACLs.

IMS-AKA DDoS is not supported in releases prior to S-Cz7.3.0M1. Upgrades from those versions to S-Cz7.4.0, therefore, does not require this simultaneous reboot.

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-CZ7.4.0 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.

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-CZ7.4.0 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+, S-CZ7.4.0+
- Acme Packet 4500, Transcoding NIU: S-CX6.3.7M2+ or S-CZ7.2.0+, S-CZ7.3.0+, S-CZ7.4.0+
- Acme Packet 6300, Transcoding NIU: S-CZ7.1.2+, S-CZ7.2.0+, S-CZ7.3.0+, S-CZ7.4.0+

Oracle Communications Session Element Manager

Oracle Communications Session Element Manager (SEM) versions 7.5M3 and later support this GA release of the Oracle Communications Session Border Controller . Partial support is available in earlier 7.5 versions of SEM, if desired. Contact your Sales representative for further support and requirement details.

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-CZ7.4.0M1 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 4500, 4600, 6100 and 6300, the Oracle Communications Session Router may run on other platforms.

As of release S-CZ7.4.0, the Oracle Netra Server X3-2, X5-2 are supported for the Oracle Communications Session Router application.

Table 1-6 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)

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-Cz7.4.0 GA:

- S-Cz7.2.0m6p7

The patch baseline, the most recent patch build from which the GA build was created, is SCZ730m2p1.

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
- C2.3.2
- 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
- C3.1.4
- C3.1.5
- C3.1.6

2

New Features in Service Provider Release S-CZ7.4.0

This section lists and describes features developed and released new for S-Cz7.4.0.

> **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.

SNMP IPv6 Transport

SNMP traps support IPv6 formatted addresses.
This feature description is found in the ACLI Configuration Guide, System Configuration chapter. Related content can be found in the Monitoring and Troubleshooting guide.

Transmitted Byte and Packet Count Report for Media Sessions

This release adds support for gathering both the number of bytes transmitted and the number of packets transmitted by the SBC to the Quality of Service (QoS) statistics already available for reporting on media sessions. The support also extends the system capability to gather such statistics from media interworking calls, in addition to non-media interworking and SRTP session calls. The system gathers and reports the transmitted bytes and packets information using the RADIUS protocol.
Feature information is found in Appendix C and D of the Accounting Guide and the Monitoring and Troubleshooting Guide, Performance Management chapter.

Viewing Active Audio and Video Call Statistics

The **show sessions** and **show sipd codec** CLI commands identify and display media processing statistics, such as the aggregate call count for active audio and video calls, and codec information per call.
Feature information is found in the Monitoring and Troubleshooting (Performance Management chapter) guides.

Advanced Logging

Advanced Logging allows targeted logging by overriding log levels, so that only a specific SIP request and its related messages get logged. The system matches criteria that you configure to determine which requests to log. The system also logs all messages related to the request, such as any responses, in-dialog messages, media, timers, and so on. Advanced Logging supports

multiple matching criteria for incoming requests and rate limiting. Advanced log files are smaller than debug files because the system logs only the specified number of matches in the specified period of time. Since the files are smaller, Advanced Logging uses fewer system resources than debug logging. To make searching easier, the system labels each log.
This feature description is found in the Monitoring and Troubleshooting Guide, Log Management chapter.

Datapath Watchdog Timer and SNMP Trap Generation

The Oracle Communications Session Border Controller's datapath watchdog timer performs periodic background checks on the continuity of the data path.
This feature description is found in the Monitoring and Troubleshooting Guide, Fault Management chapter.

SNMP Trap to Indicate Detection of Resource Contention

An SNMP trap is generated when a worker thread experiences a deadlock.
Feature information is found in the Monitoring and Troubleshooting (Fault Management chapter) guide.

Software Worker Threads Watchdog Timer and Health Check Trap

The Oracle Communications Session Border Controller monitors specific software threads for faults and provides the user with configurable actions to take in case of thread failure. The system registers applicable threads to this watchdog and assumes a thread has failed when it does not respond. By default, the Oracle Communications Session Border Controller generates information about the event and reboot history. For HA configurations, the system synchronizes this watchdog configuration and simultaneously operates on both the active and standby Oracle Communications Session Border Controllers.
This feature description is found in the Monitoring and Troubleshooting Guide, Fault Management chapter.

Datapath Watchdog Timer Expiration Trap

The Oracle Communications Session Border Controller's datapath watchdog timer performs periodic background checks on the continuity of the data path.
This feature description is found in the Monitoring and Troubleshooting Guide, Fault Management chapter.

System Reboot after Gateway Unreachable Event

Oracle Communications Session Border Controllers in an HA pair can be configured so that after a gateway unreachable event initiates a switchover, the newly standby system (where the event occurred) is rebooted.
This feature description is found in the Monitoring and Troubleshooting Guide, Fault Management chapter.

Packet Loss Alarms for Access Control Lists

The Oracle Communications Session Border Controller reports packet loss on traffic associated with Access Control Lists (ACLs) using alarms. These alarms use the Oracle Communications Session Border Controller's system's alarm management and user display mechanisms. The user can configure three **media-manager** parameters to set thresholds for these alarms.
This feature description is found in the ACLI Configuration Guide, Security chapter.

NIU-Based Processor Buffer Depletion Recovery

The following suite of three features will failover an Oracle Communications Session Border Controller in an HA pair for certain related NIU-based processor and input buffer conditions.

- Fast Failover after NIU-processor Core Crash
- Failover After Non-responsive NIU-processor Core
- Failover and Reboot on Filling up Input Queue

Feature information is found in the Monitoring and Troubleshooting Guide, Fault Management chapter.

CPU Load Limiting Enhancement

CPU load limiting on the Oracle Communications Session Border Controller is enhanced to provide the load-limit option with new configurable value that establishes a range within which the system rejects some SIP requests. When the utilization exceeds this range, the system rejects all new SIP requests.

Feature information is found in the Monitoring and Troubleshooting Guide, Performance Management 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.

DDoS for IMS-AKA

The Oracle Communications Session Border Controller supports DDoS protection for IMS-AKA. This can be enabled on the realm interface for the access network when the **access-control-trust-level** configuration element is set to **low** or **medium**.
This feature description is found in the ACLI Configuration Guide, IMS chapter.

IMS-AKA SROP Support

The SIP Registration Overload Protection (SROP) feature supports registrations via IMS-AKA. From the endpoint's perspective, overload protection for IMS-AKA endpoints is the same as for other environments. From the Oracle Communications Session Border Controller's perspective, however, overload protection functions differently with IMS-AKA, using ACLs to manage connectivity with the endpoint. De-registration support remains the same, either explicitly by UE signaling or by registration timeout. The ingress realm must be set to low or medium trust level.
This feature description is found in the ACLI Configuration Guide, IMS chapter.

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.

UPDATE Interworking

The Oracle Communications Session Border Controller can be configured to convert UPDATE methods (with or without SDP) to INVITE methods inside a dialog that has already been established. SDP is inserted when the UPDATE message doesn't have it. The method is modified from UPDATE to INVITE for the duration of an UPDATE based transaction and the SBC creates an ACK message to acknowledge the INVITE response.
This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter.

Call Leg PRACK Interworking

The Oracle Communications Session Border Controller can be configured to apply PRACK interworking to call legs during and after dialog establishment to convert UPDATE methods (with or without SDP) to INVITE methods for the duration of the UPDATE based transactions.
This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter.

SIP Assymetric Preconditions Support

This feature allows you to reserve network resources for a session before the called party is alerted by establishing preconditions for individual call legs. Currently, the Oracle Communications Session Border Controller transparently passes precondition attributes in SIP signaling and the UEs negotiate preconditions end to end. However, some networks support the SIP preconditions and other networks do not. To help provide precondition interworking between these networks, the Oracle Communications Session Border Controller supports SIP preconditions on a per call leg basis.
This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter.

Locally Generated SIP Response with RFC 3326 Reason

The Oracle Communications Session Border Controller issues a 503 Service Unavailable SIP response code when it fails to fulfill an apparently valid request because it is undergoing maintenance or is temporarily overloaded and so cannot process the request. This feature changes the reason phrase in the SIP response from the generic "Service Unavailable" to one that specifies the overload condition when exceeding the capacity for license sessions, transcoding license sessions, or DSP resources.
This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter.

Configurable number of PING timeouts to trigger SA Out Of Service

By default, if the Oracle Communications Session Border Controller does not receive a response to the ping from the session-agent, it marks it as out-of-service. You can configure the number of ping failures that the Oracle Communications Session Border Controller can receive before it marks the session-agent as out-of-service. This is achieved by configuring the OPTIONS parameter in the session-agent with a ping-failure value, where value is the number of ping response failures. This is true for both the keep-alive and continuous-ping modes.

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

TGRP and Trunk Context Acme Packet Specific AVP

The Oracle Communications Session Border Controller supports a dynamic reading of the initial INVITE message of the session Contact header and Request URI tag parameter. This facilitates populating the Trunk Group and Trunk Context parameters into the existing AVPs.
This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter.

Inclusion of P-Asserted-Identity and Diversion headers in SIPREC metadata

The Oracle Communications Session Border Controller supports some call transfer scenarios in which the contents of the P-Asserted-Identity, Diversion and History-info headers must be included in the SIPREC metadata for in-dialog requests (re-INVITE and UPDATE) as well as initial requests.
This feature description is found in the Call Monitoring Guide, Call Traffic Monitoring chapter.

Selective INVITE Holding for NPLI

When configured to use external policy servers, the Oracle Communications Session Border Controller allows the user to manage INVITE forwarding behavior based on preferences for inclusion of NPLI information. This forwarding behavior differs, depending on whether or not the call is an emergency call. The system also refers to external policy server, sip-interface and sip-config configuration to further specify when it forwards applicable INVITEs.
This feature description is found in the ACLI Configuration Guide, External Policy Servers 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.

