Oracle® Enterprise Session Border Controller

Release Notes

Release E-CZ7.4.0

May 2019

Oracle Enterprise Session Border Controller Release Notes, Release E-CZ7.4.0

Contents

About This Guide

1 Oracle Enterprise Session Border Controller Description

2 Specifications and Requirements

Supported Hardware and Software Platforms 2-1

Supported Platforms, Image Files, and Boot Files 2-1

Platform Boot Loaders 2-2

Upgrade Information 2-2

Supported SPL Engines 2-3

CPU Support for the Acme Packet 4500 2-4

NIU and Feature Group Requirements 2-4

QoS NIU Version Requirement for Acme Packet 3820 and Acme Packet 4500 2-6

System Capacities 2-6

3 New Features and Enhancements

Acme Packet 3900 Platform 3-1

- The Acme Packet 3900 Platform Physical Interfaces 3-2
- SNMP Hardware Reporting 3-3
- Acme Packet 3900 MIBS Paths 3-3
- NIU Port Numbering Reference for the Acme Packet 3900 Platform 3-4
- Configure the Acme Packet 3900 Physical Interface 3-4

Transmitted Bytes and Packets for Call Detail Records 3-5

Web GUI Widgets for Displaying Communications Monitor Statistics 3-6

4 Inherited Features

E-Cz7.3.0M1 Maintenance Release Features 4-1

E-Cz7.3.0M2 Maintenance Release Features 4-3

5 Known Issues

List of Known Issues 5-1

6 Caveats

List of Caveats 6-1

7 Limitations

List of Limitations 7-1

8 E-CZ7.4.0m1

Upgrade Information 8-1

Build Notes 8-1

List of Tables

2-1 Acme Packet 1100 NIU and Feature Group Support Matrix 2-5

2-2 Acme Packet 3900 NIU and Feature Group Support Matrix 2-5

2-3 Acme Packet 4500 NIU and Feature Group Support Matrix 2-5

2-4 Acme Packet 4600 NIU and Feature Group Support Matrix 2-5

2-5 Acme Packet 6300 NIU and Feature Group Support Matrix 2-5

2-6 Virtual Machine and Feature Group Support Matrix 2-6

About This Guide

This guide provides information about the Oracle® Enterprise Session Border Controller (E-SBC) and the E-CZ7.4.0 and E-CZ7.4.0m1 releases.

Documentation Set

The following table describes the E-Cz7.4.0 documentation set.

Document Name	Document Description
ACLI Configuration Guide	Contains information about the installation, configuration, and administration of the Enterprise E-SBC.
Acme Packet 1100 Hardware Installation Guide	Contains information related to the hardware components, features, installation, start-up, operation, and maintenance of the Acme Packet 1100.
Acme Packet 3900 Hardware Installation Guide	Contains information related to the hardware components, features, installation, start-up, operation, and maintenance of the Acme Packet 3900.
Release Notes	Contains information about this release, including platform support, new features, caveats, known issues, and limitations.
Web GUI User Guide	Contains information about using the tools and features of the E-SBC Web GUI.

Related Documentation

The following table describes related documentation for the Oracle® Enterprise Session Border Controller. You can find the listed documents on http://docs.oracle.com/en/industries/communications/ in the "Session Border Controller Documentation" and "Acme Packet" sections.

Document Name	Document Description
Accounting Guide	Contains information about the E-SBC accounting support, including details about RADIUS accounting.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.

Document Name	Document Description
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
Administrative Security Essentials	Contains information about the E-SBC support for its Administrative Security license.
HDR Resource Guide	Contains information about the E-SBC Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Maintenance and Troubleshooting Guide	Contains information about E-SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the E-SBC family of products.

Revision History

The following table describes updates to this guide.

Date	Description
November 1, 2016	Initial Release
November 30, 2016	• Adds the Inter-working Function (IWF) Caveats
February 3, 2017	• Adds support for the Acme Packet 3900 to "Interim QoS Updates"
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.
April 2017	• Adds the note about Web GUI support to the Platform Bootloaders topic.
May 2017	• Updated upgrade Paths section with the following note: Online, HA upgrades on VM-based systems are not supported between E-C[XZ]6.x.x and E-CZ7.x.x releases.
June 2017	• Adds Acme Packet 3900 High Availability Known Issue. • Adds the Interim QoS Update Known Issue.
August 2017	• Adds the M1 maintenance release chapter.
September 2017	• A limitation regarding the **packet-trace remote** command was added.
October 2017	Adds the following Caveat • Interface Utilization Support

Date	Description
November 2017	• Removes IPSec support.
January 2018	• Adds the Caveat about not running packet trace simultaneously with certain replication features.
March 2018	• Adds the Comm-Monitor item to Caveats.
May 2018	• Adds Caveat stating no 'packet trace remote' on the Acme Packet 3900
June 2018	• Adds the Acme Packet 3900 to the " Upgrade the Acme Packet 1100 ,Acme Packet, and VME Platforms" topic.
May 2019	• Updates Transcoding caveats with Local Media Playback incompatibility.

1

Oracle Enterprise Session Border Controller Description

The Oracle® Enterprise Session Border Controller (E-SBC) connects disparate Internet Protocol (IP) communications networks while mitigating security threats, curing interoperability problems, and ensuring reliable communications. The E-SBC protects and controls real-time voice, video, and Unified Communications (UC) as they traverse IP network borders.

Overview

Available in software and appliance configurations, the E-SBC is highly scalable and includes an industry-leading feature set.

- Strong security. As the E-SBC protects IP telephony and UC infrastructure, services, and applications, it also ensures confidentiality, integrity, and availability. The E-SBC protects against fraud, service theft, malicious attacks, system overloads, and other events that affect service.
- Easy interoperability. The E-SBC provides extensive signaling and media control features to help businesses overcome interoperability challenges that commonly occur when interfacing with public IP network services. The E-SBC also performs protocol interworking and dial plan management for integration with legacy systems.
- Assured reliability. The E-SBC ensures Public Switched Telephone Networks (PSTN)-like availability and service quality for IP communications. The E-SBC enforces service quality, balances loads across trunks, and reroutes sessions around interface disruptions to optimize network performance, circumvents equipment and facility problems, and ensures business continuity.

Functions and Modes

Businesses install the E-SBC at Session Initiation Protocol (SIP) network borders, where enterprise communications systems interface with public network services and where disparate multi-vendor systems must be managed.

Customers use the E-SBC to:

- Connect to SIP trunking services and the Internet
- Access communications services
- Communicate securely with remote workers
- Manage sessions across a multi-vendor UC environment
- Connect contact center locations and Business Process Outsourcing (BPO) services

2

Specifications and Requirements

Oracle recommends that you review the following specifications and requirements before using the E-Cz7.4.0 release.

Supported Hardware and Software Platforms

The following platforms support the Oracle® Enterprise Session Border Controller (E-SBC) with identical functionality, except for the number of concurrently supported Session Initialization Protocol (SIP) audio calls.

- The Virtual Machine Edition (VME), which supports VMware, can also run on a generic server in a virtual environment. Oracle recommends that you configure the virtual machine with a minimum of 4GB of RAM and 4 CPUs.
- The Oracle Hardware Edition runs on the Acme Packet 1100, Acme Packet 3900, Acme Packet 4500, Acme Packet 4600, and Acme Packet 6300 platforms.

Supported Platforms, Image Files, and Boot Files

The baseline for the E-Cz7.4.0 release is the E-Cz7.3.0M2 GA release.

Platforms

The following platforms support the E-Cz7.4.0 release.

- Oracle Hardware Platforms: Acme Packet 1100, Acme 3900, Acme Packet 4500, Acme Packet 4600, and Acme Packet 6300
- Virtual Platforms: VMWare 5.5 ESXi Hypervisor

Image and Boot Files for Hardware

Use the following files for new installations and upgrades.

Oracle Hardware

- Image file: `nnECZ740p1.64.bz`.
- Bootloader file: `nnECZ740p1.boot`.

Image and Boot Files for Virtual Machines

Use the following files to upgrade virtual machine deployments.

