Oracle® Session Border Controller

Maintenance Release Guide
Release SCZ730

May 2017

Notices

Contents

About this Guide

The Maintenance Release Guide provides information about the contents of maintenance releases related to Oracle Communications Session Border Controller S-CZ7.3.0. This information can be related to defect fixes, to adaptations made to the system software, and to adaptations ported to this release from prior releases. When applicable, this guide contains explanations of defect fixes to the software and step-by-step instructions, if any, for how to enables these fixes on your system. This guide contains explanations of adaptations including conceptual information and configuration steps.

Purpose of this Document

Designed as a supplement to the main documentation set supporting Oracle Communications Session Border Controller release S-CZ7.3.0, this document informs you of changes made to the software in the maintenance releases of S-CZ7.3.0. Consult this document for content specific to maintenance releases. For information about general Oracle Communications Session Border Controller features, configuration, and maintenance, consult the Related Documentation listed in the section below and then refer to the applicable document.

Organization

The Maintenance Release Guide is organized chronologically by maintenance release number, started with the oldest available maintenance release and ending with the most recently available maintenance release.

This document contains a Maintenance Release Availability Matrix, showing when and if given maintenance releases have been issued and the date of issue. Each available maintenance release constitutes one chapter of this guide.

In certain cases, a maintenance release will not have been made generally available. These cases are noted in the Maintenance Release Availability Matrix. When Oracle has not made a maintenance release available, there will be no corresponding chapter for that release. Therefore, you might encounter breaks in the chronological number of maintenance release.

Maintenance Release Availability Matrix

The table below lists the availability for version S-CZ7.3.0 maintenance releases.

Maintenance Release Number	Availability
S-CZ7.3.0M1	March 8, 2016
S-CZ7.3.0M2	August 12, 2016
S-CZ7.3.0M3	May 23, 2017

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.

Document Name	Document Description
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.
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

Date	Description
March, 2016	- Initial Release
June, 2016	- Update MIB topic for apThreadOverloaded values
August, 2016	- Adds M2 content
January, 2017	- Adds IMS-AKA DDoS upgrade note
May, 2017	- Adds M3 content - Corrects M3 release date - Adds Upgrade Caveat for Acme Packet 4500/3820 to M3 chapter

1

SCZ730M1

This section provides descriptions, explanations, and configuration information for the contents of Maintenance Release SCZ7.3.0M1. Maintenance Release content supercedes that distributed with the point release.

The following SPL engine versions are supported by this software:

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

Current patch baseline: SCZ7.3.0p3

Please refer to the *Oracle® Communications Session Border Controller & Session Router Release Notes*, Release S-CZ7.3.0 for changes to the Known Issues section based on the S-CZ7.3.0M1 release.

Neighbor 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-CZ7.3.0M1:

- SCZ712m5p3
- SCZ720m6
- SCZ730p1

Content Map

The following table identifies the new content in this SCZ7.3.0 M1 Maintenance Release documentation.

Content Type	Description
Behavioral Change	Bandwidth Request Change
Adaptation	Managing Bandwidth Requests for Transcoded Calls
Adaptation	Video Conferencing Support for Polycom Terminals
Adaptation	Saving SDP from Early Dialog Messages
Adaptation	Oracle Operations Monitor Statistics
Adaptation	Process Level CPU Thread Monitoring
Adaptation	Per-Realm Media Guard Timers
Adaptation	DNS Entry Maximum TTL
Adaptation	DNS Re-query over TCP
Adaptation	DNS Queries on the Command Line
Adaptation	Support Millisecond Granularity for acct-session-time
Adaptation	Override Alphanumeric Ordering of Session Agents with Same IP
Adaptation	Call Detail Record Sequence Number in Filename
Adaptation	TSM Security Traversing Gateway Mode
Forward Merge	Inheriting features from SCZ7.2.0M6, as listed below
Inherited Feature	SIP Pre-emptive Symmetric Media Latching
Inherited Feature	Asynchronous SIP-Diameter Communication
Inherited Feature	Flow Description AVP Change for Media Release
Inherited Feature	DDoS Enhancement for IMS-AKA

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.

Two behavioral changes are included in this release to better assure proper bandwidth requests:

- AAR bandwidth requests for transcoded calls—The Oracle Communications Session Border Controller uses the SDP sent or received on the same realm as the external policy server to calculate the bandwidth information it presents in an AAR. This ensures that the Oracle Communications Session Border Controller receives bandwidth allocation information that is applicable to the leg that the policy server is serving.

- AAR bandwidth requests for dual stack calls—If the Oracle Communications Session Border Controller receives a call that switches between IPv4 and IPv6, the bandwidth that it presents in the AAR is based on the address space used by the call on the same realm as the external policy server. This ensures that the Oracle Communications Session Border Controller receives bandwidth allocation information that is applicable to the leg that the policy server is serving.

In previous Oracle Communications Session Border Controller versions, the bandwidth information presented in the AARs lines described above were not certain to be correct for the target codec or IP version.

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.

The Oracle Communications Session Border Controller can change a call's egress answer b=AS line to a value based on the media profile configuration of the codec to which the media is being transcoded. This ensures that the Oracle Communications Session Border Controller makes bandwidth requests that are applicable to the leg on which that codec is used.

Use the syntax below to specify 124 kbps for a media profile's b=AS line.

```
(media-profile)#as-bandwidth 124
```

The parameter's default value is zero, meaning it is disabled. The range is from 0 to 4294967295, measured in kbps.

The Oracle Communications Session Border Controller can modify a b=AS: line at both the SDP media level and SDP session level. Session level b=AS modification does not use an **as-bandwidth** setting.

The Oracle Communications Session Border Controller updates a media level b=AS: line to the configured **as-bandwidth** value only for the Egress SDP Answer, not the offer.

The Oracle Communications Session Border Controller modifies a session level b=AS: value only if every m-line in the SDP also has a b=AS: value. If an incoming message has SDP with a session level b=AS value, and every m-line in the SDP has a b=AS value, then the Oracle Communications Session Border Controller updates the outgoing message's session level b=AS value to the sum of the transcoding/IPv4-IPv6 adjusted media level b=AS values in the outgoing message. If an incoming message has SDP with a session level b=AS value, but not every m-line in the SDP has a b=AS value, the Oracle Communications Session Border Controller does not modify the session level b=AS value in the outgoing message.

When the Oracle Communications Session Border Controller updates a b=AS: line in the egress answer's SDP to a configured **as-bandwidth** value, and the original ingress offer SDP already had a b=AS: line, the Oracle Communications Session Border Controller changes the egress answer SDP's b=AS: back to the ingress offer's b=AS: value, not to the configured **as-bandwidth** value.

Important operational considerations include:

- The value can be understood as IP neutral, meaning the system recognizes when the call is IPv4 to IPv6 interworking, and adjusts the value of the b=AS line to compensate for the IP version of the applicable leg. The Oracle Communications Session Border Controller does this for both transcoded and non-transcoded calls in both the egress offer and answer.
- The configuration has no effect if the initial message received has no b=AS line.
- The configuration has no effect if the m line is not transcoded.
- The system does not change a session b=AS value if the SDP has a media line with b=AS value of 0.

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.

The Oracle Communications Session Border Controller supports operations in a video conferencing environment with Polycom H323 terminals and a Polycom MCU (Multipoint Conferencing Unit) by relaying H.239/H.245. The Oracle Communications Session Border Controller implements the following messages appropriately:

- Miscellaneous command message with subtype such as multiPointModeCommand, cancelMultipointModeCommand
- Conference Indication message with subtype such as terminalNumberAssign, terminalYouAreSeeing

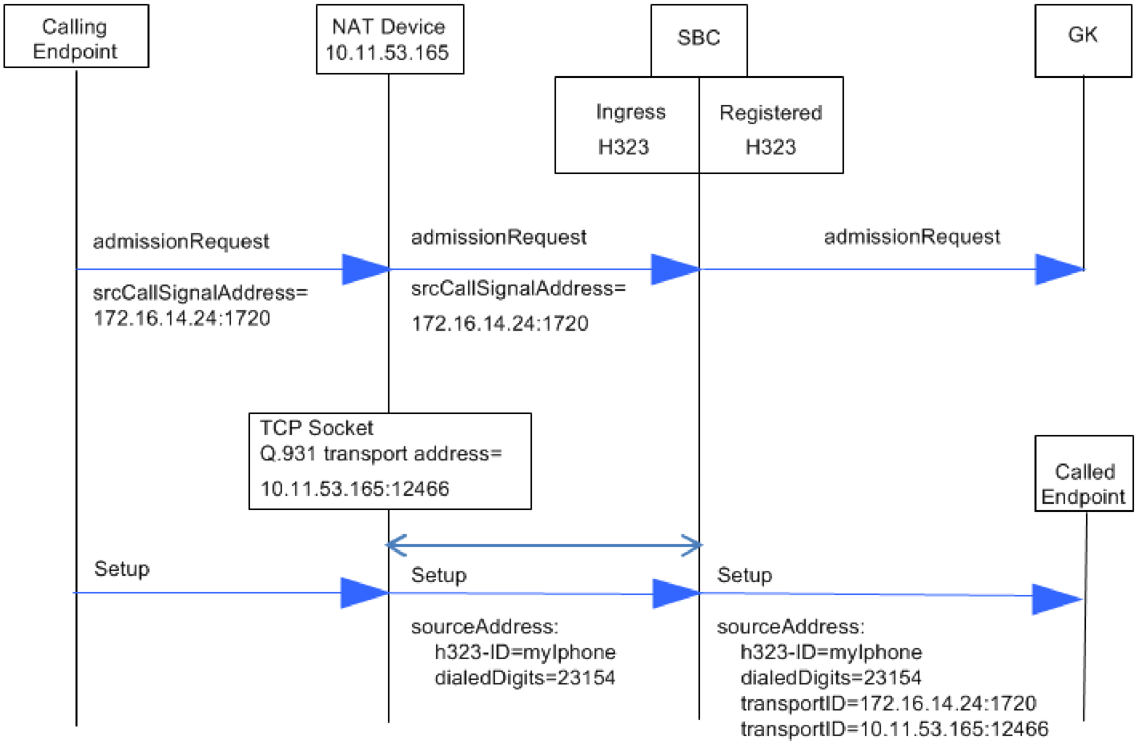
The Oracle Communications Session Border Controller can also resolve a video conference billing issue caused by a NAT device. NAT devices change the sourceCallSignalAddress in a Setup message to the IP address of the NAT device. Deployments that rely on this address in CDRs to bill for the service need this address to be that of the original station behind the NAT. The user sets the **`addSrcCallSignalAddr`** option in the **`h323-stack`** that receives the incoming Setup to cause the Oracle Communications Session Border Controller to present the desired address.

The srcCallSignalAddress field in the admissionRequest message received by the Oracle Communications Session Border Controller often contains the transportAddress of the calling endpoint. This field is optional for the admissionRequest message. If configured with the option and presented with this field, the Oracle Communications Session Border Controller saves the address for later use in outgoing Setup messages. If the srcCallSignalAddress field in the admissionRequest message is not present, or is equal to 0.0.0.0, the Oracle Communications Session Border Controller does not save it.

Having stored this address, the Oracle Communications Session Border Controller uses it following the steps below. Note that the Setup message in this scenario is preceded by the admission request and confirmation messages from the gatekeeper for the call.

1. Add the srcCallSignalAddress, saved from the admissionRequest message, into the sourceAddress field of the outgoing Setup message. The Oracle Communications Session Border Controller adds this address in the format of an AliasAddress of type transportID after any other AliasAddresses that are normally included from the incoming Setup sourceAddress field.
2. Add the remote transport address of the incoming Q.931 TCP connection, into the sourceAddress field of the outgoing Setup message. The Oracle Communications Session Border Controller adds this address in the format of an AliasAddress of type transportID, after the alias that was added in step 1.

The call flow diagram below depicts the Oracle Communications Session Border Controller adding addresses in accordance with this feature.


Calling Endpoint
NAT Device 10.11.53.165
SBC
GK
Ingress H323
Registered H323
admissionRequest
srcCallSignalAddress= 172.16.14.24:1720
admissionRequest
srcCallSignalAddress= 172.16.14.24:1720
admissionRequest
TCP Socket Q.931 transport address= 10.11.53.165:12466
Called Endpoint
Setup
Setup
Setup
sourceAddress: h323-ID=myIphone dialedDigits=23154
sourceAddress: h323-ID=myIphone dialedDigits=23154 transportID=172.16.14.24:1720 transportID=10.11.53.165:12466

Use the syntax below to set this option on the h323-stack receiving the incoming Setup.

```
(h323-stack)# options +addSrcCallSignalAddr
```

The user can find this process confirmed in the log.h232d log file.

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.

Consider a SIP dialog with early media that proceeds by establishing call scenarios in which the final 200 OK does not include any SDP. This messaging may include multiple 183 (Session Progress) messages with SDP that differ from each other and include different To tags, establishing multiple early dialogs. In these scenarios, the Oracle Communications Session Border Controller uses the saved SDP from the dialog that matches the dialog indicated in the 200 OK's To tag to anchor the media. If the 200 OK includes SDP, the Oracle Communications Session Border Controller uses that SDP to anchor the media.

Note: The user can disable this behavior, for example, to use the functional behavior in Oracle Communications Session Border Controller version S-CZ7.2.0 and below, which is to use the last SDP seen as the source for SDP. Deployments that rely on this behavior must revert to it using the **sip-config**'s **dont-save-early-dialog-sdp** option parameter.

```
ORACLE(sip-config)# options +dont-save-early-dialog-sdp
```

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 Command shows three types of aggregate statistics for all clients, including:

- Client State
- Socket Statistics
- Other Aggregate Statistics

The Oracle Communications Session Border Controller's **show comm-monitor** command shows the Lifetime statistics. The command runs without or with arguments, including:

- **show comm-monitor**—Shows client connection states and aggregate stats
- **show comm-monitor by-client <IP-Addr>**—Shows client stats
- **show comm-monitor errors**—Shows Errors captured by the Session Monitor
- **show comm-monitor internal**—Shows Oracle Communications Session Border Controller traffic-specific counters

Example command output without arguments is presented below:

```
ORACLE# show comm-monitor
Client                     State        PROTOCOL
=================================================
192.168.42.10:4739      Out-of-Service       TCP
192.168.42.11:4739      Connecting           TCP
192.168.42.12:4739      In-Service           TCP

15:06:10-35 (recent)
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                       0          0          0
Buffer Allocation Error                 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
```

show comm-monitor

Syntax

```
show comm-monitor <by-client client-IP> | <errors> | <internal> | stats
```

Displays statistics related to connections between the Oracle Communications Session Border Controller's Communications Monitor probe and any configured Communications Monitor servers. The maximum statistic value is 999999, after which the system restarts the counters from zero.