TSCF Statistics

This version of the Oracle Communications Session Border Controller provides extensive statistics to monitor TSCF status and traffic.

- Security MIB - IPSec tunnel status and statistics
- Security MIB - TSCF operation status and statistics
- Security Traps - TSCF operation status
- ACLI - Show sipd sessions now includes TSCF statistics
- HDR - New group for TSCF statistics
- ACLI - New show tscf-stats command
- ACLI - Update to show comm-monitor command to collect and report on TSCF statistics

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 are noted below.

Reactive Transcoding Mode

When setting up transcoded calls the Oracle Communications Session Border Controller reserves a Digital Signaling Processor (DSP) resource for the incoming SDP offers that need transcoding. The default behavior is to pre-book the DSP resource and use it when the system's egress policy qualifies the SDP offer for transcoding.
This feature description is found in the ACLI Configuration Guide, Transcoding chapter.

Session Router Features

The features listed in this section are related to the Oracle Communications Session Router. Locations of the features descriptions within the Oracle Communications Session Border Controller documentation set are noted.

Session Agent Identification Enhancement

The Oracle Communications Session Border Controller uses the Ingress Session Agent Identification to match the incoming requests to its respective Session Agents. CAC (Call Admission Control) is performed for the inbound traffic based on the originating endpoint of the Session Agents regardless of the IP address.
This feature description is found in the ACLI Configuration Guide, Session Routing chapter.

3
Inherited Features

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

- S-CZ7.3.0 M1 and M2

These features were not included in S-CZ7.3.0 GA docset.

S-CZ7.3.0 Maintenance Release Features

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

Advanced Logging

An Advanced logging feature is added to the S-Cz7.3.0M2 release that allows the user to narrow the scope of the output collected in logs. Advanced logging is enhanced over the S-Cz7.3.0M2 release in S-Cz7.4.0 release to encompass additional operational sources from which the system can execute advanced logging.

This feature description is found in the Monitoring and Troubleshooting Guide, Logs chapter. Additional feature information is found in the ACLI Reference Guide.

Behavioral Changes to Bandwidth Requests

The Oracle Communications Session Border Controller can evaluate transcoding and IPv4 to IPv6 call scenarios and mitigate between end stations and policy servers to request appropriate bandwidth.
This feature description is found in the ACLI Configuration Guide, External Policy Server chapter.

Updating the b=AS line for Transcoded Calls

The Oracle Communications Session Border Controller can evaluate transcoding call scenarios and mitigate between end stations and policy servers to request appropriate bandwidth. The user can configure a specific value to be included in the SDP's b=AS line to ensure that it requests the correct bandwidth for transcoded calls. Depending on the transcoding scenario, this value may or may not be used.
This feature description is found in the ACLI Configuration Guide, Transcoding chapter. Additional information is found in the ACLI Reference Guide.

Video Conferencing Support for Polycom Terminals

The Oracle Communications Session Border Controller includes support for Polycom video conferencing that implements messaging properly and presents proper addressing information for session billing, as described below.
This feature description is found in the ACLI Configuration Guide, H.323 Signaling chapter.

Selecting SDP within Multi-Dialog Call Scenarios

By default, the Oracle Communications Session Border Controller saves SDP presented in a series of early dialogs using To tags to differentiate between dialogs. If the session continues

with a 200OK that does not include SDP, the Oracle Communications Session Border Controller refers to the To tag to identify the dialog from which the Oracle Communications Session Border Controller selects the SDP for the media flow. This complies with 3GPP TS 24.628, TS 24.182 and RFC 5009 behavior for sessions supporting early media.
This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter.

Oracle Operations Monitor Statistics

The Oracle Communications Session Border Controller collects statistics on the operations of its communications monitor probe, which provides protocol traffic information to Oracle Communications' Session Monitor. The user displays information about the connections to Session Monitor servers using the **show comm-monitor** command. The user can set all comm-monitor statistics to zero using the command **reset comm-monitor**.
This feature description is found in the Call Monitoring Guide, Call Traffic Monitoring chapter. Additional information is found in the ACLI Reference Guide.

Thread Level Load Monitoring and Alarms

The Oracle Communications Session Border Controller provides a thread-level monitoring for CPU usage, specifically including three critical traffic processes: SIP, ATCP and MBCD. Applicable information is found in the ACLI Reference Guide.

Per-Realm Media Guard Timers

Oracle Communications Session Border Controller realm configurations support media guard timers whose settings take precedence over global media guard timers configured in the media manager. Both generic flow and TCP-specific flow timer settings are available. The user configures these timers in seconds in the realm-config.
This feature description is found in the ACLI Configuration Guide, Realm and Nested Realms chapter. Additional information is found in the ACLI Reference Guide.

DNS Entry Maximum TTL

DNS maximum time to live (TTL) is user-configurable and complies with RFCs 1035 and 2181.
This feature description is found in the ACLI Configuration Guide, System Configuration chapter. Additional information is found in the ACLI Reference Guide.

DNS Re-query over TCP

The Oracle Communications Session Border Controller DNS supports the truncated (TC) header bit in DNS responses as defined in RFC 2181 and a re-query over TCP.
This feature description is found in the ACLI Configuration Guide, System Configuration chapter.

DNS Queries on the Command Line

Users can perform Domain Name Services (DNS) queries from the command line. Positive results are added to the DNS cache.
Applicable information is found in the ACLI Reference Guide.

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

Support millisecond granularity for acct-session-time

Some accounting features require greater precision. The attribute **acct-session-time** can be configured to be in milliseconds.

This feature description is found in the Accounting Guide, Configuring Accounting chapter.

Override Alphanumeric Ordering of Session Agents with same IP address

The Oracle Communications Session Border Controller can associate an incoming call with a Session Agent based upon the **precedence** attribute for systems that have the same IP address, rather than the alphanumeric order of hostname.
This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter.

Call Detail Record Sequence Number in Filename

To assist in the identification of lost Call Detail Record (CDR) files, the customer can enable the **file-seq-number** attribute to assign a sequence number to append to the file. A separate configuration element, **temp-remote-file**, allows for the prepending of the characters "tmp-" to CDR files during transfer.
This feature description is found in the Accounting Guide, Configuring Accounting chapter. Additional information is found in the ACLI Reference Guide.

TSM Security Traversing Gateway Mode

The Security Traversing Gateway (STG) is a specific implementation of the TSCF, and is responsible for maintaining tunnels between the client and server, and handles encapsulation and de-encapsulation for IMS service data. Tunnel types include TLS and DTLS tunnels.
This feature description is found in the ACLI Configuration Guide, Tunneled Services Control Function chapter.

SIP Pre-emptive Symmetric Media Latching

The Oracle Communications Session Border Controller (SBC) supports symmetric media latching within a realm. However, when two SBCs are in different realms and both realms are configured for symmetric latching, then both will wait for received media packets from the other before transmitting, which results in dropped calls. This feature lets the user configure the SBC to transmit its RTP packets pre-emptively to the peer SDP connection address and then to re-latch the peer RTP source address after receiving the first RTP packet from that peer.
This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter. Additional information is found in the ACLI Reference Guide.

Asynchronous SIP-Diameter Communication

The Oracle Communications Session Border Controller's Diameter-based external policy server support now offers an asynchronous mode in which the SBC does not wait for a Diameter Authorization-Authentication Answer (AAA) response to an Authorization-Authentication Request (AAR) before allowing the SIP 200 OK to proceed through the SBC.
This feature description is found in the ACLI Configuration Guide, External Policy Servers chapter. Additional information is found in the ACLI Reference Guide.

Flow-Description AVP Change for Media Release

The Rx interface between the Oracle Communications Session Border Controller (SBC) and the Policy Server (PS) assumes that the media is always managed by the SBC and that the IP address and port number of one end of a service flow will always correspond to one present on the SBC. However, there are times when the media is released by the SBC, but a policy server request is still required. In these cases the flow descriptions should accurately represent the IP addresses of the two endpoints instead of that of the SBC. This feature lets the user configure the SBC to change the payload of the Flow-Description Attribute Value Pair (AVP) in the Diameter AAR messaging from the SBC to the PS, depending on whether the media is managed or released by the SBC.

This feature description is found in the ACLI Configuration Guide, External Policy Servers chapter. Additional information is found in the ACLI Reference Guide.

DDoS Enhancement for IMS-AKA

The Oracle Communications Session Border Controller's IMS-AKA support includes the ability to dynamically create trusted ACLs and install corresponding NAT flows using secure ports negotiated during registration. Using ACLs for this traffic mitigates against denial of service attacks. The user must configure the **"enhanced-acl-promote="tcp,udp""** option on the access side sip-interface and ensure that dynamic ACL functionality is enabled on the access realm. Without this configuration, the Oracle Communications Session Border Controller uses a wild carded source port and a destination port of 5060 an no ACL to manage this traffic.
This feature description is found in the ACLI Configuration Guide, IMS chapter.

RADIUS and Diameter Statistics

The SBC can display both RADIUS and Diameter accounting protocol statistics, including Diameter message related statistics, on the Rx (policy server) and Rf (accounting server) interfaces.
This feature description is found in the Accounting Guide, Configuring Accounting chapter. Additional information is found in the ACLI Reference Guide.

TCP Connection Tools

The S-Cz7.3.0M2 and S-Cz7.4.0 releases add or enhance multiple show commands to display more information on TCP traffic and connections.

This feature description is found in the Monitoring and Troubleshooting Guide, Fault Management chapter. Additional feature information is found in the ACLI Reference Guide.

Blocking TSCF Inter-client Communication

The **inter-client-block** assigned service is a specific implementation of the TSCF, and is responsible for preventing clients using TSCF from communicating directly with other TSCF clients. Without the use of this assigned-services mode, any TSCF client could directly send traffic to other TSCF clients on any realm on the TSCF server. The blocking of this type of inter-client communication capability enhances security.