- Image file: `nnECZ740p1.64.bz`
- Bootloader file: `nnECZ740p1.boot`

Platform Boot Loaders

Oracle® Enterprise Session Border Controller (E-SBC) platforms require a boot loader to load the operating system and application software. New software releases include the corresponding boot loader, which the E-SBC launches during application installation. Note that software upgrades do not update the boot loader. You must manually set the compatibility. For example, suppose you want to install the software image with the filename `nnECZ750.bz`. Use the corresponding boot loader file named `nnECZ750.boot`. From the command line, use the **show version boot** command to view the boot loader version. You must install the boot loader file as /boot/bootloader on the target system.

Stage 1 and Stage 2 Boot Loaders

The Acme Packet 4500 uses the Stage 1 and Stage 2 boot loaders, which must be dated July 3, 2013 (MOS patch #1815632) or later. Network booting for release 7.x by way of FTP and TFTP on the Acme Packet 4500 requires the November 2013 or later boot loader.

Stage 3 Boot Loader

Every new software release contains a system software image and the Stage 3 boot loader. All platforms require the Stage 3 boot loader, and the Stage 3 boot loader is compatible with previous releases. Oracle recommends that you upgrade the Stage 3 boot loader before booting the new system image.

> **Note:**
>
> The E-SBC does not support uploading the boot loader by way of the Web GUI.

Upgrade Information

The E-Cz7.4.0 release supports the following behavior for upgrades.

Upgrade Paths

You can upgrade directly to E-Cz7.4.0 from the following previous releases.

- E-C[xz]6.4 to E-Cz7.4
- E-Cz7.x to E-Cz7.4

Upgrade the Acme Packet 1100, Acme Packet 3900, and VME Platforms

In the E-Cz7.4.0 release, the software TLS and software SRTP features no longer require license keys. The change affects the upgrade process for the Acme Packet 1100 platform and the Virtual Machine Edition (VME) platform. After you upgrade either platform from E-Cz7.3.0 to E-Cz7.4.0, you must run the `setup product` command to re-activate the features that formerly depended on license keys.

Upgrade to the Acme Packet 3900 Platform

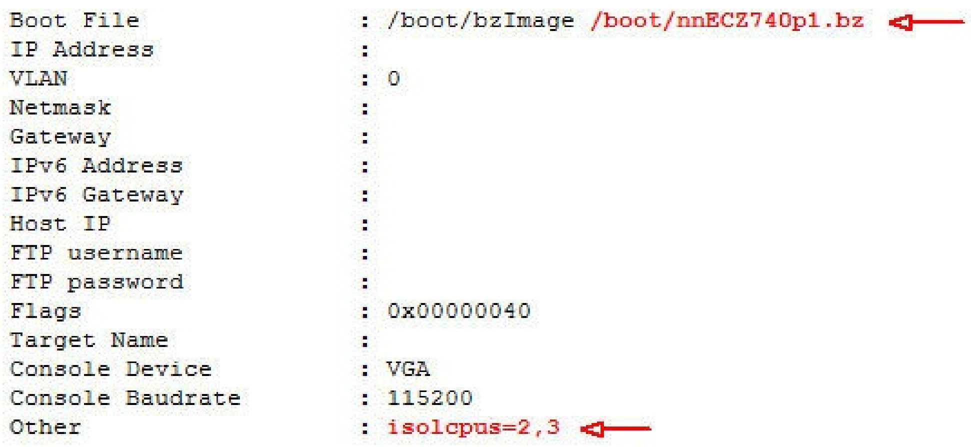
When upgrading from the Acme Packet 3820 to the Acme Packet 3900, Oracle supports only an offline upgrade. You can upgrade the other Acme Packet platforms while online.

Upgrade on VMware ESXi 5.5 and 5.6

> **Note:**
>
> Online, HA upgrades on VM-based systems are not supported between E-C[XZ]6.x.x and E-CZ7.x.x releases.

Before upgrading to E-Cz7.4.0, Oracle recommends that you configure the virtual machine with a minimum of 4GB of RAM and 4 CPUs. During the upgrade you must replace the bootloader and the image files as a set and perform other tasks, such as setting isolated CPUs and allocating cores in datapath-config. Use the `nnECZ740p1.bz` image file and the `nnECZ740p1.boot file`. You must also enter a specific setting for the `Other` boot parameter.

Set the boot parameters for E-Cz7.4.0, as follows:



```
Boot File                 : /boot/bzImage /boot/nnECZ740p1.bz
IP Address                :
VLAN                      : 0
Netmask                   :
Gateway                   :
IPv6 Address              :
IPv6 Gateway              :
Host IP                   :
FTP username              :
FTP password              :
Flags                     : 0x00000040
Target Name               :
Console Device            : VGA
Console Baudrate          : 115200
Other                     : isolcpus=2,3
```

See the S-cZ7.2.9 *VNF Essentials Guide* for more information.

> **Note:**
>
> If you ever need to downgrade, you must reinstate the original bootloader and image files as a set.

Supported SPL Engines

Each release supports a number of versions of the SBC Programming Language (SPL) engine, which is required to run SPL plug-ins on the Oracle® Enterprise Session Border Controller (E-SBC).

This release supports the following versions of the SPL engine.

- C2.0.0
- C2.0.1
- C2.0.2

- C2.0.9
- C2.1.0
- C2.1.1
- C2.2.0
- C2.2.1
- C2.3.1
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.0.7
- C3.1.0
- C3.1.1
- C3.1.2
- C3.1.3
- C3.1.4
- C3.1.5
- C3.1.6

Use the `show spl` command to see the version of the SPL engine running on the E-SBC.

CPU Support for the Acme Packet 4500

The following requirements for CPU support apply to the Acme Packet 4500.

The system supports only the 64-bit CPU2 on the Acme Packet 4500, and only CPU revision MOD-0026-xx. The system does not support CPU revision MOD-0008-xx.

Board Revision	Minimum Version
3	v3.18
4	v4.10

NIU and Feature Group Requirements

The following tables list the feature groups for all hardware and virtual platforms that require a specific Network Interface Unit (NIU). In the tables, the ✓ character indicates the feature set that requires the supported NIU.

Table 2-1 Acme Packet 1100 NIU and Feature Group Support Matrix

NIU	IPSec	SRTP	QoS	Transcoding	ISDN PRI
Acme Packet 1100 Ethernet interface	✗	✓	✓	✓ (requires transcoding module)	✗
Acme Packet 1100 TDM interface	Not applicable	Not applicable	Not applicable	Not applicable	✓

Table 2-2 Acme Packet 3900 NIU and Feature Group Support Matrix

NIU	IPSec	SRTP	QoS	Transcoding	ISDN PRI
4x1Gig	✗	✓	✓	✓ (requires transcoding module)	✗
Quad-Span TDM interface	Not applicable	Not applicable	Not applicable	Not applicable	✓

Table 2-3 Acme Packet 4500 NIU and Feature Group Support Matrix

NIU	IPSec	SRTP	QoS	Transcoding
Clear (RJ45)	✗	✗	✗	✗
Clear (SFP)	✗	✗	✗	✗
ETCv2	✓	✓	✓	✗
Encryption	✓	✓	✗	✗
QoS	✗	✗	✓ **	✗
Encryption & QoS	✓	✓	✓ **	✗
Transcoding	✗	✗	✓ ***	✓

Table 2-4 Acme Packet 4600 NIU and Feature Group Support Matrix

NIU	IPSec	SRTP	QoS	Transcoding
4x1Gig or 2x10Gig NIU	✓	✓	✓	✓ (requires transcoding module)

Table 2-5 Acme Packet 6300 NIU and Feature Group Support Matrix

NIU	IPSec	SRTP	QoS	Transcoding
2x10Gig NIU	✓	✓	✓	Transcoding Carrier Unit

Table 2-6 Virtual Machine and Feature Group Support Matrix

	IPSec	SRTP	QoS	Transcoding
Virtual Machine	✗	✓	✓	✓ (G729, PCMU, PCMA)

Footnotes

- * The system does not support an ETCv1 Card with 4GB RAM. This NIU is identified by a revision lower than 2.09. Use the **show prom-info phy** command and see the ETC NIU **Functionalrev** attribute to confirm compatibility.
- ** IPv4, only.
- *** IPv4, only. Non-transcoded calls, only.
- **** Limited codec support. G711u, G711a, G729

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

A Network Interface Unit (NIU) that supports the Quality of Service (QoS) feature group on the Acme Packet 3820 and the Acme Packet 4500, except the two Enhanced Traffic Control (ETC) cards, requires QoS Field Programmable Gate Array (FPGA) revision 2.19 or higher for the E-CZ7.4.0M1 release. The 2.20 FPGA upgrade image is available at My Oracle Support, https://support.oracle.com/, with a customer account.

