ORACLE
COMMUNICATIONS

Oracle Communications Acme Packet 1100 Session Boarder Controller with BroadCloud R21

Technical Application Note

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Intended Audience

This is a technical document intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of Oracle Enterprise Session Border Controller (E-SBC) as well as service provider based session border controller. It assumes that the reader is familiar with basic operations of Oracle Session Border Controller AP1100, 3800/4000 and 6000 series platforms.

Document Overview

This Oracle technical application note outlines the recommended configurations for the Oracle Session Border Controller AP1100 series for connecting Broadcloud R21 customers. The solution contained within this document has been certified on Oracle's Acme Packet OS ECZ750P3.BZ.

Broadcloud platform delivers a broad range of unified communications services including video, voice, hosted call center, conferencing, messaging and mobility, for businesses and consumers worldwide.

This application note has been prepared as a means of ensuring that Broadcloud and Oracle AP1100 E-SBC are configured in the optimal manner.

Introduction

Audience

This is a technical intended for telecommunications engineers with the purpose of configuring the Oracle Enterprise Session Border Controller (E-SBC) and Broadcloud. There will be steps that require navigating Broadcloud as well as the Acme Packet Command Line Interface (ACLI). Understanding the basic concepts of TCP/UDP, IP/Routing and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

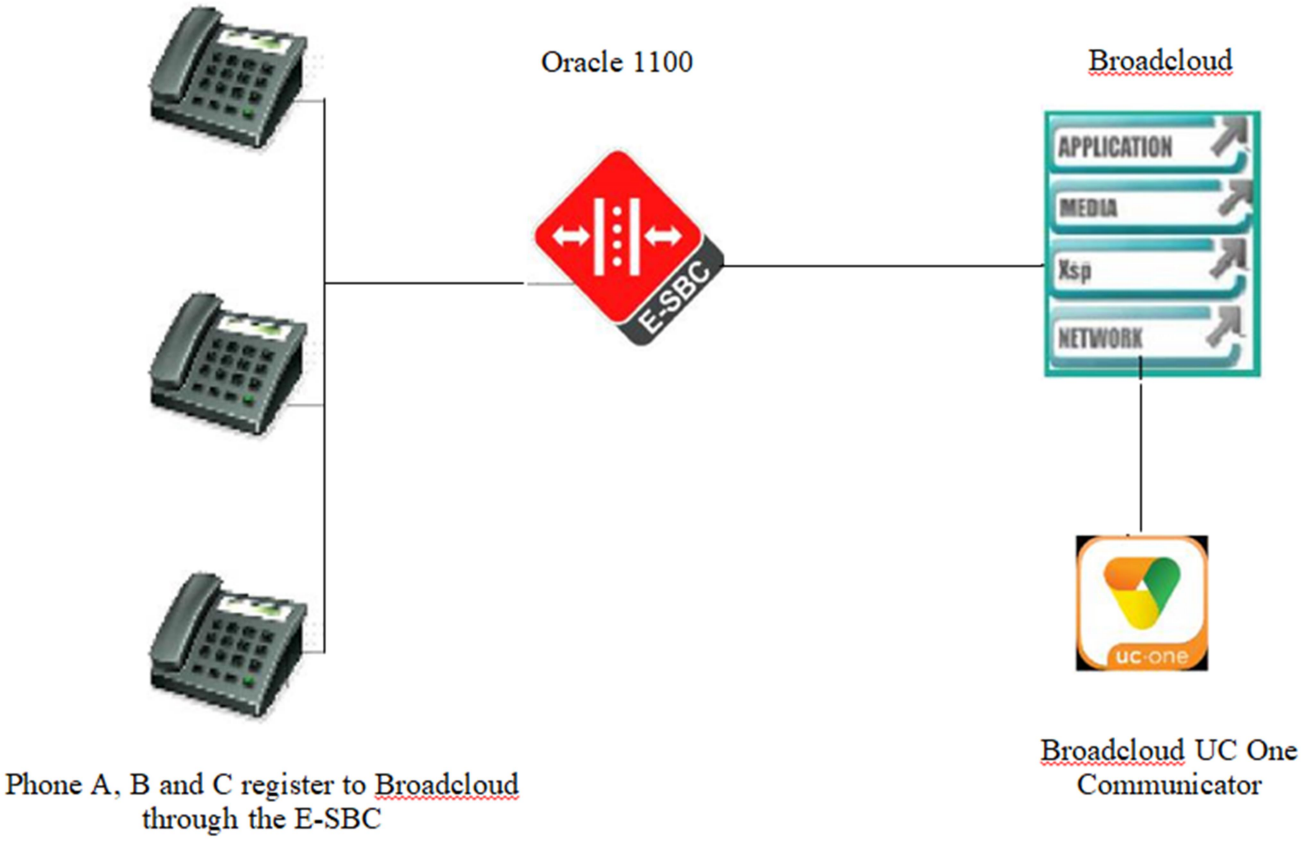
Prior to reading this Quick Guide, read the BroadCloud SIP Trunking Service Definition document, available from BroadCloud's knowledgebase at xchange.broadsoft.com. The document describes how to provision SIP Trunk Groups, SIP Trunk Users and SIP Trunk Mobility Users. All BroadCloud configuration notion will be in noted <…>