Running the command without arguments displays the following information:

- Client connection states, presented in a connection sequence order, including:
  - Out-of-Service – Connection is not established.
  - Connecting – Trying to Connect to the Oracle Communications Session Border Controller.
  - Connected – Oracle Communications Session Border Controller connected but not able to collect stats.
  - In-Service – Oracle Communications Session Border Controller connected and able to collect stats.
- Aggregate Socket Statistics, including:
  - Socket Message Sent—Number of Socket Message Sent.
  - Socket Message Dropped—Number of Socket Messages dropped
  - Socket Send Error—Number of Socket Send Errors
  - Socket Not Ready—Number of Sockets Not Ready
  - Socket Timeouts—Number of Socket timeouts
  - Socket Disconnects—Number of Socket disconnects
  - Socket Reconnects—Number of Socket Reconnects
- Client connection statistics, including:
  - Handshake Msg Sent—Count for number of handshakes sent from the Oracle Communications Session Border Controller to the Session Monitor server
  - Handshake Msg ACK—Count for number of handshakes acknowledged by the Communications Monitor server
  - Handshake Msg NAK—Count for number of handshakes not acknowledged by the Communications Monitor server
  - Keep Alive—Signal which keeps the connection between the Oracle Communications Session Border Controller and the Communications Monitor Server
  - SIP UDP Send Msg Sent—UDP Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
  - SIP UDP Recv Msg Sent—UDP Message received sent by the Oracle Communications Session Border Controller to SIP client or the Oracle Communications Session Border Controller to the SIP server
  - SIP TCP Send Msg Sent—TCP Message sent from SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
  - SIP TCP Recv Msg Sent—TCP Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server
  - SIP SCTP Send Msg Sent—SCTP Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
  - SIP SCTP Recv Msg Sent—SCTP Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server
  - ENUM Sent Msg Sent—ENUM Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
  - ENUM Recv Msg Sent—ENUM Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server

Arguments

by-client <client-IP>—Shows the same statistics as the command presents without arguments, but limits the output to the specified client.

errors—Display information on errors that may occur between the Oracle Communications Session Border Controller and the client.

- Buffer Error—The number of errors occurring on the connection related to Oracle Communications Session Border Controller buffer space.
- Socket Message Dropped—The number of messages traversing the specified socket that the Oracle Communications Session Border Controller has dropped.
- Socket Disconnects—The number of times a connection between the Oracle Communications Session Border Controller and the client has been lost.

internal—Shows the same statistics as the command presents without arguments, but limits the output to statistics related to the Oracle Communications Session Border Controller's perspective. Information displayed includes:

- SIP UDP Send Msg Sent—UDP Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
- SIP UDP Recv Msg Sent—UDP Message received sent by the Oracle Communications Session Border Controller to SIP client or the Oracle Communications Session Border Controller to the SIP server
- SIP TCP Send Msg Sent—TCP Message sent from SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
- SIP TCP Recv Msg Sent—TCP Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server
- SIP SCTP Send Msg Sent—SCTP Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
- SIP SCTP Recv Msg Sent—SCTP Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server
- ENUM Sent Msg Sent—ENUM Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
- ENUM Recv Msg Sent—ENUM Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server

stats—Shows the same statistics as entering the command without an argument.

Example

```
ORACLE# show comm-monitor by-client 123.1.11.5
```

Thread Level Load Monitoring and Alarms

The Oracle Communications Session Border Controller provides a thread-level monitoring for CPU usage, specifically including three critical traffic processes: SIP, ATCP and MBCD.

Several mechanisms are available for monitoring CPU usage on a per-thread basis: ACLI commands, alarms, HDR, traps and MIBs. The thread usage table MIB object is found in **ap-usbcsys.mib**. It supports the output of process and thread utilization information. HDR information is produced as a comma separated value file whose data can be displayed in a formatted fashion via command line. The system sends SNMP traps when any of the SIP, ATCP worker threads or MBCD tasks exceed configured thresholds. Users can construct a Threshold Crossing Alarm (TCA) which issues minor, major and critical system alarms when the thread usage level exceeds pre-configured values. These Thread Overload Alarms follow the example in the *Configurable Alarm Thresholds and Traps* section.

ACLI

The following commands display thread-level load statistics:

- **show processes**: add sipd, atpcd and overload arguments
- **show queues atcpd**
- **show queues sipd**

Alarms

The user-configurable alarm may be created to notify the user of any problematic usage of CPU resources by specific processes at a thread-level basis.

To create alarms, the user sets the **alarm-threshold** > **type** with the following values to create the corresponding threshold crossing alarm.

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

When a thread alarm is active due to crossing a pre-configured threshold, the system sends the **apUsbcSysThreadUsageExceededTrap** trap.

When the thread's load falls below the threshold that triggered the alarm, the system sends the **apUsbcSysThreadUsageClearTrap** trap.

The user can get this information using the **display-alarms** command.

Historic Data Recording (HDR)

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

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

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

SNMP MIBs and Traps

Thread Level Load Monitoring information can be retrieved via SNMP by from MIB objects in the `ap-usbcsys.mib`. In addition, traps are available to send off-system notifications.

There are two types of traps that provide process-level thread threshold indicators.

- Traps managed by the process-level thread alarm configurations, which use the alarm configuration as triggers. These traps include:
  - **apUsbcSysThreadUsageExceededTrap**
  - **apUsbcSysThreadUsageClearTrap**
- Traps managed by Symmetric Multi-processing (SMP)-aware task load limiting function's configurations, which use the use the SMP Transport, SIP and Media limiting configurations as triggers. These traps include:
  - **apUsbcSysThreadUsageOverloadEnableTrap**
  - **apUsbcSysThreadUsageOverloadDisableTrap**

Information in overload enable/disable traps include the threshold type, the overload alarm exceeded or cleared as well as the overload method activated or de-activated.

The system follows the SMP-Aware Task Load Limiting rules described in the *Oracle® Communications Session Border Controller Troubleshooting and Maintenance Guide* to determine the action(s) it takes when crossing these thresholds.

The system manages these traps by applying a function similar to CPU overloading limit to smooth the output and avoid issuing too many traps. Each trap contains the thread name. The usage exceeded trap also contains current thread usage.

For SIP, ACTP and MBCD, traps display the threshold type, the overload alarm exceeded or cleared, or the overload method activated or de-activated.

MIB Support for Process-Specific CPU Thread Monitoring

Detail on applicable MIB objects is provided below. The *Oracle® Communications Session Border Controller Configuration Guide* fully documents SNMP community and trap configuration.

Applicable MIB Objects

The Oracle Communications Session Border Controller includes the set of MIB objects shown below within ap-usbcsys.mib that parse usable information for process level CPU thread monitoring.

Table 1: MIB Objects for Process-specific CPU Thread Monitoring

MIB Object	Object ID 1.3.6.1.4.1.9148.3.17.1.2	Description
apUsbcSysThreadObjects		A collection of objects providing the USBC thread level statistics.
apUsbcThreadUsageTableObject	.1	An identifier provided for each object in the thread usage table.
apUsbcThreadUsageTable	.1.1	A table to hold the thread usage information, on a Session Border Controller.
apThreadUsageEntry	.1.1.1	A table entry designed to hold the thread usage information, on a Session Border Controller.
apThreadId	.1.1.1.1	The instance index of the thread.
apThreadName	.1.1.1.2	The name of the thread.
apThreadCurrentUsage	.1.1.1.3	The current cpu usage of the thread. Multiply by 100 from % value.
apThreadOverloaded	.1.1.1.4	Indicator if thread is in overload control.
apUsbcThreadEventTableObject	.2	An object within the table holding thread event information.
apUsbcThreadEventTable	.2.1	A table to hold the thread event information, on a Session Border Controller. These are all read only.
apThreadEventEntry	.2.1.1	A table entry designed to hold the thread event information, on a Session Border Controller.
apThreadEventPendingCurrent	.2.1.1.1	The event pending Active counter.
apThreadEventPendingCurhigh	.2.1.1.2	The event pending High counter.
apThreadEventPendingWindow	.2.1.1.3	The event pending window.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.17.1.2	Description
apThreadEventPendingTotal	.2.1.1.4	The event pending Total counter.
apThreadEventPendingMaximum	.2.1.1.5	The event pending PerMax counter.
apThreadEventPendingHigh	.2.1.1.6	The event pending High counter.
apThreadEventDroppedCurrent	.2.1.1.7	The event dropped Active counter.
apThreadEventDroppedCurhigh	.2.1.1.8	The event dropped High counter.
apThreadEventDroppedWindow	.2.1.1.9	The event dropped window.
apThreadEventDroppedTotal	.2.1.1.10	The event dropped Total counter.
apThreadEventDroppedMaximum	.2.1.1.11	The event dropped PerMax counter.
apThreadEventDroppedHigh	.2.1.1.12	The event dropped High counter.
apThreadLatencyPendingAverage	.2.1.1.13	The thread average latency.
apThreadLatencyPendingMax	.2.1.1.14	The thread max latency.
apThreadLatencyProcessingAverage	.2.1.1.15	The thread average latency.
apThreadLatencyProcessingMax	.2.1.1.16	The thread max latency.
apUsbcSipObjects	.3	An object grouping SIPD-related per-thread CPU utilization information.
apSipNumberOfThreads	.3.1	Number of SIP threads.
apSipAverageCpuUtil	.3.2	Average CPU utilization.
apSipPendingAverageLatency	.3.3	The average latency of SIP Pending events.
apSipPendingMaxLatency	.3.4	The max latency of SIP Pending events.
apSipProcessingAverageLatency	.3.5	The average latency of SIP Processing events.
apSipProcessingMaxLatency	.3.6	The max latency of SIP Processing events.
apUsbcAtcpObjects	.4	An object grouping ATCP-related per-thread CPU utilization information.
apAtcpNumberOfThreads	.4.1	Number of ATCP threads.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.17.1.2	Description
apAtcpAverageCpuUtil	.4.2	Average CPU utilization.
apAtcpPendingAverageLatency	.4.3	The average latency of ATCP Pending events.
apAtcpPendingMaxLatency	.4.4	The max latency of ATCP Pending events.
apAtcpProcessingAverageLatency	.4.5	The average latency of ATCP Processing events.
apAtcpProcessingMaxLatency	.4.6	The max latency of ATCP Processing events.
apUsbcMbcdObjects	.5	An object grouping MBCD-related per-thread CPU utilization information.
apMbcdNumberOfThreads	.5.1	Number of MBCD threads.
apMbcdAverageCpuUtil	.5.2	Average CPU utilization.

apUSBC Traps (ap-usbcsys.mib)

The following traps are found in `ap-usbcsys.mib`.

Trap Name	Description
apUsbcSysThreadUsageExceededTrap 1.3.6.1.4.1.9148.3.17.2.2.1.1	The trap is generated when a thread is exceeding pre-defined usage.
apUsbcSysThreadUsageClearTrap 1.3.6.1.4.1.9148.3.17.2.2.1.2	The trap is generated when a thread is dropping back under pre-defined usage.
apUsbcSysThreadUsageOverloadEnableTrap 1.3.6.1.4.1.9148.3.17.2.2.1.3	The trap is generated when a thread cpu overload is activated.
apUsbcSysThreadUsageOverloadDisableTrap 1.3.6.1.4.1.9148.3.17.2.2.1.4	The trap is generated when a thread cpu overload is de-activated.

ACLI Commands

show processes

Syntax

```
show processes <process>
```

The show processes command, executed without arguments, displays statistics for all active processes. The following task information is displayed: names of tasks, entries, task identification codes, task priorities, status, program counter, error numbers, and protector domain (PD) identification.

Arguments

<process> The following is a list of each process argument:

- sysmand—Display sysmand process statistics related to the system’s startup tasks
- acliSSH0— Show acliSSH0 process statistics
- acliSSH1—Show acliSSH1 process statistics
- acliSSH2—Show acliSSH2 process statistics
- acliSSH3— Show acliSSH3 process statistics
- acliSSH4— Show acliSSH4 process statistics
- acliTelnet0— Show acliTelnet0 process statistics
- acliTelnet1— Show acliTelnet1 process statistics
- acliTelnet2— Show acliTelnet2 process statistics
- acliTelnet3— Show acliTelnet3 process statistics
- acliTelnet4— Show acliTelnet4 process statistics
- ebmd— Show embd process statistics
- h323d— Show h323d process statistics
- lid— Show lid process statistics
- pusher— Show pusher process statistics
- snmpd— Show snmpd process statistics
- cliworker— Show CliWorker process statistics
- berpd—Display statistics for the border element redundancy protocol tasks; only accessible if your system is operating in an HA node
- lemd—Display lemd process statistics
- brokerd—Display brokerd process statistics
- mbcd—Display mbcd process statistics related to the middlebox control daemon
- radd—Display radd process statistics related to RADIUS; only accessible if your Oracle Communications Session Border Controller is using RADIUS
- algd—Display algd process statistics
- sipd—Display sipd process statistics
- atcpd—Display atcpd processes
- acliConsole—Display acliConsole process statistics

current—Show the date and time that the current monitoring period began and statistics for the current application process events. The following fields explain the output of the show processes current command:

- Svcs—Number of times the process performs actions for different services (e.g., sockets, timeout queues, etc.)
- TOQ—Number of active timers (in the Timed Objects) placed in the timeout queue
- Ops—Number of times the process was prompted (or polled) to perform an action
- Rcvd—Number of messages received by the process
- Sent—Number of messages sent by the process
- Events—Number of times a TOQ entry timed out
- Alrm—Number of alarms the process sent
- Slog—Number of times the process wrote to the system log
- Plog—Number of times the process wrote to the process log
- CPU—Average CPU usage over the last minute
- Now—CPU usage for the last second

total —Display the total statistics for all of the application processes applicable to your Oracle Communications Session Border Controller. The following fields explain the output of the show processes total command:

- Svcs—Number of times the process performed actions for different services (e.g., sockets, timeout queues, etc.)
- Rcvd—Number of messages received by the process
- Sent—Number of messages sent by the process
- Events—Number of times a TOQ entry timed out
- Alarm—Number of alarms the process sent
- Slog—Number of times the process wrote to the system log
- Plog—Number of times the process wrote to the process log
- CPU—Average CPU usage since last reboot
- Max—Maximum percentage of CPU usage in a 60 second period

collect—Show collector process statistics

CPU —Display information about the CPU usage for your Oracle Communications Session Border Controller, categorized on a per task/process basis. The following fields explain the output of the show processes cpu command:

- Task Name—Name of the Oracle Communications Session Border Controller task or process
- Task Id—Identification number for the task or process
- Pri—Priority for the CPU usage
- Status—Status of the CPU usage
- Total CPU—Total CPU usage since last reboot in hours, minutes, and seconds
- Avg—Displays percentage of CPU usage since the Oracle Communications Session Border Controller was last rebooted
- Now—CPU usage in the last second

all — concatenate the show process command for all running prcoesses

memory—Show memory process statistics

top—The show processes top command displays realtime updates of per-process CPU utilization.

overload— show overload status for all supported processes (sipd, atcpd and mbcd).