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

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

System Capacities

System capacities vary across the range of Oracle® Enterprise Session Border Controller (E-SBC) platforms. You can query the system for the capacities of a particular platform by executing the **show platform limit** command.

3 New Features and Enhancements

The E-Cz7.4.0 release includes the following new features and enhancements.

Features and Enhancements	Description
Acme Packet 3900 Platform	Adds the Acme Packet 3900 platform to the Enterprise line of Oracle session border controllers to fill the space created by the end-of-life Acme Packet 3820 platform. The Acme Packet 3900 platform is also the larger capacity sibling of the Acme Packet 1100 platform.
Communication Monitor Statistics Web GUI Widget	Adds widgets to the Web GUI for displaying Communications Monitor errors, internal messages, and statistics data.
Eliminate License Keys Dependency	Removes the need to use license keys for software TLS and software SRTP on the Acme Packet 1100 platform, the Acme Packet 3900 platform, and VME.
Transmitted Bytes and Packets for Call Detail Records	Adds support for gathering and reporting the number of bytes transmitted and the number of packets transmitted by the E-SBC to the existing types of QoS statistics gathered for reporting. Adds support for gathering QoS statistics for media interworking calls in addition to non-media interworking and SRTP session calls. The system can gather and report the same information using the RADIUS protocol.

Acme Packet 3900 Platform

The Oracle® Enterprise Session Border Controller (E-SBC) supports the Acme Packet 3900 platform, which replaces the end-of-life Acme Packet 3820 platform and fills the resulting space in the product line with updated components, capacities, features, and functionality. Oracle designed the Acme Packet 3900 platform to provide SIP-trunking support and remote-branch connectivity for organizations that need higher performance and capacities than the Acme Packet 1100 and Network Functions Virtualization (NFV) platforms can provide, but not as much as the Acme Packet 4600 platform provides. The Acme Packet 3900 platform shares the same management interfaces and operational model currently used in the other Acme Packet platforms supported by the E-SBC.

Hardware Support

The Acme Packet 3900 hardware provides the following:

- 1 management interface at 1Gbps
- 4 media and signalling interfaces at 10/100/1000Mbs
- 1 HA interface at 10/100/1000Mbs
- 4 USB ports
- Hardware transcoding support for up to 5 Digital Signal Processor (DSP) modules
- 1 quad-span Time Division Multiplexing (TDM) PCIe card

Software Support

The Acme Packet 3900 platform adds the following software support to the Acme Packet 3820 platform:

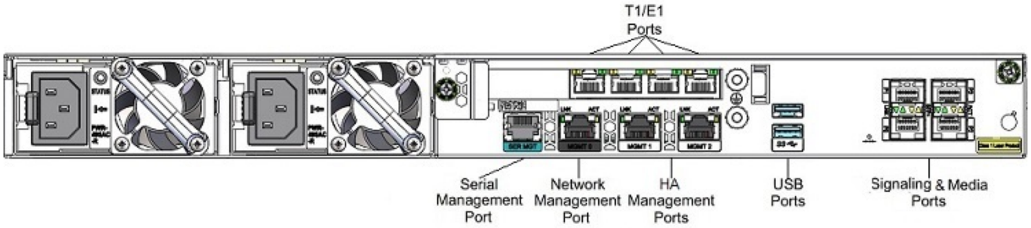
- Audio transcoding and transrating for Opus and SILK
- IPv4 and IPv6 Interworking
- Logging, including the TDM log
- Ten second interim update for QoS
- Time Division Multiplexing (TDM), TDM interface, and Quad Span for TDM
- Transcoding and encryption in the same session

The Acme Packet 3900 platform runs the 64-bit image, only.

The Acme Packet 3900 Platform Physical Interfaces

The Acme Packet 3900 platform uses one Network Interface Unit (NIU) that contains all external interfaces with ports for T1 and E1, serial management, network management, USBs, and media management.

The following illustration shows the NIU labels and ports, which you need to know about when you perform the phy-interface configuration.



Ports key

- T1/E1—For Time Division Multiplexing (TDM) quad span
- SER MGT—For console access for administrative and maintenance purposes
- MGMT0—For EMS control, RADIUS accounting, CLI management, SNMP queries and traps, and other network management functions
- MGMT1 and MGMT2—For High Availability (HA), or for network management with no HA configuration
- USB—For a storage device, or for installing software
- P0 - P3—For signaling and media traffic on copper or fiber optic cable

SNMP Hardware Reporting

The Acme Packet 3900 platform relies on a specific set of MIB objects, in addition to the standard MIB objects.

The Acme Packet 3900 platform supports MIB objects for power supplies, fans, temperature sensors, system information, transcoding DSP(s), wancom ports, media ports, and the product OID. The Standard MIBs (such as MIB-2 objects) are supported.

The Acme Packet 3900 monitors the following environmental parameters by way of SNMP:

Updates to sysObjectID OID in the ap-products.mib.

- Updates the apNetNet 3000Series object to include the apNetNet 3900 object.

Updates to the entity OID in ap-entity-vendortype.mib.

- Updates the apevPowerSupply object to include the apevPowerSupply 500 W object.

Acme Packet 3900 MIBS Paths

Paths for Acme Packet 3900 MIBS.

SNMPv2-SMI::mib-2.47.1.1.1.1.2.1 = STRING: "Acme Packet 3900 Chassis"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.2 = STRING: "Intel(R) Xeon(R) CPU D-1548 @ 2.00GHz"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.3 = STRING: "495 Watt Power Supply"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.4 = STRING: "500 Watt Power Supply"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.5 = STRING: "Assy, 2-fan unit of 40x10"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.6 = STRING: "Sensor of fan speed"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.7 = STRING: "Assy, Acme Packet 3900 Main Board"

```
SNMPv2-SMI::mib-2.47.1.1.1.1.2.8 = STRING: "Sensor of temperature"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.9 = STRING: "Management Port 0 10/100 Ethernet Copper"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.10 = STRING: "Management Port 1 10/100 Ethernet Copper"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.11 = STRING: "Management Port 2 10/100 Ethernet Copper"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.12 = STRING: "Media port - Logical Slot 0 Port 0"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.13 = STRING: "Media port - Logical Slot 0 Port 1"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.14 = STRING: "Media port - Logical Slot 1 Port 0"

SNMPv2-SMI::mib-2.47.1.1.1.1.2.15 = STRING: "Media port - Logical Slot 1 Port 1"
```

NIU Port Numbering Reference for the Acme Packet 3900 Platform

When performing the phy-interface configuration, refer to the following table for mapping each NIU label and operation-type to the appropriate slot and port parameters.

NIU Label	Operation Type	Slot	Port
Mgmt 0	Maintenance	0	0
Mgmt 1	Maintenance	0	1
Mgmt 2	Maintenance	0	2
P0	Media	0	0
P1	Media	0	1
P2	Media	1	0
P3	Media	1	1

Configure the Acme Packet 3900 Physical Interface

Decide the number and type of physical interfaces that you need.

Determine the slot and port numbering that you need to enter for the each physical interface. See the port numbering table.

If you are configuring High Availability (HA), refer to the HA documentation and follow the instructions for setting special parameters in the physical interface configuration.

1. **name**—Set a name for the interface using any combination of characters entered without spaces. For example: **Internet** (for a Fast Ethernet media and signaling interface) or **maint0** (for a maintenance interface).
2. **admin-state**—Leave the administrative state parameter set to **enabled** to receive and send media and signaling on an interface. Select **disabled** to prevent media and signaling from being received and sent. The default for this parameter is **enabled**. Valid values: enabled | disabled

3. **operation-type**—Select the type of physical interface connection to use. Default: **control**. Valid values:

   - **media**—Use to configure media interfaces that carry production traffic.
   - **management**—Use to configure the management physical interfaces for management protocols and High Availability (HA).
   - **control**—Also used to configure management physical interfaces.

4. **slot**—Set the slot number for this physical interface. Refer to the appropriate port numbering reference for the platform.

5. **port**—Set the port number for this physical interface. Refer to the appropriate port numbering reference for the platform.

6. **auto-negotiation**—Leave this parameter set to **enabled**, so that the E-SBC and the device to which it is linked can automatically negotiate the duplex mode and speed for the link.

