Oracle® Communications Session Border Controller

Maintenance Release Guide
Release S-CX6.4.0
Formerly Net-Net Session Director

March 2015

ORACLE

Notices

Contents

Preface

About this guide

The S-CX6.4.0 Maintenance Release Guide provides information about the contents of maintenance releases related to release S-CX6.4.0. This information can be related to defect fixes, to adaptations made to the system software, and to adaptations ported to this release as forward merges. 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 release S-CX6.4.0, this document informs you of changes made to the software in the maintenance releases of S-CX6.4.0. Consult this document for content specific to maintenance releases. For information about general release 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-CX6.4.0 maintenance releases.

Mainenance release number	Availability Notes
S-CX6.4.0M1	June 14, 2013
S-CX6.4.0M2	July 22, 2013
S-CX6.4.0M3	September 12, 2013
S-CX6.4.0M4	February 14, 2014

Mainenance release number	Availability Notes
S-CX6.4.0M5	June 19, 2014
S-CX6.4.0M6	March 27, 2015

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 and Maintenance Guide	Contains information about the components and installation of the Acme Packet 4500 system.
Acme Packet 3820 Hardware Installation and Maintenance Guide	Contains information about the components and installation of the Acme Packet 3800 system.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the Oracle Communications Session Border Controller.
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 logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about support for the Administrative Security license.

1

S-CX6.4.0M1

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net OS Release S-CX6.4.0M1.

Current SPL Engine Version: C2.0.1

Current patch baseline:

Content Map

This section provides a table listing all content in Net-Net OS Release S-CX6.4.0M1.

Content Type	Description
Forward Merge	S-CX6.3.0M4
Adaptation	DDoS Protection fromdevices behind a NAT
Adaptation	AF-Application-Identifier AVP support
Adaptation	Authenticated NTP
Adaptation	SDP Alternate Connectivity - IPV6/IPV4 Dual offer support
Adaptation	IPv6 support for static flow
Adaptation	LRT Limitations
Defect	Latching and stream mode set to inactive

DDoS Protection from Devices Behind a NAT

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

Restricting the Number of Endpoints behind a NAT

Each new source IP address and source IP port combination now counts as an endpoint for a particular NAT device. After the configured value of a single NAT's endpoints is reached, subsequent messages from behind that NAT are dropped and the NAT is demoted. This is set with the max-endpoints-per-nat parameter located in both the access-control and realm-config configuration elements.

Counting Invalid Messages from Endpoints behind a NAT

The Oracle Communications Session Border Controller also counts the number of invalid messages sent from endpoints behind the NAT. Once a threshold is reached, that NAT is demoted. Numerous conditions are counted as Errors/Invalid Messages from an endpoint. The aggregate of all messages from endpoints behind the NAT are counted against the NAT device, in addition to the existing count against the endpoint. This threshold is set with the nat-invalid-message-threshold parameter located in both the access-control and realm-config configuration elements.

As a unique case, the absence of a REGISTER message following a 401 response is counted as an invalid message from the end point. And if that endpoint is behind a NAT, this scenario will be counted as invalid message from that NAT device as well. You set a timeout period in which the REGISTER message must arrive at the Oracle Communications Session Border Controller. This period is set with the wait-time-for-invalid-register parameter located in the realm config.

DDoS Protection Configuration realm-config

To set the DDoS Protection from devices behind NATs in the realm-config:

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. max-endpoints-per-nat— Set the maximum number of endpoints that can exist behind a NAT before demoting the NAT device. Valid values are 0-65535, with 0 disabling this feature. This parameter is also found in the access control configuration element.
4. nat-invalid-message-threshold—Set the maximum number of invalid messages that may originate behind a NAT before demoting the NAT device. Valid values are 0-65535, with 0 disabling this feature. This parameter is also found in the access control configuration element.
5. wait-time-for-invalid-register—Set the period (in seconds) that the Oracle Communications Session Border Controller counts before considering the absence of the REGISTER message as an invalid message.
6. Type **done** to save your configuration.

DDoS Protection Configuration access-control

To set the DDoS Protection from devices behind NATs in the access-control configuration element:

1. Access the access-control configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# access-control
ORACLE(access-control)#
```

2. Type select to choose and configure an existing object.

```
ORACLE(access-control)# select
<src-ip>:
1: src 0.0.0.0; 0.0.0.0; realm01; ; ALL
selection:1
```

3. max-endpoints-per-nat— Set the maximum number of endpoints that can exist behind a NAT before demoting the NAT device. Valid values are 0-65535, with 0 disabling this feature. This parameter is also found in the access control configuration element.
4. nat-invalid-message-threshold—Set the maximum number of invalid messages that may originate behind a NAT before demoting the NAT device. Valid values are 0-65535, with 0 disabling this feature. This parameter is also found in the access control configuration element.
5. Type done to save your work and continue.

SNMP Trap support

The following trap is sent by the Oracle Communications Session Border Controller whenever a NAT device is blacklisted due to the triggers listed in this feature. Reasons are not included in the trap, but are available from the syslogs.

```
apSysMgmtExpDOSTrap     NOTIFICATION-TYPE
        OBJECTS         { apSysMgmtDOSIpAddress,  apSysMgmtDOSRealmID ,
                          apSysMgmtDOSFromUri }
        STATUS          deprecated
        DESCRIPTION
              "This trap is generated when an IP is placed on a deny list due
              to denial-of-service attempts, and provides the ip address that
              has been demoted, the realm-id of that IP, and (if available)
              the URI portion of the SIP From header of the message that
              caused the demotion."
        ::= { apSysMgmtDOSNotifications 2 }
```

Ensure that the enable-snmp-monitor-traps parameter in the system-config configuration element is enabled for the Oracle Communications Session Border Controller to send out this trap.

Syslog Support

Set the syslog-on-demote-to-deny parameter in the media-manager-config to enabled to generate syslog on endpoint demotion from untrusted to deny. NAT device demotion will also generate a unique syslog message with accompanying text explaining that it is the NAT device demotion event.

Debugging

The show sip acl command now includes counts of Blocked NAT devices.