Requirements

- Fully functioning Broadcloud R.21
- Oracle Enterprise Session Border Controller AP 1100 or any Oracle ESBC appliance or VM edition running Net-Net OS ECZ750p3.bz. Note: the configuration running on the SBC is backward/forward compatible with any release in the 7.5.0 stream.

Lab Configuration

The following diagram illustrates the lab environment created to facilitate certification testing (IP addressing/Port below is only a reference; they can change per your network specifications).



Configuring the Oracle E-SBC

In this section we describe the steps for configuring a Net-Net E-SBC for use with Broadcloud.

In Scope

The following Step-by-Step guide configuring the Net-Net E-SBC assumes that this is a newly deployed device dedicated to a single customer.

Note that Oracle Communications offers several products and solutions that can interface with Broadcloud. This document covers the setup for the Net-Net E-SBC platforms software ECZ750P3.BZ or later. A Net-Net 1100-series (AP1100) platform was used as the platform for developing this guide. If instructions are needed for other Oracle Communications products, please contact your Oracle Communications representative.

Out of Scope

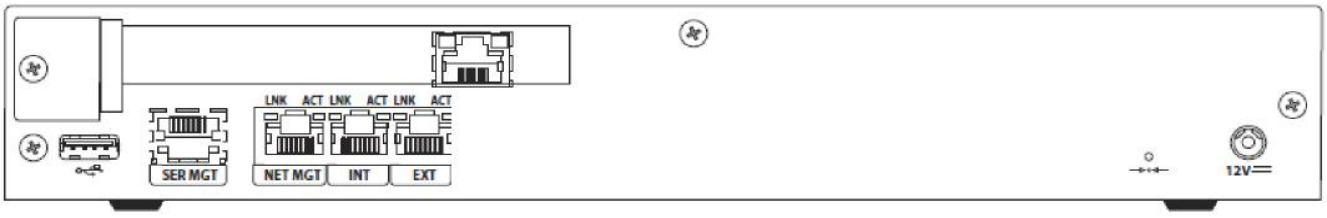
- Configuration of Network management including SNMP and RADIUS

What you will need

- Serial Console cross over cable with RJ-45 connector
- Terminal emulation application such as PuTTYor HyperTerm
- Passwords for the User and Superuser modes on the Net-Net E-SBC
- Signaling IP address and port of Broadcloud
- Signaling and media IP addresses and ports to be used on the Net-Net E-SBC facing Endpoints and Broadcloud
- IP address of the enterprise DNS server

SBC getting started

Once the Net-Net E-SBC is racked and the power cable connected, you are ready to set up physical network connectivity.



Plug the INT (slot 0 port 0) interface into your endpoints facing network and the EXT (slot 1 port 0) interface into your Broadcloud (server-facing) network as shown in the diagram above. Once connected, you are ready to power on and perform the following steps.
All commands are in bold, such as **configure terminal**; parameters in bold red such as **1100-BSFT-1** are parameters which are specific to an individual deployment.