Example

```
ORACLE# show processes sysmand
```

show queues atcpd

Syntax

The **show queues atcpd** command displays thread-level CPU usage information for the atcpd protocol threads.

```
ORACLE# show queues atcpd
atcpd01 (Active) -- Period -- -------- Lifetime --------
Active High Total Total PerMax High
Event Pending 0 2 37 37 37 2
Event Dropped 0 0 0 0 0 0

---- Latency ----
Events Average Maximum
Pending 37 0.001 0.045
Processing 37 0.023 0.867

CPU Usage = 0.0%
CPU Overloaded = No

atcpd02 (Active) -- Period -- -------- Lifetime --------
Active High Total Total PerMax High
```

```
Event Pending 0 2 37 37 37 2
Event Dropped 0 0 0 0 0 0

---- Latency ----
Events Average Maximum
Pending 37 0.000 0.032
Processing 37 0.012 0.465

CPU Usage = 0.0%
CPU Overloaded = No

atcpd03 (Active) -- Period -- -------- Lifetime --------
Active High Total Total PerMax High
Event Pending 0 2 28 28 28 2
Event Dropped 0 0 0 0 0 0

---- Latency ----
Events Average Maximum
Pending 28 0.000 0.017
Processing 28 0.001 0.048

CPU Usage = 0.0%
CPU Overloaded = No
```

show queues sipd

Syntax

The **show queues sipd** command displays thread level cpu usage information for the SIP protocol threads.

```
ORACLE# show queues sipd
sipd01 (Active) -- Period -- -------- Lifetime --------
Active High Total Total PerMax High
Event Pending 0 2 37 37 37 2
Event Dropped 0 0 0 0 0 0

---- Latency ----
Events Average Maximum
Pending 37 0.001 0.045
Processing 37 0.023 0.867

CPU Usage = 0.0%
CPU Overloaded = No

sipd02 (Active) -- Period -- -------- Lifetime --------
Active High Total Total PerMax High
Event Pending 0 2 37 37 37 2
Event Dropped 0 0 0 0 0 0

---- Latency ----
Events Average Maximum
Pending 37 0.000 0.032
Processing 37 0.012 0.465

CPU Usage = 0.0%
CPU Overloaded = No

sipd03 (Active) -- Period -- -------- Lifetime --------
Active High Total Total PerMax High
Event Pending 0 2 28 28 28 2
Event Dropped 0 0 0 0 0 0

---- Latency ----
Events Average Maximum
```

```
Pending 28 0.000 0.017
Processing 28 0.001 0.048

CPU Usage = 0.0%
CPU Overloaded = No
```

HDR Groups

thread-event

Reports pending and dropped events per protocol as well as calculates latency.

Position	Statistic	Type	Timer Value	Range	Description
1	TimeStamp				Time Stamp
2	Thread Name	string	N/A	alphanumeric	Protocol (sipd, atcpd or mbcd) and optional numeric
3	Event Pending Current	counter	N/A	32767	Pending Event: Current count; number of occurrences in the current window
4	Event Pending CurHigh	counter	N/A	32767	Pending Event: Highest count between position 3 and the previous high
5	Event Pending Window	counter	N/A	32767	Pending Event: Total count in the current window plus the previous window
6	Event Pending Total	counter	N/A	32767	Pending Event: Total count after reset
7	Event Pending Maximum	counter	N/A	32767	Pending Event: Maximum count in the current window
8	Event Pending High	counter	N/A	32767	Pending Event: Highest count in a window after reset
9	Event Dropped Current	counter	N/A	32767	Dropped Event: Current count; number of occurrences in the current window
10	Event Dropped CurHigh	counter	N/A	32767	Dropped Event: Highest count between position 9 and the previous high
11	Event Dropped Window	counter	N/A	32767	Dropped Event: Total count in the current window plus the previous window
12	Event Dropped Total	counter	N/A	32767	Dropped Event: Total count after reset
13	Event Dropped Maximum	counter	N/A	32767	Dropped Event: Maximum count in the current window
14	Event Dropped High	counter	N/A	32767	Dropped Event: Highest count in a window after reset
15	Latency Pending Average	integer	millsecond	32767	Average pending latency in a window

Position	Statistic	Type	Timer Value	Range	Description
16	Latency Pending Max	integer	millsecond	32767	Maximum pending latency in a window
17	Latency Processing Average	integer	millisecond	32767	Average pending latency in a window; PegStat
18	Latency Processing Max	integer	millisecond	32767	Maximum pending latency in a window; PegStat

thread-usage

Reports CPU thread usage per protocol and an overload condition.

Position	Statistic	Type	Timer Value	Range	Description
1	TimeStamp				Time Stamp
2	Thread Name	string		alphanumeric	Protocol (sipd, atcpd or mbcd) and optional numeric
3	Current Usage	gauge		0-100	Percentage usage of CPU thread
4	Overloaded	integer		1; 2; 3	1 Not applicable; 2 True; 3 False

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.

Media guard timer parameters configured within a realm use the same syntax and define the same windows as the global timers. They differ in that they affect flows that traverse the realm only. Applicable timers include:

- **`flow-time-limit`**
- **`initial-guard-timer`**
- **`subsq-guard-timer`**
- **`tcp-flow-time-limit`**
- **`tcp-initial-guard-timer`**
- **`tcp-subsq-guard-timer`**

Per-realm media guard timer settings differ slightly from the global timers:

- The default value of -1 disables the realm setting, allowing the system to fall back to the global timer settings.
- A value of 0 disables the use of that type of timer for all flows traversing that realm, regardless of whether there are enabled ingress, egress or global settings.
- Timer ranges differ, as documented in the command reference.

Important operational considerations include:

- The system refers to both ingress and egress realm settings to time each flow, using the lower settings to resolve setting conflicts.

- Upon the expiry of the flow timer sequence, the Oracle Communications Session Border Controller sends a BYE that includes reason header indicating that the system has cleared the session due to media flow guard timer expiry.
- This feature interacts with guard-notify-gap in the media manager. When a flow guard timer expiry is received by MBCD, and if the required 'gap' since the last notification has not elapsed, the system queues the new notification to be sent when the required notify gap time has elapsed.

Note: Media guard timers in static flow configurations are not impacted by per-realm (or global) media timers. Per-realm and global timers are for dynamic flows.

realm-config - Media Guard Timers

This realm-config includes the following flow timers, with settings that take precedence over the global flow timers, configured in the media manager.

Parameters

flow-time-limit Enter the total time limit in seconds for the flow. The Oracle Communications Session Border Controller notifies the signaling application when this time limit is exceeded. This field is only applicable to dynamic flows. A value of 0 seconds disables this function and allows the flow to continue indefinitely.

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

initial-guard-timer Enter the time in seconds allowed to elapse before first packet of a flow arrives. If first packet does not arrive within this time limit, Oracle Communications Session Border Controller notifies the signaling application. This field is only applicable to dynamic flows. A value of 0 seconds indicates that no flow guard processing is required for the flow and disables this function.

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

subsq-guard-timer Enter the maximum time in seconds allowed to elapse between packets in a flow. The Oracle Communications Session Border Controller notifies the signaling application if this timer is exceeded. This field is only applicable to dynamic flows. A field value of zero seconds means that no flow guard processing is required for the flow and disables this function.

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

tcp-flow-time-limit Enter the maximum time in seconds that a media-over-TCP flow can last

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

tcp-initial-guard-timer Enter the maximum time in seconds allowed to elapse between the initial SYN packet and the next packet in a media-over-TCP flow

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

tcp-subsq-guard-timer Enter the maximum time in seconds allowed to elapse between all subsequent sequential media-over-TCP packets

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

Path

Path: **realm-config** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal** > **media-manager** > **realm-config**.

Release

First appearance: S-CZ7.3.0

RTC Status

flow-time-limit, initial-guard-timer, and subsq-guard-timer are supported. The remaining parameters are not supported.

DNS Entry Maximum TTL

DNS maximum time to live (TTL) is user-configurable and complies with RFCs 1035 and 2181.

One can set the DNS maximum TTL on the Oracle Communications Session Border Controller permitting the DNS entry information to be held until that time is exceeded. One can specifiy the **dns-max-ttl** parameter per network interface and/or to support the DNS ALG feature. The default value is 86400 seconds (24 hours). When the Oracle Communications Session Border Controller configured maximum value has been exceeded, the DNS TTL value is set to the configured maximum and a log entry is written. Otherwise the Oracle Communications Session Border Controller honors the lower value in the DNS response. The Oracle Communications Session Border Controller restricts all DNS entries minimum TTL value of 30 seconds, which the system's implementation of SIP requires.

DNS Entry Max TTL Configuration per Network Interface

Set parameter for DNS entry maximum time to live (TTL) value per network interface.

1. Access the **network-interface** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# network-interface
ORACLE(network-interface)
```

2. Select the **network-interface** object to edit.

```
ORACLE(network-interface)# select
<name>:<sub-port-id>:


ORACLE(network-interface)#
```

3. **dns-max-ttl—** set to the maximum time for a DNS record to remain in cache.
   - **Minimum: 30—** The lowest value to which the **dns-max-ttl** parameter can be set (in seconds)
   - **Maximum: 2073600—** The maximum value (in seconds) for which the **dns-max-ttl** parameter can be set.
   - **Default: 86400—** The value in seconds which the system uses by default.
4. Type **done** to save your configuration.

DNS Entry Maximum TTL Configuration for DNS ALG

Set parameter for DNS entry maximum time to live (TTL) value in **dns-config** for the DNS ALG feature.

dns-config

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

```
ORACLE# configure terminal
ORACLE(configure)# media-manager
ORACLE(media-manager)# dns-config
ORACLE(dns-config)# select
```

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

   ```
   ORACLE(dns-config)# select
   client-realm:

   ORACLE(dns-config)#
   ```

3. **dns-max-ttl—** set to the maximum time for a DNS record to remain in cache.

   - **Minimum: 30—** The lowest value to which the **dns-max-ttl** parameter can be set (in seconds)
   - **Maximum: 2073600—** The maximum value (in seconds) for which the **dns-max-ttl** parameter can be set.
   - **Default: 86400—** The value in seconds which the system uses by default.

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

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.

DNS queries start on UDP ports with the limit of 512 bytes. Longer responses require that the result not be cached and that the truncated (TC) header bit is set. After receiving a DNS response with the TC header set, the Oracle Communications Session Border Controller will initiate a re-query to the DNS server over TCP. The option **dns-tcp-for-truncated-response** in **realm-config** can be set to **no** to disable this behavior.

DNS Re-query over TCP Config

Enable feature to support setting the truncated header bit and initiating a DNS re-query over TCP.

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

   ```
   ORACLE# configure terminal
   ORACLE(configure)# media-manager
   ORACLE(media-manager)# realm-config
   ORACLE(realm-config)#
   ```

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

   ```
   ORACLE(realm-config)# select
   identifier:
   1: realm01 left-left:0 0.0.0.0

   selection: 1
   ORACLE(realm-config)#
   ```

3. **dns-tcp-for-truncated-response—** Set the options parameter by typing **options**, a Space, a plus sign (+), the option name, and queal sign (=) and then **yes** or **no** and then press Enter. The default behavior is to set the truncated header bit and initiate a DNS re-query over TCP.

   ```
   ORACLE(realm-config)# option +dns-tcp-for-truncated-response=no
   ```

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

DNS Queries on the Command Line

Users can perform Domain Name Services (DNS) queries from the command line. Positive results are added to the DNS cache.

Currently the SIP proxy agent issues DNS queries to find the Serving Call Session Control Function (S-CSCF) from a SIP invite or a SIP registration event. A user can perform these same DNS queries from the command line, both with and without the use of the local DNS cache.

The command to first query the local DNS cache and then perform an external DNS query (if needed) is **show dns lookup** with the following parameters: <realm> <type> <name>.

Arguments	Value
realm	Realm name to use for DNS cache lookup key
type	Type of DNS query • A for IPv4 lookup • AAAA for IPv6 lookup • SRV for service recod • NAPTR for naming authority pointers
name	FQDN of DNS name to lookup

To perform a manual external DNS query with no cache lookup, issue the **show dns query** command with the following parameters: <realm> <type> <name>.

Arguments	Value
realm	Realm name to use to find the network interface
type	Type of DNS query • A for IPv4 lookup • AAAA for IPv6 lookup • SRV for service recod • NAPTR for naming authority pointers
name	FQDN of DNS name to lookup

show dns lookup

Perform a domain name services (DNS) query, first by an internal DNS cache lookup and then, if no results are found, perform an external DNS query from the command line.

Syntax

show dns lookup <arguments>

Arguments <arguments> Available **show dns lookup** arguments:

- realm— Realm name to use for DNS cache lookup key
- type— Type of DNS query:
  - A for IPv4 lookup
  - AAAA for IPv6 lookup
  - SRV for service records, e.g. SRV_sip_tcp.abc.com
  - NAPTRY for naming authority pointers, e.g. NAPTR.abc.com
- name— Fully qualified domain name (FQDN) of DNS name to lookup

Release

Initial release: S-CZ7.3.0M1

show dns query

Perform a manual external Domain Name Services (DNS) query from the command line.

Syntax

show dns query <arguments>

Arguments <argments> Available **show dns query** arguments:

- realm— Realm name to use to find network interface
- type— Type of DNS query:
  - A for IPv4 lookup
  - AAAA for IPv6 lookup
  - SRV for service records, e.g. SRV_sip_tcp.abc.com
  - NAPTRY for naming authority pointers, e.g. NAPTR.abc.com
- name— Fully qualified domain name (FQDN) of DNS name to lookup

Release

Initial release: S-CZ7.3.0M1

Set Acct-session-time attribute to milliseconds

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

The RADIUS attribute **acct-session-time** uses seconds as its default. You can set this to a millisecond granularity in the **account-config** configuration element using the option **millisecond-duration**. This option setting is required for the RADIUS CDR display, Diameter RF accounting and locally-generated CDR comma separated value (CSV) files behaviors.

Note: Changing to millisecond granularity violates RFC 2866.

Configure acct-session-time for millisecond granularity

Set the option for millsecond granularity for the **acct-session-time** attribute.

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

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

2. Type **select** to begin configuring this object.
3. **options**—Set the **options** parameter by typing **+options**, a Space, the option name **millsecond-duration** and then press Enter.
4. Type **done** to save your configuration.

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.

To change inbound behavior from an outbound one, customers can configure several Session Agents (SAs) with the same IP address to different hostnames. By default, the system uses alphanumeric order to determine sorting. The attribute **precedence** provides a user-controlled mechanism to determine order for Session Agents. The rules of **precedence** are as follows:

- The default value is zero. This does not activate **precedence**.
- It is configurable with integer value from 1 to 4,294967,295
- The lowest value is considered first, followed by Session Agents with the same IP of increasing values
- After SAs with **precedence** set to a value higher than one are assigned, those with the default of zero are considered (e.g. alphanumeric order sorting is followed)
- Should two Session Agents have the same value of **precedence**, alphanumeric sorting rules apply

This attribute in the Session Agent configuration does not interact with the Session Agent Group construct as the latter is used for egress routing. For this same reason, **precedence** does not apply to surrogate registration, nor registration refresh.

For example, these settings cause the hosts abb123 and aaa456 to be preferred first and aaa123 last:

```
SA1: IP=192.168.139.5, hostname-aaa456, precedence=1
SA1: IP=192.168.139.5, hostname-abb123, precedence=1
SA1: IP=192.168.139.5, hostname-abc123, precedence=33
SA1: IP=192.168.139.5, hostname-aaa123, precedence=44
```

Override Alphanumeric Ordering of Session Agents with Same IP Configuration

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 just the alphanumeric ordering of hostname. Setting **precedence** to zero retains alphanumeric sorting

Enter the prerequisites here (optional).

Enter the context of your task here (optional).

1. Access the **session-agent** configuration element.

   ```
   ORACLE# configure terminal
   ORACLE(configure)# session-router
   ORACLE(session-router)# session-agent
   ORACLE(session-agent)
   ```

2. Select the **session-agent** object to edit.

   ```
   ORACLE(session-agent)# select
   <hostname>:
   1: 192.168.100.101:1813

   selection: 1
   ORACLE(session-agent)#
   ```

3. **precedence**—Set the importance level of this IP/hostname combination for Session Agents. To be considered for **precedence**, a value of 1 or more is required.

   - **Minimum: 0**
   - **Maximum: 4,294,967,295**
   - **Default: 0**

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

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.

Sometimes there are failures in the transmission of CDR files due to underlying network or infrastructure issues. Customers can identify missing files through the combination of a timestamp (YYYYMMDDMM) and 9-digit unique sequence numbers (SNs) appended to the file. This behavior is enabled through the

file-seq-number attribute. The SN will start from one at boot time. This attribute replaces the use of alpha characters (a-z) appended to the CDR file name when more than one file is created in the same minute.

Separately, one can set the **temp-remote-file** attribute so the characters "tmp-" are prepended to the CDR file during transfer. Once delivered, the file will be renamed on the remote host to remove "tmp-".

For example, with both attributes enabled, a file named **`tmp-cdr<timestamp>-<9-digit-sequence-number>`** would be created and upon complete transfer to the destination renamed **`cdr<timestamp>-<9-digit-sequence-number>`**.

CDR Sequence Number in Filename Configuration

To assist in the identification of lost Call Detail Record (CDR) files, the customer can enable the **file-seq-number** attribute to allow a sequence number to append to the file.

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

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

2. Type **select** to begin configuring this object.
3. **file-seq-number**—set this to enabled for the system to assign a 9 digit file sequence number to append to a CDR file. The default is disabled.
   - **enabled | disabled**
4. Type **done** to save your configuration.

Temp-remote-file creation for CDR files during transfer Configuration

The configuration element **temp-remote-file** allows for the prepending of the characters "tmp-" to Call Detail Record (CDR) files during transfer. When the transfer ends successfully, the system removes the characters "tmp-".

1. Access the **push-receiver** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# account-config
ORACLE(account-config)# push-receiver
ORACLE(push-receiver)#
```

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

```
ORACLE(push-receiver)# select
server:
1: server = 192.168.100.101, port = 21

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

3. **temp-remote-file**—set the state of this element to enabled for the system to prepend the characters "tmp-" to a CDR file during transfer. The default is disabled
   - **enabled | disabled**
4. Type **done** to save your configuration.

TSM Security Traversing Gateway Mode

Oracle Communications Tunneled Session Controller Function (OCTSCF) is a feature on the Oracle Communications Session Border Controller (OCSBC). The TSCF dramatically improves firewall traversal for real-time communications and Over-the-Top (OTT) VoIP applications and reduces the dependency on SIP/TLS and SRTP by encrypting access-side VoIP within standardized tunnels. As calls or sessions traverse a Tunnel Session Management (TSM) tunnel, the SBC will route all SIP and RTP traffic from within the TSM tunnel to the network core (or appropriate destination).

As implemented by Oracle Communications, TSM/TSCF terminology includes:

- TSC client—Sometimes referred to as a Tunneled Service Element (TSE). It facilitates TSCF tunnel creation and management within client applications residing on network elements.
- TSC server—The SBC that is used to terminate TSC tunnels.
- Tunnel Session Management (TSM)—The overall solution that covers both the TSC Server and TSC Client.
- TSCF (Tunneled Services Control Function)—The actual function that runs on the SBC. TSCF is often used in the naming of the ACLI configuration and management objects.

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.

To deploy TSC clients (such as softphones, SIP-enabled iOS/Android applications or contact center agent applications), customers and 3rd party ISVs need to incorporate the TSM's open source software libraries (TSC or STG clients) into their applications which will establish SSL connections (TLS or DTLS) to the TSC server. If the STG is to be implemented, you must use the Oracle Software Developer Kit (SDK), release 1.4 or above.

TSC client sends encapsulation data to the STG through the tunnel, and the STG decrypts data and forwards to the SBC, then SBC will do IMS business data handling. When CM-IMS core network tries to send data to the client using security tunnel mode, the SBC will send data to STG, which will do data encapsulation and forward to client via security tunnels.

Note: The STG feature is not intended for all customer use. Consult your Oracle representative to understand the circumstances indicating the use of this feature.

STG Supported Platforms

These are the platforms supported for the initial release of the Security Traversing Gateway (STG):

- Acme Packet 4600
- Acme Packet 6100
- Acme Packet 6300

STG Prerequisites

In order to activate STG Mode, you must first fulfill the following prerequisites:

- Configure at least one TSE built with SDK version 1.4 and above
- Provision a TSCF Interface

Note: Refer to "TSCF Interface Configuration" for details.

The default TSM parameters are the same as the default parameters of a TSE configured with SDK version 1.4.

STG Configuration

From superuser mode, use the following command path to access assigned-services configuration mode.

```
ORACLE# configure terminal
ORACLE(configure)# security
ORACLE(security)# tscf
ORACLE(security)# tscf-interface
ORACLE (tscf-interface)# select
```

```
<RealmID>:
1: access 172.168.31.99:7000
selection:  1
ACMEPACKET (tscf-interface)# assigned-services STG
```

Note: There are other assigned services that may be listed in addition to STG. These include SIP, redundancy, and DDT. The list must be comma delimited. Example: SIP, STG

STG Keep-Alive Mechanism

Keep Alive Request Command Messages (CMs) are sent periodically at 66% of the keep alive interval negotiated through **Configuration Request** and **Configuration Response** CMs. **Configuration Request** CMs are sent by either the TSE or TSM and **Configuration Response** CMs are sent by the either the TSE or TSM. If **Keep Alive Request** CMs are not received within the configured keep alive interval, the tunnel transport is terminated and tunnel renegotiation is started. If the keep alive interval is not negotiated correctly because the **Configuration Response** CM doesn't include it, a default value is used. The **Keep Alive Request** CMs are transmitted by both of the ends of the tunnel once, so if the tunnel transport packet loss is present, premature tunnel termination is possible.

STG Configuration Resume

If contact is lost between the TSM and the TSE during configuration, the tunnel goes into TSM persistence. The TSE transmits a **Configuration Resume** CM with the tunnel ID (TID), to which the TSE responds with a Configuration Resume Response, also with the TID. This mechanism is used instead of a **Tunnel Resume** mechanism.

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.

In a call forwarding scenario where a media server (MS) behind Network Address Translation (NAT) is between two SBCs, both SBCs will detect NAT, so both will wait to receive RTP packets before latching to the RTP source address. This feature prevents this by adding the new value **pre-emptive** to the configuration option parameter **symmetric-latching** in the configuration element **realm-config**. When the value is set to **pre-emptive**, the SBC sends the RTP packets to the received SDP connection address without waiting on the latch. Once the RTP packets are received from the peer endpoint, the SBC detects the NAT address mapping; if there is a change in the RTP source address, the SBC re-latches to the new RTP source address. Subsequent RTP packets are then sent to the peer RTP source address. This is also the behavior when there is an UPDATE or reINVITE with the SDP message.

Pre-emptive Symmetric Media Latching Configuration

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

```
ORACLE# configure terminal
ORACLE(configure)# media-manager
ORACLE(media-manager)# realm-config
ORACLE(realm-config)#
```

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

```
ORACLE(realm-config)# select
identifier:
1: realm01 left-left:0 0.0.0.0
```

```
selection: 1
ORACLE(realm-config)#
```

3. **symmetric-latching** — identifies whether and how to enable symmetric latching in the realm. The default value is **disabled**.
    - **disabled**
    - **enabled**
    - **pre-emptive** — symmetric latching is enabled but the SBC sends RTP packets to the received SDP connection address without waiting on the latch
4. Type **done** to save your configuration.

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.

One of the fundamental behaviors in the Oracle Communications Session Border Controller's Diameter model relies on the external policy server making an authorization decision which is then communicated to the SBC. Part of the call authorization sequence of events involves the SBC waiting for an external policy server's response before the SBC can completely set up, modify, or update the call. The long pause that the endpoints experience, while the SBC holds up SIP flows waiting for the external policy server's response, can lead to unnecessary call failure situations.

In some Diameter-based external policy server deployments, the media traverses a Cable Modem Termination System (CMTS) at the edge of the network; the CMTS gates may be established by a Policy Server to dynamically enable QoS from a UE toward another UE. If no gate is established then the media traverses the CMTS and is admitted to the network with a "best-effort" network path.

As QoS sessions might not be the most important priority to a network, Oracle now allows network operators the ability to decouple the call set up (signaling) from the request for bandwidth. The SBC's default external policy server model is the synchronous model, in which the SBC sends a policy server request based on a SIP or SDP trigger point, and the SIP signaling is held until a response is returned from the Policy Sever. In the asynchronous model the request that the SBC sends to the Policy Server flows in an asynchronous state with respect to SIP messaging; that is, the SBC allows the SIP session to proceed naturally, and does not pause for outstanding Policy Server answers to be received. The establishment of a SIP session is not affected by Policy Server answers, or answer timeouts, related to the SIP session. To enable the asynchronous model, the new parameter **asynchronous-mode** has been added to the **ext-policy-server** configuration element, with a default of **disabled** so as not to affect current default behavior.

Note: Oracle Communications recommends that, for each SBC, the same model be used for all external policy server configuration instances. Failure to follow this guideline could result in complex interactions from a timing perspective which might lead to dropped or degraded calls.

Serialized Diameter Messaging

After the Oracle Communications Session Border Controller sends a Diameter request, it will not send another Diameter request, such as a Session Termination Request (STR), with the same Session-ID Attribute Value Pair (AVP) until the original request receives a response or times out.

Access networks with complex policy server structures can allow non-sequential delivery of Diameter requests into a Cable Modem Termination System (CMTS), even if Diameter message delivery was correctly ordered on the TCP connection between the SBC and a lower-tiered external policy server.

The SBC now prevents the external policy server from receiving out-of-order messages at the application layer by serializing them. The SBC serializes Diameter messages to ensure that a Diameter request for one session-ID is not sent until an answer is received from the previous request for the same session-ID. The SBC applies this constraint while waiting for a Diameter response or when considering a Diameter request timeout (15 seconds). Serialized Diameter messaging is always enforced for Diameter-based external policy server communication.

SIP-Diameter Communication Configuration

1. Access the **ext-policy-server** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# media-manager
ORACLE(media-manager)# ext-policy-server
ORACLE(ext-policy-server)#
```

2. Select the **ext-policy-server** object to edit.

```
ORACLE(ext-policy-server)# select
<name>:1:  name=extpol1

selection: 1
ORACLE(ext-policy-server)#
```

3. **asynchronous-mode —** identifies whether to use the asynchronous mode of signaling on the external policy server interface rather than the default synchronous mode. Allowable values are **enabled** and **disabled**. The default is **disabled.**
4. Type **done** to save your configuration.

Flow-Description AVP Change for Media Release

The current implementation of 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.

In the case where the media is released, only incomplete flow information may be provided to the Policy Server because not all IP addresses and port numbers are known from the SDP offer. Media release is enabled on a per realm basis with the following settings in the **`realm-config`** configuration element:

```
        mm-in-realm                     disabled
        mm-in-network                   disabled
        mm-in-system                    disabled
        mm-same-ip                      disabled
        msm-release                     enabled
```

When the realm is configured for external bandwidth management, the media layer checks if any of the configuration parameters for media release have been invoked. If none of the media release parameters are invoked (meaning that the SBC is managing the media), then the signaling application constructs the bandwidth request to the PS as it currently does. If the media layer detects that the realm is configured to possibly release media, then a few more operations are performed to correctly populate the bandwidth request to the PS. If the media has been released for the session, the signaling application inserts the IP port of the called endpoint into the bandwidth request instead of the IP port for the SBC. If the media has not yet been released, the media layer determines if the initial signal is an OFFER or an ANSWER. If it is an ANSWER the IP port in the bandwidth request will be that of the SBC because the SBC is managing the media for the session. If it is an OFFER, the signaling application inserts an empty IP port into the bandwidth request and sets a flag in the bandwidth request indicating unqualified flow information at this time. This occurs regardless of the value of the parameter **reserve-incomplete** in the **ext-policy-server** configuration element.

To enable this behavior on the Rx interface, the new parameter **media-release** has been added to the **ext-policy-server** configuration element.