```
ACMEPACKET# show sipd acl
13:57:28-71
SIP ACL Status            -- Period -- -------- Lifetime --------
                Active    High   Total       Total  PerMax    High
Total Entries        0       0       0           0       0       0
Trusted              0       0       0           0       0       0
Blocked              0       0       0           0       0       0
Blocked NATs         0       0       0           0       0       0
ACL Operations          ---- Lifetime ----
                Recent      Total  PerMax
ACL Requests         0          0       0
Bad Messages         0          0       0
Promotions           0          0       0
Demotions            0          0       0
Trust->Untrust       0          0       0
Untrust->Deny        0          0       0
```

AF-Application-Identifier AVP Generation

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

The Oracle Communications Session Border Controller can populate the AF-Application-Identifier AVP with the IMS Communication Service Identifier (ICSI). 3GPP TS 24.173 defines the ICSI format as:

urn:urn-xxx:3gppservice.ims.icsi.mmtel

An ICSI appears in one of the following three SIP headers in an INVITE:

- P-Assured-Service
- P-Preferred-Service
- Accept-Contact

This AF-Application-Identifier AVP is inserted into an AAR and sent to the PCRF when the Oracle Communications Session Border Controller (as P-CSCF) receives an INVITE.

When the Oracle Communications Session Border Controller has an ICSI value from the access UE and the core, it uses the value received from the core. ICSI values received from the network supercede a configured default ICSI value. When the INVITE is received from the access side, ICSI values are taken from the access side until values are received from the core side. If no valid ICSI value is received in a message, and the Oracle Communications Session Border Controller is not configured with a default-icsi value, the external policy server object's hostname is used for the ICSI value sent to the PCRF. If an INVITE does not contain SDP, no AAR is generated.

AF-Application-Identifier AVP generation occurs for access and core initiated calls.

AVP Generation on Initial INVITE from UE

The Oracle Communications Session Border Controller receives the UE's INVITE. When configured to send an AAR on receipt of the INVITE, the AF-Application-Identifier AVP is populated with the contents of one of the following headers (in order of precedence) if present:

- P-Assured-Service (this header is only expected from trusted UEs)
- P-Preferred-Service
- Accept-Contact

If none of the above three headers are present, the default value of AF-Application-Identifier shall be used.

If the Oracle Communications Session Border Controller is not configured to send an AAR on receipt of an INVITE, the value from the 3 headers will be cached for later AF-Application-Identifier generation.

AVP Generation on response to Initial INVITE from UE

The Oracle Communications Session Border Controller receives the response (1xx or 200 OK) to the original INVITE. When configured to send an AAR on receipt of the response, the AF-Application-Identifier AVP is populated with the contents of one of the following headers (in order of precedence) if present:

- P-Assured-Service
- P-Preferred-Service
- Accept-Contact header is not expected

Values obtained in this step supercede any value set from the initial INVITE step. If none of the three headers are present, the value determined in the INITIAL invite step is used for the AF-Application-Identifier AVP contents.

AVP generation on reINVITE from UE

The Oracle Communications Session Border Controller can receive a re-INVITEs from the core. The Oracle Communications Session Border Controller populates the AF-Application-Identifier AVP with one of the following headers (in order of precedence) if present:

- P-Assured-Service (this header is only expected from trusted UEs)
- P-Preferred-Service
- Accept-Contact

If none of the three headers are present, the default AF-Application-Identifier value is used.

Responses to the Re-Invites will be treated in the similar manner.

Examples

Example 1:

Received from access UE	Received from core	Sent to PCRF
INVITE with SDP P-A-S, P-P-S, or A-C header contains “P1”		AAR with AF-A-I AVP contains “P1”
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P2”	AAR with AF-A-I AVP contains “P2”
re-INVITE with SDP P-A-S, P-P-S, or A-C header contains “P3”		AAR with AF-A-I AVP contains “P2”
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P4”	AAR with AF-A-I AVP contains “P4”

Example 2:

Received from access UE	Received from core	Sent to PCRF
INVITE with no SDP		No AAR generated
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P2”	AAR with AF-A-I AVP contains “P2”
re-INVITE with SDP P-A-S, P-P-S, or A-C header contains “P3”		AAR with AF-A-I AVP contains “P2”
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P4”	AAR with AF-A-I AVP contains “P4”

Example 3:

Received from access UE	Received from core	Sent to PCRF
INVITE with no SDP		No AAR generated

Received from access UE	Received from core	Sent to PCRF
	200 OK with SDP No P-A-S, P-P-S, or A-C headers	AAR with AF-A-I AVP contains default AF-A-I value.
re-INVITE with SDP P-A-S, P-P-S, or A-C header contains “P3”		AAR with AF-A-I AVP contains “P3”
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P4”	AAR with AF-A-I AVP contains “P4”

Example 4:

Received from access UE	Received from core	Sent to PCRF
INVITE with SDP P-A-S, P-P-S, or A-C header contains “P1”		AAR with AF-A-I AVP contains “P1”
	200 OK with no SDP	AAR with AF-A-I AVP contains “P1”
re-INVITE with SDP P-A-S, P-P-S, or A-C header contains “P3”		AAR with AF-A-I AVP contains “P1”
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P4”	AAR with AF-A-I AVP contains “P4”

Example 5:

Received from access UE	Received from core	Sent to PCRF
INVITE with no SDP		No AAR generated