This feature description is found in the ACLI Configuration Guide, Tunneled Services Control Function chapter.

4

Interface Changes

This chapter summarizes ACLI, SNMP, HDR, Alarms, and RADIUS changes (where applicable) for S-CZ7.4.0. 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-CZ7.4.0

Command	Description
show trap-receiver	Enhanced to display IPv6 addresses
show snmp-community-table	Enhanced to display IPv6 addresses
show sessions	Enhanced to identify and display media processing statistics, such as the aggregate call count for active audio and video calls, and codec information per call.
show sipd codec	Enhanced to identify and display media processing statistics, such as the aggregate call count for active audio and video calls, and codec information per call.
show tscf-stats	This command displays TSCF statistical information.
show comm-monitor	Enhanced to include TSCF information.

The following table summarizes the ACLI configuration command changes that first appeared in a release prior to Oracle Communications Session Border ControllerS-CZ7.4.0, but are new to this major release.

Command	Description
show comm-monitor	Displays statistics related to the configured communications monitor. Allows for execution with additional parameters to narrow the output.
reset comm-monitor	Sets all communications monitor statistics to zero.
show processes	Enhanced to include thread-level CPU usage statistics.
show queues atcpd	Displays thread-level CPU usage information for the atcpd protocol threads.
show queues sipd	Displays thread-level CPU usage information for the sipd protocol threads.
show dns lookup	Instructs the system to performs a first query the local DNS cache and then perform an external DNS query, if needed.
show queues query	Instructs the system to performs a manual external DNS query with no cache lookup.

Command	Description
show policy-server	Displays statistics for the Rx interface.
show accounting <IP:Port> <DiamMsg>	Shows statistics on the specified diameter messages exchanged with a configured external accounting server.
show accounting all <DiamMsg>	Shows statistics on the specified diameter messages exchanged with all configured external accounting servers.
show accounting connections	Shows status information on all external accounting servers.
show radius accounting [all | <IP:Port>]	Shows the status of all or the specified established RADIUS accounting connection(s).
show sipd tcp	Shows the status of all TCP sockets.
show sipd tcp connections	Shows the status of all active TCP connections.

ACLI Configuration Element Changes

This section summarizes the ACLI configuration element changes that first appear in release Oracle Communications Session Border ControllerS-CZ7.4.0

System Features

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

Accounting Features

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

IMS/VoLTE Features

There are no new configuration elements, nor new parameters for IMS-Volte features in this release.

Signaling Features

New Parameters	Description
session-router > **sip-advanced-logging**	Allows the user to configure one or multiple advanced logging scenarios.
session-router > **sip-advanced-logging** > **conditions**	Allows the user to configure one or more condition(s) upon which the system begins advanced logging.
session-router > **sip-config** > **local response-map-entries**	Adds the values of **q.850-cause** and **q.850-reason** in the **local-response-map-entries** configuration element to the reason header when the value of **add-reason header** in the **sip-config** configuration element is **enabled**.

New Parameters	Description
session-router > **sip-interface** > **asymmetric-preconditions**	Identifies whether to enable preconditions interworking on the interface. Allowable values are **enabled** and **disabled**. The default is **disabled**. You cannot enable asymmetric preconditions unless you have first set the value of **sip-interface > options** to **100rel-interworking**.
session-router > **sip-interface** > **asymmetric-preconditions-mode**	Identifies, when the value of **asymmetric-preconditions** is **enabled**, whether to send egress INVITEs immediately or to delay them until preconditions have been met. Allowable values are **send-with-delay** and **send-with-nodelay**. The value **send-with-delay** delays INVITEs on the egress interface until preconditions are met on the ingress interface. The value **send-with-nodelay** forwards INVITEs to the egress interface immediately, but holds the responses until preconditions are met on the ingress interface. The default is **send-with-nodelay**.
session-router > **sip-interface** > **add-sdp-in-msg**	Identifies the messages in which to insert SDP offers or answers. The only allowable value is **18xresp** which, for an offerless INVITE that needs preconditions, causes the SBC to insert the SDP, as configured in the media profile names listed in **add-sdp-profiles-in-msg**, in the 18x (183) response towards the UE. The default is null (no value).
session-router > **sip-interface** > **add-sdp-profiles-in-msg**	Identifies a list of media profiles that contain, based on the codec, the SDP to insert in the 18x response when **add-sdp-in-msg** is configured.

Transcoding Features

New Parameters	Description
media-manager > **reactive-transcoding**	Enables of disables the reactive transcoding functionality

TSCF Features

New Configuration Elements	New Parameters and Description
security > **tscf** > **tscf-interface** > **assigned-services** > **inter-client-block**	Setting this value prevents clients using TSCF from communicating directly with other TSCF clients.

Security Features

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

Inherited Features

The following table summarizes the ACLI configuration element changes that first appeared in a release prior to Oracle Communications Session Border ControllerS-CZ7.4.0, but are new to this major release.

New Parameters	Description
session-router > **media-profile** > **as-bandwidth**	Sets the bandwidth amount to be requested within the context of a media profile.
media-manager > **flow-time-limit**	The time that a dynamic flow has been inactive, after which the system notifies the application and can be removed.
media-manager > **initial-guard-timer**	The initial time before the first traffic appears on a dynamic flow, after which the system notifies the application and can be removed.
media-manager > **subsq-guard-timer**	The maximum time in seconds allowed to elapse between all subsequent sequential packets.
media-manager > **tcp-flow-time-limit**	The maximum time in seconds that a media-over-TCP flow can last.
media-manager > **tcp-initial-guard-timer**	The maximum time in seconds allowed to elapse between the initial SYN packet and the next packet in a media-over-TCP flow.
media-manager > **tcp-subsq-guard-timer**	The maximum time in seconds allowed to elapse between all subsequent sequential media-over-TCP packets.
system > **network-interface** > **dns-max-ttl**	The maximum time for a non-ALG DNS record to remain in cache.
media-manager > **dns-config** > **dns-max-ttl**	The maximum time for a DNS record managed by the DNS ALG to remain in cache.
session-router > **session-agent** > **precedence**	Sets the importance level of this IP/hostname combination for Session Agents, allowing the system to choose a specific agent when there are multiple agents with the same IP address.
session-router > **account-config** > **file-seq-number**	Allows the system to assign a 9-digit file sequence number to append to a CDR filename.
session-router > **session-agent** > **push-receiver** > **temp-remote-file**	Allows the system to prepend of the characters "tmp-" to Call Detail Record (CDR) files during transfer.
media-manager > **realm-config** > **symmetric-latching**	Adds the pre-emptive mode value to instruct the system to use pre-emptive mode, in addition to simply enabling or disabling symmetric latching in the realm.
media-manager > **ext-policy-server** > **asynchornous-mode**	Instructs the system to use the asynchronous mode of signaling on the external policy server interface rather than the default synchronous mode.
media-manager > **ext-policy-server** > **media-release**	Instructs the system to change the payload of the Flow-Description Attribute Value Pair (AVP) in the Diameter AAR messaging from the SBC to the PS, depending on whether the media is managed or released by the SBC.
media-manager > **untrusted-drop-threshold**	Percent untrusted traffic value at which the system generates an alarm.
media-manager > **trusted-drop-threshold**	Percent trusted traffic value at which the system generates an alarm.
media-manager > **dynamic-trusted-drop-threshold**	Percent dynamic trusted traffic value at which the system generates an alarm.

New Parameters	Description
security > **tscf** > **tscf-interface** > **assigned-services** > **stg**	This STG value is not intended for all customer use. Consult your Oracle representative to understand the circumstances indicating the use of this feature.
system > **system-config** > **alarm-threshold** > **type** > **cpu-sipd**	Configures the system to generate alarms based on CPU usage by the sipd daemon.
system > **system-config** > **alarm-threshold** > **type** > **cpu-atcp**	Configures the system to generate alarms based on CPU usage by the atcp daemon.
system > **system-config** > **alarm-threshold** > **type** > **cpu-mbcd**	Configures the system to generate alarms based on CPU usage by the mbcd daemon.
session-router > **session-agent** > **precedence**	Defines the agent selection precedence when the system chooses between Session Agents with same IP address.

Alarms

This section summarizes the Alarm changes that appear in the Oracle Communications Session Border Controller version S-CZ7.4.0.

ACL Alarms

The following alarms are added to report on ACL traffic conditions:

- ACL_UNTRUSTED_DROP_OVER_THRESHOLD
- ACL_TRUSTED_DROP_OVER_THRESHOLD
- ACL_DYNAMIC_TRUSTED_DROP_OVER_THRESHOLD

Thread Usage Alarms

Alarms are added to report on thread usage conditions, based on the following alarm-threshold types:

- cpu-sipd
- cpu-atcp
- cpu-mbcd

Accounting

This section summarizes the Accounting changes that appear in the Oracle Communications Session Border Controller version S-CZ7.4.0.

The Acme-Packet-Specific-Extension-Rf AVP items now includes additional AVPs for media QoS statistics.

Application SNMP/MIB Changes

This section summarizes the Application SNMP/MIB changes that appear in the Oracle Communications Session Border Controller version S-CZ7.4.0.

The following MIB object files are updated, as follows:

- ap-usbcsys.min-Objects and traps added to support CPU thread monitoring.
- ap-smgmt.mib-Traps added to report deadlock events.
- ap-sip.mib-Objects and traps added to monitor video statistics.
- ap-security.mib-Objects and traps added to monitor TSCF operation.

HDR

This section summarizes the HDR changes that appear in the Oracle Communications Session Border Controller version S-CZ7.4.0.

There are two HDR groups available to record Thread Level Load Monitoring information:

- thread-event: reports pending and dropped events per protocol as well as calculating latency
- thread-usage: reports CPU thread usage per protocol and an overload condition

The data captured by these two HDR groups corresponds to the show queues atcpd and show queues sipd ACLI command output.