   When you enable auto-negotiation, the E-SBC begins to negotiate the link to the connected device at the duplex mode you configure. When you disable auto-negotiation, the E-SBC does not engage in a negotiation of the link and operates only at the duplex mode and speed you set.

7. **duplex-mode**—Set the duplex mode, only when auto-negotiation is disabled. Default:**full**.

8. **speed**—Set the speed in Mbps of the physical interfaces; this field is only used if the auto-negotiation field is set to disabled. Default: **100**. Valid values: 10 | 100 | 1000.

9. **virtual-mac**—Refer to E-SBC High Availability (HA) documentation to learn how to set this parameter on an HA interface.

Transmitted Bytes and Packets for Call Detail Records

The E-Cz7.4.0 release adds support for gathering both the number of bytes transmitted and the number of packets transmitted by the Oracle® Enterprise Session Border Controller (E-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.

For media interworking calls and SRTP sessions, the system displays the following information.

- Bytes and packets received
- Lost packets (locally observed and as reported by RTCP)
- Jitter (locally observed and as reported by RTCP) on ingress packets, only
- Maximum Jitter (locally observed and as reported by RTCP) on ingress packets, only
- Latency (as reported by RTCP) on ingress packets, only
- Maximum Latency (as reported by RTCP) on ingress packets, only

For non-media interworking calls, media interworking calls, and SRTP sessions, the system displays the following information.

- Bytes and packets transmitted

The E-SBC captures the statistics about media sessions in the STOP records of Call Detail Records (CDR) logs for up to two flows per leg. Use the account-config object to specify how you want the E-SBC to generate the logs. The log file structure depends on the following settings:

account-config protocol = RADIUS

account-config generate-start = INVITE|OK

account-config cdr-output-inclusive = enabled|disabled

The following newly added, Vendor Specific Attributes record octets of bytes transmitted:

Attribute Name	Attribute Value
Acme-Calling-Octets-Transmitted_FS1	240
Acme-Calling-Octets-Transmitted_FS2	244
Acme-Called-Octets-Transmitted_FS1	242
Acme-Called-Octets-Transmitted_FS2	246

The following newly added, Vendor Specific Attributes record packets transmitted:

Attribute Name	Attribute Value
Acme-Calling-Packets-Transmitted_FS1	241
Acme-Calling-Packets-Transmitted_FS2	245
Acme-Called-Packets-Transmitted_FS1	243
Acme-Called-Packets-Transmitted_FS2	247

Note that availability of the VSAs depends on configuration of vsa-id-range field in account config and the QoS license. Without the QoS license, the system cannot display the VSAs and reports 0 for the values for the CDR and RADIUS statistics in the log messages.

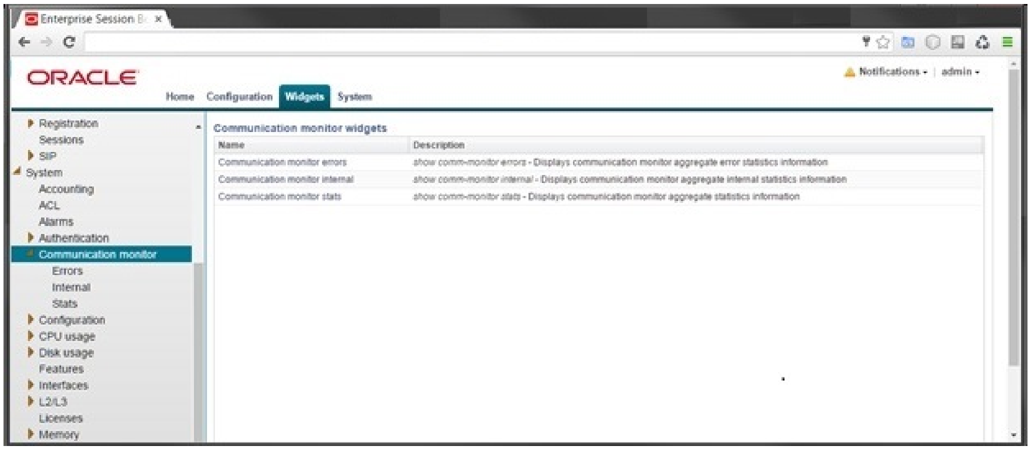
When you configure the vsa-id-range field in account config with Vendor Specific Attribute IDs other than the new QoS-related VSA IDs, the system does not include the new VSAs in RADIUS messages even with QoS monitoring license.

The additional QoS reporting requires no ACLI configuration change.

Web GUI Widgets for Displaying Communications Monitor Statistics

When you want to use the Web GUI to see statistics about connections between the Oracle® Enterprise Session Border Controller (E-SBC) Communications Monitor probe and any configured Communication Monitor, you can use the Errors, Internal, and Stats elements located on the Widgets tab under the Communication Monitor object.

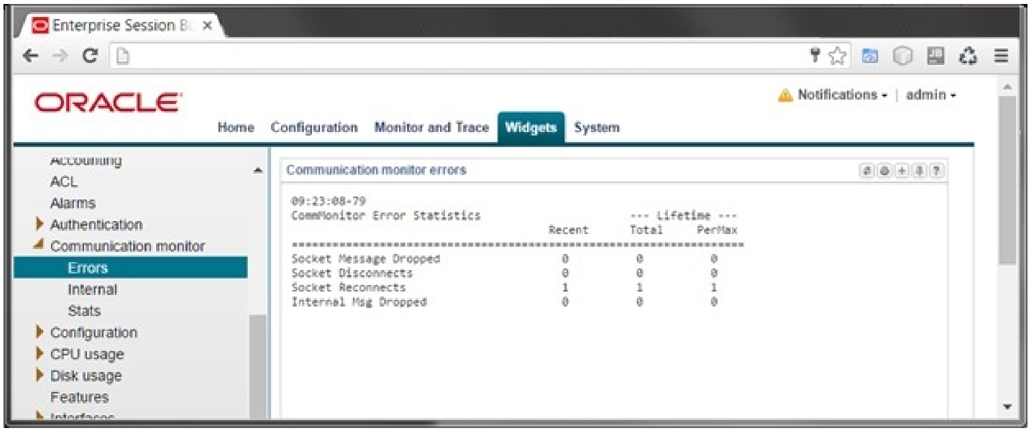
The Communications Monitor object expands to display the available elements for displaying comm-monitor statistics.



Communication monitor widgets

Name	Description
Communication monitor errors	show comm-monitor errors - Displays communication monitor aggregate error statistics information
Communication monitor internal	show comm-monitor internal - Displays communication monitor aggregate internal statistics information
Communication monitor stats	show comm-monitor stats - Displays communication monitor aggregate statistics information

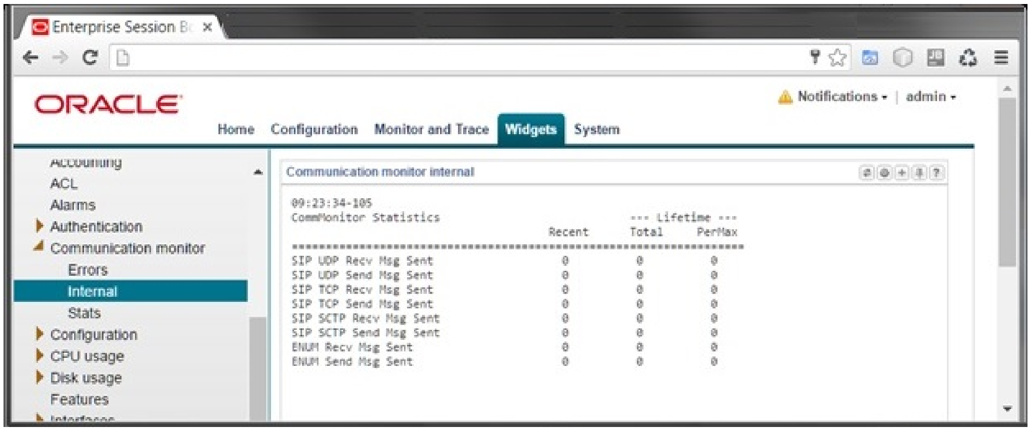
The Errors widget displays the following data about errors that occurred between the E-SBC and the client, along with the number of occurrences.