	183 with SDP No P-A-S, P-P-S, or A-C headers	AAR with AF-A-I AVP contains ext-policy-server’s “hostname”
PRACK with SDP P-A-S, P-P-S, or A-C header contains “P1”		AAR with AF-A-I AVP contains “P1”
	200 OK with no SDP	No AAR generated
	200 OK (INVITE) with SDP P-A-S, P-P-S, or A-C header contains “P4”	AAR with AF-A-I AVP contains “P4”

Example 6:

Received from access UE	Received from core	Sent to PCRF
INVITE with SDP P-A-S, P-P-S, or A-C header contains “P1”		AAR with AF-A-I AVP contains “P1”
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P2”	AAR with AF-A-I AVP contains “P2”
	re-INVITE with SDP P-A-S, P-P-S, or A-C header contains “P3”	AAR with AF-A-I AVP contains “P3”
200 OK with SDP P-A-S, P-P-S, or A-C header contains “P4”		AAR with AF-A-I AVP contains “P3”

AVP Generation on Initial INVITE from core

The Oracle Communications Session Border Controller receives the original INVITE. When configured to send an AAR on receipt of the INVITE, the AF-Application-Identifier AVP is populated with the contents of one of the following headers (in order of precedence) if present:

- P-Assured-Service
- P-Preferred-Service
- Accept-Contact

If none of the above three headers are present, the default value of AF-Application-Identifier shall be used.

If the Oracle Communications Session Border Controller is not configured to send an AAR on receipt of an INVITE, the value from the 3 headers will be cached for later AF-Application-Identifier generation.

AVP Generation on response to initial INVITE from core

The Oracle Communications Session Border Controller receives the response (1xx or 200 OK) to the original INVITE. When configured to send an AAR on receipt of the response, if none of the three headers (P-Assured-Service, P-Preferred-Service, or Accept-Contact) were present in the original INVITE, the Oracle Communications Session Border Controller populates the AF-Application-Identifier AVP with the contents of one of the following headers (in order of precedence) if present:

- P-Assured-Service (this header is only expected from trusted UEs)
- P-Preferred-Service
- Accept-Contact header is not expected

If none of the three headers are present, the value determined in the INITIAL invite step is used for the AF-Application-Identifier AVP contents.

AVP generation on reINVITE from core

The Oracle Communications Session Border Controller can receive re-INVITEs from the core. The Oracle Communications Session Border Controller populates the AF-Application-Identifier AVP with one of the following headers (in order of precedence) if present:

- P-Assured-Service (this header is only expected from trusted UEs)
- P-Preferred-Service
- Accept-Contact

If none of the three headers are present, the default AF-Application-Identifier value is used.

Responses to the Re-Invites will be treated in the similar manner.

Example 1:

Received from core	Received from access UE	Sent to PCRF
INVITE with SDP P-A-S, P-P-S, or A-C header contains “P1”		AAR with AF-A-I AVP contains “P1”
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P2”	AAR with AF-A-I AVP contains “P1”
re-INVITE with SDP P-A-S, P-P-S, or A-C header contains “P3”		AAR with AF-A-I AVP contains “P3”
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P4”	AAR with AF-A-I AVP contains “P3”

Example 2:

Received from core	Received from access UE	Sent to PCRF
INVITE with no SDP		No AAR generated
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P2”	AAR with AF-A-I AVP contains “P2”
re-INVITE with SDP P-A-S, P-P-S, or A-C header contains “P3”		AAR with AF-A-I AVP contains “P3”
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P4”	AAR with AF-A-I AVP contains “P3”

Example 3:

Received from core	Received from access UE	Sent to PCRF
INVITE with no SDP		No AAR generated
	200 OK with SDP No P-A-S, P-P-S, or A-C headers	AAR with AF-A-I AVP contains ext-policy-server hostname.
re-INVITE with SDP P-A-S, P-P-S, or A-C header contains “P3”		AAR with AF-A-I AVP contains “P3”

Received from core	Received from access UE	Sent to PCRF
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P4”	AAR with AF-A-I AVP contains “P3”

Example 4:

Received from core	Received from access UE	Sent to PCRF
INVITE with SDP P-A-S, P-P-S, or A-C header contains “P1”		AAR with AF-A-I AVP contains “P1”
	200 OK with no SDP	AAR with AF-A-I AVP contains “P1”
re-INVITE with SDP P-A-S, P-P-S, or A-C header contains “P3”		AAR with AF-A-I AVP contains “P3”
	200 OK with SDP P-A-S, P-P-S, or A-C header contains “P4”	AAR with AF-A-I AVP contains “P3”

Example 5:

Received from core	Received from access UE	Sent to PCRF
INVITE with no SDP		No AAR generated
	183 with SDP No P-A-S, P-P-S, or A-C headers	AAR with AF-A-I AVP contains ext-policy-server’s “hostname”
PRACK with SDP P-A-S, P-P-S, or A-C header contains “P1”		AAR with AF-A-I AVP contains “P1”
	200 OK with no SDP	No AAR generated
	200 OK (INVITE) with SDP P-A-S, P-P-S, or A-C header contains “P4”	AAR with AF-A-I AVP contains “P1”

Example 6:

Received from core	Received from access UE	Sent to PCRF
INVITE with SDP P-A-S, P-P-S, or A-C header contains “P1”		AAR with AF-A-I AVP contains “P1”
	200 OK with SDP	AAR with AF-A-I AVP contains “P1”

Received from core	Received from access UE	Sent to PCRF
	P-A-S, P-P-S, or A-C header contains “P2”	
	re-INVITE with SDP P-A-S, P-P-S, or A-C header contains “P3”	AAR with AF-A-I AVP contains “P1”
200 OK with SDP P-A-S, P-P-S, or A-C header contains “P4”		AAR with AF-A-I AVP contains “P4”

Authenticated NTP

The Oracle Communications Session Border Controller can authenticate NTP server requests using MD5. The configured MD5 keys are encrypted and obscured in the ACLI. You configure an authenticated NTP server with its IP address, authentication key, and the key ID. Corresponding key and key IDs are provided by the NTP server administrator.

To configure an authenticated NTP server:

1. Access the ntp-config configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# ntp-sync
ACMEPACKET(ntp-config)#
```