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 causes the Oracle Communications Session Border Controller to instantiate NAT flows that are managed by dynamic, trusted ACLs for IMS-AKA traffic. The system installs/deletes flows and ACLs for traffic from the endpoint's secure client port to the system's secure server port for both TCP and UDP. Note that IMS-AKA allows the endpoints to switch between TCP and UDP. In addition, the system installs/deletes a flow and ACL from an endpoint's secured server port to the system's secure client port for when the endpoint registers over TCP. This flow supports new SIP requests toward the Oracle Communications Session Border Controller.

If an endpoint registers over UDP, the system does not install the additional flow and ACL for SIP requests.

After security parameter negotiation and the IMS-AKA registration are successful, encrypted signaling and data passes through these secure ports. The system uses applicable SIP signaling actions to trigger the addition and deletion of these flows and ACLs. The system also deletes flows when the associated contact expires.

If IMS-AKA initiates re-registration, the security association's parameters are renegotiated. On successful re-registration, ACLs corresponding to old security associations are dropped and new ones are installed.

The user enables this behavior using the option syntax shown below on the access sip-interface.

```
ACMEPACKET(sip-interface)# options +enhanced-acl-promote="tcp,udp"
```

In addition, the user must have configured the access realm for dynamic ACLs by setting the **`access-control-trust-level`** to anything other than "none".

The user can monitor statistics on applicable ACLs using the **`show acl`** command. The user can monitor statistics on applicable flows using the **`show nat`** and **`show mbcd`** commands.

Note: Development on this feature is reworked in version S-Cz7.4.0 of the SBC. This requires users upgrading deployments with this feature from S-Cz7.3.0M1 or later to S-Cz7.4.0 to perform a simultaneous reboot of the active and secondary HA nodes after the upgrade. This is not required when upgrading from versions earlier than S-Cz7.3.0M1.

2

SCZ730M2

This section provides descriptions, explanations, and configuration information for the contents of Maintenance Release SCZ7.3.0M2. Maintenance Release content supercedes that distributed with the point release.

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

Current patch baseline: SCZ7.3.0m1p9

Please refer to the *Oracle® Communications Session Border Controller & Session Router Release Notes*, Release S-CZ7.3.0 for changes to the Known Issues section based on the S-CZ7.3.0M2 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-CZ7.3.0M2:

- SCZ7.2.0m6p3

Content Map

The following table identifies the new content in this SCZ7.3.0 M2 Maintenance Release documentation.

Content Type	Description
Adaptation	Advanced Logging
Adaptation	Detailed statistics for Diameter interfaces (Rx and Rf)
Adaptation	Application and platform level debug tools on TCP connection leaks
Adaptation	Securing inter-client communication between TSCF clients
Adaptation	Enhancement to show platform CLI command
Capacity Increase	Increased TLS Certificate Storage Limits—Increases the public certificate limit to 50 and the private certificate limit to 20 on the Acme Packet 3820 with either an ETC1 or ETC2 NIU.

Advanced Logging

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

You can deploy advanced logging via configuration. Define sip-advanced-logging under session-router. This method reconfigures the system and the configuration persists after a system reboot.

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

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

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

- Received Session-Agent. By IP address or hostname
- Request Type. Such as INVITE vs. SUBSCRIBE
- Received Realm Name.
- Request URI. User and host. Limited to 2 condition entries, when using both types.

- To header. User and host. Limited to 2 condition entries, when using both types.
- From header. User and host. Limited to 2 condition entries, when using both types.
- Call-id. Matches the Call-id header.
- Rate Limiting. By specified number of matched requests over a specified period of time.
- Scope of Logging. Options include Request Only, Transaction, All Relating to Session, All Relating to Session and Media.

Configure Advanced Logging - Configure Mode

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

When configuring multiple `sip-advanced-logging` configurations, note the following:

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

1. From Configure Mode, go to `session-router > sip-advanced-logging` and configure the following.
   - Name. Name to display on the log message for this set of criteria.
   - Level. Type one: zero, none, emergency, critical, major, minor, warning, notice, info, trace, debug, or detail.
   - Scope. Type one: request-only, transaction, session, or session-and-media.
   - Matches-per-window. Type a number between 1 and 999999999 for how many matches to log per window of time.
   - Window-size. Type a number between 1 and 999999999 seconds for the length of time the logging window is open.
   - Type conditions.

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

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

sip-advanced-logging

The sip-advanced-logging configuration element allows you to configure advanced logging objects on the Oracle Communications Session Border Controller.

Parameters

name Name to display on the log message for this set of criteria.

level Log level for this advanced logging set of criteria. This corresponds to the system's available log levels.

- Default: DEBUG
- Values: ZERO | NONE | EMERGENCY | CRITICAL | MAJOR | MINOR | WARNING | NOTICE | INFO | TRACE | DEBUG | DETAIL

scope The range of SIP messages and, if configured, media for which this advanced logging criteria creates log messages.

- Default: session-and-media
- Values: request-only | transaction | session | session-and-media

matches-per-window The number of matches, within the window size, for which the system generates log messages.

- Default: 1
- Values: An integer between 1 and 999999999

window-size The amount of time, in seconds, to sample for matches within the traffic.

- Default: 1
- Values: An integer between 1 and 999999999

condition Type this parameter to enter the adv-logging-conditions subelement. Specify the match criteria for which the system creates log messages. Each logging criteria set supports multiple match conditions.

Path: **sip-advanced-logging** is an element of the session-router path. The full path from the topmost ACLI prompt is: configure terminal > session-router > sip-advanced-logging.

Release

First appearance: E-C7.1.0

RTC Status

Supported

Note: This is a multiple instance configuration element.

sip-advanced-logging > condition

The sip-advanced-logging's condition subelement allows you to configure multiple sets of matching criteria for the associated sip-advanced-logging element on the Oracle Communications Session Border Controller.

Parameters

match-type A string identifying the type of information within the SIP message on which the system attempts to find a matching value.

- Default: recv-agent
- Values: request-type | recv-agent | recv-realm | request-uri-user | request-uri-host | to-header-user | to-header-host | from-header-user | from-header-host

match-value A string the system uses as the matching string within the SIP message.

- If the match-type is "request-type", valid values include:
  - REGISTER | INVITE | ACK | BYE | CANCEL | PRACK | OPTION | INFO | SUBSCRIBE | NOTIFY | REFER | UPDATE | MESSAGE | PUBLISH
- For all other match-types, enter the string the system must find in the message.

Path: **adv-log-condition** is a subelement of the sip-advanced-logging element. The full path from the topmost ACLI prompt is: configure terminal > session-router > sip-advanced-logging > condition.

Release

First appearance: E-C7.1.0

RTC Status

Supported

Note: This is a multiple instance configuration subelement.

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.

Use the following commands to view RADIUS and Diameter statistics:

- **`show policy-server`**
- **`show accounting`**
- **`show radius accounting`**

Rx Interface Statistics

Only Diameter messages traverse the Rx interface. Use the **show policy-server** command to display statistics for the Rx interface.

show policy-server

The **show policy-server** command lets you view specific information about a supplied policy server object. The syntax is:

```
show policy-server [[standby | <Name> | <IP_Address:Port>] [<DiamMsg>]] |
[connections]
```

Following is an example of the **show policy-server <Name>** command:

```
ORACLE# show policy-server server1
name = server1
-----------------------------------------
    Server:port           Priority         State       TCP-Failures
Diameter-Failures
   192.168.42.13:1817         0             inactive
2261              0

-----------------------------------------
15:29:27-182


Local IPPort         Remote IPPort        Socket State
--------------------------------------------------------
10.196.143.9:41743   10.196.0.209:3870    CONNECTED



-----------------------------------------
10:53:02-197
Bandwidth Policy Server          --  Recent -- -------- Lifetime --------
                           Active    High   Total      Total  PerMax    High
Sockets                         1       1       0          2       1       1
Connections                     0       0       0          9       1       1
Client Transactions             0       0       0          9       1       1
  Reserve Requests Sent         -       -       0          0       0
  Update Requests Sent          -       -       0        241     211
  Remove Requests Sent          -       -       0        241     241
  Requests Re-Trans             -       -       0          0       0
  Install Resp Received         -       -       0        241     241
  Reject Resp Received          -       -       0          0       0
  Remove Resp Received          -       -       0        241     241
  Errors Received               -       -       0          0       0
  Transaction Timeouts          -       -       0          0       0
  Errors                        -       -       0          0       0
Server Transactions             0       0       0         30      30      29
  Requests Received             -       -       0          0       0
  Dup Req Received              -       -       0          0       0
  Success Resp Sent             -       -       0         30      30
  Error Resp Sent               -       -       0          0       0
  Requests Dropped              -       -       0          0       0
CER Sent                        -       -       0          0
0
CEA Success                     -       -       0          0       0
CEA Errors                      -       -       0          0       0
AAR Sent                        -       -       0          0
0
AAA Success                     -       -       0          0       0
AAA Errors                      -       -       0          0       0
STR Sent                        -       -       0          0       0
STA Success                     -       -       0          0       0
STA  Errors                     -       -       0          0       0
RAR Rcvd                        -       -       0          0       0
RAA Success                     -       -       0          0       0
RAA Errors                      -       -       0          0       0
DWR Sent                        -       -       0          0       0
DWA Success                     -       -       0          0       0
DWA Errors                      -       -       0          0       0
DWR Rcvd                        -       -       0          0       0
DWA Sent Success                -       -       0          0       0
DWA Sent Errors                 -       -       0          0       0
ASR Rcvd                        -       -       0          0       0
ASA Success                     -       -       0          0       0
ASA Errors                      -       -       0          0       0


-----------------------Summary Stats---------------------
10:53:02-197
Bandwidth Policy Server          --  Recent -- -------- Lifetime --------
                           Active    High   Total      Total  PerMax    High
Sockets                         1       1       0          2       1       1
Connections                     0       0       0          9       1       1
Client Transactions             0       0       0          9       1       1
  Reserve Requests Sent         -       -       0          0       0
  Update Requests Sent          -       -       0        241     211
  Remove Requests Sent          -       -       0        241     241
  Requests Re-Trans             -       -       0          0       0
  Install Resp Received         -       -       0        241     241
  Reject Resp Received          -       -       0          0       0
  Remove Resp Received          -       -       0        241     241
  Errors Received               -       -       0          0       0
  Transaction Timeouts          -       -       0          0       0
  Errors                        -       -       0          0       0
Server Transactions             0       0       0         30      30      29
  Requests Received             -       -       0          0       0
  Dup Req Received              -       -       0          0       0
  Success Resp Sent             -       -       0         30      30
  Error Resp Sent               -       -       0          0       0
  Requests Dropped              -       -       0          0       0
CER Sent                        -       -       0          0
0
```

```
CEA Success                     -       -       0          0       0
CEA Errors                      -       -       0          0       0
AAR Sent                        -       -       0          0
0
AAA Success                     -       -       0          0       0
AAA Errors                      -       -       0          0       0
STR Sent                        -       -       0          0       0
STA Success                     -       -       0          0       0
STA  Errors                     -       -       0          0       0
RAR Rcvd                        -       -       0          0       0
RAA Success                     -       -       0          0       0
RAA Errors                      -       -       0          0       0
DWR Sent                        -       -       0          0       0
DWA Success                     -       -       0          0       0
DWA Errors                      -       -       0          0       0
DWR Rcvd                        -       -       0          0       0
DWA Sent Success                -       -       0          0       0
DWA Sent Errors                 -       -       0          0       0
ASR Rcvd                        -       -       0          0       0
ASA Success                     -       -       0          0       0
ASA Errors                      -       -       0          0       0
```

Following is an example of the **show policy-server <IP_Address:Port>** command:

```
ORACLE# show policy-server 192.168.42.13:1817

-----------------------------------------
    Server:port           Priority         State       TCP-Failures
Diameter-Failures
   192.168.42.13:1817         0             inactive
2261              0

-----------------------------------------
15:29:27-182


Local IPPort         Remote IPPort        Socket State
--------------------------------------------------------
10.196.143.9:41743   10.196.0.209:3870    CONNECTED



-----------------------------------------
10:53:02-197
Bandwidth Policy Server          --  Recent -- -------- Lifetime --------
                           Active    High   Total      Total  PerMax    High
Sockets                         1       1       0          2       1       1
Connections                     0       0       0          9       1       1
Client Transactions             0       0       0          9       1       1
  Reserve Requests Sent         -       -       0          0       0
  Update Requests Sent          -       -       0        241     211
  Remove Requests Sent          -       -       0        241     241
  Requests Re-Trans             -       -       0          0       0
  Install Resp Received         -       -       0        241     241
  Reject Resp Received          -       -       0          0       0
  Remove Resp Received          -       -       0        241     241
  Errors Received               -       -       0          0       0
  Transaction Timeouts          -       -       0          0       0
  Errors                        -       -       0          0       0
Server Transactions             0       0       0         30      30      29
  Requests Received             -       -       0          0       0
  Dup Req Received              -       -       0          0       0
  Success Resp Sent             -       -       0         30      30
  Error Resp Sent               -       -       0          0       0
  Requests Dropped              -       -       0          0       0
```

```
CER Sent                        -       -       0          0
0
CEA Success                     -       -       0          0       0
CEA Errors                      -       -       0          0       0
AAR Sent                        -       -       0          0
0
AAA Success                     -       -       0          0       0
AAA Errors                      -       -       0          0       0
STR Sent                        -       -       0          0       0
STA Success                     -       -       0          0       0
STA  Errors                     -       -       0          0       0
RAR Rcvd                        -       -       0          0       0
RAA Success                     -       -       0          0       0
RAA Errors                      -       -       0          0       0
DWR Sent                        -       -       0          0       0
DWA Success                     -       -       0          0       0
DWA Errors                      -       -       0          0       0
DWR Rcvd                        -       -       0          0       0
DWA Sent Success                -       -       0          0       0
DWA Sent Errors                 -       -       0          0       0
ASR Rcvd                        -       -       0          0       0
ASA Success                     -       -       0          0       0
ASA Errors                      -       -       0          0       0


-----------------------Summary Stats---------------------
10:53:02-197
Bandwidth Policy Server          --  Recent -- -------- Lifetime --------
                           Active    High   Total      Total  PerMax    High
Sockets                         1       1       0          2       1       1
Connections                     0       0       0          9       1       1
Client Transactions             0       0       0          9       1       1
  Reserve Requests Sent         -       -       0          0       0
  Update Requests Sent          -       -       0        241     211
  Remove Requests Sent          -       -       0        241     241
  Requests Re-Trans             -       -       0          0       0
  Install Resp Received         -       -       0        241     241
  Reject Resp Received          -       -       0          0       0
  Remove Resp Received          -       -       0        241     241
  Errors Received               -       -       0          0       0
  Transaction Timeouts          -       -       0          0       0
  Errors                        -       -       0          0       0
Server Transactions             0       0       0         30      30      29
  Requests Received             -       -       0          0       0
  Dup Req Received              -       -       0          0       0
  Success Resp Sent             -       -       0         30      30
  Error Resp Sent               -       -       0          0       0
  Requests Dropped              -       -       0          0       0
CER Sent                        -       -       0          0
0
CEA Success                     -       -       0          0       0
CEA Errors                      -       -       0          0       0
AAR Sent                        -       -       0          0
0
AAA Success                     -       -       0          0       0
AAA Errors                      -       -       0          0       0
STR Sent                        -       -       0          0       0
STA Success                     -       -       0          0       0
STA  Errors                     -       -       0          0       0
RAR Rcvd                        -       -       0          0       0
RAA Success                     -       -       0          0       0
RAA Errors                      -       -       0          0       0
DWR Sent                        -       -       0          0       0
DWA Success                     -       -       0          0       0
DWA Errors                      -       -       0          0       0
DWR Rcvd                        -       -       0          0       0
DWA Sent Success                -       -       0          0       0
DWA Sent Errors                 -       -       0          0       0
ASR Rcvd                        -       -       0          0       0
ASA Success                     -       -       0          0       0
ASA Errors                      -       -       0          0       0
```

