Oracle® Communications Session Border Controller

Maintenance Release Guide
Release S-C[xz]6.3.9
Formerly Net-Net Session Director

December 2014

ORACLE

Notices

Contents

Preface

About this Guide

The S-CX6.3.9 Maintenance Release Guide provides information about the contents of maintenance releases related to release S-CX6.3.9. This information can be related to defect fixes, to adaptations made to the system software, and to adaptations ported to this release of the Acme Packet OS 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 release S-CX6.3.9, this document informs you of changes made to the software in the maintenance releases of S-CX6.3.9. 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-CX6.3.9 maintenance releases.

Maintenance release number	Availability Notes
S-CX6.3.9M1	November 26, 2012
S-CX6.3.9M2	December 31, 2012
S-CX6.3.9M3	August 30, 2013
S-CX6.3.9M4	January 28, 2014

Maintenance release number	Availability Notes
S-CX6.3.9M5	December 18, 2014

Related Documentation

The following table lists the members that comprise the documentation set for this release:

Document Name	Document Description
Acme Packet 4500 System Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4500 system.
Acme Packet 3800 Hardware Installation 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 SBC.
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 Net-Net SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), 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 SBC's accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the SBC's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the SBC's support for its Administrative Security license.

Revision History

Date	Revision Number	Description
S-C[xz]6.3.9M1		
November 26, 2012	Revision 1.00	Software for the Service Provider and Enterprise platforms: Server Edition, VM Edition, and Oracle Hardware Edition. Features include: - Communications Monitoring Probe performance improvements - SIP Monitor & Trace (SMT) performand and functionality improvements
February 14, 2013	Revision 1.01	Added a limitation section to this release note.
S-C[xz]6.3.9M2		

Date	Revision Number	Description
December 31, 2012	Revision 1.01	Software for the Service Provider and Enterprise platforms: Server Edition, VM Edition, and Oracle Hardware Edition. Features include: Addition of the Personal Profile Manager (PPM) web service support as part of Avaya Aura Session Manager and Aura System Manager. SIPREC update feature Bug fixes for the suppression of SIP messages that are not necessary.
March 8, 2013	Revision 1.02	Software for the Service Provider and Enterprise platforms: Server Edition, VM Edition, and Oracle Hardware Edition. Features include: Addition of a limitation section to this guide. Addition of Personal Profile Manager (PPM) proxy support Addition of SIPREC Ping support Addition of SIPREC Sends Update Message support Addition of SIPREC Re-INVITE Collision and Back-off Support
July 9, 2013	Revision 1.03	Combined S-C[xz]6.3.9M1 & M2 documentation into this one Maintenance Guide. All subsequent S-C[xz]6.3.9 maintenance releases will be added to this guide.
S-C[xz]6.3.9M3		
August 30, 2013	Revision 1.04	Software for the Service Provider and Enterprise platforms: Server Edition, VM Edition, and Oracle Hardware Edition. Features include: Licensing removed from the USB dongle. Licensing now appears only under the Help->About link in the Web GUI application. Update to latest version of OpenSSL library Updates SPL engine to version C2.0.2
S-C[xz]6.3.9M4		
January 28, 2014	Revision 1.05	Adds M4 content. See the M4 chapter for detail.
S-C[xz]6.3.9M5		
December 18, 2014	Revision 1.06	Adds M5 content. See the M5 chapter for detail.

1

S-C[xz]6.3.9M1

Platform Support

Release S-C[xz] 6.3.9 M1 runs on the following platforms:

- Oracle Hardware: Acme Packet 3820, Acme Packet 4500
- Server Edition (SE): HP DL120 G7, HP DL320e G8, and Dell R210 II
- Virtual Machine Edition (VME): VMWare and Hyper-V

Software Images

This section describes software images for this release.

For Oracle Hardware

If you are using Oracle hardware, use the following software image: nnSCX639m1.tar. The x in the file name corresponds to Oracle hardware.

The latest software is packaged in .tar format. Older releases were packaged as .xz format. When upgrading from releases previous to 6.3.9, please assure bootloader build date is 1/19/2012 or newer.

All Other Hardware or Software-only

If you are using hardware other than Oracle's or running this software as a VM, use the file defined in this section for your needs. The z in the file name corresponds to non-Oracle hardware or VM.

- Single system image file: nnSCX639m1.bz
- Boot Media Creator: nnSCX639m1-img-usb.exe
- Virtual Machine VMWare: nnSCX639m1-img-bin.ova
- Virtual Machine Hyper-V: nnSCX639m1-img-bin.vhd

For software-only options, the following file is pre-loaded on the USB stick for [z] builds: SWR-0028-00.tar.

Browser Support

You can use any of the following Web browsers to access Oracle's Web GUI:

- Internet Explorer versions 9.0 and higher

- Mozilla Firefox versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher

Note: After upgrading your Oracle SBC software, you should clear your browser cache before using the Oracle SBC Web GUI.

Content Map

The following table identifies the new features in Release S-C[xz] 6.3.9 M1.

Content Type	Description
Adaptation	Palladion Probe Enhancement
Adaptation	Web GUI Enhancements

New Features

This section lists the new features available in S-C[xz]6.3.9M1.

Features include:

- *Palladion Probe Enhancement*
- *NN-ESD Web GUI Enhancements*

Palladion Probe Enhancement

Performance enhancements were made to the Palladion Probe functionality. Release S-C[xz]6.3.9M1 simplifies the operation of software-based Palladion probes by enabling the transmission of IPFIX data to one or more Palladion Mediation Engines, possibly on different sub-nets. This enhancement requires a slight change in the ACLI hierarchy -- specifically, the removal of the network-interface parameter from the comm-monitor configuration object, and its transfer to the monitor-collector configuration object.

Consequently, users who are migrating from a previous S-C[xz]6.3.9 release to S-C[xz]6.3.9M1 must be aware of the following anomaly. After the upgrade, probes based/anchored on media interfaces revert to the default network-interface value of wancom0:0.

The following illustrates a pre-S-C[xz]6.3.9M1 configuration.

```
comm-monitor
       state                     enabled
       qos-enable                disabled
       sbc-grp-id                0
       tls-profile
       network-interface         M10:0
       monitor-collector
              address            172.16.29.102
              port               4739
```

The following illustrates the upgraded S-C[xz]6.3.9M1 configuration.

```
comm-monitor
       state                     enabled
       qos-enable                disabled
       sbc-grp-id                0
       tls-profile
       monitor-collector
              address            172.16.29.102
              port               4739
              network-interface  wancom0:0
```

Note: Restoration of prior service requires a simple workaround, namely, the update of the network-interface parameter to its original value of M10:0.

Oracle Communications Session Border Controller Web GUI Enhancements

Performance enhancements were made to the SIP Monitor and Trace functionality in the Oracle Communications Session Border Controller Web GUI.