2. Type select.

```
ORACLE(ntp-config)# select
```

3. Access the auth-servers configuration element

```
ORACLE(ntp-config)# auth-servers
ORACLE(auth-servers)#
```

4. ip-address — Enter the IP address of the NTP server that supports authentication.
5. key-id — Enter the key ID of the key you enter in the next step. This value’s range is 1 - 999999999.
6. key — Enter the key used to secure the NTP requests. The key is a string 1 - 31 characters in length.
7. Type done to save your work.
8. Type exit to return to the previous configuration level.
9. Type done to save the parent configuration element.

SDP Alternate Connectivity

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

Each realm on the Oracle Communications Session Border Controller can be configured with an alternate family realm on which to receive media in the alt family realm parameter in the realm config. As deployed, one realm will be IPv4, and the alternate will be IPv6. The Oracle Communications Session Border Controller creates the outbound INVITE with IPv4 and IPv6 addresses to accept the media, each in an a=altc: line and each in its own realm. The IP addresses inserted into the a=altc: line are from the egress realm’s and alt-realm-family realm’s steering pools. Observe in the image how the red lines indicate the complementary, alternate realms.

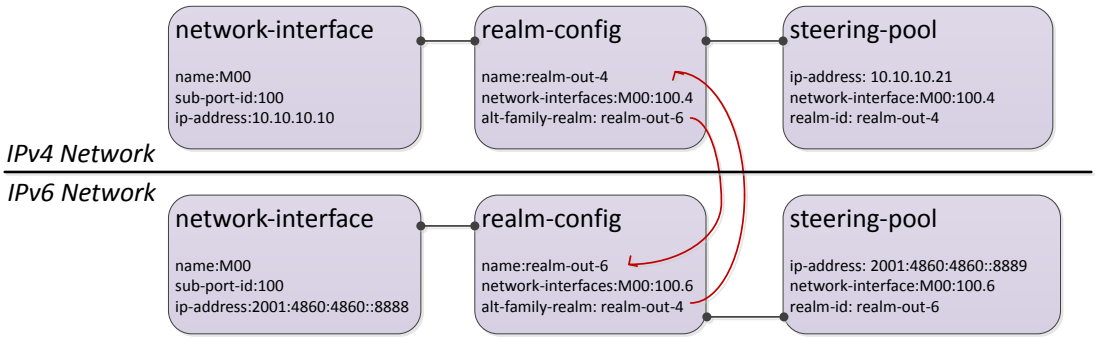
You can configure the order in which the a=altc: lines appear in the SDP in the pref-address-type parameter in the realm-config. This parameter can be set to

- IPv4 - SDP contains the IPv4 address first
- IPv6 - SDP contains the IPv6 address first
- NONE - SDP contains the native address family of the egress realm first

In the 200OK to the INVITE, the callee chooses either the IPv6 or IPv4 address to use for the call's media transport between itself and Oracle Communications Session Border Controller. After the Oracle Communications Session Border Controller receives the 200OK, the chosen flow is installed, and the unused socket is discarded.

For two realms from different address families to share the same physical interface and vlan, you use a .4 or .6 tag in the network-interface reference. When IPv4 and IPv6 realms share the same network-interface and VLAN, you identify them by realm name and network-interface configured as:

- IPv4 - <phy-interface>:<vlan>.4
- IPv6 - <phy-interface>:<vlan>.6



If the INVITE's egress realm is IPv6, pref-address-type = NONE, the outbound SDP has these a=altc: lines:

```
a=altc:1 IPv6 2001:4860:4860::8889 20001
a=altc:2 IPv4 10.10.10.21 20001
```

If the INVITE's egress realm is IPv6, pref-address-type = IPv4, the outbound SDP has these a=altc: lines:

```
a=altc:1 IPv4 10.10.10.21 20001
a=altc:2 IPv6 2001:4860:4860::8889 20001
```

SDP Alternate connectivity supports B2B and hairpin call scenarios. SDP Alternate connectivity also supports singleterm, B2B, and hairpin call scenarios.

When providing SDP alternate connectivity for SRTP traffic, in the security policy configuration element, the network-interface parameter's value must be configured with a .4 or .6 suffix to indicate IPv4 or IPv6 network, respectively.

SDP Alternate Connectivity Configuration

To configure SDP alternate connectivity:

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. alt-realm-family — Enter the realm name of the alternate realm, from which to use an IP address in the other address family. If this parameter is within an IPv4 realm configuration, you will enter an IPv6 realm name.
4. pref-address-type — Set the order in which the a=altc: lines suggest preference. Valid values are:
   - none — address family type of egress realm signaling
   - ipv4 — IPv4 realm/address first
   - ipv6 — IPv6 realm/address first
5. Type **done** to save your configuration.

BG RTP Flow Installed When mode=inactive

By default, the Oracle Communications Session Border Controller does not install an RTP flow for H.248 calls that contain SDP mode =inactive. H.248.37 indicates that when call is signaled with sdp mode= inactive, both RTP and RTCP flows should be installed. To explicitly set the system to install both flows, add the install inactive nat flow option in the bgf config configuration element.

Prerequisites

To ensure individual flows are installed for RTP and RTCP, add the hnt-rtcp =enabled option in the media-manager-config. This ensures that nat-flows are installed as un-collapsed.

BG RTP Flow Configuration

To configure an RTP flow for H.248 calls with SDP = inactive:

1. Navigate to the sip-config configuration element.

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

2. Type select to begin configuring this object.

```
ORACLE(bgf-config)# select
```

3. options—Configure the install-inactive-nat-flow option:

```
ORACLE(bgf-config)# options +install-inactive-nat-flow
ORACLE(bgf-config)#
```

4. Save and activate your configuration.

LRT Limitations

S-CX6.4.0M1 removes the Oracle Communications Session Border Controller's limitation of loading a maximum of 40 LRT tables at boot time.

Current Oracle Communications Session Border Controller LRT performance:

- ~500 LRT tables can be loaded during boot time
- 100,000 entries per LRT file
- 2,000,000 LRT entries total per system

These capabilities are subject to the following constraints:

- The Oracle Communications Session Border Controller can not be configured with ~500 LRT files each with 100,000 entries.
- Actual performance that affects the interaction among the three performance attributes varies with system memory and configuration.

2

S-CX6.4.0M2

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net OS Release S-CX6.4.0M2.

Current SPL Engine Version: C2.0.1

Current patch baseline: 640m1p1

Content Map

This section provides a table listing all content in Release S-CX6.4.0M2.

Content Type	Description
Defect	RCSe TLS/TCP Re-use Connections
Hardware Support	The ETC2 NIU is fully supported in this release (no documentation required)

RCSe TLS/TCP Re-Use Connections

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

Field experience uncovered an implementation deficiency associated with these persistent connections particularly within RCSe deployments. The basic scenario is as follows:

1. The UE registers in a TLS realm on SBC1. SBC1 stores the IP:Port from VIA (and Contact) as alias of the currently established connection.
2. The UE transits to another realm/sip-port (same or different Oracle Communications Session Border Controller) without previously unregistering or closing the TCP connection with the TLS sip-port on SBC1.
3. UE goes back to the TLS realm in SBC1 and establishes a new connection — same source IP as in Step 1, but a different port as in Step 1.