Following are two examples of the **show policy-server <IP_Address:Port> <DiamMsg>** command. The first example displays statistics related to the Diameter message CER:

```
ORACLE# show policy-server  192.168.209.12:3871 CER

-----------------------------------------
    Server:port           Priority         State       TCP-Failures
Diameter-Failures
   192.168.209.12:3871         0
active

-----------------------------------------
14:34:11-140
Bandwidth Policy Server          --  Recent -- -------- Lifetime --------
                           Active    High   Total      Total  PerMax    High


CER Sent                        -       -       0          0       0
Retrans                         -       -       0          0
0
TimeOut                         -       -       0          0       0
Success                         -       -       0          0       0
1xxx                            -       -       0          0
0
3xxx                            -       -       0          0
0
4xxx                            -       -       0          0
0
5xxx                            -       -       0          0       0
```

The second example displays statistics related to the Diameter message DWR:

```
ORACLE# show policy-server  192.168.209.12:3871 DWR

-----------------------------------------
    Server:port           Priority         State       TCP-Failures
Diameter-Failures
   192.168.209.12:3871         0
active

-----------------------------------------
14:34:11-140
Bandwidth Policy Server          --  Recent -- -------- Lifetime --------
                           Active    High   Total      Total  PerMax    High

DWR Sent                        -       -       0          0       0
Retrans                         -       -       0          0
0
TimeOut                         -       -       0          0       0
Success                         -       -       0          0       0
1xxx                            -       -       0          0
0
3xxx                            -       -       0          0
0
4xxx                            -       -       0          0
0
5xxx                            -       -       0          0       0
```

```
------------------------------------------
DWR Rcvd                        -       -       0          0       0
Retrans                         -       -       0          0
0
TimeOut                         -       -       0          0       0
Success                         -       -       0          0       0
1xxx                            -       -       0          0
0
3xxx                            -       -       0          0
0
4xxx                            -       -       0          0
0
5xxx                            -       -       0          0       0
```

Following is an example of the **show policy-server connections** command:

```
ORACLE# show policy-server connections

Local IPPort               Remote IPPort               Socket State
---------------------------------------------------------------------
10.196.143.9:41743         10.196.0.209:3870           CONNECTED
```

Rf Interface Statistics

Both Diameter and RADIUS messages traverse the Rf interface. The two commands that display statistics for the Rf interface are **show accounting** and **show radius accounting**.

show accounting

The **show accounting** command lets you view specific information about a configured external accounting server. The syntax is:

```
show accounting [[<IPPort> | All] [<DiamMsg>]] | [connections]
```

Following is an example of the **show accounting** command without any arguments:

```
ORACLE# show accounting

13:05:03-102
Accounting Status:
                               -- Period -- -------- Lifetime --------
                 Active    High   Total      Total  PerMax    High
Request Queue         0       0       0        200     200       2
Client Trans          0       2       8       1670     408       4
Server Trans          0       0       0          0       0       0
Sockets               2       2       0          2       2       2
Connections           1       2       2        318       3       2

Total Accounting Server Stats:
                           ---- Lifetime ----
                    Recent      Total  PerMax
Msgs Queued              0        200     200
Msgs Discarded           0          0       0
Wait Queue Asks          0        200     200
Wait Queue Pops          0        200     200
Msgs Reclaimed           0          0       0
Msgs Sent                0        200     200
Msg Send Failed          0          0       0
Msgs ReSent              0          0       0
Msgs Rcvd                0        200     200
Msgs Processed           0        200     200
Conn Timeouts            2        386       4
Bad State Drops          0          0       0
Bad Type Drops           0          0       0
Bad Id Drops             0          0       0
```

```
Auth Failed Drops        0          0       0
Invalid peer Msgs        0          0       0
Protocol errors          0          0       0
Transient Failures       0          0       0
Permanent Failures       0          0       0

Total Accounting Server Diameter msg Stats:
                           ---- Lifetime ----
                    Recent      Total  PerMax
CER Sent                 2        318       3
CEA Success              2        318       3
CEA Errors               0          0       0
ACR Sent                 0        200     200
ACA Success              0        200     200
ACA Errors               0          0       0
DWR Sent                 2        317       3
DWA Success              0          0       0
DWA Errors               0          0       0
DWR Rcvd                 0          0       0
DWA Sent Success         0          0       0
DWA Sent Errors          0          0       0

Total Accounting Server SIPD to RADD msg Stats:
                           ---- Lifetime ----
                    Recent      Total  PerMax
Acct Type Start          0        100     100
Acct Type Stop           0        100     100
Acct Type Interim        0          0       0
Acct Type Event          0          0       0

Server 1 :
----------------- 10.196.0.209:3868 -----------------
Connection state: UNAVAIL
Socket FD: -1
Reconnect attempt in 1s
Pending: 0 of 255
Current RTT: 4 ms (before failure)
   Local IPPort          Remote IPPort     Socket State
 10.196.143.7:0    10.196.0.209:3868      INITIAL

Server 2 :
----------------- 10.196.0.209:3870 -----------------
Connection state: READY
Socket FD: 469
Pending: 0 of 255
Current RTT: 5 ms
   Local IPPort          Remote IPPort     Socket State
 10.196.143.7:56819    10.196.0.209:3870      CONNECTED
```

Following is an example of the **show accounting <IPPort>** command:

```
ORACLE# show accounting 10.196.0.209:3868

----------------- 10.196.0.209:3868 -----------------
Connection state: READY
Socket FD: 147
Pending: 0 of 255
Current RTT: 5 ms
    Local IPPort        Remote IPPort      Socket State
10.196.143.13:44820   10.196.0.209:3868      CONNECTED
                           ---- Lifetime
----
                    Recent      Total
PerMax
```

```
Msgs Sent                2          2
2
Send Failed              0          0
0
Msgs ReSent              0          0
0
Msgs Rcvd                2          2
2
Msgs Processed           2          2
2
Conn Timeouts            0          0
0
Bad State Drops          0          0
0
Bad Type Drops           0          0
0
Bad Id Drops             0          0
0
Auth Failed Drops        0          0
0
Invalid peer Msgs        0          0
0
Protocol errors          0          0
0
Transient Failures       0          0
0
Permanent Failures       0          0
0
                           ---- Lifetime
----
                    Recent      Total
PerMax
CER Sent                 0          0
0
CEA Success              0          0
0
CEA Errors               0          0
0
ACR Sent                 2          2
2
ACA Success              2          2
2
ACA Errors               0          0
0
DWR Sent                 0          0
0
DWA Success              0          0
0
DWA Errors               0          0
0
DWR Rcvd                 0          0
0
DWA Sent Success         0          0
0
DWA Sent Errors          0          0       0
```

Following is an example of the **show accounting ALL** command:

```
ORACLE# show accounting ALL

12:45:20-118
Accounting Status:
                               -- Period -- -------- Lifetime
--------
```

```
                 Active    High   Total      Total  PerMax
High
Request Queue         0       1       2          2       2
1
Client Trans          0       2       4          4       4
2
Server Trans          0       0       0          0       0
0
Sockets               2       2       0          0       0
2
Connections           1       1       0          0       0
1

Total Accounting Server Stats:
                           ---- Lifetime ----
                    Recent      Total  PerMax
Msgs Queued              2          2       2
Msgs Discarded           0          0       0
Wait Queue Asks          2          2       2
Wait Queue Pops          2          2       2
Msgs Reclaimed           0          0       0
Msgs Sent                2          2       2
Send Failed              0          0       0
Msgs ReSent              0          0       0
Msgs Rcvd                2          2       2
Msgs Processed           2          2       2
Conn Timeouts            3          3       3
Bad State Drops          0          0       0
Bad Type Drops           0          0       0
Bad Id Drops             0          0       0
Auth Failed Drops        0          0       0
Invalid peer Msgs        0          0       0
Protocol errors          0          0       0
Transient Failures       0          0       0
Permanent Failures       0          0       0

Total Accounting Server Diam Stats:
                           ---- Lifetime ----
                    Recent      Total  PerMax
CER Sent                 0          0       0
CEA Success              0          0       0
CEA Errors               0          0       0
ACR Sent                 2          2       2
ACA Success              2          2       2
ACA Errors               0          0       0
DWR Sent                 0          0       0
DWA Success              0          0       0
DWA Errors               0          0       0
DWR Rcvd                 0          0       0
DWA Sent Success         0          0       0
DWA Sent Errors          0          0       0
Total Accounting Server sipd to radd Stats:
                           ---- Lifetime ----
Acct Type Start          1          1       1
Acct Type Stop           1          1       1
Acct Type Interim        0          0       0
Acct Type Event          0          0       0

Server 1 :
----------------- 10.196.0.209:3868 -----------------
Connection state: READY
Socket FD: 147
Pending: 0 of 255
Current RTT: 5 ms
```

```
    Local IPPort        Remote IPPort      Socket State
10.196.143.13:44820   10.196.0.209:3868      CONNECTED
                           ---- Lifetime
----
                    Recent      Total
PerMax
Msgs Sent                2          2
2
Send Failed              0          0
0
Msgs ReSent              0          0
0
Msgs Rcvd                2          2
2
Msgs Processed           2          2
2
Conn Timeouts            0          0
0
Bad State Drops          0          0
0
Bad Type Drops           0          0
0
Bad Id Drops             0          0
0
Auth Failed Drops        0          0
0
Invalid peer Msgs        0          0
0
Protocol errors          0          0
0
Transient Failures       0          0
0
Permanent Failures       0          0
0
                           ---- Lifetime
----
                    Recent      Total
PerMax
CER Sent                 0          0
0
CEA Success              0          0
0
CEA Errors               0          0
0
ACR Sent                 2          2
2
ACA Success              2          2
2
ACA Errors               0          0
0
DWR Sent                 0          0
0
DWA Success              0          0
0
DWA Errors               0          0
0
DWR Rcvd                 0          0
0
DWA Sent Success         0          0
0
DWA Sent Errors          0          0       0
```

Following are two examples of the **show accounting <IPPort> <DiamMsg>** command. The first example displays statistics related to the Diameter message DWR for a single server:

```
ORACLE# show accounting 10.196.0.209:3868  DWR

Server 1 :
----------------- 10.196.0.209:3868 -----------------
Connection state: READY
Socket FD: 448
Pending: 0 of 255
Current RTT: 1 ms
   Local IPPort        Remote IPPort   Socket State
10.196.143.9:41743   10.196.0.209:3870   CONNECTED
                                         ---- Lifetime ----
                                      Recent      Total    PerMax
-------------------------------------------------------------------------
DWR Sent                                 0             0         0
Retrans                                  0             0         0
TimeOut                                  0             0         0
1xxx                                     0             0         0
Success                                  0             0         0
3xxx                                     0             0         0
4xxx                                     0             0         0
5xxx                                     0             0         0
------------------------------------------
DWR Rcvd                                 0             0
0
1xxx                                     0             0         0
Success                                  0             0         0
3xxx                                     0             0         0
4xxx                                     0             0         0
5xxx                                     0             0         0
```

The second example displays statistics related to the Diameter message CER for all servers:

```
ORACLE# show accounting ALL CER

Total Accounting Server Stats for diameter message cer
                           ---- Lifetime ----
                    Recent      Total  PerMax
CER Sent                 5        300       3
Retrans                  0          0       0
Timeout                  0          0       0
1xxx                     0          0       0
Success                  5        300       3
3xxx                     0          0       0
4xxx                     0          0       0
5xxx                     0          0       0

Server 1 :
----------------- 10.196.0.209:3868 -----------------
Connection state: READY
Socket FD: 426
Pending: 0 of 255
Current RTT: 4 ms
   Local IPPort          Remote IPPort     Socket State
 10.196.143.7:43424    10.196.0.209:3868      CONNECTED

Accounting Server Stats for diameter message cer
                           ---- Lifetime ----
                    Recent      Total  PerMax
CER Sent                 5        299       3
Retrans                  0          0       0
Timeout                  0          0       0
1xxx                     0          0       0
Success                  5        299       3
3xxx                     0          0       0
```

```
4xxx                     0          0       0
5xxx                     0          0       0

Server 2 :
------------------ 10.196.0.209:3870 -----------------
Connection state: READY
Socket FD: 469
Pending: 0 of 255
Current RTT: 5 ms
   Local IPPort          Remote IPPort     Socket State
 10.196.143.7:56819    10.196.0.209:3870      CONNECTED

Accounting Server Stats for diameter message cer
                           ---- Lifetime ----
                    Recent      Total  PerMax
CER Sent                 0          1       1
Retrans                  0          0       0
Timeout                  0          0       0
1xxx                     0          0       0
Success                  0          1       1
3xxx                     0          0       0
4xxx                     0          0       0
5xxx                     0          0       0
```

Following is an example of the **show accounting connections** command:

```
ORACLE# show accounting connections

Server 1 :
------------------ 10.196.0.209:3868 -----------------
Connection state: READY
Socket FD: 448
Pending: 0 of 255
Current RTT: 1 ms
   Local IPPort        Remote IPPort   Socket State
10.196.143.9:41743   10.196.0.209:3868   CONNECTED
Server 2 :
------------------ 10.196.0.209:3870 -----------------
Connection state: READY
Socket FD: 448
Pending: b3.9:41744   10.196.0.209:3870   CONNECTED
```

show radius accounting

The **show radius** command with the **accounting** argument lets you view the status of established RADIUS accounting connections only. A successful RADIUS connection is displayed as READY, and an unsuccessful connection is displayed as DISABLED. If you attempt to execute this argument for a Diameter accounting server, the command will be blocked with the message
Accounting configured for DIAMETER. Please use "show accounting".
The **accounting** argument has its own argument: **[All | <IPPort>]**. Invoking the **accounting** argument without an argument displays a summary of the accounting statistics for all RADIUS servers; the **IPPort** argument displays complete accounting statistics for a specific RADIUS server and the **All** argument displays complete accounting statistics for all RADIUS servers.