In addition, for SIP Monitor and Trace to trigger interesting-events, the monitoring-filters object must be configured via the ACLI.

The following example shows the monitoring-filter configured to include all session data (*).

```
sip-monitoring
    state                   enabled
    monitoring-filters      *
    interesting-events
    type                    local-rejection
    trigger-threshold       0
    trigger-timeout         0
    trigger-window          30
```

The following example shows the monitoring-filter configured to include only the session data configured for Filter1.

```
sip-monitoring
    state                     enabled
    monitoring-filters        filter1
    interesting-events
    type                      local-rejection
    trigger-threshold         0
    trigger-timeout           0
    trigger-window            30
```

For more information about configuring interesting-events, see the *Oracle® Enterprise Session Border Controller User Guide*.

Limitations

The following table lists limitations in Release Version S-C[xz]6.3.9M1.

Limitation
Web Server
High-frequency logging into and out of the GUI using an automation script (a rate faster than humanly possible) results in a system crash. It is not expected that manual testing will produce this issue.
SIPREC
This release fully supports SIPREC on the SBC Server Edition. However, on Acme Packet 3800s and Acme Packet 4500s, there is a session recording limit of approximately 50 sessions. If you require SIPREC on Acme Packet 3800s and/or Acme Packet 4500s, Oracle strongly encourages you to use Release Version S-CX6.3.9.
Local Policy
This release requires the "Routing" license to configure a next-hop in a Local Policy. This limitation will be resolved in the S-C[xz] 6.3.9 Final.
Media-released Hairpinned Session

Limitation
For media-released hairpinned sessions, a NAT entry is incorrectly left installed upon termination of the session. This leads to future sessions failing with a 503 reason code. This limitation will be resolved in the S-C[xz] 6.3.9 Final.
Hyper-V
The following are specific limitations when using Hyper-V: - Limited session capacity when using Hyper-V hypervisor (50 media sessions). - Network booting is not supported due to Microsoft Firewall Test (MSFT) driver defect. - Dynamic Host Configuration Protocol (DHCP) is not supported due to the MSFT driver defect. - Microsoft does not support USB pass-through via hypervisor. - Virtual LAN (VLAN) tagging is not supported with Hyper-V in Windows 2008 R2. - When using High Availability (HA), the wancom interfaces should be configured as "Legacy Network Adaptors". - Microsoft System Center Virtual Machine Manager (MS-SCVMM) should not be used to deploy Oracle Virtual Machine Edition (VME) products due to a Virtual Hard Disk (VHD) import defect.

2

S-C[xz]6.3.9M2

Platform Support

Release S-C[xz] 6.3.9 M2 runs on the following platforms:

- Oracle Hardware: Acme Packet 3820, Acme Packet 4500
- Server Edition (SE): HP DL120 G7, HP DL320e G8, and Dell R210 II
- Virtual Machine Edition (VME): VMWare and Hyper-V

Software Images

This section describes software images for this release.

For Oracle Hardware

If you are using Oracle hardware, use the following software image:
nnSCX639m2.tar. The x in the file name corresponds to Oracle hardware.

The latest software is packaged in format. Older releases were packaged as format. When upgrading from releases previous to 6.3.9, please assure bootloader build date is 1/19/2012 or newer. You can download the most recent bootloader from the Oracle support site: .

All Other Hardware or Software-only

If you are using hardware other than Oracle's or running this software as a VM, use the file defined in this section for your needs. The z in the file name corresponds to non-Oracle hardware or VM.

- Single system image file: nnSCX639m2.bz
- Boot Media Creator: nnSCX639m2-img-usb.exe
- Virtual Machine VMWare: nnSCX639m2-img-bin.ova
- Virtual Machine Hyper-V: nnSCX639m2-img-bin.vhd

For software-only options, the following file is pre-loaded on the USB stick for [z] builds: SWR-0028-00.tar.

Browser Support

You can use any of the following Web browsers to access Oracle's Web GUI:

- Internet Explorer versions 9.0 and higher
- Mozilla Firefox versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher

Note: After upgrading your Oracle SBC software, you should clear your browser cache before using the Oracle SBC Web GUI.

Content Map

The following table identifies the new features in Release S-C[xz] 6.3.9 M2.

Content Type	Description
Adaptation	2770 - Personal Profile Manager (PPM) Proxy
Adaptation	SIPREC Ping Support
Adaptation	2261 - SIPREC Re-INVITE Collision and Back-off Support

New Features

This section lists the new features available in S-C[xz]6.3.9M2:

- *Personal Profile Manager (PPM) Proxy*
- *SIPREC Ping Support*
- *SIPREC Re-INVITE Collision and Back-off Support*

Personal Profile Manager (PPM) Proxy

Release S-C[xz]6.3.9 M2 includes a new Personal Profile Manager (PPM) proxy. PPM is a web service that runs as part of Avaya Aura Session Manager and Aura System Manager. Local and remote SIP clients may download configuration data from the PPM proxy using SOAP messages over HTTP or HTTPS, enabling soft keys to be customized and contact lists to be loaded. Unfortunately, in enterprise networks certain messages may refer to private IP addresses, which are not routable from remote clients. Oracle now incorporates an application proxy in the Oracle SBC for such messages, replacing the internal IP addresses with the
Oracle SBC's external SIP interface IP address.

The PPM proxy supports incoming messages over HTTP and HTTPS on a configurable IP address / port. If using HTTPS, the PPM proxy uses a selectable server certificate for Transport Layer Security (TLS).

Remote clients accessing the PPM proxy are authenticated by HTTP digest authentication, using their SIP credentials. The PPM proxy forwards such challenges and responses transparently to the PPM web service for which it is configured.