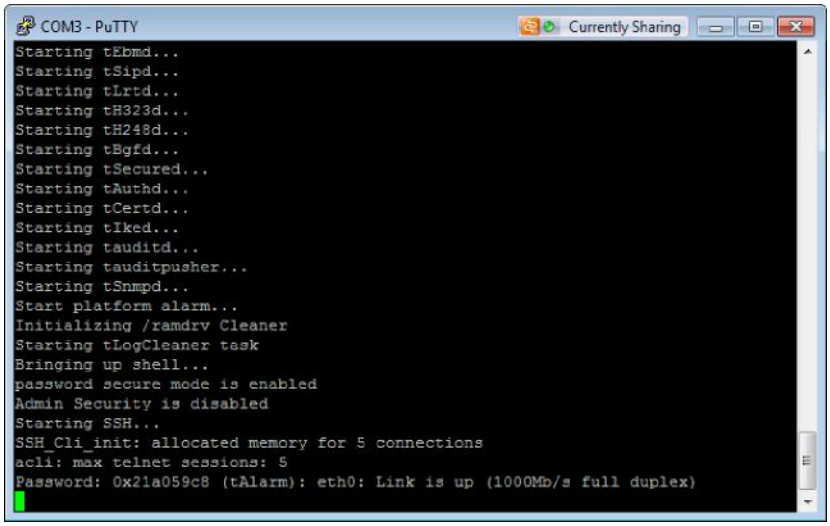
Note: The ACLI is case sensitive.

1. **Establish the serial connection to the Net-Net SBC.**

   Confirm the Net-Net SD is powered off and connect the serial console cable to the Net-Net SD to a workstation running a terminal emulator application such as PuTTy. Start the terminal emulation application using the following settings:

   - Baud Rate=115200
   - Data Bits=8
   - Parity=None
   - Stop Bits=1
   - Flow Control=None

Start the Net-Net SD and confirm that you see the following output from the bootup sequence.



2. **Login to the Net-Net SD and enter the configuration mode**

   Enter the following commands to login to the Net-Net SD and move to the configuration mode. Note that the default Net-Net SBC password is “acme” and the default super user password is “packet”.

```
Password: acme
1100-BSFT-1> enable
Password: packet
1100-BSFT-1# configure terminal
1100-BSFT-1 (configure)#
```

You are now in the Global Configuration mode.

3. Initial Configuration – Assign the management Interface an IP address

To assign an IP address, one has to configure the bootparams on the Net-Net SD, by going to 1100-BSFT-1#configure terminal --- >bootparams

- Once you type “bootparam” you have to use “carriage return” key to navigate down
- A reboot is required if changes are made to the existing bootparams

1100-BSFT-1#(configure)bootparam

```
'.' = clear field; '-' = go to previous
field; q = quit
boot device      : eth0
processor number : 0
host name        : acmesystem
```

```
file name                : /boot/nnECZ750p3.bz--- >location where
the software is loaded on the SBC
inet on ethernet (e)     : 172.18.255.134:ffff0000 --- > This is
the ip address of the management interface of the SBC, type the
IP address and mask in hex
inet on backplane (b)    :
host inet (h)            :
gateway inet (g)         : 172.18.0.1 --- > gateway address here
user (u)                 : vxftp
ftp password (pw) (blank = use rsh)      : vxftp
flags (f)                :
target name (tn)         : 1100-BSFT-1
```

SBC configuration key elements

The following section walks you through specific elements which require change for the Oracle Enterprise SBC to work with Broadcloud:

- **static-flow**: When a Broadcloud client registers to the Broadcloud server through the E-SBC, it downloads the config file from the server. Hence, static-flow is enabled on the E-SBC to allow the HTTP and HTTPS requests and responses from the client to pass through to the server.
- **media-manager -* options:** dont-terminate-assoc-legs: When hairpinned calls are ended because of signaling failures on one call leg, the Oracle E-SBC deletes both legs' media flows simultaneously by default. In addition, when the first hairpinned call leg is torn down, the second call leg is gracefully released immediately. When dont-terminate-assoc-legs is configured, the orphaned call leg in the hairpin scenario will be torn down after the initial guard timer expires.
- **survivability:** The survivability feature is enabled on the E-SBC by configuring this element. This feature is the Oracle E-SBC's ability of a Remote Office/Branch Office to detect the loss of communication over SIP-based telephony to Broadcloud. When loss of communication is detected over the SIP service, the Oracle E-SBC dynamically switches into Survivable Mode, locally handling call processing and providing limited additional server functionality.
- **service-health:** When Survivability Mode is enabled on the E-SBC, the system is able to detect any loss of connection (and subsequent re-connection) to the Broadcloud server based on a health score. For the purpose of health monitoring, a sip-interface and one or more attached session agents are logically grouped together by configuring a"service-tag" parameter to indicate the name of the session agent group. The service health score of the group is based upon the health status of the session agents within the group ; in this case the SA for Broadcloud AS1 is included.
- **session-agent -* auth-attribute:** This element is configured for digest authentication. The attributes listed in the auth-attribute are used by the E-SBC to send the authentication information when challenged by Broadcloud.
- **surrogate-agent:** A surrogate agent is needed to register the E-SBC to the Broadcloud server on behalf of the phone. Surrogate registration requires registration-caching to be set to enabled on the sip-interface of Broadcloud realm.
- **SIP manipulations:**
    - Add100rel: This is configured to add the Require: 100rel header as Broadcloud supports early
    - media.
    - AllowEvents: This is added as an out-manipulation on the sip-interface facing the Broadcloud
    - server.
        - Broadcloud: This header-rule adds the Allow-eventsBroadcloudSubscriberData header to all the REGISTER requests going out of the E-SBC
        - AddOTG: Broadcloud requires the use of otg header param in the From header, and this HMR adds it to the From header.
        - add_iptel: This sip-manipulation adds the tgrp and trunkContext to the Contact header which Broadcloud mandates.