Communication monitor errors

```
09:23:08-79
CommMonitor Error Statistics                          --- Lifetime ---
                                         Recent      Total      PerMax
======================================================================
Socket Message Dropped                       0          0          0
Socket Disconnects                           0          0          0
Socket Reconnects                            1          1          1
Internal Msg Dropped                         0          0          0
```

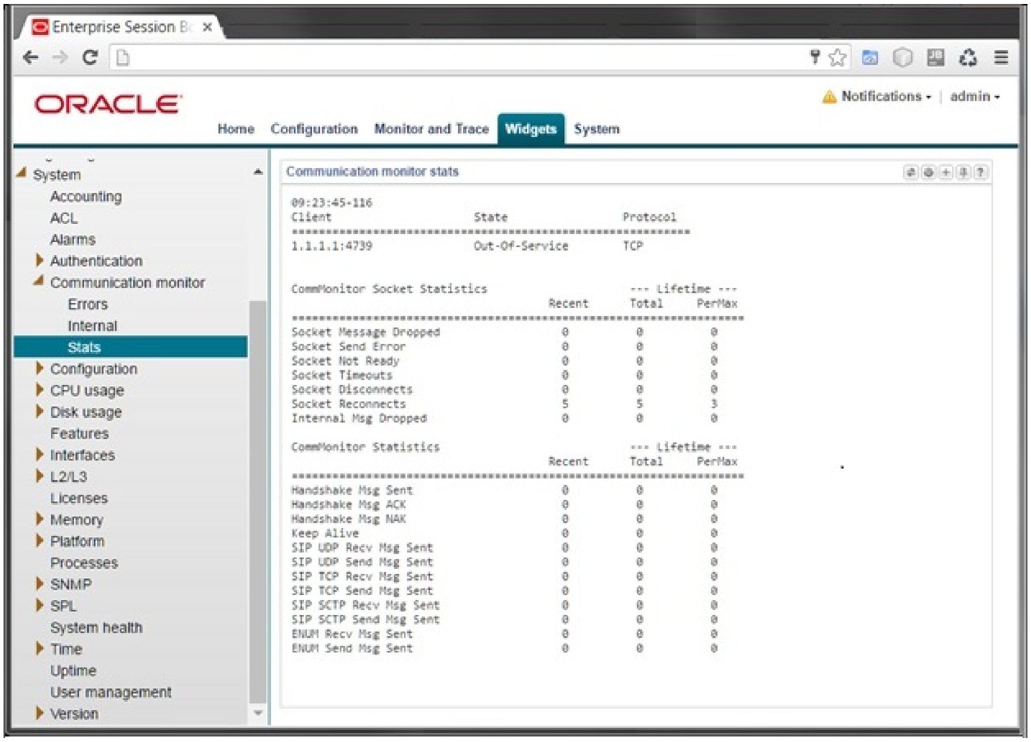
The Internal widget displays the following data from the perspective of the E-SBC, whether coming from the SIP client to the E-SBC or coming from the SIP server to the E-SBC, along with the number of occurrences:



Communication monitor internal

```
09:23:34-105
CommMonitor Statistics                                --- Lifetime ---
                                         Recent      Total      PerMax
======================================================================
SIP UDP Recv Msg Sent                        0          0          0
SIP UDP Send Msg Sent                        0          0          0
SIP TCP Recv Msg Sent                        0          0          0
SIP TCP Send Msg Sent                        0          0          0
SIP SCTP Recv Msg Sent                       0          0          0
SIP SCTP Send Msg Sent                       0          0          0
ENUM Recv Msg Sent                           0          0          0
ENUM Send Msg Sent                           0          0          0
```

The Statistics widget displays the following data about connection states, socket statistics, and connection statistics.



```
09:23:45-116
Client                    State               Protocol
==============================================================
1.1.1.1:4739              Out-Of-Service      TCP


CommMonitor Socket Statistics                      --- Lifetime ---
                                       Recent      Total      PerMax
==================================================================
Socket Message Dropped                   0           0          0
Socket Send Error                        0           0          0
Socket Not Ready                         0           0          0
Socket Timeouts                          0           0          0
Socket Disconnects                       0           0          0
Socket Reconnects                        5           5          3
Internal Msg Dropped                     0           0          0

CommMonitor Statistics                             --- Lifetime ---
                                       Recent      Total      PerMax
==================================================================
Handshake Msg Sent                       0           0          0
Handshake Msg ACK                        0           0          0
Handshake Msg NAK                        0           0          0
Keep Alive                               0           0          0
SIP UDP Recv Msg Sent                    0           0          0
SIP UDP Send Msg Sent                    0           0          0
SIP TCP Recv Msg Sent                    0           0          0
SIP TCP Send Msg Sent                    0           0          0
SIP SCTP Recv Msg Sent                   0           0          0
SIP SCTP Send Msg Sent                   0           0          0
ENUM Recv Msg Sent                       0           0          0
ENUM Send Msg Sent                       0           0          0
```

The preceding example shows the "Out-Of-Service" state, but the widget can also display the following states:

- Connecting—Trying to connect to the E-SBC.
- Connected—Connected, but cannot collect statistics.
- In-Service—Connected, and can collect statistics.

Note:

The widgets can display up to the maximum value of 999999 for any statistic, after which the system restarts the counter from zero.

4

Inherited Features

The E-Cz7.4.0 release inherits the following features and enhancements from the E-Cz7.3.0 M1 and M2 releases.

E-Cz7.3.0M1 Maintenance Release Features

Documentation for the following features previously appeared only in the E-Cz7.3.0M1 *Maintenance Release Guide* because Oracle does not update the full documentation set for a maintenance release. Oracle integrates the maintenance release content into the full documentation set upon the next major release. The following list provides a short description and location of each feature integrated into the E-Cz7.4.0 documentation set from the E-Cz7.3.0M1 release.

Active Directory Call Routing

For configuring an LDAP query with multiple attributes, the Oracle® Enterprise Session Border Controller (E-SBC) allows the **and** and **or** operators for more granular condition-based call routing.
See "Configuring LDAP Transactions" in the *ACLI Configuration Guide*.

Enhanced Video Call Statistics

The ECZ30M1 release adds H.264 to video call statistics. The **show sipd codecs <realm ID>** command displays media-processing statistics per SIP traffic. This command displays statistics per realm and requires a realm argument.
See "Show SIPD Codecs" in the *ACLI Configuration Guide*.

H323 Destination Based Address Routing

Users of H.323 video conferencing applications typically need to dial a publicly routable IP address to join the conference. When the Oracle® Enterprise Session Border Controller (E-SBC) is deployed in a VPN environment, the E-SBC translates the dialed IP address as it routes the call from ingress to egress. When the H.323 destination address-based routing feature is enabled, the E-SBC populates the destinationAddress/AliasAddress field with the IP address of the destination IP system and uses that information to define the next-hop. This is option requires enablement.
See "H.323 Destination Address Based Routing" in the *ACLI Configuration Guide*.

Increased ISP Monitoring and Tracing Sessions

The ECZ730M1 release increases the number of supported SIP monitoring and tracing sessions from 2,000 to 4,000 for all platforms except the Acme Packet 3820.
See "Introduction" in the SIP Monitor and Trace chapter in the *ACLI Configuration Guide*.

License Widget

The License widget on the Web GUI provides a workspace where you can view, add, and delete Oracle® Enterprise Session Border Controller (E-SBC) licenses.
See "License Widget" in the *Web GUI User Guide* and in the Help system.

Locally Generated SIP Response on License Exhaustion

The default 503 message for the error that the Oracle® Enterprise Session Border Controller (E-SBC) sends when the licensed session capacity is reached is "503 licensed session capacity reached". You can customize the number for this error message in the SIP Status field and you can customize the reason in the SIP Reason field when you configure local response map entries.
See "SIP-SIP Calls Configuration" in the *ACLI Configuration Guide*, "Add a Local Response Map" in the *Web GUI Guide*, and "Add a Local Response Map" in the Help system.

Opus Codec Transcoding Support

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

PKCS 12 Container Import and Export Capability

The Oracle® Enterprise Session Border Controller (E-SBC) supports Public Key Cryptography Standard (PKCS) #12 for bundling a private key with the associated X.509 public key certificate in a file for archiving, importing, and exporting. The E-SBC does not support bundling all members of the chain of trust.
See "PKCS #12 Container Import and Export Capability" in the *ACLI Configuration Guide*.