The problem arises at Step 3. If the Oracle Communications Session Border Controller has not detected that the TLS connection established in Step 1 has been effectively terminated, it will not update the alias connection to that established in Step 3, but instead continue to attempt to use the Step 1 connection.

This means that the next message from the core side to the UE will fail, since the Oracle Communications Session Border Controller will attempt to send the message of the dead TLS connection — that is using the IP address:port pair passed in Step 1.

All communications to this UE will fail until it sends the next message to the Oracle Communications Session Border Controller, when the alias connection will be update to the TLS connection in Step 3.

To resolve this issue, the Oracle Communications Session Border Controller needs to always update the alias table when it receives a new inbound connection on the configured sip-interface.

Option Configuration Guidelines

The following table lists the full range of options that pertain to TLS/TCP Connection reuse with an emphasis on use in RCSe environments

Option	Connection Behavior
reuse-connections	Use/retain first inbound connection until explicitly closed
reuse-connections=latest	Use the last inbound connection, update the alias for each new connection
reuse-connections=no	Establish new connection at each UE access
NOT CONFIGURED	Equivalent to reuse-connections=no

RCSE TLS/TCP Re-Use Connections Configuration

To configure the reuse-connections option:

1. From Superuser mode, use the following command sequence to navigate to the sip-interface configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# sip-config
ORACLE(sip-config)# sip-interface
ORACLE(sip-interface)# option reuse-connections=latest
ORACLE(sip-interface)#
```

2. Use done, exit, and verify-config to complete configuration.

3

S-CX6.4.0M3

This chapter provides descriptions, explanations, and configuration information for the contents of Net-Net OS Release S-CX6.4.0M3.

Current SPL Engine Version: C2.0.1

Current patch baseline: S-CX640m2p1

Content Map for S-CX6.4.0M3

This section provides a table listing all content in Release S-CX6.4.0M3.

Content Type	Description
Adaptation	DSCP Byte QoS Markings for DNS and ENUM

Differentiated Services for DNS and ENUM

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

Certain service providers mandate support for Differentiated Services (DS) on all traffic streams exiting any network element. This mandate requires that network elements function as a DS marker — that is as a device that sets the Distributed Services Codepoint (DSCP) in the Differentiated Services field of the IP header.

Previous software releases provided the capabilities to mark standard SIP and Real-Time Protocol (RTP) messages. Release S-CX6.4.0M3 adds the capability to mark DNS and ENUM queries.

For basic information about DS, refer to:

- The Net-Net S-CX6.4.0 4000 ACLI Configuration Guide (Realm-Based Packet Marking in Realms and Nested Realms), which provides information on currently supported DS marking of SIP and RTP packets
- *IETF RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* (http://www.ietf.org/rfc/rfc2474.txt)
- *IETF RFC 2475, An Architecture for Differentiated Services* (*http://www.ietf.org/rfc/rfc2475.txt*).

DS provides a mechanism to define and deliver multiple and unique service classifications that can be offered by a service provider. Specific service classifications are identified by a DSCP, essentially a numeric index. The DSCP

maps to a per-hop-behavior (PHB) that defines an associated service class. PHBs are generally defined in terms of call admission controls, packet drop criteria, and queue admission algorithms. In theory, DS supports 64 distinct classifications. In practice, however, network offerings generally consist of a much smaller suite, which typically includes:

- Default PHB - required best effort service — defined in RFC 2474
- Expedited Forwarding (EF) PHB - low-loss, low-latency — defined in RFC 3246, An Expedited Forwarding PHB
- Assured Forwarding (AF) PHB - assured delivery within subscriber limits — defined in *RFC 2597, Assured Forwarding PHB Group*, and *RFC 3260, New Terminology and Clarifications for Diffserv*
- Class Selector PHBs - maintain compatibility with previous TOS (type of service) precedence usage — defined in RFC 2474

Marking of DNS and ENUM queries requires the creation of a Differentiated Services media policy, and the assignment of such a policy to a specific realm.

Differentiated Services for DNS and ENUM Configuration

To create a Differentiated Services media policy:

1. From Superuser mode, use the following ACLI command sequence to move to media-policy configuration mode.

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

2. Use the required name parameter to provide a unique identifier for this media-policy instance.

```
ORACLE(media-policy)# name diffServeDnsEnum
ORACLE(media-policy)#
```

3. Use the tos-settings command to move to tos-settings configuration mode.

```
ORACLE(media-policy)# tos-settings
ORACLE(tos-settings)#
```

4. Use the required media-type parameter to identify the packet-type subject to Diffentiated Services marking.

   For DNS/ENUM packets, use message/dns.

```
ORACLE(tos-settings)# media-type message/dns
ORACLE(tos-settings)#
```

5. Use the required tos-value parameter to specify the 6-bit DSCP to be included in the Differentiated Services field of the IP header.

   Specify the DSCP as an integer (within the range from 0 to 63). The DSCP can be expressed in either decimal or hexadecimal format.

```
ORACLE(tos-settings)# tos-value 0x30
ORACLE(tos-settings)#
```

6. Other displayed parameters, media-attributes and media-sub-type, can be safely ignored.
7. Use the done and exit commands to complete Differentiated Services media policy configuration and return to media-policy configuration-mode.