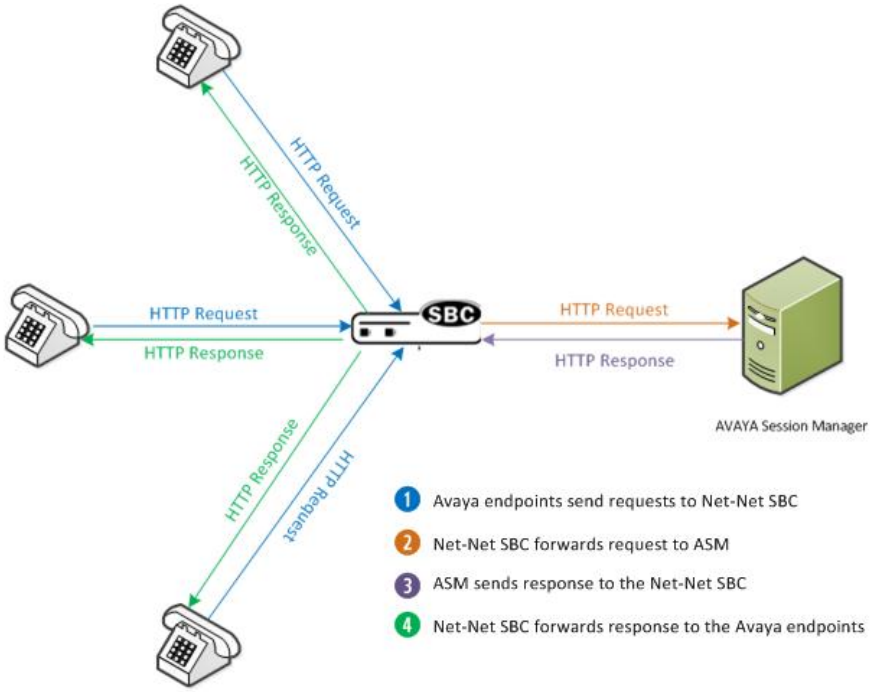
Since the PPM proxy could potentially be a target of a denial-of-service (DoS) attack, the Oracle SBC allows you to set DoS rules to protect the proxy port as part of standard configurations. For configuring DoS on the Oracle Enterprise Session Border Controller, see the .

The Oracle SBC functions as an HTTP Application Layer Gateway (ALG) for HTTP/HTTPS traffic that originates on Avaya endpoints and terminates on the Avaya Session Manager (ASM) as follows:

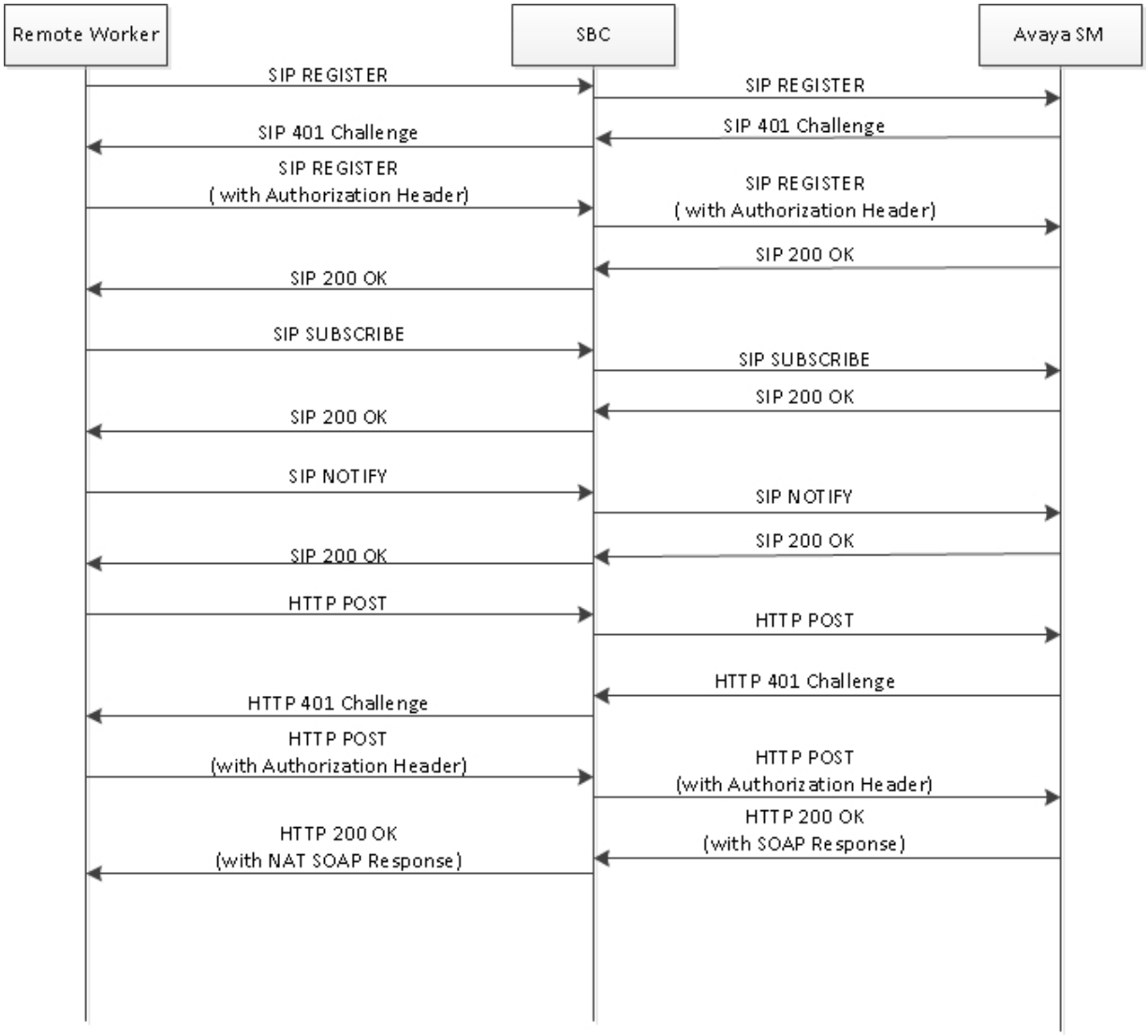
- 1 The Oracle SBC receives HTTP requests from Avaya endpoints on a user configurable IP address and port.
- 2 The Oracle SBC then forwards the requests to a user configurable destination which is the IP address and port of the ASM.
- 3 The response to the HTTP request is sent from the ASM to the Oracle SBC.
- The Oracle SBC parses the HTTP response and searches for getHomeServerResponse and getHomeCapabilitiesResponse messages. If the getHomeServerResponse message is found, the Oracle SBC replaces any text between the <PpmServer> or <SipServer> tags with the IP address of the public interface on

which the HTTP-ALG is configured. If the getHomeCapabilitesResponse is found, the Oracle SBC replaces any text contained between the <ServiceURI> tags with the IP address of the public interface on which the HTTP-ALG is configured.

- 4 After the Oracle SBC is done processing the response, it forwards the response to the originating Avaya endpoint. The following illustration shows how the Oracle SBC sends/receives HTTP requests/responses to the Avaya Session Manager.



The following is the call flow that occurs as the HTTP/HTTPS requests and responses are passed between the Avaya endpoints, the Oracle SBC, and the ASM.



Configuring the PPM Proxy on the Oracle SBC

To configure the PPM proxy on the Oracle SBC, you use the http-alg object and the http-alg->private or http-alg->public objects under session-router. Use the following procedure to configure the PPM proxy on the Oracle SBC.

To configure the PPM proxy:

1. In Superuser mode, type configure terminal and press Enter.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)#
```

2. Type session-router and press Enter.

```
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)#
```

3. Type http-alg and press Enter.