Quad-Span for TDM

If you want the Oracle® Enterprise Session Border Controller (E-SBC) to handle more Time Division Multiplexing (TDM) calls than the single-span TDM card allows, you must order the optional quad-span TDM card. The quad-span card increases the maximum number of TDM calls by providing four ports to connect up to four PSTN or TDM networks. Each port handles one span of voice channels plus the corresponding signaling channel. With the quad-span card, T1 TDM calls can increase from 23 to 92 and E1 TDM calls can increase from 30 to 120.
See "Quad Span for TDM" in the *ACLI Configuration Guide*. See "Configure Time Division Multiplexing" in the *Web GUI Guide* and in the Help system.

SILK Codec Transcoding Support

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

Suite B Support

The Oracle® Enterprise Session Border Controller (E-SBC) supports Suite B for Transport Layer Security (TLS).

See "Suite B and Cipher List Support" in the *ACLI Configuration Guide*, in the *Web GUI Guide*, and in the Help system.

Set TDM Configuration Wizard

The Set TDM Configuration wizard is a tool that you use to complete the Time Division Multiplexing (TDM) configuration after you create the tdm-object. The wizard completes the configuration by creating the realm, SIP interface, steering pools, and other necessary configuration elements including the network interface and the physical interface for SIP call routing. If you have an SRTP license, the wizard also creates the media-sec-policy object, enables the secured-network attribute for the sip-interface object, and configures the media-sec-policy attribute for realm-config. You can run the wizard from either the Web GUI or the ACLI. See "Set TDM Configuration Wizard" in the *ACLI Configuration Guide*, in the *Web GUI Guide*, and in the Help system.

Telephony Fraud Protection

You can configure the Oracle® Enterprise Session Border Controller (E-SBC) to protect against fraudulent calls by using lists of phone numbers to block, allow, redirect, and rate limit calls, according to rules that you configure to manage fraudulent traffic. The lists reside together in a single file that you specify as the source file in the fraud protection configuration. You can enable and manage fraud protection from the Web GUI, but only in Expert mode. You can enable fraud protection from the ACLI, but you cannot manage fraud protection from the ACLI. Telephony Fraud Protection is part of the advanced license. If you owned an Advanced license before the introduction of Telephony Fraud Protection, you must re-enable the license to access this feature.
See "Telephony Fraud Protection" in the *ACLI Configuration Guide*, in the *Web GUI Guide*, and in the Help system.

Web GUI Enhancements

The E-CZ730M1 release includes the following enhancements to the Web GUI.

- Adds the Settings button to the User Management Table widget for configuring the auto-refresh time.
- Adds the opt, boot, and crash partitions to the Disk Usage widget.
- Hides unconfigured objects from the display in the Configuration Inventory Widget.
- Shows the name of the object and the sub-object in the results of a global search.
- Opens the edit dialog when you double-click an item in a delimited file.

E-Cz7.3.0M2 Maintenance Release Features

Documentation for the following features previously appeared only in the E-Cz7.3.0M2 *Maintenance Release Guide* because Oracle does not update the full documentation set for a maintenance release. Oracle integrates the maintenance release content into the full documentation set upon the next major release. The following list provides a short description and location of each feature integrated into the E-Cz7.4.0 documentation set from the E-Cz7.3.0M2 release.

Access the Web GUI with HTTPS

To provide secure access to the Web GUI from the Web server, you can enable HTTPS by creating a Transport Layer Security (TLS) profile. The E-SBC does not require either the hardware Security Service Module (SSM) or the software TLS license when configuring `certficate-record`, `tls-profile`, and `tls-global` for an HTTPS connection to the Web GUI from the Web server.

See "Access the Web GUI with HTTPS" in the *Web GUI User Guide*.

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.
See "Advanced Logging" in the *ACLI Configuration Guide*. See "Configure Advanced Logging" in the *Web GUI User Guide* and in the Help system.

Audit Logs - Web GUI

The Oracle® Enterprise Session Border Controller (E-SBC) can record user actions in audit logs by way of the Web GUI. The audit logs record the creation, modification, and deletion of all user-accessible configuration elements, as well as attempted access to critical security data such as public keys. For each logged event, the system provides the associated user-id, date, time, event type, and success or failure data.
See "Configure Audit Logging" in the *Web GUI User Guide* and in the Help system.

CLIP and COLP Support for TDM

The Time Division Multiplexing (TDM) option on the Acme Packet 1100 supports Calling-Line Identification Presentation (CLIP) and Connected-Line Identification Presentation (COLP) to provide ISDN facility messages. With CLIP and COLP support enabled, each party on the call can receive identification of the other.
See "Time Division Multiplexing" and "Configure Time Division Multiplexing" in the *ACLI Configuration Guide*, in the *Web GUI User Guide*, and in the Help system.

Configure Subnet Ranges in SNMP Community

The SNMP system can dynamically originate SNMP GET requests from any host among a wide range of IP addresses. Due to the distributed nature of a typical network, the SNMP GET request may come from any IP address on an /8 netblock. It is not feasible to add all 16,777,216 possible IP addresses, one-by-one, to the snmp-community configuration. The solution for the Oracle® Enterprise Session Border Controller (E-SBC) is to allow subnet ranges in the snmp-community configuration. Such configuration allows the (E-SBC) to accept SNMP GET requests from any host in the specified subnet.
See "Configure Subnet Ranges in SNMP Community" in the *ACLI Configuration Guide*, in the *Web GUI User Guide*, and in the Help system.

Disable Server Certificate Validation

With the growth of video conferencing adoption and B2B video in all IP networks, Oracle® Enterprise Session Border Controller (E-SBC) customers may want to conduct video conferencing with a destination where the Certificate Authority (CA) is not pre-loaded in the E-SBC. In such a scenario the E-SBC cannot successfully establish a TLS session, due to lacking the correct root CA certificate to validate the server certificate. To handle the scenario in which a TLS session lacks the correct root CA, the "ignore-root-ca=yes" tls-profile option allows the E-SBC to ignore the root CA certificate during the validation process.
Appears in the *E-CZ730M2 Maintenance Release Guide*, only.

Preserve SIPREC with SIP REFER Header

When the Oracle® Enterprise Session Border Controller (E-SBC) generates a new INVITE as part of terminating a SIP REFER, the E-SBC evaluates the SIPREC configuration of the realms and session agents involved in the new call leg and responds accordingly. The REFER and Transfer mechanism automatically preserves the UCID, XUCID, GUID, GUCID, and UUI in the metadata, and can forward this information to the Session Recording Server. The E-SBC can Start, Stop, Pause, and Resume SIPREC sessions in response to any re-INVITE, UPDATE, new INVITE, REFER, or specified SIP Response Message.
See "Preserve SIPREC with SIP REFER Header" in the *ACLI Configuration Guide*.

Secure the ACP Communications Link with TLS

You can use the Transport Layer Security (TLS) protocol to secure the communications link between the Oracle® Enterprise Session Border Controller (E-SBC) and the Oracle Communications Session Delivery Manager (SDM). Note that the systems use Acme Control Protocol (ACP) for this messaging.
See "Secure the ACP Communications Link with TLS" in the in the *ACLI Configuration Guide*, in the *Web GUI User Guide*, and in the Help system.

Security Enhancements

Note the following security enhancements.

- Oracle increased the default RSA key size for the E-SBC certificate from 1024 to 2048. See "Configuring Certificates" in the *ACLI Configuration Guide*. See "Add a Certificate Record" in the in the *Web GUI User Guide*, and in the Help system.
- Oracle changed the default message-digest algorithm from SHA1 to SHA256. See "Supported Encryption" in the *ACLI Configuration Guide*. See "Add a Certificate Record" in the in the *Web GUI User Guide*, and in the Help system.
- Oracle disabled the arcfour cipher and any 96-bit Keyed-Hash Method Authentication Code (HMAC) algorithms. The SSH key exchange initialization message no longer sends arcfour and 96-bit HMAC algorithms. The preceding changes appear in the *E-CZ730M2 Maintenance Release Guide*, only.

Suite B Support

The Oracle® Enterprise Session Border Controller (E-SBC) supports full control of selecting the ciphers that you want to use for Transport Layer Security (TLS). The system defaults to ALL for the cipher list parameter in the TLS profile configuration. Oracle recommends that you delete ALL and add only the particular ciphers that you want, choosing the most secure ciphers for your deployment.
See "Suite B and Cipher List Support" in the *ACLI Configuration Guide*, in the *Web GUI User Guide*, and in the Help system.