In addition, there is a new group for capturing operational statistics on TSCF.

5

Caveats and Known Issues

This chapter lists the caveats, known issues, limitations, and behavioral changes for this release. Oracle updates this Release Notes document to distribute issue status changes. Check the latest revisions of this document to stay informed about these issues.

Older Caveats Fixed in This Release

The following caveats have been fixed in SCZ7.4.0:

- QoS reporting is now supported for transcoded calls.

Caveats

This section presents Oracle Communications Session Border Controller issues that are inherent to this major version of the product.

Interface Utilization Support

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

System Tools

The system feature that sends a Gateway Unreachable Trap and Reboot for HA does not work on an Acme Packet 4500 that does not include a hard disk.

Transcoding

Only SIP signaling is supported with transcoding.

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

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

The following media-related features are not supported in pooled transcoding scenarios:

- Lawful intercept
- 2833 IWF
- Fax scenarios
- RTCP generation for transcoded calls

- T.140-Baudot Relay
- OPUS/SILK codecs
- SRTP and Transcoding on the same call
- Asymmetric DPT in SRVCC call flows
- Media hairpinning
- QoS reporting for transcoded calls
- Multiple SDP answers to a single offer
- PRACK Interworking
- Asymmetric Preconditions

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.

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 and the Acme Packet 4500.

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.

High Availability Configuration

HA redundancy is unsuccessful when you create the first SIP interface, or the first time you configure the Session Recording Server on the Oracle Communications Session Border

Controller (SBC). Oracle recommends that you perform the following work around during a maintenance window.

1. Create the SIP interface or Session Recording Server on the primary SBC, and save and activate the configuration.
2. Reboot both the Primary and the Secondary.

Known Issues

This table lists S-Cz7.4.0 known issues. The user can reference defects by Service Request number and can identify the issue, any workaround, when the issue was found, and when it was fixed using this table. Issue descriptions not carried forward from previous versions' Release Notes and documented herein are not relevant to this release. The user can review delivery information, including defect fixes via this release's Build Notes.

Unsupported Features

ID	Description	Found In	Fixed In
	This version's enhancement to SMP-Aware Task Load Limiting, which adds a second parameter to the sip-config's load-limit option, is currently not supported.	SCZ740	

System Tools

ID	Description	Found In	Fixed In
	The Communications Monitor Probe does not work in this release.	SCZ740	SCZ740p1
	The Communications Monitor Probe cannot connect to the mediation engine (OCOM server) over an SBC's media interface.	SCZ740	SCZ740p1
	The **show interfaces brief** command incorrectly shows **pri-util-addr** information in its output.	SCZ740	
	The SBC incorrectly generates a core dump as it reboots, even though its **sw-health-check-action** option is set to only **logandreboot**.	SCZ740	SCZ740p1
26338219	The **packet-trace remote** command does not work with IPv6.	SCZ740	

Physical Interface

ID	Description	Found In	Fixed In
	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	SCZ720	

PRACK Interworking Function (IWF)

ID	Description	Found In	Fixed In
	Call scenarios that include PRACK IWF in conjunction with SRTP are not supported.	SCZ740	SCZ740p1
	The PRACK IWF is not supported with offer-less INVITE scenarios.	SCZ740	SCZ740p1

IMS-AKA DDoS

ID	Description	Found In	Fixed In
	During IMS-AKA registration, the SBC is not dropping non-IPSec packets.	SCZ740	SCZ740p1
	During IMS-AKA registration, an ACL entry with a trust-level of low is not being demoted from untrusted to denied.	SCZ740	SCZ740p1
	If the user has configured the new ims_aka option, they must also configure sip-interfaces with an ims-aka-profile entry.	SCZ740	
	When an SBCoperating on an Acme Packet 6300 fails over, the secondary can successfully add new ACL entries, but it also retains old ACL entries that it should delete.	SCZ740p1	SCZ740p3

IMS-AKA SIP Registration Overload Protection

ID	Description Workaround	Found In	Fixed In
	An initial IMS-AKA registration works, but re-registration and De-registration doesn't work if the trust-level=medium	SCZ740	SCZ740p1

SBC Running as an SLB Cluster Member

ID	Description	Found In	Fixed In
	Rebalancing is unavailable on the OCSLB 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.	SCZ730	

SIP

ID	Description	Found In	Fixed In
28650852	The SBC changes the value of the P-Early-Media header in a 183 message to the sip-interface's **p-early-media-direction** parameter setting.	SCZ740	

Accounting

ID	Description	Found In	Fixed In
	RADIUS stop records for IWF calls may display inaccurate values.	SCZ730b6	

IPv6

ID	Description	Found In	Fixed In
	Media interfaces configured for IPv6 do not support multiple VLANs.	SCZ730	

H.323

ID	Description	Found In	Fixed In
	SIP-H323 hairpin calls with DTMF tone indication interworking is not supported.	S-CZ720a5	
	The SBC crashes when the user has configured an H323 stack supporting SIP-H323-SIP calls with its **max-calls** parameter set to a value that is less than its **q931-max-calls** parameter. Workaround: For applicable environments, configure the H323 stack's **max-calls** parameter to a value that is greater than its **q931-max-calls** parameter.	S-CZ740	
	HA Redundancy is not supported for H.323 calls.		

Session Router

ID	Description	Found In	Fixed In
	If after upgrading to a S-CZ7.4.0 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.		
	When the session-router is configured with a operation-mode of session, it is failing to correctly clear sessions.	S-Cz7.2.0	

MSRP

ID	Description	Found In	Fixed In
	When configured for MSRP with IPv6, and running on the Acme Packet 6300, the SBC may experience inordinate packet loss errors and chunked file transfer may fail.	SCZ730	SCZ740p1
	Chunked file transfers fail when configured for MSRP and running on the Acme Packet 6300 or 4500.	SCZ740	
	When running MSRP over TLS with infinite call hold times, the SBC terminates sessions by sending a BYE.	SCZ730	SCZ740p1
	When running MSRP over TLS load tests, the SBC intermittently sends inappropriate 503 responses to SIP requests.	SCZ730M2	SCZ740

TSCF

ID	Description	Found In	Fixed In
24313811	When running TSM, the SBC crashes after setting up approximately 2500 TLS tunnels/calls.	SCZ730M2	

ID	Description	Found In	Fixed In
	The SBC is unable to synchronize all tunnels across an HA pair when the number of idle TSM tunnels exceeds 120k. The user can verify current tunnel count with the **show tscf address-pool all** command.	SCZ740	

On-line Upgrade for HA Systems

ID	Description	Found In	Fixed In
22322673	When running S-CZ7.4.0 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.	SCZ7.3.0P1	

SRTP

ID	Description	Found In	Fixed In
	On the Acme Packet 3820, the SBC inappropriately begins to send 503 responses to requests over SRTP when it reaches approximately 1600 sessions.	SCZ730M2	
24355937	On the Acme Packet 4500, the SBC begins to send 503 responses to messages over SRTP when it reaches approximately 1600 sessions. It then crashes, producing a DPWD error.	SCZ730M2	SCZ740p1

P-CSCF

ID	Description	Found In	Fixed In
24346106	If a UE successfully registers two contacts on the SBC's P-CSCF, and the S-CSCF is out of service, the SBC sends a 504 for a session on the first contact and a 403 for a session on the second contact.	SCZ730M2	SCZ740p1

High Availability

ID	Description	Found In	Fixed In
23253731	After an HA switchover, the new standby SBC retains some IMS-AKA subscriber TCP sockets. The user can clear these sockets by rebooting the SBC.	SCZ730M2	

Pooled Transcoding

ID	Description	Found In	Fixed In
28062411	Calls that require SIP/PRACK interworking as invoked by the 100rel-interworking option on a SIP interface do not work in pooled transcoding architectures.	SCZ740	SCZ740M2
28071326	Calls that require LMSD interworking as invoked by the lmsd-interworking option on a SIP interface do not work in pooled transcoding architectures. During call establishment, when sending the 200 OK back to the original caller, the cached SDP is not included.	SCZ740	SCZ740M2

Limitations

This section documents the limitations in this software release of which the user should be aware.

IPv6 Wancom Interfaces on the Acme Packet 4500

The Acme Packet 4500 does not support IPv6 addressing on management (wancom) interfaces.

A

SCZ740M1

This section provides descriptions, explanations, and configuration information for the contents of Maintenance Release SCZ7.4.0M1. Maintenance Release content supercedes that distributed with the point release.

In addition to those documented in the Supported SPL Engines section of these release notes, this release also supports SPL engine version C3.1.7.

Current patch baseline: SCZ7.4.0p8

Please refer to this Release Notes' Known Issues section for known issue changes applicable to this release.

Patch Equivalency

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

Neighbor Release Patch Equivalency for S-CZ7.4.0M1:

- SCZ7.4.0p8
- SCZ7.3.0m3p2
- SCZ7.2.0m6p10

Deprecated Features

The features listed in this section are removed from the Oracle Communications Session Border Controller's, beginning with this version.

Weak Ciphers

The SCZ7.4.0M1 version of the Oracle Communications Session Border Controller deprecates the following ciphers, adhering to recent OpenSSL changes intended to eliminate weak ciphers:

- All DES-CBC ciphers, including:
  - TLS_DHE_RSA_WITH_DES_CBC_SHA
  - TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA

Remove any prior Oracle Communications Session Border Controller version configuration that used these ciphers, and do not configure a security profile with the expectation that these ciphers are available. Note also that TLS profiles using the **ALL** (default) value to the **cipher-list** parameter no longer use these ciphers.

> **Note:**
>
> The ACLI still prints these ciphers when you run **cipher-list ?**. Despite printing them in ACLI output, the system does not support them within service operations.

Content Map

The following table identifies the new content in this SCZ7.4.0 M1 Maintenance Release documentation.