```
ORACLE(tos-settings)# done
tos-settings
        media-type                  message/dns
        media-sub-type
        tos-value                   0x30
        media-attributes
ORACLE(tos-settings)# exit
ORACLE(media-policy)#
```

8. If necessary, repeat steps 2 through 7 to create additional Differentiated Services media policies.
9. Assign this media policy to the target realm via the media-policy parameter in a realm-config object.

4

S-CX6.4.0M4

This chapter provides descriptions, explanations, and configuration information for the contents of Release S-CX6.4.0M4.

Current SPL Engine Version: C2.2.0

Current patch baseline: S-CX640M3p3

Content Map for S-CX6.4.0M4

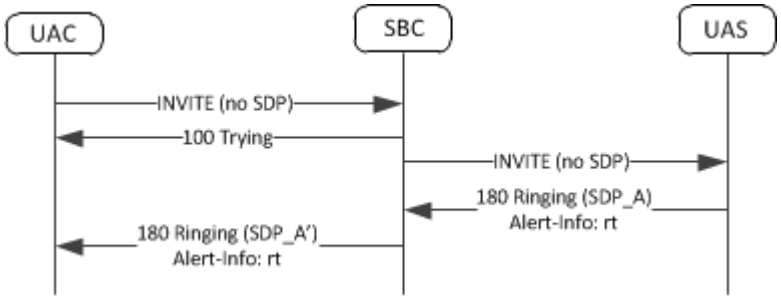
This section provides a table listing all content in Release S-CX6.4.0M4.

Content Type	Description
Adaptation	LMSD Offerless Invite Handling
Adaptation	DNS-SRV Session Agent Recursion Error Handling
Adaptation	Configurable DNS Response Size

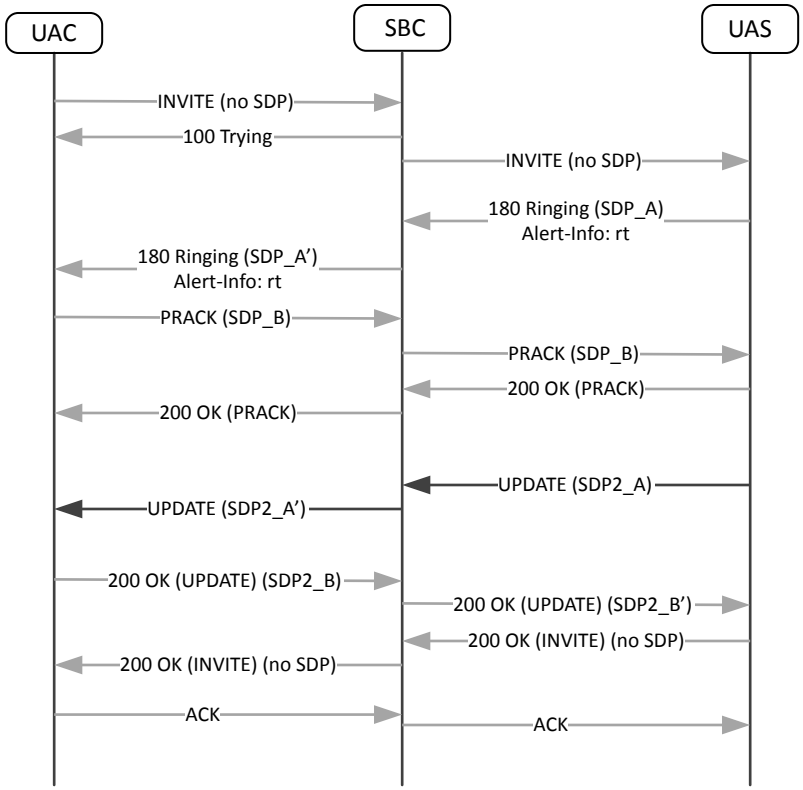
LMSD Offerless INVITE handling

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

When LMSD Interworking is configured on a SIP interface, and when the UAS includes SDP in the 180 Ringing message (and the Alert-Info header is set to rt), the Oracle Communications Session Border Controller no longer strips the SDP when forwarding the 180 back to the UAC.



When LMSD interworking is configured on a SIP interface, and in the case that an early dialog has been established (a dialog where the final 2xx class response to INVITE request has not yet arrived), some call flows include an UPDATE later in the call. The Oracle Communications Session Border Controller now forwards the Update message, SDP included, directly to the UAC, whereas before it responded to the UAS's UPDATE locally.

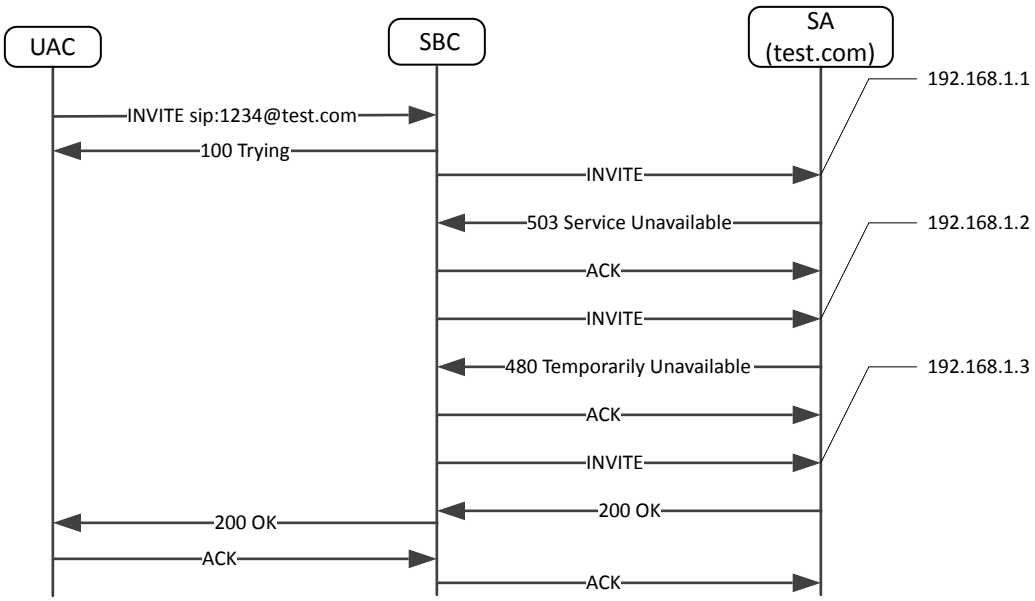


DNS-SRV Session Agent Recursion Error Handling

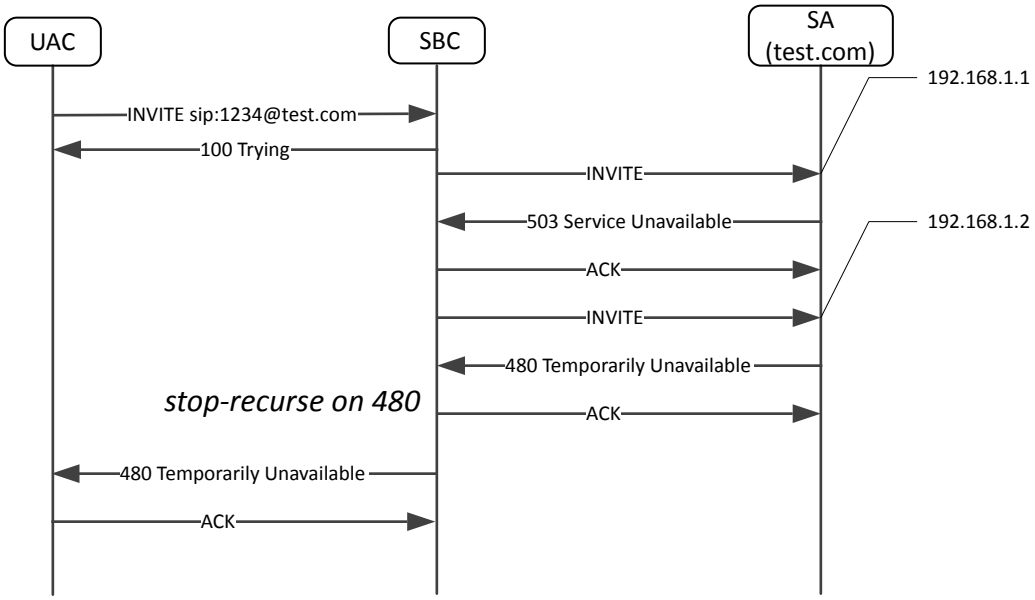
When a session request is sent from the Oracle Communications Session Border Controller to a session agent, and an error response is received (or a transport failure occurs), the Oracle Communications Session Border Controller attempts to reroute the message through the list of dynamically resolved IP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

This feature concerns the case when a session agent is configured with an FQDN in the hostname parameter and the **dns-load-balance** or **ping-all-addresses** option is configured. This configuration sets up the load balancing / redundancy behavior for the SBC to use all addresses returned in the SRV/A-record for that session agent. In previous versions of the SBC software, only when a 503 failure from the SA was received would the SBC resend the session request to the next dynamically resolved IP address (on the SRV/A record list).

By adding the **recurse-on-all-failures** option to a session agent, the Oracle Communications Session Border Controller will resend a session request to the next address on the list after a 4xx or 5xx failure response has been received from a session agent.



If the SBC receives a failure response from the session agent, and the number of that failure is configured in the **stop-recurse** parameter, no further session requests will be forwarded to additional addresses from the SRV/A record list. The error message will be forwarded back to the UA.



Configurable DNS Response Size

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

This functionality is useful when large numbers of SRV records will be returned in a DNS query thereby eliciting a large-sized DNS response. This behavior should be configured on the realm where the DNS servers are located.

To extend the valid DNS response size, add the **dns-max-response-size** option to the realm configuration. If this option is not configured, the Oracle Communications Session Border Controller uses the default maximum response size of 512 bytes, and information past the 512th byte will be ignored.

Do not add the **dns-max-response-size** option to realms where DNS queries are not being performed. Ensure that the realm where this option is configured is referenced in a transport realm's **dns-realm** parameter. Only the local value of the **dns-max-response-size** option is used for the realm; there is no inheritance of this value.

DNS Response Size 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. Add the **dns-max-response-size** option to the realm with a value between 513 — 65535.