SBC Configuration

```
filter-config
        name                                    all
local-policy
        from-address                            *
        to-address                              8325624170
        source-realm                            sip-trunk
        policy-attribute
               next-hop                                 medpool.lync2013.com
               realm                                    towards-ep
local-policy
        from-address                            *
        to-address                              *
        source-realm                            towards-ep
        policy-attribute
                next-hop                                <OUTBOUND PROXY>
                realm                                   sip-trunk
                app-protocol                            SIP
local-policy
        from-address                            *
        to-address                              978
        source-realm                            towards-ep
        state                                   disabled
        policy-attribute
                next-hop                                10.0.210.75
                realm                                   towards-ep
media-manager
        hnt-rtcp                                enabled
        options                                 dont-terminate-assoc-legs
network-interface
        name                                    s0p0
        ip-address                              192.168.3.78
        netmask                                 255.255.255.0
        gateway                                 192.168.3.150
        hip-ip-list                             192.168.3.78
        ftp-address                             192.168.3.78
        icmp-address                            192.168.3.78
        ssh-address                             192.168.3.78
        dns-domain                              lync2013.com
 network-interface
        name                                    s0p1
        ip-address                              155.212.214.171
        pri-utility-addr                        155.212.214.172
        sec-utility-addr                        155.212.214.173
        netmask                                 255.255.255.0
        gateway                                 155.212.214.1
        dns-ip-primary                          8.8.8.8
        dns-domain                              <REGISTER DOMAIN>
        hip-ip-list                             155.212.214.171
        icmp-address                            155.212.214.171
phy-interface
        name                                    s0p0
        operation-type                          Media
        virtual-mac                             00:08:25:06:c1:2e
phy-interface
        name                                    s0p1
        operation-type                          Media
```

```
        port                                    1
        virtual-mac                             00:08:25:06:c1:2f
realm-config
        identifier                              sip-trunk
        network-interfaces                      s0p1:0
        mm-in-realm                             enabled
realm-config
        identifier                              towards-ep
        network-interfaces                      s0p0:0
        mm-in-realm                             enabled
service-health
        service-tag
                service-tag-string                      test-surv
                sa-health-profile
                        session-agent-hostname                  as.iop1.broadworks.net
session-agent
        hostname                                <OUTBOUND PROXY>
        port                                    0
        realm-id                                sip-trunk
        ping-method                             OPTIONS
        ping-interval                           30
        out-translationid                       removePlus
        refer-call-transfer                     enabled
session-agent
        hostname                                medpool.lync2013.com
        port                                    5068
        transport-method                        StaticTCP
        realm-id                                towards-ep
        ping-method                             OPTIONS
        ping-interval                           30
        ping-all-addresses                      enabled
        out-translationid                       AddPlus
        refer-call-transfer                     enabled
        auth-attributes
                auth-realm                              BroadWorks
                username                                <SIP USER>
                password                                ********

sip-config
        registrar-domain                          *
        registrar-host                            *
        registrar-port                            5060
        trans-expire                              30
        options                                   max-udp-length=0
                                                  register-grace-timer=20
                                                  session-timer-support
        sip-message-len                           65535
       extra-method-stats                        enabled
```

```
sip-feature
        name                                    eventlist
        require-mode-inbound                    Pass
        require-mode-outbound                   Pass
sip-interface
        realm-id                                sip-trunk
        sip-port
               address                                  155.212.214.171
               allow-anonymous                          agents-only
        redirect-action                         Proxy
        min-reg-expire                          7200
        registration-interval                   7200
        route-to-registrar                      enabled
        uri-fqdn-domain                         <REGISTER DOMAIN>
        spl-options                             broadsoftSurvivability
        out-manipulationid                      AllowEvents
        rfc2833-payload                         127
        rfc2833-mode                            preferred
        service-tag                             test-surv
sip-interface
        realm-id                                towards-ep
        sip-port
               address                                  192.168.3.78
        sip-port
               address                                  192.168.3.78
               port                                     5068
               transport-protocol                       TCP
        redirect-action                         Proxy
        nat-traversal                           always
        registration-caching                    enabled
        min-reg-expire                          7200
        registration-interval                   7200
        route-to-registrar                      enabled
        options                                 reuse-connections
        out-manipulationid                      NAT_IP
        rfc2833-payload                         127
        rfc2833-mode                            preferred
sip-manipulation
        name                                    Add100rel
        header-rule
               name                                     AddRequired
               header-name                              Required
               action                                   add
               methods                                  INVITE
               new-value                                100rel
sip-manipulation
        name                                    AllowEvents
        header-rule
               name                                     BroadWorks
               header-name                              Allow-Events
               action                                   add
               comparison-type                          boolean
               msg-type                                 request
```

```
                methods                                 REGISTER
                new-value                               BroadWorksSubscriberData
sip-manipulation
        name                                    addOTG
        header-rule
                name                                    addOTG_From
                header-name                             From
                action                                  manipulate
                msg-type                                request
                methods                                 INVITE
                element-rule
                        name                                    otgFrom
                        parameter-name                  otg
                        type                                    header-param
                        action                                  add
                        new-value                               oracletrunkgroup
sip-manipulation
        name                                    add_iptel
        header-rule
                name                                    contact
                header-name                             Contact
                action                                  manipulate
                msg-type                                request
                methods                                 INVITE
                element-rule
                        name                                    tgrp
                        parameter-name                  tgrp
                        type                                    uri-user-param
                        action                                  add
                        new-value
                                                                                        t
                grpGroupA element-rule
                        name                                    trunkContext
                        parameter-name                  trunkcontext
                        type                                    uri-user-param
                        action                                  add
                        new-value                               "172.19.193.15"
        header-rule
                name                                    BroadWorks
                header-name                             Allow-Events
                action                                  add
                comparison-type                 boolean
                msg-type                                request
                methods                                 REGISTER
                new-value                               BroadWorksSubscriberData sip-
monitoring
        match-any-filter                        enabled
        monitoring-filters                      all
spl-config
        spl-options                             broadsoftSurvivability
        plugins
                name                                    BroadsoftSurvivability.1.0.spl
```

```
        steering-pool
        ip-address                      192.168.3.78
        start-port                      10000
        end-port                        20000
        realm-id                        towards-ep
steering-pool
        ip-address                      155.212.214.171
        start-port                      25000
        end-port                        35000
        realm-id                        sip-trunk
surrogate-agent
        register-host                   <OUTBOUND PROXY>
        register-user                   <SIP USER>
        realm-id                        towards-ep
        customer-next-hop               <OUTBOUND PROXY>
        register-contact-host           155.212.214.171
        register-contact-user           <SIP USER>
        password                        <SIP PASSWORD>
        register-expires                60
        route-to-registrar              disabled
        auth-user                       <SIP USER>
        max-register-attempts           0
        register-retry-time             30

survivability
        state                           enabled
        service-tag                     test-surv
        reg-expires                     7600
        prefix-length                   10
system-config
        hostname                        BSFT-ISR-1100
        location                        lab
        process-log-level               DEBUG
        comm-monitor
               state                            enabled
               monitor-collector
                      address                           172.18.255.71
              default-gateway                   172.18.0.1
              source-routing                    enabled
web-server-config
```