```
ACMEPACKET(session-router)# http-alg
ACMEPACKET(http-alg)#
```

4. name—Enter the name (unique identifier) of the HTTP proxy. Valid values are alpha-numeric characters. Default is blank.
5. state—Enter the operational status of the HTTP proxy. Valid values are:

- enabled - (default) Enables the HTTP proxy.
- disabled - Disables the HTTP proxy.

6. description—Enter a description of the HTTP proxy. Valid values are alpha-numeric characters. Default is blank.
7. private—Allows you to configure a private/core-side interface (inside the network) for forwarding the incoming HTTP SOAP Requests received from the public side.
8. public—Allows you to configure a public-side interface (outside the network) to receive incoming HTTP SOAP Requests from the remote worker.

Private Settings on the Oracle SBC 1

To set a private setting on the Oracle SBC:

1. Type private and press Enter.

```
ACMEPACKET(http-alg)# private
ACMEPACKET(private)#
```

   The private /core side is used to communicate with the Avaya Session Manager (ASM) and forward the incoming HTTP SOAP Requests received from the public side (from outside the network). You define the IP address, port, and TLS certificate used in establishing communication with the ASM by setting this private object.

2. realm-id—Name of the realm that the Oracle SBC uses to proxy the HTTP request. Valid values are alpha-numeric characters. Default is blank.
3. address—IPv4 or IPv6 IP address from which the Oracle SBC forwards the incoming HTTP request. Valid values must be in the format of 0.0.0.0. Default is blank.
4. destination-port—Port on which the destination server is listening for HTTP traffic. Valid values are 1 to 65535. Default is 80.
5. tls-profile—The TLS profile used to establish a secure connection with the destination server. Setting this attribute enables HTTP proxy to listen for HTTPS traffic. Valid values are alpha-numeric characters. Default is blank.
6. destination-address—IPv4 or IPv6 IP address of the destination server to which the HTTP request is forwarded. Valid values must be in the format of 0.0.0.0. Default is blank.
7. Type done and press Enter.

```
ACMEPACKET(private)# done
ACMEPACKET(private)#
```

8. Type exit and press Enter.

```
ACMEPACKET(private)# exit
ACMEPACKET(http-alg)#
```

9. Type exit and press Enter.

```
ACMEPACKET(http-alg)# exit
ACMEPACKET(session-router)#
```

10. Save the configuration.

Private Settings on the Oracle SBC 2

To set a public setting on the Oracle SBC:

1. Type public and press Enter.

```
ACMEPACKET(http-alg)# public
ACMEPACKET(public)#
```

   The public side (outside the network) is used to receive incoming HTTP SOAP Requests from the remote worker. You define the IP address, port, and TLS certificate used to establish a connection with the remote worker by setting this public object.

2. realm-id—Name of the realm that the Oracle SBC uses to listen for the HTTP request. Valid values are alpha-numeric characters. Default is blank.

3. address—IPv4 or IPv6 IP address on which the Oracle SBC is listening for HTTP traffic. Valid values must be in the format of 0.0.0.0. Default is blank.
4. port—Port on which the Oracle SBC is listening for HTTP traffic. Valid values are 1 to 65535. Default is 80.
5. tls-profile—The TLS profile used to establish a secure connection with the remote worker. Setting this attribute enables HTTP proxy to listen for HTTPS traffic. Valid values are alpha-numeric characters. Default is blank.
6. Type done and press Enter.

```
ACMEPACKET(public)# done
ACMEPACKET(public)#
```

7. Type exit and press Enter.

```
ACMEPACKET(public)# exit
ACMEPACKET(http-alg)#
```

8. Type exit and press Enter.

```
ACMEPACKET(http-alg)# exit
ACMEPACKET(session-router)#
```

9. Save the configuration.

PPM XML Mapping to ACLI Parameters

Each of the PPM parameters in the ACLI map to specific XML tags. The following table provides the XML/ACLI parameter mapping.

Parameter Name	XML Tag
http-alg	httpAlg
name	name
state	state
description	description
private	private
realm-id	RealmID
address	address
destination-address	destination-address
destination-port	destination-port
tls-profile	tlsProfile
public	public
realm-id	RealmID
address	address
port	port
tls-profile	tlsProfile

Example PPM Proxy Configuration

The following is an example of a the PPM proxy configuration with private enabled.

```
session-router# show
    http-alg
        name                          Avaya
        state                         enabled
        description                   Avaya Proxy
```

```
        private
            realm-id                realmA
            address                 172.45.6.7
            destination-port        80
            tls-profile             t1s1
            destination-address     123.456.78.1
        public
            realm-id
            address
            port
            tls-profile
```

SIPREC Ping Support

On the Oracle SBC, you can now check the connectivity between the Oracle SBC and the session recording server (SRS) using two new, optional ping commands via the ACLI:

- ping-method - SIP message or method for which to ping the SRS.
- ping-interval - Amount of time, in seconds, that the Oracle SBC waits before it pings the SRS in subsequent intervals. For example, if this parameter is set for 60 seconds, the Oracle SBC pings the SRS every 60 seconds.

This SIPREC ping is a signal that the Oracle SBC transmits to the connected SRS requesting a response pertaining to the message type that you specify for the ping-method. It uses the ping-interval to determine how long it should wait before sending another ping to the SRS. Once configured (save and activated) the
Oracle SBC uses this feature to perform SIP-based pinging to determine if the SRS is reachable or not.

Configuring SIPREC Ping on the Oracle SBC

To configure SIPREC ping on the Oracle SBC, you use the ping-method and the ping-interval objects under call-recording-server. Use the following procedure to configure SIPREC ping on the Oracle SBC.

To configure SIPREC ping:

1. In Superuser mode, type configure terminal and press Enter.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)#
```

2. Type session-router and press Enter.

```
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)#
```

3. Type call-recording-server and press Enter.

```
ACMEPACKET(session-router)# call-recording-server
ACMEPACKET(call-recording-server)#
```

4. ping-method—Enter the message or method type for which the Oracle SBC uses in a ping request to the SRS to determine if it is reachable or not. Default is blank. Valid values are:

BYE	OPTIONS
UPDATE	SUBSCRIBE
CANCEL	NOTIFY

5. ping-interval—Enter the amount of time, in seconds, that the Oracle SBC waits before it pings the SRS in subsequent intervals. Valid values are 0 to 99999. Default is 0 (zero). The setting of zero disables the ping interval.
6. Type done and press Enter.

```
ACMEPACKET(call-recording-server)# done
ACMEPACKET(call-recording-server)#
```

7. Type exit and press Enter.

```
ACMEPACKET(call-recording-server)# exit
ACMEPACKET(session-router)#
```

8. Type exit and press Enter.

```
ACMEPACKET(session-router)# exit
ACMEPACKET(configure)#
```

9. Save the configuration.

Example SIPREC Ping Configuration

The following is an example of a SIPREC ping configuration.

```
call-recording-server# show
        name                          SRS1
        description                   session recording server
        realm                         realmA
        mode                          selective
        destination                   132.43.5.6
        port                          5060
        transport-method              DynamicTCP
        ping-method                   OPTIONS
        ping-interval                 60
```

In the above example, the Oracle SBC sends a ping request to the SRS using the OPTIONS value every 60 seconds to determine if the SRS is reachable or not.