```
ORACLE(realm-config)#options dns-max-response-size=4196
```

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

5

S-CX6.4.0M5

This chapter provides descriptions, explanations, and configuration information for the contents of Release S-CX6.4.0M5.

Current SPL Engine Version: C2.0.0, C2.0.1, C2.02

Current patch baseline: S-CX640M4p1

Content Map for S-CX6.4.0M5

This section provides a table listing all content in Release S-CX6.4.0M5.

Content Type	Description
-	No new content.

6

S-CX6.4.0M6

This chapter provides descriptions, explanations, and configuration information for the contents of Release S-CX6.4.0M6.

- Current SPL Engine Version: C2.0.0, C2.0.1, C2.0.2, C2.2.0, C2.2.1, C2.3.0
- Current patch baseline: S-CX640M5p6

Content Map for S-CX6.4.0M6

The following table classifies and lists the new content in this release.

Content Type	Description
Library Update	OpenSSL upgrade to 1.0.0(o)
Adaptation	Minimum Advertised SSL/TLS Version
Adaptation	SNMP Reporting of Message Rate Statistics
Adaptation / Behavioral Change	ifDesc object values are updated

Minimum Advertised SSL/TLS Version

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

Oracle Communications Session Border Controller uses OpenSSL in its SSL/TLS connections. Due to at least one vulnerability, the Poodle attack (CVE-2014-3566), SSLv3 is deemed insecure. Oracle Global Product Security (GPS) suggests that SSLv3 be disabled by default. Setting the option **sslmin** advertises the minimum version the server supports. Should you have SSLv3 set as the **tls-version** in any **tls-profile**, you will need to set **sslmin** to that version, if configured. It would be a configuration error if **sslmin** is greater than the **tls-version** value in any **tls-profile**.

Note: Note: The next SSL/TLS version after SSLv3 is TLS1.0.

In **security-config**, the **sslmin** option values can be: sslv3, tls1.0 or tls1.1. This change is platform-independent and applies to all Oracle Communications Session Border Controller.

Minimum Advertised SSL/TLS Version Configuration

Configuring the option **sslmin** to at least tls1.0 for security purposes, provided no **tls-version** in a **tls-profile** requires SSLv3.

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

```
ORACLE# configure terminal
ORACLE(configure)# security
ORACLE(security)# security-config
ORACLE(security-config)#
```

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

```
ORACLE(security-config)#

ORACLE(security-config)#
```

3. **options**— Set the options parameter by typing **options**, a space, a plus sign, the option name **sslmin=** and then one of the valid values. Valid values are:

   - sslv3
   - tls1.0
   - tls1.1

```
ORACLE(security-config)#options +sslmin=sslv3
```

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

SNMP Reporting of Message Rate Statistics

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

Message rate statistics are available through four tables. These tables correspond to SIP Method message rate per SIP Interface, SIP Method message rate per SIP Agent, DNS ALG message rate, and ENUM server message rate. Ensure that the **extra-method-stats** parameter in the **sip-config** is enabled for the system to collect these statistics.

apSIPRateIntfStatsTable

This table, found in the Ap-sip.mib, provides a listing of SIP message rate statistics per SIP interface. It conveys the same information displayed in the show sipd rate interface command. The table is indexed by the SIP Interface index and SIP method. The SIP Interface to index number mapping is found in the apSipInterface table in Ap-sip.mib. The SIP method to index mapping is found in the ApSipMethod object in Ap-tc.mib.