Content Type	Description
Adaptation	RTP Timestamp Synchronization

RTP Timestamp Synchronization

The Oracle Communications Session Border Controller maintains the continuity of egress transcoded media streams during HA switchover by synchronizing the RTP timestamps between active and standby systems.

For a new call, the transcoding resources are allocated and each session is configured with an initial RTP timestamp value. This process is repeated independently on both the active and standby systems to maintain approximately the same timestamps. This minimizes the difference between active and standby-side interpretation of the current RTP timestamp for a new session.

During HA operation, the active system maintains new timers that check for transcoded sessions lasting fifteen minutes or more. The active system re-synchronizes the RTP timestamp after fifteen minutes. This prevents the RTP timestamps from drifting due to clocking differences between active and standby hardware.

In addition, when the standby system boots, it performs a complete session sync with the active system for all currently active sessions.

S-CZ7.4.0M1 Build Notes

This section lists all intermediate patches through S-CZ7.4.0M1 and the bug fixes delivered within. This information duplicates the text file included within the media package.

nnSCZ740m1 - 9/1/2017

- Bug #24605288: "show enum rate" command fails to display requests sent counters.

  Problem: "show enum rate" command fails to display requests sent counters.
- Bug #25876680: RPH header r-value 'esnet.0' not handled properly

  Problem: SBC rejecting the call when RPH header contain r-value 'esnet.0'
- Bug #26030032: Leaked forwarding rules during TCP registrations

  Problem: After the new registration using ephemeral TCP source port Y has finished the SLB has two trusted forwarding rules, one with ephemeral TCP source port X and another with ephemeral TCP source port Y. The rule with ephemeral TCP source port X remains in the SLB indefinitely, but the assumption is that it should be deleted when the second registration triggers addition of the rule for ephemeral TCP source port Y. In the SBC only

one registration cache entry is ever present as the same SBC Contact header cookie is used for both the first and second registrations.

- Bug #26316830: USM Stops Accepting TCP Connections

  Problem: Customer is performing overnight load test on USM and found that USM stops accepting any new connections from the UE.

- Bug #24305070: Switchover triggered by data path failures

  Problem: Amcc Scratch buffer IFREEL OPT-1 cannot handle IPv6 to IPv4 Interworking issue.

- Bug #25360947: Customer is reporting CPU spikes on 2 6300 HA pairs

  Problem: SIPD threads can spin and consume high CPU when order-codecs is configured in codec-policy, and the SBC reorders codecs when the SDP contains more than one codec with the same name.

- Bug #25559154: sipd crash

  Problem: Sipd crash when communication session has been terminated prior to the recording dialog being established.

- Bug #20728163: SCTP error "Resource temporarily unavailable" after Invite

  Problem: SCTP error "Resource temporarily unavailable" after Invite

- Bug #22815250: SBC is not matching on the manipulation-string

  Problem: HMR supports built-in variables for common components of the SIP message available for use in your HMRs to improve performance and reduce development complexity.$LOCAL_IP, $LOACL_PORT, $REMOTE_IP, $REMOTE_PORT, $MANIP_STRING, $MANIP_PATTERN while Element Rule Processing with "action" value is "store" and "match-value" is "BuiltIn Variable", above BuiltIn variable failing to resolve

- Bug #22983472: large SNMP process delay (~2 minutes))

  Problem: Using third party SNMP scripts to snmpwalk a network interface table '/proc/net/dev' with 658 or more vlan interfaces configured, the IF-MIB walk of interface indexes can take up to 2 minutes to complete.

- Bug #23193382: sbc does not send update as refresher in session-timer-config setup

  Problem: The SBC does not send update as refresher in session-timer-config setup

- Bug #23221280: SCZ730m1p3 sipd crash (SEGFAULT)

  Problem: SCZ730m1p3 sipd crash (SEGFAULT)

- Bug #23230729: SBC experienced DPWD crash on NN4500 with ETC NIU

  Problem: ECC DDR errors cause NIU card to crash

- Bug #23243087: sipd crash on SCZ720m6p3

  Problem: SIPD crashed while applying configuration changes.

- Bug #23618418: Issues with interfaces on 7xx Software

  Problem: Multiple issues with the media interfaces for the line card which include interfaces won’t come up on reboot, leds going off during the boot up, gateways unreachable

- Bug #23706151: Wrong health score in alarm

Problem: When two cables are unplugged from the SBC the health score goes down to 0 but the alarm displays it to be 50.

- Bug #24491935: SBC generating a flood of INVITEs during a 407 without auth

  Problem: Surrogate agent did not handle the error case of the 407 message with missing Authenticate header, leading to an INVITE loop

- Bug #24554284: SBC Reported CPU Alarms for Core-0 Consuming 100% and tMedSts Consuming 96%

  Problem: Intermittent RCU stall. Process "tMEedSts" occupying 96% on CPU Core-0

- Bug #24702635: 4500 SCZ720 sipd crash when adding or removing ENUM servers from config

  Problem: Sipd crash when adding or removing ENUM servers from configuration. Two crashes are reported with this defect: 1) load_local_policy() of SipProxy 2)TimedObject destrcutor of SipTRIPProcess.

- Bug #24702918: Audio Quality issues after SBC upgrade to SCZ720m6p6

  Problem: Audio quality goes down due to packet loss. Analysis determined that the duplex bit in the np3700 register was not getting set for 100M speed and thus the interface was running in half duplex, resulting in packet loss.

- Bug #24765715: could not identify psipcontact

  Problem: Logs filled with "Alarm - MINOR could not identify psipcontact"

- Bug #24831292: Customer is reporting registration count dropped

  Problem: During activate sip is queuing commands to atcpd to set tos setting for TCP sockets. This causes mbuf exhaustion and loss of registrations.

- Bug #25023340: SNMP stopped reporting

  Problem: tSnmpd deadlocked after several weeks of normal operation

- Bug #25041276: tMbcd crash on SCZ7.2.0 MR-6 Patch 7

  Problem: Mbcd crash when customer removed enum ip and performed save-activate

- Bug #25091209: SPL Media Release API

  Problem: Oracle SPL Consulting have identified customer with a need for media of selective calls to be released in order to preserve bandwidth through the satellite link between end point and SBC. Due to other requirements of the SBC, namely transcoding, they were unable to achieve this need using native SBC configuration.

- Bug #25092954: The current acl untrusted drop count is high

  Problem: customer saw the acl trusted/untrusted drop count at the large number with very high drop ratio such as 61% and delta drop value is 2379269109~3468811723 and most time is during switch over from active to standby and cause the issue on standby side.

- Bug #25105759: setAclDropLogEventMod is set to 1 but log.npsoft does not display logevent

  Problem: setAclDropLogEventMod is set to 1 but log.npsoft does not display logevent

- Bug #25108295: Sipd crash

  Problem: SIPD crashed when sending a ping message to a session-agent

- Bug #25111988: Unclear exit code for "reboot standby SBC on gateway unreachable" feature

Problem: Unclear exit code for "reboot standby SBC on gateway unreachable" feature

- Bug #25128475: SD stops processing sip signaling - Lock timeout events seen

  Problem: Customer reported deadlock issue in sipd thread wherein sipd threads locking each other recursively across different functions and appears as if there are many deadlocks. Deadlock happened among SipSurrogateReg, SipSession, SipUser, SipSAGroup and SessionStats.

  ```
  SipUser and SipSurrogateReg are locking each other causing deadlock
  Nov 21 13:14:44.802 [PROC] (1) Lock timeout occured for
  Nov 21 13:14:44.877 [PROC] (1) [bt]: (1) /usr/acme/usbc :
  default_lock_timeout(LockBase const&)
  Nov 21 13:14:44.877 [PROC] (1) [bt]: (2) /usr/acme/usbc :
  MutexLock::lock(unsigned int)
  Nov 21 13:14:44.877 [PROC] (1) [bt]: (3) /usr/acme/usbc :
  SipSurrogateReg::invalidate_registrar

  Nov 21 13:14:44.801 [PROC] (5) Lock timeout occured for
  Nov 21 13:14:44.832 [PROC] (5) [bt]: (1) /usr/acme/usbc :
  default_lock_timeout
  Nov 21 13:14:44.832 [PROC] (5) [bt]: (2) /usr/acme/usbc :
  MutexLock::lock(unsigned int)
  ```

- Bug #25164804: When codec-policy is added to access realm telephone-event is stripped to core

  Problem: When opus:48000 and telephone-event:48000 are received in an sdp and egress codec-policy is configured to add PCMU SBC should be adding telephone-event:8000 since telephone-event was in the ingress offer.

- Bug #25192650: Add additional info to debug logging for Cavium 68XX platforms

  Problem: Additional Cavium ECC error reporting has been requested for 6100/6300 platforms

- Bug #25286990: ENUM server timeout after config change

  Problem: When there is a configuration change in dns-ip in network-interface or enum-config enum-servers, ENUM servers are getting timeout.

- Bug #25298391: SNMP values cannot be retrieved for some codec MIB objects

  Problem: Following MIB object values cannot be retrieved through SNMP request.

  ```
  apCodecRealmCountT140
  apCodecRealmCountBAUDOT
  apCodecRealmCountH264
  ```

- Bug #25299558: Kernel Crash

  Problem: The issue was a kernel crash caused by a bad RIP value from the ntpMonitor's call to the Linux OS ntpq.

- Bug #25311682: PRACK IWF v2 forces PRACK in call

  Problem: PRACK IWF forces PRACK if "Supported:100rel" is present.

- Bug #25316666: Segmentation Fault: etc_sys_show_dimms

  Problem: Segmentation Fault: etc_sys_show_dimms

- Bug #25318238: SBC drops calls with SIP 500 error while TCP socket connection is being setup

  Problem: SBC drops calls with SIP 500 error while TCP socket connection is being setup.

- Bug #25333504: PHY status stays on "initial" even if taking traffic

  Problem: SNMP get of apEnvMonCardState always returns "initial"

- Bug #25337203: Some information not available in running-config in the new version

  Problem: Some information missing when executing "show running-config" command.