Surrogate Registration

The surrogate registration feature lets the E-SBC explicitly register on behalf of a Internet Protocol Private Branch Exchange (IP-PBX). After you configure a surrogate agent, the E-SBC periodically generates a REGISTER request and authenticates itself using a locally configured username and password, with the E-SBC as the contact address. Surrogate registration also manages the routing of calls from the IP-PBX to the core and from the core to the IP-PBX.

See "Surrogate Registration" in the *ACLI Configuration Guide*.

TCP Connection Tools

Transmission Control Protocol (TCP) connection tools can assist you in gauging performance, identifying potential memory leaks, and debugging connections for performance tracking and improvement.
See "TCP Connection Tools" in the *ACLI Configuration Guide*.

Web GUI Access with the Admin Security License

To provide secure access to the Web GUI from the Web server, you can enable HTTPS by creating a Transport Layer Security (TLS) profile. The E-SBC does not require either the hardware Security Service Module (SSM) or the software TLS license when configuring `certficate-record`, `tls-profile`, and `tls-global` for an HTTPS connection to the Web GUI from the Web server.
See "Web GUI Access with the Admin Security License" in the *Web GUI User Guide*, and in the Help system.

Web GUI Enhancements

The ECZ7.3.0M2 release includes the following enhancements to the Web GUI.

- Configuration Tab—Adds the **Delete All**, **Upload**, and **Download** buttons to the tool bar of all top-level, multi-instance configuration objects.
- System Tab—Adds the **Refresh**, **Upload**, **Download**, and **Delete**buttons to the File Management tool bar.
- System Tab—Adds the Configuration.csv and Audit Log file types to the File Management file type list.

5 Known Issues

Oracle recommends that you review the following known issues before using the E-Cz7.4.0 release.

List of Known Issues

The following list describes important information about the behavior of the E-Cz7.4.0 release on the Oracle® Enterprise Session Border Controller (E-SBC.

File Systems

For customers using the Acme Packet 3820 and Acme Packet 4500 platforms with a hard-disk, an upgrade from pre-E-Cz7.1.0 software to E-Cz7.4.0 does not change the hard drive file system from FAT-32 to ext3 to preserve any existing data. Consequently, the SFTP application cannot provide the expected file system user security.

Workaround—Reformat the system hard-disk.

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

H.323 Calls

The system does not support HA Redundancy for H.323 calls.

Interim QoS Update

The 10 second QoS update function does not work on the Acme Packet 3900.

IPSec

- When you configure the security-association configuration element as an IPv6 SA, the system does not enable RTC.
- The system uses the default setting of "all" for the **transport-protocols** parameter in **security-policy** configuration element, regardless of configuration.

packet-trace remote Command Limitation

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

- **Defect ID**—26338219

PKCS#12 Certificates

The system cannot export CA certificates as PKCS#12.

RFC2833 to UII Inter-working

The system does not support SIP-H323 hairpin calls with DTMF tone indication Inter-working.

SIP Over TCP

The system supports no more than 500 SIP Interfaces with SIP over TCP.

Subnet Configuration

Do not configure media and management (wancom) interfaces with the same subnet, regardless of VLAN.

Redundancy Configuration

Do not use the 169.254.16.x or 169.254.21.x networks in redundancy-config (including the network-interface configuration for the wancom1 and wancom2 interfaces), when installed on an Acme Packet platform that includes a transcoding card. The system uses the networks to provide software to transcoding Digital Signalling Processors (DSP). When you configure the redundancy configuration with the 169.254.16.x or 169.254.21.x networks, the system cannot route the software properly.

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

High Availability

Description	Found In	Fixed In
The Acme Packet 3900 does not support high availability.	E-CZ7.4.0 GA	E-CZ7.4.0p3
The Acme Packet 3900 exhibits lengthened audio blackouts during an HA switchover.	E-CZ7.4.0p3	

6

Caveats

Oracle recommends that you review the following caveats before using the E-CZ7.4.0 release.

List of Caveats

The following list provides important information about the behavior of the E-Cz7.4.0 release on the Oracle® Enterprise Session Border Controller (E-SBC).

Patch Immediately

The software shipped on the Acme Packet 3900 requires a patch before you attempt to configure the device. Oracle recommends that you download the patch as soon as possible. In the meantime, do not configure SIPREC on the Acme Packet 3900 as shipped because doing so prevents an online upgrade to the necessary patch. Go to Oracle MOS (https://support.oracle.com) and download the E-Cz7.4.0p1 release. Use the nnECZ740p1.bz image file and update the boot loader with the nnECZ740p1.boot file.

Interface Utilization Support

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

Archive Logs Support

The Acme Packet 4500 platform does not support archiving log files without an HDD installed.

Configure call-recording-server-id

Deprecated—The call-recording-server-id configuration element.

DTMF Interworking Support

The system does not support:

- RFC 2833 interworking with H.323
- SIP-KPML to RFC2833 conversion for transcoded calls

Fragmented Ping Support

The E-SBC does not respond to inbound fragmented ping packets.

FTP Support

The E-SBC FTP Server is deprecated. Only SFTP server services are supported.

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

H.323 Signaling Support

When the system runs both H.323 and SIP traffic, configure each protocol (H.323 and SIP) in a separate realm.

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 E-SBC.

Work around—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 E-SBC, and save and activate the configuration.
2. Reboot both the Primary and the Secondary.

High Availability During a Forced Switchover

When forcing a switchover, the standby member of a High Availability (HA) pair successfully becomes the active member, but the former active member re-starts before becoming the standby member.

The issue affects the Acme Packet 4500 with DSPs and LDAP config, when you issue the "notify berpd force" command on either the active member or the standby member of the HA pair.

If you find it necessary to avoid the re-start situation, delete the LDAP configuration and any local policy that references LDAP.

> **Note:**
>
> The re-start does not cause a service interruption.

High Availability Synchronization During an Upgrade

When upgrading the software, the standby member of a High Availability (HA) pair goes Out-of-Service and does not sync.

The issue affects the standby member of an HA pair on the Acme Packet 4500 with DSPs, when upgrading from the E-CZ7.2.0x and E-CZ7.3.xx releases.

Workaround—Change the "becoming-standby-time" value under "redundancy-config" to "360000" before upgrading. You can restore the previous setting after upgrading.

High Availability Synchronization with High Call Rates

When the Acme Packet 6300 experiences call rates over 650 CPS, SIP and MBCD may not synchronize.

HMR action on Call-ID

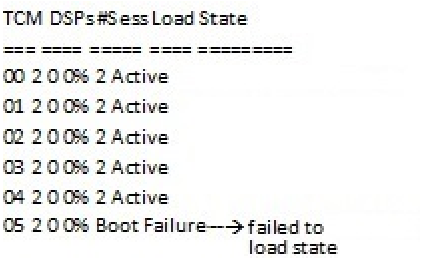
Deprecated—HMR operations on Call-ID.

Intermittent DSP Boot Disruption

When upgrading the software, intermittent Digital Signal Processor (DSP) boot disruptions occur on some DSP slots. Affects the Acme Packet 4500 with DSPs, when upgrading from either the E-Cz7.2.0x or the E-Cz7.3.0m1x releases. The system displays a DSP "Boot Failure" message such as:

```
CRITICAL ALARM - DSP#1 Boot Failure!
        writing stats to file/opt/logs/dump.xcode-boot
```

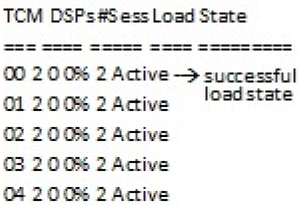
Critical alarm example



```
TCM DSPs #Sess Load State
=== ==== ===== ==== =========
00 2 0 0% 2 Active
01 2 0 0% 2 Active
02 2 0 0% 2 Active
03 2 0 0% 2 Active
04 2 0 0% 2 Active
05 2 0 0% Boot Failure--→ failed to
                          load state
```

When the system displays a DSP "Critical Alarm - Boot Failure" message while re-starting, perform a re-start. All of the DSPs come up, as expected. To confirm that the DSPs are operational, use the `show xcode xlist` command.