Configuring the Broadcloud Server

This section identifies Broadcloud lab requirements and configuration required as a prerequisite for executing this test plan.

2.1.1 Broadcloud Lab Requirements

This test plan requires a standard redundant Broadcloud lab installation. Components required for a standard redundant lab installation include:

- Application Server (primary)
- Application Server (secondary)
- Media Server
- Network Server (1)
- Network Server (2)
- POP3/IMAP4/SMTP Server

2.1.2 Broadcloud Configuration

This section identifies configuration requirements to enable Broadcloud for SIP requests from the SBC.

2.1.3 Broadcloud Configuration for Premise-based SBCs

Customer premise-based SBCs, including ALGs, Edge Gateways, and similar devices are deployed at the customer site. Typically, servicing a limited number of users in the same enterprise and are hosted by a single pair of Broadcloud Application Servers. There is no Broadcloud configuration required for this model.

However, if the premise-based SBC typically fronts multiple enterprises and/or is also frequently deployed as a hosted/carrier-based SBC, then complete the configuration for Hosted SBCs.

2.1.4 Broadcloud Configuration for Hosted SBCs

Hosted (or carrier-based) SBCs sit in the service provider network. They may service many enterprises across diverse locations and may front multiple Application Server clusters. Hosted SBCs must direct SIP requests to the Broadcloud Network Server to determine the hosting Application Server for the user.

Access redirect eliminates the need for the SBC to configure static mapping of access devices to Application Server clusters. The SBC sends all out-of-dialog requests to the Broadcloud Network Server, which responds with a *302 Redirect* containing an ordered list of the Application Servers to be contacted.

The Broadcloud Network Server must be configured with an Origination Redirect policy to enable it to respond correctly to SIP requests from the SBC. This eliminates the need to configure the SBC with static mapping of access equipment to Application Server clusters. The SBC sends all out-of-dialog requests to the Broadcloud Network Server, which responds with a *302 Redirect* containing an ordered list of the Application Servers to be contacted.

2.1.4.1 Enable Line/Port Synchronization

For the Network Server to associate a request from the SBC to a specific Application Server cluster, line/port synchronization must be enabled.

Enable synchronization via the Application Server CLI.

```
AS_CLI/Interface/NetServSync> set syncLinePorts true
AS_CLI/Interface/NetServSync> set syncTrunkGroups true
```

```
AS_CLI/Interface/NetServSync> get
syncFlag = true
syncLinePorts = true
syncDeviceManagementInfo = true
syncTrunkGroups = true
```

Restart the Application Server after enabling synchronization.

If there are Broadcloud users already configured on the system, then existing line/ports must be dumped to file on the Application Server and uploaded to the Network Server as described in the Network Server and Application Server Synchronization section of the Broadcloud Maintenance Guide [8].

2.1.4.2 Configure Origination Redirect Policy

Complete the following steps to enable the Network Server to perform Origination Redirect for requests from the SBC.