TCP Connection Tools

Transmission Control Protocol (TCP) connection tools can assist you in gauging performance, identifying potential memory leaks, and debugging connections for performance tracking and improvement.

The **show ip tcp** command shows the following socket connections by state:

- inbound

- outbound
- listen
- IMS-AKA

The **show sipd tcp** and **show sipd tcp connections** commands display counters to track usage. Use the **reset sipd** command to reset the counters.

TCP and SCTP State Connection Counters

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

The **show ip tcp** command includes the following section of counters that correspond to counts of TCP states per active connections, including counts differentiated by inbound, outbound, listen and IMS-AKA connections.

```
Connections By State:
        0       CLOSED
        0       LISTEN
        0       SYN_SENT
        0       SYN_RCVD
        0       ESTABLISHED
        0       CLOSE_WAIT
        0       FIN_WAIT_1
        0       CLOSING
        0       LAST_ACK
        0       FIN_WAIT_2
        0       TIME_WAIT

Inbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
         50    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


Outbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          1    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


Listen Socket Connection By State:
          0    CLOSED
          2    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


IMSAKA Inbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


IMSAKA Outbound Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


IMSAKA Listen Socket Connection By State:
          0    CLOSED
          0    LISTEN
          0    SYN_SENT
          0    SYN_RCVD
          0    ESTABLISHED
          0    CLOSE_WAIT
          0    FIN_WAIT_1
          0    CLOSING
          0    LAST_ACK
          0    FIN_WAIT_2
          0    TIME_WAIT


        Number of Connections Counted = 0
        Maximum Connection Count = 0
        Maximum Number of Connections Supported = 220000
```

The **show ip sctp** command includes the following section of counters that correspond to counts of SCTP states per active connections.

```
Connections By State:
                0       CLOSED
                0       BOUND
                0       LISTEN
                0       COOKIE_WAIT
                0       COOKIE_ECHOED
                0       ESTABLISHED
                0       SHUTDOWN_SENT
                0       SHUTDOWN_RECEIVED
                0       SHUTDOWN_ACK_SENT
                0       SHUTDOWN_PENDING

        Number of Connections Counted = 0
        Maximum Connection Count = 0
        Maximum Number of Connections Supported = 10000
```

The output of the state counters indicates the number of connections currently in each state. The statistics from the counters do not accumulate like many of the other statistics in the **show ip** command tree. Most states are ephemeral, and you may see many "0" counters for states other than LISTEN and ESTABLISHED.

show sipd tcp connections

The **show sipd tcp connections** command displays Transmission Control Protocol (TCP) connection information details on remote and local address/port and connection states for analysis. Oracle recommends that you use the command only during non-peak times or maintenance windows.

The s**how sipd tcp connections** command displays all SIP/TCP connections including each connection's direction, type, state, local and remote addresses, SIP interface and IMS-AKA details. Arguments include:

- sip-interface—Optional parameter that limits output to sockets in the specified sip-interface
- start start—Integer indicating which connection to start displaying. This can be a negative number. When the number selected for the start variable is greater than the number of TCP connections, the system displays nothing.
- start-count start—Integer as per above plus the count integer, specifying how many TCP connections to display from the start.
- all—Display all of the sipd tcp connections. Exercise caution due to the possibility of consuming all CPU time; preferably use during a maintenance window

For example:

```
ORACLE# show sipd tcp connections

sipd tcp connections

Dir Type    State          Local Address         Remote Address        sip-
interface-id     isImsaka

    LISTEN  TCP_LISTENING  172.16.101.149:5060
net172
in  FORKED  TCP_CONNECTED  172.16.101.149:5060   172.16.23.100:51678
net172
in  FORKED  TCP_CONNECTED  172.16.101.149:5060   172.16.23.100:51679
net172
[...]
in  FORKED  TCP_CONNECTED  172.16.101.149:5060   172.16.23.100:51727
net172
in  FORKED  TCP_CONNECTED  172.16.101.149:5060   172.16.23.100:51728
net172
in  FORKED  TCP_CONNECTED  172.16.101.149:5060   172.16.23.100:51729
net172
    LISTEN  TCP_LISTENING  192.168.101.149:5060
net192
out CONNECT TCP_CONNECTED  192.168.101.149:8192  192.168.23.100:5060
net192

Connections Displayed:       53
Total Connections:           53
```

show sipd tcp

.

The **show sipd tcp** command displays TCP connection state information for the following:

- inbound
- outbound
- listen
- total
- IMS-AKA

For example:

```
ORACLE# show sipd tcp
11:11:54-110
SIP TCP Sockets               -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States              53      53     108        108     108      53
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       1      51         51      51       1
TCP_BOUND                0       1       3          3       3       1
TCP_CONNECTED           51      51      51         51      51      51
TCP_CONNECTING           0       1       1          1       1       1
TCP_LISTENING            2       2       2          2       2       2
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------

SIP Inbound TCP Sockets       -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States              50      50     100        100     100      50
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       1      50         50      50       1
TCP_BOUND                0       0       0          0       0       0
TCP_CONNECTED           50      50      50         50      50      50
TCP_CONNECTING           0       0       0          0       0       0
TCP_LISTENING            0       0       0          0       0       0
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------

SIP Outbound TCP Sockets      -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States               1       1       4          4       4       1
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       1       1          1       1       1
TCP_BOUND                0       1       1          1       1       1
TCP_CONNECTED            1       1       1          1       1       1
TCP_CONNECTING           0       1       1          1       1       1
TCP_LISTENING            0       0       0          0       0       0
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------

SIP Listen TCP Sockets        -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States               2       2       4          4       4       2
```

```
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       0       0          0       0       0
TCP_BOUND                0       1       2          2       2       1
TCP_CONNECTED            0       0       0          0       0       0
TCP_CONNECTING           0       0       0          0       0       0
TCP_LISTENING            2       2       2          2       2       2
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------
```

IMS-AKA portion of show **sipd tcp command**:

```
ORACLE# show sipd tcp
15:28:51-197
[...]

SIP IMSAKA In TCP Sockets     -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States               0       0       0          0       0       0
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       0       0          0       0       0
TCP_BOUND                0       0       0          0       0       0
TCP_CONNECTED            0       0       0          0       0       0
TCP_CONNECTING           0       0       0          0       0       0
TCP_LISTENING            0       0       0          0       0       0
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------

SIP IMSAKA Out TCP Sockets    -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States               0       0       0          0       0       0
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       0       0          0       0       0
TCP_BOUND                0       0       0          0       0       0
TCP_CONNECTED            0       0       0          0       0       0
TCP_CONNECTING           0       0       0          0       0       0
TCP_LISTENING            0       0       0          0       0       0
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0

----------------------------------------------------------------------

SIP IMSAKA Listen TCP Sockets -- Period -- -------- Lifetime --------
                    Active    High   Total      Total  PerMax    High
All States               1       1       0          2       2       1
TCP_INITIAL              0       0       0          0       0       0
TCP_STARTING             0       0       0          0       0       0
TCP_AVAILABLE            0       0       0          0       0       0
TCP_BOUND                0       0       0          1       1       1
TCP_CONNECTED            0       0       0          0       0       0
TCP_CONNECTING           0       0       0          0       0       0
TCP_LISTENING            1       1       0          1       1       1
TCP_DISCONNECT           0       0       0          0       0       0
TCP_CLOSED               0       0       0          0       0       0
----------------------------------------------------------------------
```

Updated Show Commands

show ip

Syntax

```
show ip <arguments>
```

Displays IP statistics for the Oracle Communications Session Border Controller.

Arguments

The following is a list of valid show ip arguments:

- statistics —Display detailed IP statistics
- connections —Display all TCP and UDP connections
- sctp—Display all SCTP statistics, including a list of current connections per SCTP state and systemwide counts.
- tcp —Display all TCP statistics, including a list of current connections per TCP state and differentiated by inbound, outbound, listen and IMS-AKA connections as well as systemwide counts.
- udp —Display all UDP statistics

Executing the **show ip** command with no arguments returns the equivalent of the **show ip statistics** command.

show sipd

Syntax

```
show sipd <arguments>
```

The show sipd command displays SIP statistics on your Oracle Communications Session Border Controller.

Arguments

status—Display information about SIP transactions. These statistics are given for the Period and Lifetime monitoring spans. This display also provides statistics related to SIP media events. The following statistics are displayed when using the show sipd status command.

- Dialogs—Number of end-to-end SIP signaling connections
- CallID Map—Total number of successful session header Call ID mappings
- Sessions—Number of sessions established by an INVITE
- Subscriptions—Number of sessions established by SUBSCRIPTION
- Rejections—Number of rejected INVITEs
- ReINVITEs—Number of ReINVITEs
- Media Sessions—Number of successful media sessions
- Media Pending—Number of media sessions waiting to be established
- Client Trans—Number of client transactions
- Server Trans—Number of server transactions that have taken place on the Oracle Communications Session Border Controller
- Resp Contexts—Number of current response contexts
- Saved Contexts—Total number of saved contexts
- Sockets—Number of active SIP sockets
- Req Dropped—Number of requests dropped
- DNS Trans—Number of DNS transactions
- DNS Sockets—Number of DNS Sockets
- DNS Results—Number of dns results

- Session Rate—The rate, per second, of SIP invites allowed to or from the Oracle Communications Session Border Controller during the sliding window period. The rate is computed every 10 seconds
- Load Rate—Average Central Processing Unit (CPU) utilization of the Oracle Communications Session Border Controller during the current window. The average is computed every 10 seconds. When you configure the load-limit in the SIPConfig record, the system computes the average every 5 seconds

errors —Display statistics for SIP media event errors. These statistics are errors encountered by the SIP application in processing SIP media sessions, dialogs, and session descriptions (SDP). Errors are only displayed for the lifetime monitoring span.

- SDP Offer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Offer in the Offer/Answer model (RFC 3264)
- SDP Answer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Answer in the Offer/Answer model (RFC 3264)
- Drop Media Errors—Number of errors encountered in tearing down the media for a dialog or session that is being terminated due to: a) non-successful response to an INVITE transaction; or b) a BYE transaction received from one of the participants in a dialog or session; or c) a BYE initiated by the system due to a timeout notification from MBCD
- Transaction Errors—Number of errors in continuing the processing of the SIP client transaction associated with setting up or tearing down of the media session
- Missing Dialog—Number of requests received by the SIP application for which a matching dialog count not be found
- Application Errors—Number of miscellaneous errors in the SIP application that are otherwise uncategorized
- Media Exp Events—Flow timer expiration notifications received from MBCD
- Early Media Exps—Flow timer expiration notifications received for media sessions that have not been completely set up due to an incomplete or pending INVITE transaction
- Exp Media Drops—Number of flow timer expiration notifications from the MBCD that resulted in the termination of the dialog/session by the SIP application
- Multiple OK Drops—Number of dialogs terminated upon reception of a 200 OK response from multiple UASs for a given INVITE transaction that was forked by a downstream proxy
- Multiple OK Terms—Number of dialogs terminated upon reception of a 200 OK response that conflicts with an existing established dialog on the Oracle Communications Session Border Controller
- Media Failure Drops—Number of dialogs terminated due to a failure in establishing the media session
- Non-ACK 2xx Drops—Number of sessions terminated because an ACK was not received for a 2xx response
- Invalid Requests—Number of invalid requests; an unsupported header for example
- Invalid Responses—Number of invalid responses; no Via header for example
- Invalid Messages—Number of messages dropped due to parse failure
- CAC Session Drop—Number of call admission control session setup failures due to user session count exceeded
- Expired Sessions—Number of sessions terminated due to the session timer expiring
- CAC BW Drop—Number of call admission control session setup failures due to insufficient bandwidth

  Lifetime displays show information for recent, total, and period maximum error statistics:
- Recent—Number of errors occurring in the number of seconds listed after the time stamp
- Total—Number of errors occurring since last reboot
- PerMax—Identifies the highest individual Period Total over the lifetime of the monitoring

policy—Display SIP local policy / routing statistics for lifetime duration

- Local Policy Lookups—Number of Local policy lookups
- Local Policy Hits—Number of successful local policy lookups
- Local Policy Misses—Number of local policy lookup failures

- Local Policy Drops—Number of local policy lookups where the next hop session agent group is H323
- Agent Group Hits—Number of successful local policy lookups for session agent groups
- Agent Group Misses—Number of successful local policy lookups where no session agent was available for session agent group
- No Routes Found—Number of successful local policy lookups but temporarily unable to route; session agent out of service for instance
- Missing Dialog—Number of local policy lookups where the dialog is not found for a request addressed to the Oracle Communications Session Border Controller with a To tag or for a NOTIFY-SUBSCRIBE sip request
- Inb SA Constraints—Number of successful local policy lookups where inbound session agent exceeded constraints
- Outb SA Constraints—Number of successful outbound local policy lookups where session agent exceeded constraints
- Inb Reg SA Constraints—Number of successful inbound local policy lookups where registrar exceeded constraints
- Out Reg SA Constraints—Number of successful outbound local policy lookups where registrar exceeded constraints
- Requests Challenged—Number of requests challenged
- Challenge Found— Number of challenges found
- Challenge Not Found—Number of challenges not found
- Challenge Dropped—Number of challenges dropped

server—Display statistics for SIP server events when the Oracle Communications Session Border Controller acts as a SIP server in its B2BUA role. Period and Lifetime monitoring spans for SIP server transactions are provided.

- All States—Number of all server transactions
- Initial—Number of times the “initial” state was entered after a request was received
- Queued—Number of times the “queued” state is entered because resources are temporarily unavailable
- Trying—Number of times the “trying” state was entered due to the receipt of a request
- Proceeding—Number of times a server transaction has been constructed for a request
- Cancelled—Number of INVITE transactions that received a CANCEL
- Established—Number of times the server sent a 2xx response to an INVITE
- Completed—Number of times the server received a 300 to 699 status code and entered the “completed” state
- Confirmed—Number of times that an ACK was received while the server was in “completed” state and transitioned to “confirmed” state
- Terminated—Number of times that the server received a 2xx response or never received an ACK in the “completed” state, and transitioned to the “terminated” state

client —Display statistics for SIP client events when the Oracle Communications Session Border Controller is acting as a SIP client in its B2BUA role. Period and Lifetime monitoring spans are displayed.