- Bug #25348541: SNMP request for apEnvMonCardTable is not returning the correct slot value

  Problem: SNMP walk for apEnvMonCardTable is not returning the correct slot value

- Bug #25368498: tSipd crash

  Problem: There is a deadlock on AgentStatsRow lock.

- Bug #25378489: SNMP/MIB counters for interaces all zeros in SCZ740p1

  Problem: IfTable stats showed all zero values.

- Bug #25403745: SNMP/MIB counters for Codecs incorrect for video H264

  Problem: SNMP/MIB counters for Codecs incorrect for video H264. Symptom is that H26 object does not appear as expected in snmpwalk

- Bug #25445461: Incorrect SDP version for PRACK IWF with UPDATE

  Problem: Incorrect SDP version for PRACK IWF with UPDATE. 180 & 200 SDPs should be identical.

- Bug #25445590: Incorrect SDP version for PRACK IWF with forking

  Problem: Incorrect SDP version for PRACK IWF with forking

- Bug #25453646: Prack IWF issue with delayed offer IWF

  Problem: Non-PRACK user sends an INVITE without SDP. Called party sends a provisional response with SDP (pracked), then another provisional response, and finally the 200OK without SDP. As introduced in 7.4.0, the SBC in that case only relays the SDP in the final answer 200 OK. However, the first transmission of 200 OK contains the peer IP address (as though media release was applied). If caller does not reply in time and SBC retransmits the 200 OK, the next time the SDP IP address is correct.

- Bug #25463331: PRACK IWF issue with reINVITE 200 OK (no codec added)

  Problem: PRACK IWF issue with reINVITE 200 OK (no codec added)

- Bug #25471998: Under Dynamic trusted entries the type is shown as static after acl is created

  Problem: ACLI command "show acl trusted" always shows type of dynamic entry as static after DDoS setting is enabled. These entries which are created after the EP is registered should be dynamic type.

- Bug #25477185: Forking scenario/ Problem if different PRACK negotiations

  Problem: Forking scenario/ Problem if different PRACK negotiations

- Bug #25526021: Incorrect CSeq on reINVITE for PRACK IWF call

  Problem: Incorrect CSeq on reINVITE for PRACK IWF call. Cseq is not sequential is mandated by RFC 3261. "Requests within a dialog MUST contain strictly monotonically increasing and contiguous CSeq sequence numbers (increasing-by-one) in each direction (excepting ACK and CANCEL of course, whose numbers equal the requests being acknowledged or cancelled)."

- Bug #25545502: TCP registration drop after save/activate

Problem: Performing save-activate (without any actual config changes) during registration traffic causes changes in existing TCP flow which has resulted in moving subsequent refresh registration to untrusted zone.

- Bug #25545575: Standby goes OOS on upgrading from SCZ740p1 to p2

  Problem: If we enable 'order-codec' feature and run a load test, if we reboot the Standby while load is still running, the Standby goes in OOS.

- Bug #25553886: SBC doesn't match inbound SA in child realm

  Problem: Fixed as part of Bug#24742507 in SCZ740M1.

- Bug #25560577: log entries:ebmd@MINOR Invalid call to getData

  Problem: The error message "Invalid call to getData(IPAddress) with data in base class" is being printed repeatedly to log.embd and acmelog

- Bug #25604168: SBC 4500/6300 / after upgrade to 730 sporadic NTP alarms

  Problem: Sporadic NTP alarms

- Bug #25636059: Asymmetric-preconditions does not honor UPDATE

  Problem: Asymmetric-preconditions does not honor the changes from an UPDATE received after the Initial INVITE is received at the SBC.

- Bug #25637170: sipd crash

  Problem: Sipd crash

- Bug #25649901: stop record sent by the SBC has the same timestamp for request and response time

  Problem: stop record sent by the SBC has the same timestamp for request and response time in case of no response for BYE request.

- Bug #25653789: Low MOS Value @ 3000 DTLS Sessions

  Problem: TSM was calling submit work with flow_id_max as the wqe tag. This resulted in sequential/serial processing of all de-tunneled packets, and hence, lower throughput and MOS scores.

- Bug #25688692: Wrong SDP answer in SIP ACK for delayed offer INVITE & PRACK IWF

  Problem: Wrong SDP answer in SIP ACK for delayed offer INVITE & PRACK IWF

- Bug #25750565: Ack/SDP relayed to Callee could have bad Codec in case of Forking scenario

  Problem: Ack/SDP relayed to Callee could have bad Codec in case of Forking scenario. Caller is with PRACK, the two callees are not. Invite is sent without SDP.

  The first 180 from callee 1 is PRACKed without SDP

  The first 180 from callee 2 is PRACKed with SDP

  -> The 200 OK arrives from clalee 1 with SDP. It is forwarded to the caller without SDP. The SD injects SDP into the ACK sent to callee 1. However the SDP does not correspond to the offer in 200 OK.

- Bug #25750602: SBC does not answer to SDP offer in PRACK/SDP

  Problem: SBC does not answer to SDP offer in PRACK/SDP. PRACK is not recognized as an offer.

- Bug #25750654: SD does not answer locally UPDATEs when there are several responses

Problem: SD does not answer locally UPDATEs when there are several responses.

- Bug #25779443: LRT tables are not loaded at boot time

  Problem: SBC is not able to load customer config has 2000 LRT files with 4k entries per file.

- Bug #25779686: sipd crash segmentation fault

  Problem: Sipd crash caused by improper item deletion in SipServerTrans list

- Bug #25709855: Crash while reboot after successful upgrade from 6.3.7m1p3 to 7.2.0m5p3

  Problem: Crash while rebooting, seen when upgrading from 6.3.7 to 7.2 on 4500

- Bug #25795053: Lock Timeout - All SAs using TLS transport going out of service

  Problem: All SA's using TLS transport may go out of service at the same time due to lock timeout.

- Bug #25798827: loss of registrations occurred at a time with increased register endpoints

  Problem: An explained loss of registrations occurred at a time when the number of registered endpoints should have been increasing. The SBC response time significantly increased during the same period in which registrations were declining.

- Bug #25800017: log.octCtrl flooded with QOS messages

  Problem: Non-error logs are printed for egrsCnt on 7.4.0. Example:

  ```
  Mar 28 11:14:13.633 [ETC] [ID=1]core#0 ==== Egress Counting flowId 15237
  Mar 28 11:14:13.633 [ETC] [ID=1]core#0 RTP Egress Bytes = 0
  Mar 28 11:14:13.633 [ETC] [ID=1]core#0 RTP Egress Pakcets = 0
  Mar 28 11:14:13.633 [ETC] [ID=1]core#0 RTCP Egress Bytes = 0
  Mar 28 11:14:13.633 [ETC] [ID=1]core#0 RTCP Egress Pakcets = 0
  Mar 28 11:14:13.633 [ETC] [ID=1]core#0 egrsCnt_process_delete_report_gen:
  updating egress pkts/bytes counting for flow: 38762
  ```

- Bug #25800509: SCZ7.4.0 / SIPD cpu spike at around 50k active calls

  Problem: SIPD CPU spike around 50k calls

- Bug #25813529: Asymmetric preconditions / No contact in 183

  Problem: Asymmetric preconditions / No contact in 183

- Bug #25839717: MSRP behavior change after upgrade

  Problem: Prior to S-CZ7.2.0, if MSRP B2BUA reveives a MSRP request that does not belong to the MSRP session (that negotiated the TCP connection) the request is not dropped. Since S-CZ7.2.0 MSRP B2BUA would drop such request and close the connection. Both behaviors are violations of RFC4975. What must be done is to respond with a 481 response and keep the connection up.

- Bug #25860777: Incorrect ISUP encapsulation in 200OK INVITE with 100rel-interworking

  Problem: Incorrect ISUP encapsulation in 200OK INVITE with 100rel-interworking

- Bug #25876639: apMonitorCollectionDownTrap/apMonitorCollectionClearTrap traps issues

  Problem: apMonitorCollectionDownTrap/apMonitorCollectionClearTrap traps issues

- Bug #25924535: regression between SCZ7.2.0M5P4 and SCZ7.3.0M2 with respect to SPL Engine 3.1.6

Problem: Regression between SCZ7.2.0M5P4 and SCZ7.3.0M2 with respect to SPL Engine 3.1.6

- Bug #25965739: SCZ7.4.0p4 does not pass 180 in some cases

  Problem: Customer experiencing problem with the SBC not acknowledging the 100 Trying and 180 Ringing sip messages from the far end. Therefore, continuously sending INVITE to the far end and failing.

- Bug #25985141: PRACK IWF: Regression from nnSCZ730m2p5

  Problem: When preconditions IWF is enabled, it is possible caller and callee support 100rel in which case SBC needs to interwork PRACK on both sides, however SBC incorrectly assumed the first 18x response will always carry the Require: 100rel tag. Restored SBC behavior to send PRACK when 18x had 100rel and not to send when the tag was absent.

- Bug #26006342: HA not synching, Secondary Out-Of-Service

  Problem: HA not syncing, Secondary Out-Of-Service Having siprec configured, the HA pair not to sync due to REC sync failure

- Bug #26100005: SIPREC: Music on hold not recorded when B puts A on hold

  Problem: SIPREC: Music on hold not recorded when B puts A on hold.

  For A calls B scenario, whenever a party puts other on hold, a RE-Invite is sent to SRS with two m-lines(and attributes). The party which has pressed hold has ?a line? as sendonly, and the party which goes on hold has "a line" as inactive.

  - When A puts call on hold, in a Re-Invite towards SRS, m-line for A's SDP has its "a line" as sendonly, m-line for B's SDP has its "a line" as inactive. This is expected.

  - When B puts call on hold, in a Re-Invite towards SRS, m-line for A's SDP has its "a line" as sendonly, m-line for B's SDP has its "a line" as inactive. This is not expected.