```
<127:%>- snmpwalk -v 2c -c public 172.30.68.100 apSipRateIntfStatsTable
APSIP-MIB::apSipRateIntfMsgRcvd.21.other = Gauge32: 0 messages per 10 seconds
APSIP-MIB::apSipRateIntfMsgRcvd.21.invite = Gauge32: 0 messages per 10 seconds
```

apSIPRateAgentStatsTable

This table, found in the Ap-sip.mib, provides a listing of SIP message rate statistics per SIP agent (SIP session agent). It conveys the same information displayed in the show sipd rate agentcommand. The table is indexed by the SIP agent index and SIP method. The SIP Agent to index number mapping is found in the apSipAgent table in Ap-sip.mib. The SIP method to index mapping is found in the ApSipMethod object in Ap-tc.mib.

apDnsAlgServerRateStatsTable

This table, found in the Ap-dnsalg.mib, provides a listing of message rate statistics for a specific DNS Alg Server. It conveys the same information displayed in the show dnsalg rate realm-id and show dnsalg rate server-ip-addr commands. The table is indexed by the DNS ALG realm index, DNS ALG server index. The table of rate statistics also includes the DNS ALG server IP address and IP address type (IPv4 or IPv6). If a DNS ALG realm, DNS ALG

server, lf IP address are not configured, then the combination of those indices will return no data. The DNS ALG Server to index mapping is found in the apDnsAlgServerTable in the Ap-dnsalg.mib. The DNS ALG realm to index mapping is found in the apDnsAlgConfigTable in the Ap-dnsalg.mib.

```
-<%>- snmpwalk -v 2c -c public 172.30.68.100 apDnsAlgServerRateStatsTable
MIB::apDnsAlgServerInetAddressType.37.1.ipv4."2.2.2.2" = INTEGER: ipv4(1)
APDNSALG-MIB::apDnsAlgServerInetAddressType.38.1.ipv4."4.4.4.4" = INTEGER:
ipv4(1)
APDNSALG-MIB::apDnsAlgServerInetAddress.37.1.ipv4."2.2.2.2" = Hex-STRING: 02
02 02 02
APDNSALG-MIB::apDnsAlgServerInetAddress.38.1.ipv4."4.4.4.4" = Hex-STRING: 04
04 04 04
APDNSALG-MIB::apDnsAlgServerRateMsgRcvd.37.1.ipv4."2.2.2.2" = Gauge32: 0
messages per 10 seconds
```

apEnumServerRateStatsTable

This table, found in the Ap-apps.mib, provides a listing of ENUM message rate statistics for a specific ENUM server. It conveys the same information displayed in the show enum rate command. This table is indexed by the ENUM configuration name, ENUM Server IP address and IP address type (IPv4 or IPv6).

```
-<%>- snmpwalk -v 2c -c public 172.30.68.100 apEnumServerRateStatsTable
APAPPS-MIB::apEnumServerRateMsgRcvd."enumTest".ipv4."172.30.68.85" = Gauge32:
0 messages per 10 seconds
```

SNMP Reporting of Message Rate Statistics

The message rate statistics feature enables the Oracle Communications Session Border Controller to provide message rate statistics for SIP, DNS, and ENUM traffic via ACLI and HDR output. These statistics may also be retrieved via SNMP.

Message rate statistics are available through four tables. These tables correspond to SIP Method message rate per SIP Interface, SIP Method message rate per SIP Agent, DNS ALG message rate, and ENUM server message rate. Ensure that the following parameters are enabled for the type of statistics you wish to collect:

Statistic Type	configuration element	parameter
SIP Message Rate	sip-config	extra-method-stats
DNS Message Rate	media-manager > dns-config	extra-dnsalg-stats
ENUM Message Rate	sip-config	extra-enum-stats

Interface Description in MIB

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

RFC 3635 supercedes RFC 2665. RFC 2665 recommends, but RFC 3635 requires, that all Ethernet-like interfaces use an *ifType* of ethernetCsmacd (6) regardless of the speed that the interface is running or the link-layer encapsulation in use. Heretofore, Oracle Communications Session Border Controllers could return values of fastEthernet (62) and gigaEthernet (117), but, in accordance with RFC 3635, will now return ethernetCsmacd (6) for all Ethernet interface types. To let users determine the type of Ethernet interface more readily than by some other method, Oracle has changed the syntax for *ifDescr* to include the interface type.

The current values of *ifDescr* are either the names of physical or network interfaces (for example, "wancom0", "lo", "s1p0", "Access", or "Core"), or, for sub-interfaces, interface names appended with sub-interface numbers (for example, "Access.22" or "Core.33"). This change adds to the *ifDescr* string, separated from the first part by a space, a keyword that represents the internal interface type rather than the actual queried value. The current set of possible values is {ETH, FE, GE, XE, *null*}.

Examples:

- wancom0 GE
- lo (Second part empty)
- s1p0 GE
- s0p0 XE
- Access GE
- Access.22 (Second part empty)
- Core.33 (Second part empty)

7

S-CX6.4.0M7

This chapter provides descriptions, explanations, and configuration information for the contents of Release S-CX6.4.0M7.

- Current SPL Engine Version: C2.0.0, C2.0.1, C2.0.2, C2.2.0, C2.2.1, C2.3.0, C2.3.1
- Current patch baseline: S-CX640M6p2

S-CX6.4.0M7 Content Map

The following table classifies and lists the new content in this release.

Content Type	Description
Adaptation	Configurable DNS Maximum Time to Live
Adaptation	DNS Re-query over TCP

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.