- All States—Number of all client transactions
- Initial—State when initial server transaction is created before a request is sent
- Trying—Number of times the “trying” state was entered due to the sending of a request
- Calling—Number of times that the “calling” state was entered due to the receipt of an INVITE request
- Proceeding—Number of times that the “proceeding” state was entered due to the receipt of a provisional response while in the “calling” state
- Early Media—Number of times that the “proceeding” state was entered due to the receipt of a provisional response that contained SDP while in the “calling” state
- Completed—Number of times that the “completed” state was entered due to the receipt of a status code in the range of 300-699 when either in the “calling” or “proceeding” state
- SetMedia—Number of transactions in which the Oracle Communications Session Border Controller is setting up NAT and steering ports

- Established—Number of situations when client receives a 2xx response to an INVITE, but cannot forward it because it NAT and steering port information is missing
- Terminated—Number of times the “terminated” state was entered after a 2xx message

acls—Display ACL information for Period and Lifetime monitoring spans

- Total entries—Total ACL Entries, including both trusted and blocked
- Trusted—Number of trusted ACL entries
- Blocked—Number of blocked ACL entries
- Blocked NATs—Number of blocked entries that are behind NATs

  Lifetime monitoring span is displayed for SIP ACL Operations.
- ACL Requests—Number of ACL requests
- Bad Messages —Number of bad messages
- Promotions—Number of ACL entry promotions
- Demotions—Number of ACL entry demotions
- Trust->Untrust—Number of ACL entries demoted from trusted to untrusted
- Untrust->Deny—Number of acl entries demoted from untrusted to deny

sessions—Display the number of sessions and dialogs in various states for the Period and Lifetime monitoring spans, in addition to the current Active count:

- Sessions—Identical to the identically named statistic on the show sipd status command
- Initial—Displays sessions for which an INVITE of SUBSCRIBE is being forwarded
- Early—Displays sessions for which the first provisional response (1xx other than 100) is received
- Established—Displays sessions for which a success (2xx) response is received
- Terminated—Displays sessions for which the session is ended by receiving or sending a BYE for an “Established" session or forwarding an error response for an "Initial" or "Early" session. The session will remain in the "Terminated" state until all the resources for the session are freed.
- Dialogs—Identical to the identically named statistic on the show sipd status command
- Early—Displays dialogs that were created by a provisional response
- Confirmed—Displays dialogs that were created by a success response. An "Early" dialog will transition to "Confirmed" when a success response is received
- Terminated—Displays dialogs that were ended by receiving/sending a BYE for an Established" session or receiving/sending error response "Early" dialog. The dialog will remain in the "Terminated" state until all the resources for the session are freed.

sessions all—Display all SIP sessions currently on the system

sessions by-agent <agent name>—Display SIP sessions for the session agent specified; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-ip <endpoint IP address>—Display SIP sessions for the specified IP address for an endpoint; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-user <calling or called number>—Display SIP sessions for the specified user; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-callid <call ID>—Display SIP sessions for the specified call ID; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

redundancy—Display sipd redundancy statistics. Executing the show sipd redundancy command is the equivalent to the show redundancy sipd command.

agents [hostname][method][-t]—Display statistics related to defined SIP session agents. Entering this command without any arguments list all SIP session agents. By adding the IP address or hostname of a session agent as well as a specified method at the end of the command, you can display statistics for that specific session agent and method. For a specific session agent, identified by IP address, the show sipd agents command lists:

- session agent state
    - D—disabled
    - I—in-service
    - O—out-of-service
    - S—transitioning from out-of-service to in-service
- inbound and outbound statistics
- average and maximum latency for each session agent
- maximum burst rate for each session agent as total number of session invitations sent to or received from the session agent within the amount of time configured in the burst-rate-window field

  Inbound Statistics:
- Active—Number of active sessions sent to each session agent listed
- Rate—Average rate of session invitations (per second) sent to each session agent listed
- ConEx—Number of times the constraints have been exceeded

  Outbound Statistics:
- Active—Number of active sessions sent from each session agent
- Rate—Average rate of session invitations (per second) sent from each session agent listed
- ConEx—Number of times the constraints have been exceeded

  Latency:
- Avg—Average latency for packets traveling to and from each session agent
- Max—Maximum latency for packets traveling to and from each session agent listed

-t—Append to the end of the command to specify the current time period for the max-burst value.

interface [interface-id][method]—Display SIP interface statistics. By adding the optional interface-id and method arguments you can narrow the display to view just the interface and method you want to view.

ip-cac <IP address>—Display CAC parameters for an IP address

publish—Display statistics related to incoming SIP PUBLISH messages

agent <agent>—Display activity for the session agent that you specify

- Inbound Sessions:

  Rate Exceeded—Number of times session or burst rate was exceeded for inbound sessions
- Num Exceeded—Number of times time constraints were exceeded for inbound sessions

  Outbound Sessions:
- Rate Exceeded—Number of times session or burst rate was exceeded for outbound sessions
- Num Exceeded—Number of times time constraints were exceeded for inbound sessions
- Burst—Number of times burst rate was exceeded for this session agent
- Out of Service—Number of times this session agent went out of service
- Trans Timeout—Number of transactions timed out for this session agent
- Requests Sent—Number of requests sent by way of this session agent
- Requests Complete—Number of requests that have been completed for this session agent
- Messages Received—Number of messages received by this session agent

realm—Display realm statistics related to SIP processing

routers—Display status of Oracle Communications Session Border Controller connections for session router functionality directors—Display the status of Oracle Communications Session Border Controller connections for session director functionality

<message>—Add one of the following arguments to the end of a show sipd command to display information about that type of SIP message:

- INVITE—Display the number of SIP transactions including an INVITE method
- REGISTER—Display the number of SIP transactions including a REGISTER method
- OPTIONS—Display the number of SIP transactions including an OPTIONS method
- CANCEL—Display the number of SIP transactions including a CANCEL method
- BYE—Display the number of SIP transactions including a BYE method
- ACK—Display the number of SIP transactions including an ACK method
- INFO—Display the number of SIP transactions including an INFO method
- PRACK—Display the number of SIP transactions including a PRACK method
- SUBSCRIBE—Display the number of SIP transactions including a SUBSCRIBE method
- NOTIFY—Display the number of SIP transactions including a NOTIFY method
- REFER—Display the number of SIP transactions including a REFER method
- UPDATE—Display the number of SIP transactions including an UPDATE method
- other—Display the number of SIP transactions including non-compliant methods and protocols used by specific customers

  The following lists information displayed for each individual SIP message statistic. Some or all of the following messages and events may appear in the output from a show sipd command.
- INVITE Requests—Number of times method has been received or sent
- Retransmissions—Information regarding sipd message command requests received by the Oracle Communications Session Border Controller
- 100 Trying—Number of times some unspecified action is being taken on behalf of a call (e.g., a database is being consulted), but user has not been located
- 180 Ringing—Number of times called UA identified a location where user has registered recently and is trying to alert the user
- 200 OK—Number of times request has succeeded
- 408 Request Timeout—Number of times server could not produce a response before timeout
- 481 Does Not Exist—Number of times UAS received a request not matching existing dialog or transaction
- 486 Busy Here—Number of times callee's end system was contacted successfully but callee not willing to take additional calls
- 487 Terminated—Number of times request was cancelled by a BYE or CANCEL request
- 4xx Client Error—Number of times the 4xx class of status code appeared for cases where the client seems to have erred
- 503 Service Unavail—Number of times server was unable to handle the request due to a temporary overloading or maintenance of the server
- 5xx Server Error—Number of times the 5xx class of status code appeared
- Response Retrsns—Number of response retransmissions sent and received
- Transaction Timeouts— Number of times a transaction timed out. The timer related to this transaction is Timer B, as defined in RFC 3261
- Locally Throttled—Number of locally throttled invites. Does not apply to a server.

  show sipd <message> output is divided in two sections: Server and Client, with information for recent, total, and period maximum time frames. This command also displays information about the average and maximum latency. For each type of SIP message, only those transactions for which there are statistics are shown. If there is no data available for a certain SIP message, the system displays the fact that there is none and specifies the message about which you inquired.

groups—Display cumulative information for all session agent groups on the Oracle Communications Session Border Controller. This information is compiled by totaling the session agent statistics for all of the session agents that make up a particular session agent group. While the show sipd groups command accesses the sub-commands described in this section, the main show sipd groups command (when executed with no arguments) displays a list of all session agent groups.

groups -v—Display statistics for the session agents that make up the session agent groups that are being reported. The -v (meaning “verbose”) executed with this command must be included to provide verbose detail.

groups <specific group name>— Display statistics for the specified session agent group

endpoint-ip <phone number> —Displays registration information for a designation endpoint entered in the <phone number> argument; also show IMS-AKA data

all—Display all the show sipd statistics listed above

sip-endpoint-ip—See show sipd endpoint-ip

sa-nsep-burst—Display NSEP burst rate for all SIP session agents

subscriptions-by-user—Display data for SIP per user subscribe dialog limit

rate—Displays the transaction rate of SIP messages

codecs—Displays codec usage per realm, including counts for codecs that require a license such as SILK and opus.

pooled-transcoding—Pooled transcoding information for the client and server User Agents on the P-CSCF

srvcc—Displays EATF Session information

tcp—Displays TCP connection state information for the following

- inbound
- outbound
- listen
- IMS-AKA
- total

tcp connections—Dump TCP connections for analysis. Options include:

- sip-interface—Optional parameter that limits output to sockets in the specified sip-interface
- start start—Integer indicating which connection to start display. This can be a negative number. If the number selected for the start variable is greater than the number of TCP connections, nothing will be displayed
- start-count start—Integer as per above plus the count integer, specifying how many TCP connections to display from the start.
- all—Dump all of the sipd tcp connections. Exercise caution due to the possibility of consuming all CPU time; preferably use during a maintenance window

Example

```
ORACLE# show sipd errors
```

Blocking TSCF Inter-client Communication

To deploy TSC clients (such as softphones, SIP-enabled iOS/Android applications or contact center agent applications), customers and 3rd party ISVs need to incorporate the TSM's open source software libraries (TSC clients) into their applications which will establish SSL connections (TLS or DTLS) to the TSC server. If the **inter-client-blocking** is to be implemented, you must use the Oracle Software Developer Kit (SDK), release 1.4 or above.

TSC client sends encapsulated data through the tunnel, and the TSC server decrypts data and forwards to the SBC, then SBC will do IMS business data handling. When CM-IMS core network tries to send data to the client using security tunnel mode, the SBC will send data to TSC server, which will do data encapsulation and forward to client via security tunnels.

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.

With **inter-client-block** configured, the TSCF server will check the destination address of every de-tunneled packet and compare it against all the configured TSCF address pools that are in use on the system. If the destination address falls in the range of configured TSCF address pools, then the packet will be dropped.

inter-client-block Supported Platforms

These are the platforms supported for the initial release of the **inter-client-block** service:

- Acme Packet 4600
- Acme Packet 6100
- Acme Packet 6300

inter-client-block Prerequisites

In order to activate **inter-client-block**, you must first fulfill the following prerequisites:

- Configure at least one TSE built with SDK version 1.4 and above
- Provision a TSCF Interface

Note: Refer to "TSCF Interface Configuration" for details.

The default TSM parameters are the same as the default parameters of a TSE configured with SDK version 1.4.

inter-client-block Configuration

From superuser mode, use the following command path to access assigned-services configuration mode.

```
ORACLE# configure terminal
ORACLE(configure)# security
ORACLE(security)# tscf
ORACLE(tscf)# tscf-interface
ORACLE (tscf-interface)# select
<RealmID>:
1: access 172.168.31.99:7000
selection:  1
ACMEPACKET (tscf-interface)# assigned-services inter-client-block
```

Note: In order to add **inter-client-block** to an existing list of assigned services, ensure that each service attribute is delimited by a comma. Example: SIP,STG,inter-client-block.

show platform

Syntax

```
show platform <all | cpu | cpu-load | errors | heap-statistics | kernel-
drivers | limits | memory | paths | pci>
```

The show platform command is useful for distinguishing various hardware and software configurations for the current version of software from other hardware platform on which this software may run.

Arguments

- all—Display full platform information
- cpu—Display summary CPU information
- cpu-load—Display current CPU load
- errors—Display Servicepipe write errors
- heap-statistics—Display total in-use memory for small allocations based upon TCMalloc's small allocation class sizes.
- kernel-drivers—Display included kernel drivers
- limits—Display platform related limits
- memory—Display current memory usage
- paths—Display filesystem paths
- pci—Display relevant pci bus information

Note: No argument concatenates all arguments.

3

SCZ730M3

This section provides descriptions, explanations, and configuration information for the contents of Maintenance Release SCZ7.3.0M3. Maintenance Release content supercedes that distributed with the point release.

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
- C3.1.7

Current patch baseline: SCZ7.3.0m2p5

Please refer to the *Oracle® Communications Session Border Controller & Session Router Release Notes*, Release S-CZ7.3.0 for changes to the Known Issues section based on the S-CZ7.3.0M2 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-CZ7.3.0M3:

- SCZ7.2.0m6p9

Upgrade Caveats

Acme Packet 4500/3820 with Transcoding Hardware

The S-CZ7.3.0M3 software update includes a firmware update for transcoding modules. If your system includes transcoding hardware, be aware that the initial upgrade to this release will likely require additional time to complete, which increases with the number of TCMs in your system. The additional time for the upgrade will likely cause the online upgrade process to time out when the standby system proceeds to a fully synchronized state. There are two ways to proceed if you are exposed to this situation:

1. After you reboot the standby with S-CZ7.3.0M3 for the first time, the system will likely time-out and move into an out-of-service state. You should reboot the standby a second time. Since the first reboot upgrades the DSP firmware, the second reboot only needs to synchronize, and will properly assume the standby role.
2. Prior to switchover, configure the **system** > **redundancy** > **becoming-standby-time** parameter a value high enough to give extra time for the DSP upgrade and resynchronization to occur. Oracle recommends 12 minutes (720000 ms) for this parameter.

Acme Packet 6100/6300

The Acme Packet 6100 and Acme Packet 6300 are unsupported in the initial release of S-CZ7.3.0M3 due to a high availability (HA) issue. A fix will be available in a subsequent patch.

Concept Map

The following table identifies the new content in this SCZ7.3.0 M3 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.