SIPREC Re-INVITE Collision and Back-off Support

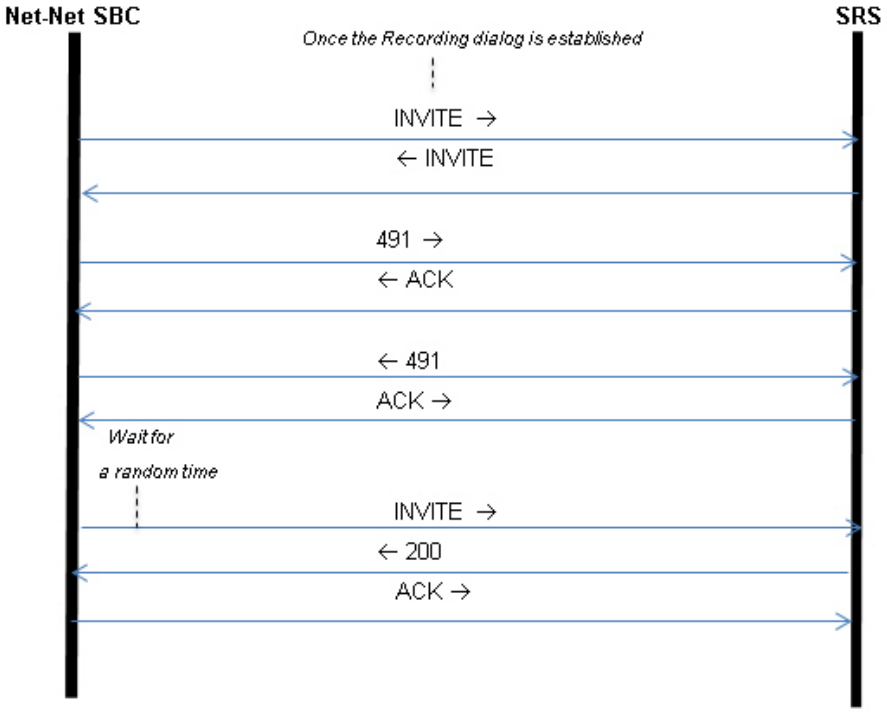
The Oracle SBC acts a back-to-back User Agent (B2BUA) in all call scenarios. However with SIPREC, the Oracle SBC acts as a User Agent Client (UAC) when connected with a session recording server (SRS). Therefore, SIP requests can originate from the Oracle SBC.

During a recording session, when the SRS establishes a recording dialog, the Oracle SBC and the SRS may send Re-INVITES to each other with updated information. When the Oracle SBC receives an INVITE while it is still waiting for the response to a previous INVITE it sent out, this produces an INVITE collision.

To avoid an INVITE collision, the Oracle SBC now sends a 491 Request Pending response back to the SRS and then waits for a random amount of time before re-trying the INVITE. It also acknowledges (ACK) any 491 response received from the other side. RFC 3261 and RFC 6141 describes the way the User Agent (UA) resolves the INVITE collision. The random wait time is chosen based on the following guidelines from RFC 3261:

- If the UAC is the owner of the Call-ID of the dialog ID (i.e., it generated the value), T (the wait time) is a randomly chosen value between 2.1 and 4 seconds in units of 10 milliseconds.
- If the UAC is not the owner of the Call-ID of the dialog ID (i.e., it did not generate the value), T (the wait time) is a randomly chosen value between 0 and 2 seconds in units of 10 milliseconds.

The following call flow diagram shows the Oracle SBC's feature to avoid INVITE collision.



Issues Resolved

The following table lists the issues resolved in Version S-C[xz] 6.3.9M2.

Description
After upgrading the Virtual Machine Edition (VME) to Release S-C[xz]6.3.9 M1, SIP Monitor and Trace in the Web GUI displayed a flood of SIP INFO and SIP OPTIONS messages. This has been corrected. Now SIP INFO and SIP OPTIONS messages outside of a dialog are NEVER captured regardless of the SIP Monitor and Trace filter settings.

Limitations

The following table lists limitations in Version S-C[xz]6.3.9M2.

Element	Limitations
Web Server	High-frequency logging into and out of the GUI using an automation script (a rate faster than humanly possible) results in a system crash. It is not expected that manual testing will produce this issue.
SIP Monitor and Trace	After a High Availability (HA) switchover, only new calls are captured on the Oracle SBC. Subsequent messages from pre-existing calls are dropped and no longer in the message log.
Hyper-V	- Limited session capacity when using Hyper-V hypervisor (50 media sessions). - Network booting is not supported due to a Microsoft Firewall Test (MSFT) driver defect. - Dynamic Host Configuration Protocol (DHCP) is not supported due to the MSFT driver defect. - Microsoft does not support USB pass-through via hypervisor.

Element	Limitations
	- Virtual LAN (VLAN) tagging is not supported with Hyper-V in Windows 2008 R2. - When using High Availability (HA), the wancom interfaces should be configured as "Legacy Network Adaptors". - Microsoft System Center Virtual Machine Manager (MS-SCVMM) should not be used to deploy Oracle Virtual Machine Edition (VME) products due to a Virtual Hard Disk (VHD) import defect.

3

S-C[xz]6.3.9M3

Platform Support

Release S-C[xz] 6.3.9 M3 runs on the following platforms:

- Oracle Hardware: Acme Packet 3820, Acme Packet 4500
- Server Edition (SE): HP DL120 G7, HP DL320e G8, and Dell R210 II
- Virtual Machine Edition (VME): VMWare and Hyper-V

Software Images

This section describes software images for this release.

For Oracle Hardware

If you are using Oracle hardware, use the following software image:
nnSCX639m3.tar. The x in the file name corresponds to Oracle hardware.

The latest software is packaged in format. Older releases were packaged as format. When upgrading from releases previous to 6.3.9, please assure bootloader build date is 1/19/2012 or newer. You can download the most recent bootloader from the Oracle support site: .

All Other Hardware or Software-only

If you are using hardware other than Oracle's or running this software as a VM, use the file defined in this section for your needs. The z in the file name corresponds to non-Oracle hardware or VM.

- Single system image file: nnSCZ639m3.bz
- Boot Media Creator: nnSCZ639m3-img-usb.exe
- Virtual Machine VMWare: nnSCZ639m3-img-bin.ova
- Virtual Machine Hyper-V: nnSCZ639m3-img-bin.vhd

For software-only options, the following file is pre-loaded on the USB stick for [Z] builds: SWR-0028-00.tar.