Success example



```
TCM DSPs #Sess Load State
=== ==== ===== ==== =========
00 2 0 0% 2 Active --→ successful
01 2 0 0% 2 Active     load state
02 2 0 0% 2 Active
03 2 0 0% 2 Active
04 2 0 0% 2 Active
```

Note that you can use the `show xcode xlist` command to check DSP status any time.

Inter-working Function (IWF)

The E-Cz7.4.0p1 release does not support IWF for

- calls between SIP and H.323 in either direction
- SRTP IPv4 to IPv6 calls

LDAP Support - Acme Packet 6300

The Acme Packet 6300 does not support LDAP.

Log File Download Error

When you attempt to download too many log files from the Web GUI at one time, the system may display an error message because the Oracle® Enterprise Session Border Controller does not have enough storage space for compressing the logs.

Work around—Download the log files in smaller chunks. Oracle recommends that you delete all log files after they are downloaded.

Media Hairpinning Support

The system does not support media hairpinning for hair-pin/spiral call flows involving both H.323 and SIP protocols.

Media Playback Support

The system does not support using the Media Playback feature in conjunction with the SIPREC feature.

MGCP Signaling Support

The system does not support Media Gateway Control Protocol (MGCP) Signaling.

Minimum Enterprise Operations Monitor Version

The Enterprise Operations Monitor (EOM) requires at least the 3.3.70 version for running large TCP packets.

Comm Monitor

Problem: When running SIP Monitor & Trace and Comm-Monitor simultaneously, while the system is passing TLS over TCP calls on a system with high load, the ESBC may fall-over and not reboot. The issue affects all platforms.

Workaround: Run SIP Monitor & Trace or Comm-Monitor individually, not simultaneously.

Packet Trace

Output from the packet trace-local feature on hardware platforms running E-Cz7.4.0 may display invalid MAC addresses for signaling packets.

Do not run packet trace simultaneously with other Oracle Enterprise Session Border Controller replication features, such as SRS, SIP Monitoring and Trace, and Call Recording. These features may interfere with each other, corrupting each one's results.

The Acme Packet 1100 and Acme Packet 3900 do not support the **packet-trace remote** command.

Phy Link Redundancy Support

The system does not support Phy Link redundancy.

Physical Interface and Network Interface RTC Support

After changing any Physical Interface configuration, you must reboot the system.

RTCP Generation Support

The system does not support Real-time Control Protocol (RTCP) generation.

SCTP Support

The system does not support Stream Control Transmission Protocol (SCTP) Multihoming.

Session Replication for Recording Support

The system does not support Session Replication for Recording. Note that the configuration continues to display the "call-recording-server-id" parameter, which Oracle recommends that you do not attempt to use. Enabling the "call-recording-server-id" parameter prevents successful TCP connections.

SIP hold-refer-reinvite

The SIP hold-refer-reinvite function becomes unresponsive on multi-core devices, such as the Acme Packet 4600 and the Acme Packet 6300.

Workaround—Add the new parameter in the following procedure to system-config on the Acme Packet 4600 and the Acme Packet 6300.

1. From the ACLI, go to **configure terminal** > **system** > **system-config**.
2. For the **Options** attribute, type **sip_threads=1**, and press ENTER.
3. Save and activate the configuration.

SIPREC Sessions

With SIPREC enabled for all sessions, the E-SBC supports no more than 4,000 sessions with infinite media hold time for the G711 codec.

The issue affects the Acme Packet 4500 with the ETC2.

SNMP Traps Limitation

The E-Cz7.4.0 release does not generate the following traps:

- apSecurityTunnelFailureNotification
- apSecurityRadiusFailureNotification
- apSecurityTunnelDPDNotification
- apSecurityOCSRDownNotification
- apSecurityOCSRUpNotification

Source-based Routing

Deprecated—The source routing feature, as configured by system-config --> source-routing. Please review the HIP information in the Network Interface section in the System Configuration chapter of the *ACLI Configuration Guide* for information about accessing Session Border Controller Administrative Applications over media Interfaces.

SPL Headers for SIP Metadata

The first time you create the SPL extension header list, you need only to save and activate the configuration for the list to take effect. When you modify the existing SPL extension header list you need to save and activate the configuration, but that alone does not cause the system to recognize the changes. You must also reboot the system for the changes to take effect. (First noticed in the E-Cz7.3.0 release.)

SRTP Caveats

The system does not support:

- MIKEY key negotiation
- The ARIA cipher
- The Linksys SRTP

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.

T.38 Fax Transcoding

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

Transcoding

The system supports:

- Only SIP signaling with transcoding
- Using Codec policies only when used with realms associated with SIP signaling

The system does not support:

- Transcoding in conjunction with Secure Real-time Transport Protocol (SRTP) on the Acme Packet 4500
- Quality of Service (QoS) for transcoded calls
- Performing SIPREC on a transcoded call
- Local Media Playback for transcoding

Web GUI and IPv4-IPv6 Support

The Web GUI supports only IPv4.

7
Limitations

Oracle recommends that you review the following limitations before using the E-CZ7.4.0 release.

List of Limitations

The following list provides important information about the limitations of the E-Cz7.4.0 release on the Oracle® Enterprise Session Border Controller (E-SBC).

Expired Password

The Web GUI does not support changing a user password. Use the `#secret enable` command from the ACLI.

H.323

The system does not support H.323 for fraud protection.

IPv6

The system does not support IPv6 for fraud protection.

TACACS

The Admin Security License does not support TACACS.

8 E-CZ7.4.0m1

Oracle recommends that you review the following information before using the E-CZ7.4.0m1 release.

Upgrade Information

Due to a correction for a High Availability issue, the E-CZ7.4.0m1 release does not support an in-service upgrade. During the maintenance window, please load the nnECZ740m1.bz image with the corresponding bootloader (nnECZ740m1.boot) and perform a simultaneous reboot on both the primary and secondary Session Border Controllers.

Build Notes

The following table provides the Build Notes for the E-CZ7.4.0m1 release.

Build Name	Build Date	Build Contents and Fixes
nnECZ740m1	7/31/2017	This patch (build 109) contains the following changes and fixes: • Bug #25704654: Update scaling calculations to work on SWDP and non-SWDP platforms Problem: Scaling calculation to determine the number of transport and sipd threads either SWDP or non-SWDP platforms are incorrect. • Bug #26281432: One-way audio in SRTP termination scenario after session refresh from RTP side. Problem: One-way audio in SRTP termination scenario after session refresh from RTP side.
nnECZ740p3	5/24/2017	This patch (build 100) contains the following changes and fixes: • Bug #25604451: Acme Packet 3900: HA Switchover Not Working Problem: Customer configured two SBCs in an HA pair. While initiating a switchover using "notify berpd force" the SBCs does not switchover as in SBC initiates switchover, but within same minute, it postpones saying secondary SBC has timed out. • Bug #25852256: (3900) interim-qos-update is missing under comm-monitor configuration Problem: interim-qos-update is missing under comm-monitor configuration for the Acme Packet 3900. • Bug #25856955: Physical media interface down , healthscore comes back to 100 in a few seconds Problem: When a cable is pulled out of a media port from the Acme Packet 3900, the systems in HA switch over but the healthscore remains at 100 and also no alarms were seen that one of the slot/port is down. • Bug #25924111: RTPEVENT not working while Transcoding G729-G711 Problem: RFC2833 telephone-event packets are not transcoded.

Build Name	Build Date	Build Contents and Fixes
nnECZ740p2	2/1/2017	This patch (build 66) contains the following changes and fixes: • 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 un-wired and down. • Bug #24766047: Sip Rec One Way Audio Intermittently Problem: SIP Rec recordings failing intermittently. • Bug #25099361: SRTP test IP4toIP6 failed, srtp packet with IP6 format received on IP4 network. Problem: SRTP calls with IPv4-IPv6 interworking was broken. • Bug #25141837: ESC: Widget SIP Session all doesn't show sip sessions under ECZ730m2p1 Problem: The sessions all widget is not showing the same data as the ACLI version. • Bug #25358351: X-coding and SRTP encryption not working Problem: X-coding and SRTP encryption not working • Bug #25360947: Customer is reporting CPU spikes on 2 Acme Packet 6300 HA pairs Problem: Customer is reporting CPU spikes on 2 Acme Packet 6300 HA pairs. • Bug #24910754: Wancom reporting 1G, switch reports 100M speed Problem: On a Security NIU, show wancom always shows 1Gig for wancom0 even when it is connected to a 10/100M switch.