1. Create a new OrigRedirect policy instance. Note that this step does not need to be repeated for additional SBCs or SBC addresses.

```
NS_CLI/Policy/OrigRedirect> add <policy instance name> true CallTypes ALL redirectOnLinePortInsteadOfDN true
```

2. Create a new routing profile in the Network Server. . Note that this step does not need to be repeated for additional SBCs or SBC addresses.

```
NS_CLI/Policy/Profile> add <routing profile name, e.g. sbcprof> OrigRedirect <policy instance name>
```

3. Create a new Routing NE for the SBC.

```
NS_CLI/System/Device/RoutingNE> add <Routing NE name, e.g. sbc1> "" 1 50 <routing profile name, e.g. sbcprof> false OnLine
InboundOnly accessRoutingNE
```

4. Associate address with SBC Routing NE. The address provisioned here must match the address in the first (VIA entry in a message from the SBC).

```
NS_CLI/System/Device/RoutingNE/Address> add <Routing NE name> <address> 1 50
```

Configuring the Oracle Enterprise Operations Monitor

In this section we describe the steps for configuring Oracle Enterprise Operations Monitor (EOM) for use with the Oracle Enterprise SBCs to monitor SIP signaling traffic on the network.

In Scope

The following guide for configuring the Oracle EOM assumes that this is a newly deployed device dedicated to a single customer. Please see the Oracle Communications Session Monitor Installation Guide on http://docs.oracle.com/cd/E60864_01/index.htm for a better understanding of the basic installation.

Out of Scope

- Basic installation as this is covered in Chapters 2 and 3 of the Oracle Communications Session Monitor Installation Guide.
- High availability.

What will you need

- Console access to the EOM server or virtual machine (VM).
- Browser-based HTTPS access to the EOM server after the initial configuration is complete.
- Administrator password for the EOM to be used.
- IP address to be assigned to EOM.

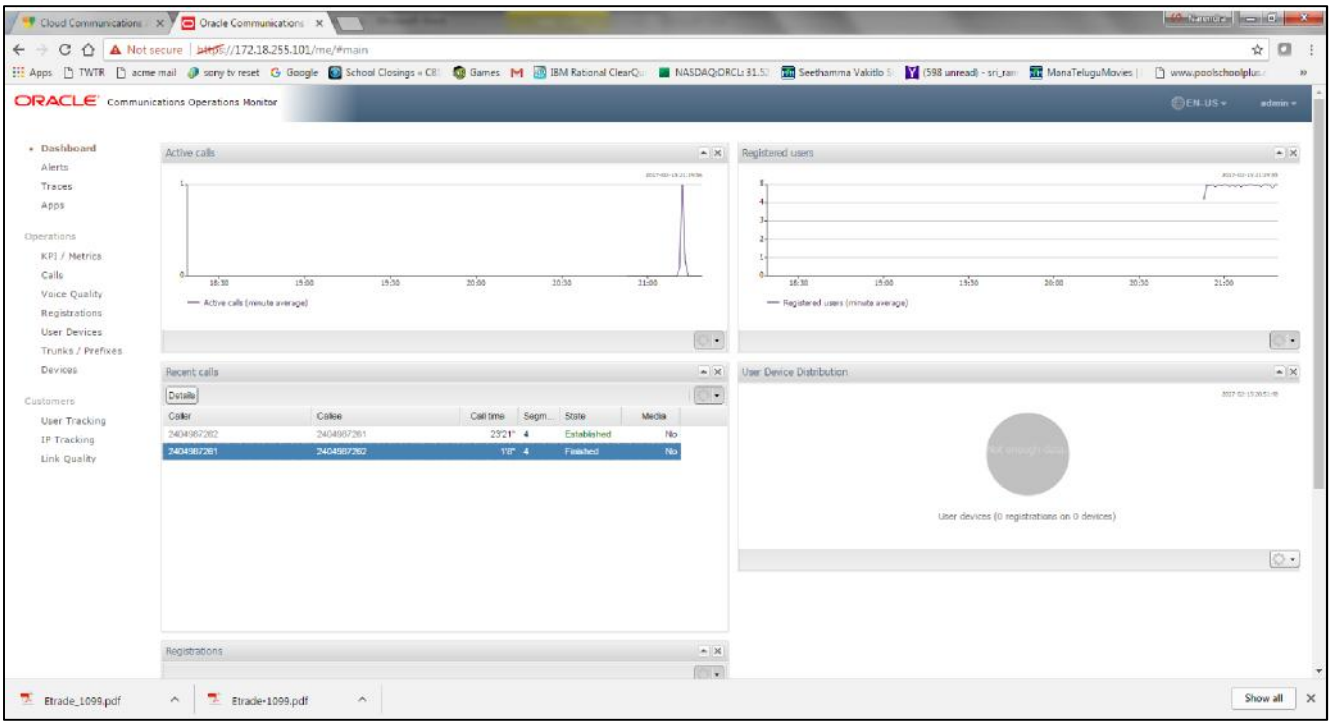
EOM – Getting Started

Ensure that the server or VM specifications meet those outlined in Chapter 1 of the Oracle Communications Session Monitor Installation Guide. Install the EOM software and configure the network parameters as outlined in Chapter 2 of the same guide. Chapter 3 details the subsequent browser-based installation. When prompted to select the "Machine Type", select the "Communications Operations Monitor" checkbox.