Browser Support

You can use any of the following Web browsers to access Oracle's Web GUI:

- Internet Explorer versions 9.0 and higher
- Mozilla Firefox versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher

Note: After upgrading your Oracle ESD software, you should clear your browser cache before using the Oracle ESD Web GUI.

Content Map

The following table identifies the new features in Release S-C[xz] 6.3.9 M3.

Content Type	Description
Library updates	Update to latest version of OpenSSL library Updates SPL engine to version C2.0.2
Licensing	Licensing information was removed from the USB dongle.

Library Updates

Release S-C[xz]6.3.9 M3 includes the latest updates to the OpenSSL library. It also updates the SPL engine to version C2.0.2.

Licensing Information

Release S-C[xz]6.3.9 M3 removes the licensing information from the USB dongle. All licensing information can now be viewed through the Oracle SBC Web GUI at the Help->About link, or by issuing the show about command in the ACLI.

For more information about displaying the license information, see the Oracle Enterprise Session Director Web GUI User Guide.

Issues Resolved

The following table lists the issues resolved in Version S-C[xz] 6.3.9 M3.

Description
Latching and stream mode set to inactive - The Service policy decision function (SPDF) process orders latching to the Border Gateway Function (BGF) in an ADD request, setting the stream mode to INACTIVE. The user equipment (UE) performs as follows: sends a dummy RTP and RTCP packet between a 180 RINGING and a 200 OK answer. sends a 200 OK and then SPDF orders latching to a BGF in a MODIFY request, setting the stream mode (towards UE) to SENDONLY. RTCP flow is correctly processed (latching occurs, flow is established), but RTP is not correctly processed. This is now corrected. Once the SBC enables the latching signal on a specific termination, the BG latches on the first incoming RTP packet, independent from the stream mode, and uses the remote source port learned through latching as the remote destination port for sending traffic.

Limitations

The following table lists limitations in Version S-C[xz]6.3.9M3.

Limitations
Web Server
High-frequency logging into and out of the GUI using an automation script (a rate faster than humanly possible) results in a system crash. It is not expected that manual testing will produce this issue.
SIP Monitor and Trace
After a High Availability (HA) switchover, only new calls are captured on the Oracle SBC. Subsequent messages from pre-existing calls are dropped and no longer in the message log.
Hyper-V
The following are specific limitations when using Hyper-V: - Limited session capacity when using Hyper-V hypervisor (50 media sessions). - Network booting is not supported due to a Microsoft Firewall Test (MSFT) driver defect. - Dynamic Host Configuration Protocol (DHCP) is not supported due to the MSFT driver defect. - Microsoft does not support USB pass-through via hypervisor. - Virtual LAN (VLAN) tagging is not supported with Hyper-V in Windows 2008 R2. - When using High Availability (HA), the wancom interfaces should be configured as "Legacy Network Adaptors". - Microsoft System Center Virtual Machine Manager (MS-SCVMM) should not be used to deploy Oracle Virtual Machine Edition (VME) products due to a Virtual Hard Disk (VHD) import defect.

4

S-C[xz]6.3.9M4

Platform Support

The following platforms support the S-C[xz]6.3.9 M4 release.

- Acme Packet: AP 3820 and AP 4500
- Server Edition. HP DL120 G7, HP DL320e G8, and Dell R210 II
- Virtual Machine Edition. VMWare and Hyper-V

Release Image File Names

Use the following files for a new deployment.

Acme Packet Hardware

- Image: nnSCX639m4.tar
- Bootloader: 01/19/2012 or newer

Server Edition. Boot Media Creator: nnSCX639m4-img-usb.exe

Virtual Machines

- VMWare: nnSCX639m4-img-bin.ova
- Hyper-V: nnSCX639m4-img-bin.vhd

Upgrade Image File Names

Use the following files to upgrade a Server Edition or virtual machine deployment.

- Image: nnSCZ639m4.bz
- Bootloader: nnSCZ639m4.boot

Browser Support

The Oracle Web GUI supports the following Web browsers.

- Internet Explorer versions 9.0 and higher
- Mozilla Firefox versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher

Note: After upgrading the Oracle SBC software, Oracle recommends that you clear the browser cache before using the Oracle SBC Web GUI.

Content Map

The following table identifies the new features in Release S-C[xz]6.3.9M4.

Content Type	Description
Adaptation	Session Border Controller Behind NAT

New Features

This section lists the new features available in S-C[xz]6.3.9M4.

Session Border Controller (SBC) Deployment Behind a Network Address Translation (NAT) Device

The S-C[xz]6.3.9M4 release provides the *Support for SBC Behind NAT* SPL plug-in for deploying the Oracle Communications Session Border Controller on the private network side of a NAT device. The *Support for SBC Behind NAT* SPL plug-in changes information in SIP messages to hide the end point located inside the private network. The specific information that the *Support for SBC Behind NAT* SPL plug-in changes depends on the direction of the call, for example, from the NAT device to the SBC or from the SBC to the NAT device.

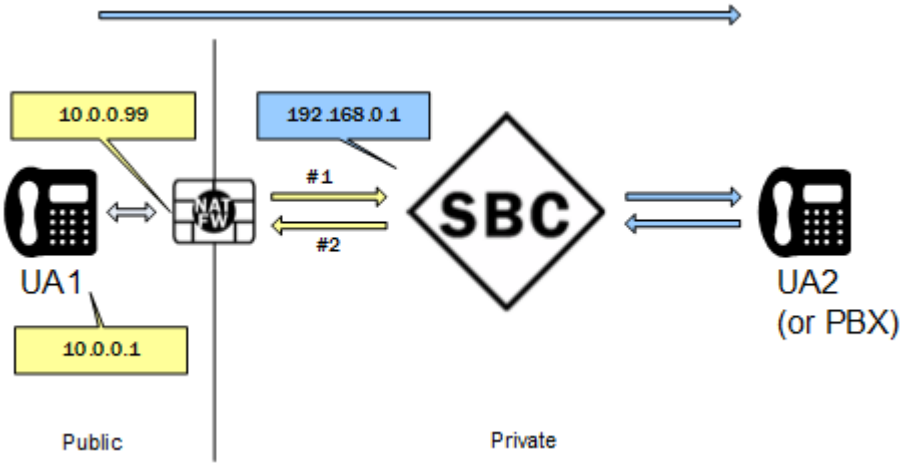
Configure the *Support for SBC Behind NAT* SPL plug-in for each SIP interface that is connected to a NAT device. One public-private address pair is required for each SIP interface that uses the SPL plug-in, as follows.

- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device.