- Bug #26108871: After registering 100k IMS_AKA endpoints and de-registering 205 ACL flow leaked

  Problem: After registering 100k IMS_AKA endpoints and de-registering 205 ACL flow leaked

- Bug #26111996: SBC does not send delete message to SLB when TCP ephemeral port changes

  Problem: With port-aware feature configured on SLB tunnel, an unchallenged TCP registration which changed ports was not cleaning up the old port endpoint on the SLB.

- Bug #26151711: packet drops causing oneway audio intermittently

  Problem: A customer may experience an issue where the default policing level was being exceeded. Added support to enable/disable media policing through media-manager configuration settings.

- Bug #26153107: Telnet, SSH, SFTP sessions hang with 4 Port GigE w/QoS & Encryption on Scz730m3

  Problem: Telnet, SSH, SFTP sessions hang with 4 Port GigE w/QoS & Encryption on Scz730m3

- Bug #26222105: Lower MOS Scores for calls with 0 RTP packets

  Problem: After upgrading to 7.3 code, there is a percentage of CDRs that are not populating the QOS data leading to the MOS value for zero packets flow being very low.

- Bug #26285153: PCSCF doesn't forward responses from UE to SCSCF

Problem: The SBC is not properly normalizing the IPv6 address in the VIA header and considering "::" equal to ":0:" Due to this, the SBC is not forwarding the 180 and 200 messages.

- Bug #26288253: nested-realms-stats parameter not working as expected

  Problem: nested-realms-stats parameter not working as expected. When session constraint is applied on parent realm, then it doesn't get enforced on child realm.

- Bug #26291758: SBC Randomly select destinations from Registration cache

  Problem: Some calls are being sent to a randomly different destinations due to an incorrect L3 IP destination address.

- Bug #26299969: ATCPD crash on scz730m2p3

  Problem: ATCPD crashes on SBC may occur when TCP connections are closed.

- Bug #26305374: Atcpd crash

  Problem: ATCPD crashes on SBC may occur when TCP connections are closed.

- Bug #26322261: sipd crash

  Problem: SBC 6300 Crash : sipd01 signal 11 (Segmentation fault) SCZ7.4.0 Patch 4

- Bug #25843405: Physical interface not coming up after reboot

  Problem: Physical interface (1G fiber) not coming up after reboot

- Bug #26401184: SBC is sending wrongformat of MAC address for "ifPhysAddress"

  Problem: ifPhysAddress with wrong format

- Bug #26365899: 404 Not Found Error Code when Target-Dialog has call-ID with IPv6 address

  Problem: When a pooled transcoded call has a callID which contains an IPV6 address enclosed in square brackets, the call fails with a 404 Not Found response.

- Bug #26441635: sipd crash

  Problem: The customer has seen at least 4 instances of a sipd crash that occurs while canceling a handover call. Based on the core dump the call flow looks like it was an alerting phase handover call that got canceled due to a 487 response to the handover invite.

- Bug #26577021: New surrogate-agent is throwing 401 Unauthorized after upgrade to SCZ730m3

  Problem: New surrogate-agent is throwing 401 Unauthorized after upgrade to SCZ730m3

- Bug #26661660: Media problem in transcoding

  Problem: No audio in transcoded calls resulting from cOCTVC1_NET_RC_RTP_MEMBER_LOCAL_UDP_PORT_ALREADY_USED error in log.xserv.

nnSCZ740p8 - 8/14/20017

- Bug #26143842: High temp alarms post 730m2p6 upgrade

  Problem: Using low-speed fan modules with ETC1 NIUs (on 4500/3820 platforms) could result in fan speed alarms when a temperature threshold is hit. The maximum RPM for low-speed fans is 12K. The SBC assumes the maximum fan speed to be 15k RPMs (as with high-speed fans) and consequently generates a fan speed alarm.

- Bug #25378489: SNMP/MIB counters for interaces all zeros in SCZ740p1

Problem: IfTable stats showed all zero values.

- Bug #26291758: SBC Randomly select destinations from Registration cache

  Problem: Some calls are being sent to a randomly different destinations due to an incorrect L3 IP destination address.

- Bug #26322261: SBC 6300 Crash : sipd01 signal 11 (Segmentation fault) SCZ7.4.0 Patch 4

  Problem: SBC 6300 Crash : sipd01 signal 11 (Segmentation fault) SCZ7.4.0 Patch 4

- Bug #26399876: ifDescr element returns not the configured phy-interface name

  Problem: ifDescr element returns lowercase values in SCZ740, while returned uppercase in SCZ720

nnSCZ740p7 - 6/13/2017

- Bug #25056689: (6300) SBC can't reach 80K QOS sessions. It sends 503 at around 68K. Problem: Max sessions capacity test failed to reach maximum sessions with QoS enabled.

- Bug #25496186: Media problem in transcoding when traffic is increased

  Problem: Some transcoding calls have no media, with certain call flows and at higher call rates.

- Bug #25545575: Standby goes OOS on upgrading from SCZ740p1 to p2

  Problem: If we enable 'order-codec' feature and run a load test, if we reboot the Standby while load is still running, the Standby goes in OOS.

- Bug #25813529: Asymmetric preconditions / No contact in 183

  Problem: Asymmetric preconditions / No contact in 183

- Bug #25985141: PRACK IWF: Regression from nnSCZ730m2p5

  Problem: When preconditions IWF is enabled, it is possible caller and callee support 100rel in which case SBC needs to interwork PRACK on both sides, however SBC incorrectly assumed the first 18x response will always carry the Require: 100rel tag. Restored SBC behavior to send PRACK when 18x had 100rel and not to send when the tag was absent.

- Bug #25989787: One way audio calls - Bug 25496186 continuation

  Problem: One-way audio with transcoded calls due to overlapping IP/port and VLANs

- Bug #26111996: SBC does not send delete message to SLB when TCP ephemeral port changes

  Problem: With port-aware feature configured on SLB tunnel, an unchallenged TCP registration which changed ports was not cleaning up the old port endpoint on the SLB.

nnSCZ740p6 - 5/24/2017

- Bug #26030032: Leaked forwarding rules during TCP registrations

  Problem: After the new registration using ephemeral TCP source port Y has finished the SLB has two trusted forwarding rules, one with ephemeral TCP source port X and another with ephemeral TCP source port Y. The rule with ephemeral TCP source port X remains in the SLB indefinitely, but the assumption is that it should be deleted when the second registration triggers addition of the rule for ephemeral TCP source port Y. In the SBC only one registration cache entry is ever present as the same SBC Contact header cookie is used for both the first and second registrations.

- Bug #23230729: SBC experienced DPWD crash on NN4500 with ETC NIU

  Problem: ECC DDR errors cause NIU card to crash

- Bug #25965739: SBC on SCZ7.4.0 p4 do not pass 180 in some cases

  Problem: Customer experiencing problem with the SBC not acknowledging the 100 Trying and 180 Ringing sip messages from the far end. Therefore, continuously sending INVITE to the far end and failing.

- Bug #26084057: DSP Boot Failure on SCZ740p4

  Problem: Latest-built DSPs fail to boot

nnSCZ740p5 - 5/8/2017

- Bug #25453646: Prack IWF issue with delayed offer IWF

  Problem: non-PRACK user sends an INVITE without SDP. Called party sends a provisional response with SDP (pracked), then another provisional response, and finally the 200OK without SDP. As introduced in 7.4.0, the SBC in that case only relays the SDP in the final answer 200 OK. However, the first transmission of 200 OK contains the peer IP address (as though media release was applied). If caller does not reply in time and SBC retransmits the 200 OK, the next time the SDP IP address is correct.

- Bug #25688692: Wrong SDP answer in SIP ACK for delayed offer INVITE & PRACK IWF

  Problem: Wrong SDP answer in SIP ACK for delayed offer INVITE & PRACK IWF

- Bug #25750565: Ack/SDP relayed to Callee could have bad Codec in case of Forking scenario

  Problem: Caller is with PRACK, the two callees are not. Invite is sent without SDP.

  The first 180 from callee 1 is PRACKed without SDP

  The first 180 from callee 2 is PRACKed with SDP -> The 200 OK arrives from callee 1 with SDP. It is forwarded to the caller without SDP.

  The SD injects SDP into the ACK sent to callee 1. However the SDP does not correspond to the offer in 200 OK.

- Bug #25750602: SBC does not answer to SDP offer in PRACK/SDP

  Problem: PRACK is not recognized as an offer.

- Bug #25779686: sipd crash segmentation fault

  Problem: Sipd crash caused by improper item deletion in SipServerTrans list

- Bug #25800017: log.octCtrl flooded with QOS messages

  Problem: Non-error logs are printed for egrsCnt on 7.4.0

  Example:

```
Mar 28 11:14:13.633 [ETC] [ID=1]core#0 ==== Egress Counting flowId 15237
=============
Mar 28 11:14:13.633 [ETC] [ID=1]core#0 RTP Egress Bytes = 0
Mar 28 11:14:13.633 [ETC] [ID=1]core#0 RTP Egress Pakcets = 0
Mar 28 11:14:13.633 [ETC] [ID=1]core#0 RTP Egress Pakcets = 0
Mar 28 11:14:13.633 [ETC] [ID=1]core#0 RTCP Egress Bytes = 0
Mar 28 11:14:13.633 [ETC] [ID=1]core#0 RTCP Egress Pakcets = 0
Mar 28 11:14:13.633 [ETC] [ID=1]core#0 egrsCnt_process_delete_report_gen:
updating egress pkts/bytes counting for flow: 38762
```

- Bug #25800509: SCZ7.4.0 / SIPD cpu spike at around 50k active calls

  Problem: SIPD CPU spike around 50k calls

nnSCZ740p4 - 3/28/2017

- Bug #24352348: Wrong rate-limits applied for certain RTP streams in transcoded call.