The following illustrations show the SBC deployed in the private network behind a NAT device, using the *Support for SBC Behind NAT* SPL plug-in. Examples follow each illustration to show where the *Support for SBC Behind NAT* SPL plug-in changes the SIP message information.

Call Initiated on the Access Side

In this illustration, UA1 invites UA2 to a session and UA2 responds.



#1. UA1 sends an INVITE through the NAT device to the Oracle Communications Session Border Controller with the following message.

```
INVITE sip:service@10.0.0.99:5060 SIP/2.0
Via: SIP/2.0/UDP 10.0.0.1:5060;branch=z9hG4bK-3539-1-0
Contact: sip:sipp@10.0.0.1:5060
…
Content-Type: application/sdp

o=user1 53655765 2353687637 IN IP4 10.0.0.1
c=IN IP4 10.0.0.1
…
```

The *Support for SBC Behind NAT* SPL plug-in looks for the public SIP Interface IP address 10.0.0.99 in R-URI, Via, Contact, and SDP. The SPL plug-in finds 10.0.0.99 in R-URI and changes it to the private SIP Interface IP address 192.168.0.1.

```
INVITE sip:service@192.168.0.1:5060 SIP/2.0
Via: SIP/2.0/UDP 10.0.0.1:5060;branch=z9hG4bK-3539-1-0
Contact: sip:sipp@10.0.0.1:5060
…
Content-Type: application/sdp

o=user1 53655765 2353687637 IN IP4 10.0.0.1
c=IN IP4 10.0.0.1
…
```

#2. The Oracle Communications Session Border Controller sends a Reply to UA1.

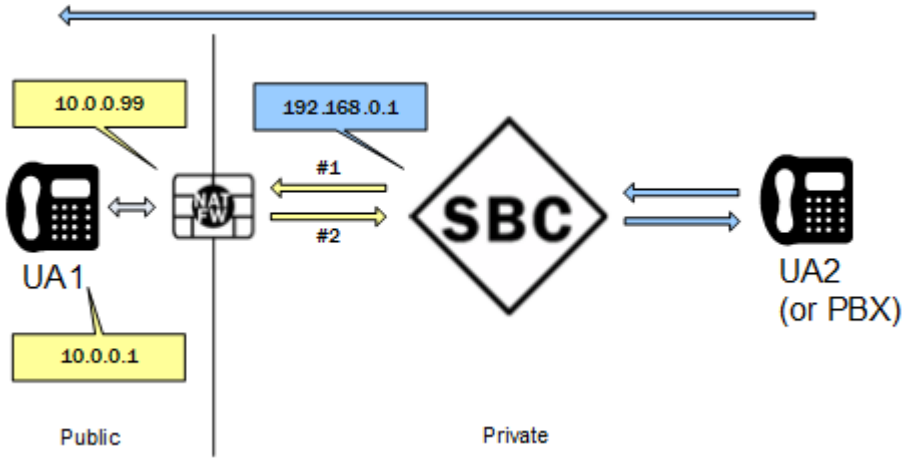
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.0.0.1:5060;received=192.168.0.70;branch=z9hG4bK-3539-1-0
Contact: <sip:192.168.0.1:5060;transport=udp>
Content-Type: application/sdp
…
o=user1 53655765 2353687637 IN IP4 192.168.0.1
c=IN IP4 192.168.0.1
…
```

The *Support for SBC Behind NAT* SPL plug-in looks for the private SIP interface IP address 192.168.0.1 in R-URI, Via, Contact, and SDP. The SPL plug-in finds 192.168.0.1 in Contact and SDP and changes it to the public IP 10.0.0.99.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.0.0.1:5060;received=192.168.0.70;branch=z9hG4bK-3539-1-0
Contact: <sip:10.0.0.99:5060;transport=udp>
Content-Type: application/sdp
…
o=user1 53655765 2353687637 IN IP4 10.0.0.99
c=IN IP4 10.0.0.99
…
```

Call Initiated on the Core Side

In this illustration, UA2 invites UA1 to a session and UA1 responds.



#1. The Oracle Communications Session Border Controller sends an Invite to UA1.

```
INVITE sip:service@10.0.0.1:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.1:5060;branch=z9hG4bKbgs21h30a8kh8okcv790.1
Contact: <sip:sipp@192.168.0.1:5060;transport=udp>
Content-Type: application/sdp
…
o=user1 53655765 2353687637 IN IP4 192.168.0.1
c=IN IP4 192.168.0.1
…
```

The *Support for SBC Behind NAT* SPL plug-in looks for the private IP address 192.168.0.1 in R-URI, Via, Contact, and SDP. The SPL plug-in finds 192.168.0.1 in Via, Contact, and SDP and changes it to the public IP address 10.0.0.99.

```
INVITE sip:service@10.0.0.1:5060 SIP/2.0
Via: SIP/2.0/UDP 10.0.0.99:5060;branch=z9hG4bKbgs21h30a8kh8okcv790.1
Contact: <sip:sipp@10.0.0.99:5060;transport=udp>
Content-Type: application/sdp
…
o=user1 53655765 2353687637 IN IP4 10.0.0.99
c=IN IP4 10.0.0.99
…
```

#2. UA1 sends a Reply to the Oracle Communications Session Border Controller.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.0.0.99:5060;branch=z9hG4bKbgs21h30a8kh8okcv790.1
Contact: <sip: 10.0.0.1:5060;transport=UDP>
Content-Type: application/sdp
…
o=user1 53655765 2353687637 IN IP4 10.0.0.1
c=IN IP4 10.0.0.1
…
```

The *Support for SBC Behind NAT* SPL plug-in looks for the private SIP interface IP address 192.168.0.1 in R-URI, Via, Contact, and SDP. The SPL plug-in finds 192.168.0.1 in Via, changes it to the public IP 10.0.0.99.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.1:5060;branch=z9hG4bKbgs21h30a8kh8okcv790.1
Contact: <sip: 10.0.0.1:5060;transport=UDP>
Content-Type: application/sdp
…
o=user1 53655765 2353687637 IN IP4 10.0.0.1
c=IN IP4 10.0.0.1
…
```

Enable the SPL Plug-In

You must enable the SPL plug-in before you configure an SPL option. The process to enable the SPL plug-in on the SBC requires the following steps.

1. Upload the SPL plug-in to the SBC.
2. Add the SPL plug-in to the SBC configuration.
3. Execute the SPL file.
4. Synchronize the SPL files across HA pairs.
5. Reset the SPL on standby nodes.
6. Configure the SPL plug-in option.

1. Upload the SPL Plug-in to the SBC

Use any CLI or interface-based FTP or SFTP application to send the SPL plug-in to the SBC. You can use the wancom or eth0 management physical interface to reach the FTP/SFTP server on the SBC.

Upload the SPL plug-in to the /code/spl directory on the SBC.

2. Add the SPL Plug-in to the SBC Configuration

Confirm that you are in Superuser mode.

On the SBC, in the spl-configuration element, configure the SPL plug-in.

1. Type configure terminal, and press <Enter>.
2. Type system, and press <Enter>.
3. Type spl-config, and press <Enter>.
4. Type select, and press <Enter>.
5. Type plugins, and press <Enter>.
6. Type name, enter a space, and type the name of the SPL plug-in file.
7. Type done.
8. Type exit.
9. Type done.

3. Execute the SPL File

Confirm that the SPL plug-in is configured on the SBC and that you exited the configuration menu.

You must save and activate the configuration.

Perform the save-config and activate-config operations on the SBC.

4. Synchronize the SPL Files Across HA Pairs

Confirm that you are in Superuser mode.

When running in an HA pair configuration, the active system and the standby system must both have the same version of the SPL plug-in installed. To facilitate configuring the standby system, you can execute the synchronize the spl ACLI command, without any arguments, to copy all of the files in the /code/spl directory from the active system to the same directory on the standby system. Note that any file on the standby system with the same name as a file on the active system is overwritten.

By adding the specific file name as an argument to the synchronize spl command, the individual, specified scripts are copied. For example:

ACMEPACKET# synchronize spl <name of the SPL plug-in file>

The synchronize spl command can only by executed from the active system in an HA pair. There is no means to synchronize spl files automatically during save and activate operations on the SBC.

Type synchronize spl, and press <Enter>.

5. Reset the SPL on Standby HA Nodes

Confirm that you are in Superuser mode.

Execute the reset spl command on all standby nodes that receive the spl file by way of the synchronize command.

Type reset spl, and press <Enter>.

6. Configure the SPL Plug-in Option

See the instructions for configuring the particular SPL plug-in option.

Configure the Session Border Controller (SBC) Behind a Network Address Translation (NAT) Device Option

Configure one public-private address pair for each SIP interface that uses the *Support for SBC Behind NAT* SPL plug-in, as follows.

- The private IP address must be the same as the SIP interface IP address.
- The public IP address must be the public IP address of the NAT device.

Before You Begin

- Confirm that the SIP interface is configured.
- Confirm that you are in the Superuser mode.

To configure the SIP interface IP addresses:

1. Type configure terminal, and press <Enter>.

```
ORACLE# configure terminal
```

2. Type system, and press <Enter>.

```
ORACLE(configure)# system
ORACLE(system)#
```

3. Type session-router, and press <Enter>.

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

4. Type sip-interface, and press <Enter>.

```
ORACLE(session-router)# sip-interface
ORACLE(sip-interface)#
```

5. Select the SIP interface, and press <Enter>.

```
ORACLE(sip-interface)# select
<RealmID>:
1: DefaultENT 172.16.1.100:5060
2: DefaultSP  192.168.0.1:5060

selection:2
System_Primary(sip-interface)#
```

6. Type spl-options +HeaderNatPrivateSipIfIp "<value>", where <value> is the private SIP interface IP address, and press <Enter>.

```
ORACLE(sip-interface)#spl-options +HeaderNatPrivateSipIfIp 192.168.0.1
```

7. Type spl-options +HeaderNatPublicSipIfIp "<value>", where <value> is the public IP address of the NAT device, and press <Enter>.

```
ORACLE(sip-interface)#spl-options +HeaderNatPublicSipIfIp 10.0.0.99
```

8. Type done, and press <Enter>.
9. Save and activate the configuration.

Limitations

The following table lists limitations in version S-C[xz]6.3.9M4.

Limitations
Web Server High-frequency logging into and out of the GUI using an automation script causes the system to stop responding. Such behavior is not expected from manual testing.
SIP Monitor and Trace After a High Availability (HA) switch over, only new calls are captured on the Oracle SBC. Subsequent messages from pre-existing calls are dropped and no longer display in the message log.
Hyper-V - Session capacity is limited to 50 media sessions, when using Hyper-V hypervisor. - Network booting is not supported due to a Microsoft Firewall Test (MSFT) driver defect. - Dynamic Host Configuration Protocol (DHCP) is not supported due to the MSFT driver defect. - Microsoft does not support USB pass-through via hypervisor. - Virtual LAN (VLAN) tagging is not supported with Hyper-V in Windows 2008 R2. - When using High Availability (HA), the wancom interfaces should be configured as "Legacy Network Adaptors". - Microsoft System Center Virtual Machine Manager (MS-SCVMM) should not be used to deploy Oracle Virtual Machine Edition (VME) products due to a Virtual Hard Disk (VHD) import defect.

Issues Resolved

The following table lists the issues resolved in Version S-C[xz]6.3.9M4.

Description
None attributed to this release.

Known Issues

The following are known issues and workarounds in version SC[xz]6.3.9M4.

Issue	Workaround
A newly rebooted SBC does not synchronize all data. This only affects SBCs running outside of virtual machines on non-Oracle hardware, for example, HP ProLiant DL120. When the standby SBC is rebooted, the system occasionally does not perform a full synchronization due to a timing issue during the boot sequence.	Under the **redundancy** configuration object, increase the **initial-time** value to 60000. Increasing this value changes the timing of the redundancy state change to allow the redundancy links in the SBC to come up before the application attempts synchronization.

5

S-C[xz]6.3.9M5

Platform Support

The following platforms support the S-C[xz]6.3.9 M5 release.

- Acme Packet: AP 3820 and AP 4500
- Server Edition. HP DL120 G7, HP DL320e G8, and Dell R210 II
- Virtual Machine Edition. VMWare and Hyper-V

Release Image File Names

Use the following files for a new deployment.

Acme Packet Hardware

- Image: nnSCX639m5.tar
- Bootloader: 01/19/2012 or newer

Server Edition. Boot Media Creator: nnSCX639m5-img-usb.exe

Virtual Machines

- VMWare: nnSCX639m5-img-bin.ova
- Hyper-V: nnSCX639m5-img-bin.vhd

Upgrade Image File Names

Use the following files to upgrade a Server Edition or virtual machine deployment.

- Image: nnSCZ639m5.bz
- Bootloader: nnSCZ639m5.boot

Browser Support

The Oracle Web GUI supports the following Web browsers.

- Internet Explorer versions 9.0 and higher
- Mozilla Firefox versions 12.0 and higher

- Google Chrome versions 19.0.1084.46m and higher

Note: After upgrading the Oracle SBC software, Oracle recommends that you clear the browser cache before using the Oracle SBC Web GUI.

Content Map

The S-Cxz6.3.9M5 Maintenance Release Guide includes the following content.

Content Type	Description
Defect	RCSe TLS/TCP Re-use Connections

Issues Resolved

The following table lists the issues resolved in Version S-C[xz]6.3.9M5.

Description
RCSe TLS/TCP Re-User Connections

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.