  Problem: Poor audio quality for transcoded calls when media policing is enabled
- Bug #25311682: PRACK IWF v2 forces PRACK in call

  Problem: PRACK IWF forces PRACK if "Supported:100rel" is present.
- Bug #25445461: Incorrect SDP version for PRACK IWF with UPDATE

  Problem: Incorrect SDP version for PRACK IWF with UPDATE. 180 & 200 SDPs should be identical.
- Bug #25445590: Incorrect SDP version for PRACK IWF with forking

  Problem: Incorrect SDP version for PRACK IWF with forking
- Bug #25463331: PRACK IWF issue with reINVITE 200 OK (no codec added)

  Problem: PRACK IWF issue with reINVITE 200 OK (no codec added)
- Bug #25526021: Incorrect CSeq on reINVITE for PRACK IWF call

  Problem: Cseq is not sequential is mandated by RFC 3261.

  "Requests within a dialog MUST contain strictly monotonically increasing and contiguous CSeq sequence numbers (increasing-by-one) in each direction (excepting ACK and CANCEL of course, whose numbers equal the requests being acknowledged or cancelled)."
- Bug #25636059: Asymmetric-preconditions does not honor UPDATE

  Problem: Asymmetric-preconditions does not honor the changes from an UPDATE received after the Initial INVITE is received at the SBC.

nnSCZ740p3 - 2/28/2017

- Bug #24751746: Suspected memory leak in nnSCZ730m1p10.64.bz

  Problem: After failover old ACL entries are not getting deleted.
- Bug #25506084: Rereg the packets are going untrusted from UE server port to SBC client port

  Problem: IMS-AKA registration refreshes results in a single dynamic ACL associated to multiple NAT flows leading to trusted pkts being erroneously marked as untrusted.
- Bug #25637890: SYN_ACK from EP's not responded by SBC when trying to establish outbound connection

  Problem: Duplicate flows were mistakenly being marked as errors during flow installs

nnSCZ740p2 - 2/8/2017

- Bug #25360947: Customer is reporting CPU spikes on 2 6300 HA pairs

  Problem: SIPD threads can spin and consume high CPU when order-codecs is configured in codec-policy, and the SBC reorders codecs when the SDP contains more than one codec with the same name.
- Bug #25167966: Surrogate-agent can't be enabled RTC

Problem: After disabling and re-enabling a surrogate-agent state from enabled to disabled, and then back to enabled again. The surrogate doesn't try to send a new REGISTER until SBC is rebooted. The from enabled to disabled,worked fine.

- Bug #25226126: PST VoLTE: show sipd tcp does not display IMS-AKA counters with calls

  Problem: show sipd tcp does not display IMS-AKA counters with active IMS-AKA calls

- Bug #25252094: RN is not recognized as lrt key when R-URI is based on tel-uri

  Problem: Querying an LRT while using the RN received in a tel-uri as the key, is unable to recognized as lrt key when R-URI is based on tel-uri. LRT query is not performed because it seems we are not recognizing the RN: In case the R-URI is based on "sip-uri" RN is taken as key and LRT query is triggered.

nnSCZ740p1 - 12/8/2016

- Bug #24661990: wancom2 showing as up/up when actually unconfigured / disconnected

  Problem: show wancom displays link to be up and running even when the interface is actually unwired and down.

- Bug #25164587: Unable to SSH into nn3820 Standby after upgrading

  Problem: Unable to SSH into nn3820 Standby after upgrading

- Bug #23230801: sdp session-id mismatch in SDP send by SBC in 183 and 200ok(update)

  Problem: sdp session-id mismatch in SDP send by SBC in 183 and 200ok(update)

- Bug #24416198: USBS core file upon reboot despite "sw-health-check-action=logandreboot" setting

  Problem: USBC core file generated despite "sw-health-check-action=logandreboot" setting.

- Bug #24609104: AP4500: SCZ720m6p7: CDRs for pooled transcoding calls are corrupted.

  Problem: In pooled-transcoding, transcoded call have less CDR then non-transcoded call

- Bug #24695344: AP4600 - 720m6p7 - Corrupted CDRs (duration and connect time fields)

  Problem: Problem: "Acct-Session-Time" and "h323-connect-time" are not populated correctly in most cases for established calls after upgrade. Field "Acct-Session-Time" equals 0 and "h323-connect-time" equals "00:00:00.000 UTC Jan 01 1970", which were the default values.

- Bug #24718727: PRACK IWF: SRTP call results in no audio when UPDATE is in call flow

  Problem: PRACK IWF: SRTP call results in no audio when UPDATE is in call flow

  Usecase1:

  CallerA and CalledB supports SRTP.

  1. CallerA initiate SIP call INVITE with SDP1 (codec AMR PCMU) and a=crpto.
  2. Verify that INVITE sent to CalledB with header Supported:100rel, SDP (codec AMR PCMU) and a=crpto line in SDP.
  3. CalledB sends 18X with SDP1? (codec AMR),100rel and a=crpto line in SDP.
  4. Verify that SBC sends PRACK for 18X to CalledB.
  5. Verify SBC sends 18X to CallerA with SDP1? (codec AMR)

6. CalledB sends 200OK for PRACK.
7. CalledB sends UPDATE with SDP (codec AMR) and a= crypto line in SDP.
8. Verify SBC sends 200OK for UPDATE locally with SDP2? (codec AMR) to CalledB.
9. On receiving 200 OK (without SDP) for INVITE from CalledB, verify SBC sends 200OK with SDP2? (codec AMR) to CallerA and receives an ACK.
10. SBC forwards ACK to CalledB.
11. Verify audio at both ends.

When UPDATE is part of call flow and 200 OK in step 9 comes without SDP, it results in no audio.

Without UPDATE and with SDP in 200OK in step 9, results in two-way audio.

- Bug #24797974: Reboot is required when trust-level is changed else IMS_AKA registration fails

  Problem: Changing access-control-trust-level within realm-config results in NAT misses
- Bug #24850165: TSM: HDR miscellaneous spelling issues in counter names

  Problem: TSM: Counter-Total number of tunnels time out- is missing in SNMP mib file, and has been added
- Bug #24910754: wancom reporting 1G, switch reports 100M speed

  Problem: On NIUs with security, show wancom always shows 1Gig for wancom0 even when its connected to a 10/100M switch.
- Bug #24921197: Active node reboot after numerous "Too many open files" errors

  Problem: Active node reboot after numerous "Too many open files" errors
- Bug #24937374: sipd crash observed on Session Router

  Problem: sip thread goes unresponsive/deadlocked trying to print a log for dnsServerList
- Bug #24942467: SD doesn't accept Secured IMS-AKA msg in case of enabling SROP & trust-level=low

  Problem: During v6 registrations, after a 401 is sent, no subsequent registration messages are received by SIP
- Bug #24957492: Initial IMS-AKA REG works, but Re/DeREG doesn't work if trust-level=medium

  Problem: During v6 registrations, after a 401 is sent, no subsequent registration messages are received by SIP
- Bug #24965336: PRACK IWF: SD retransmits PRACK for usecase3

  Problem: For an offerless INVITE when UAS responds 18x with SDP, SD sends PRACK. UAS sends 200OK for PRACK but SD keeps re-transmitting PRACK.
- Bug #25024651: trust-level=low ACL entry is not getting demoted from untrusted to deny list

  Problem: trust-level=low ACL entry is not getting demoted from untrusted to deny list
- Bug #25036381: Non IPSec packets are not dropped by SBC during registration process

  Problem: Non IPSec packets are not dropped by SBC during registration process
- Bug #25057852: Rseq not send by SBC in 180 with sdp on 100 rel interworking enabled interface

Problem: Rseq not send by SBC in 180 with sdp on 100 rel interworking enabled interface.

100 rel-interworking enbaled on caller side.

Invite send with header Supported: 100rel

Invite fwded to core and core responds with 180 ringing with sdp.

SBC forwards 180 ringing to caller but with out Rseq.

When caller supports 100rel and SBC have this enabled on access, SBC should have send 180 reliably.

- Bug #25058174: Preconditions: SBC not transcoding the negotiated payload

  Problem: Preconditions: SBC not transcoding the negotiated payload
- Bug #25065393: Call Fails After Successful IMS-AKA REGISTER and Active System Reboot

  Problem: Call Fails After Successful IMS-AKA REGISTER and Active System Reboot
- Bug #25098374: TSM: Counter-Total number of tunnels time out- is missed in SNMP mib file

  Problem: TSM: Counter-Total number of tunnels time out- is missed in SNMP mib file
- Bug #25099850: SMP Load Shedding: Calls do not get rejected after threshold

  Problem: SMP Load Shedding: Calls do not get rejected after threshold
- Bug #25106454: HealthCheck Failure:_Z17suspend_this_taskPKcPKv

  Problem: HealthCheck Failure:_Z17suspend_this_taskPKcPKv
- Bug #25142462: ACL entry for TCP from UE server port to SBC client port is not getting demoted

  Problem: ACL entry for TCP from UE server port to SBC client port is not getting demoted
- Bug #25152323: Random call drops after upgrading to SCZ7.4.0

  Problem: Random call drops after upgrading to SCZ7.4.0
- Bug #25185506: (6300) unsuccessful IPv6 registration - SBC is dropping 401 message

  Problem: Registration drops in NIU due to trusted miss lookups

B

SCZ740M2

The Oracle Communications Session Border Controller (SBC), software release S-CZ7.4.0M2 eliminates two feature functionality omissions in the area of Pooled transcoding. The S-CZ7.4.0M2 software release supports 100rel PRACK interworking and lMSD interworking with pooled transcoding. The software release also includes software defect corrections as would a standard patch. If you do not use pooled transcoding, the S-CZ7.4.0M2 release can be understood as a patch release. If you do use Pooled transcoding, you get the benefit of these two additional functions.

Please refer to this Release Notes' Known Issues section for known issue changes applicable to this release.