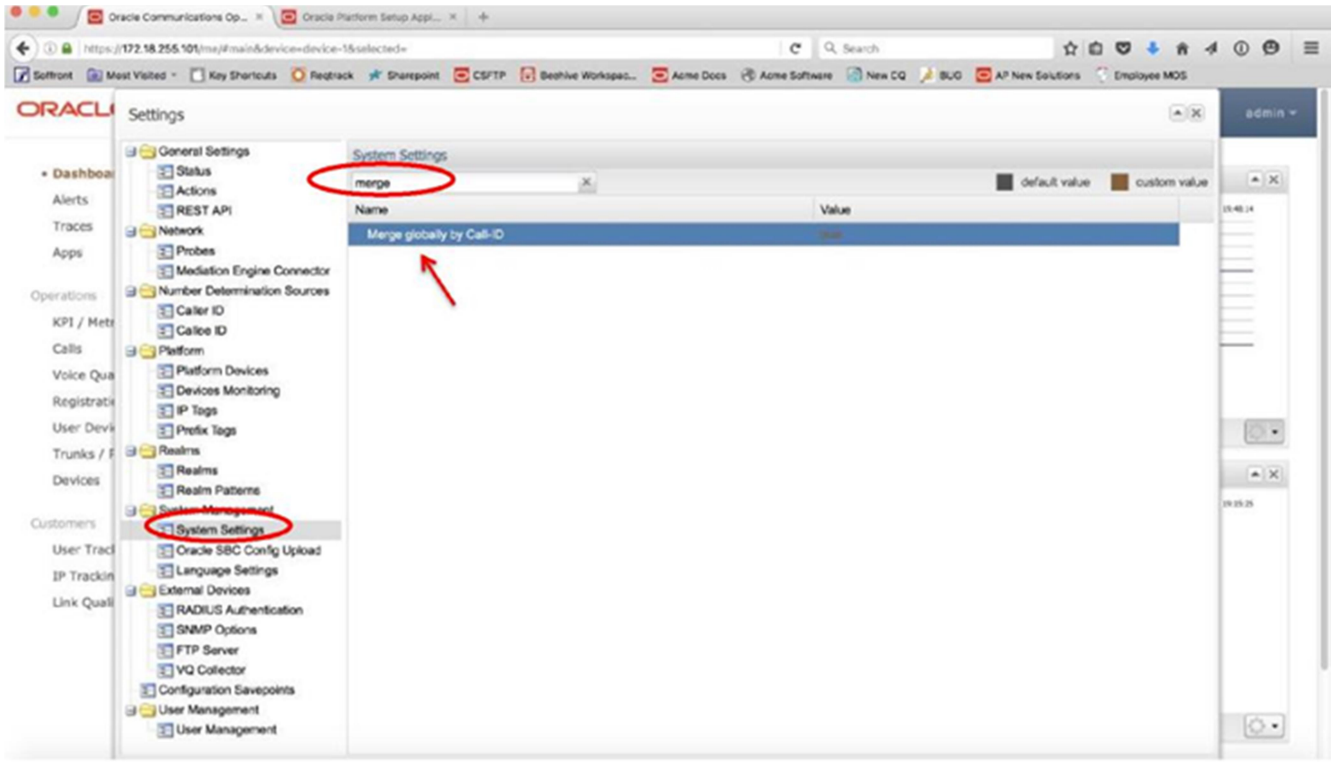
Configuring EOM to Display All Legs of a Call in a Single Report

This allows all call legs on both sides of the E-SBC to be displayed in a single report, making analysis and troubleshooting easier.

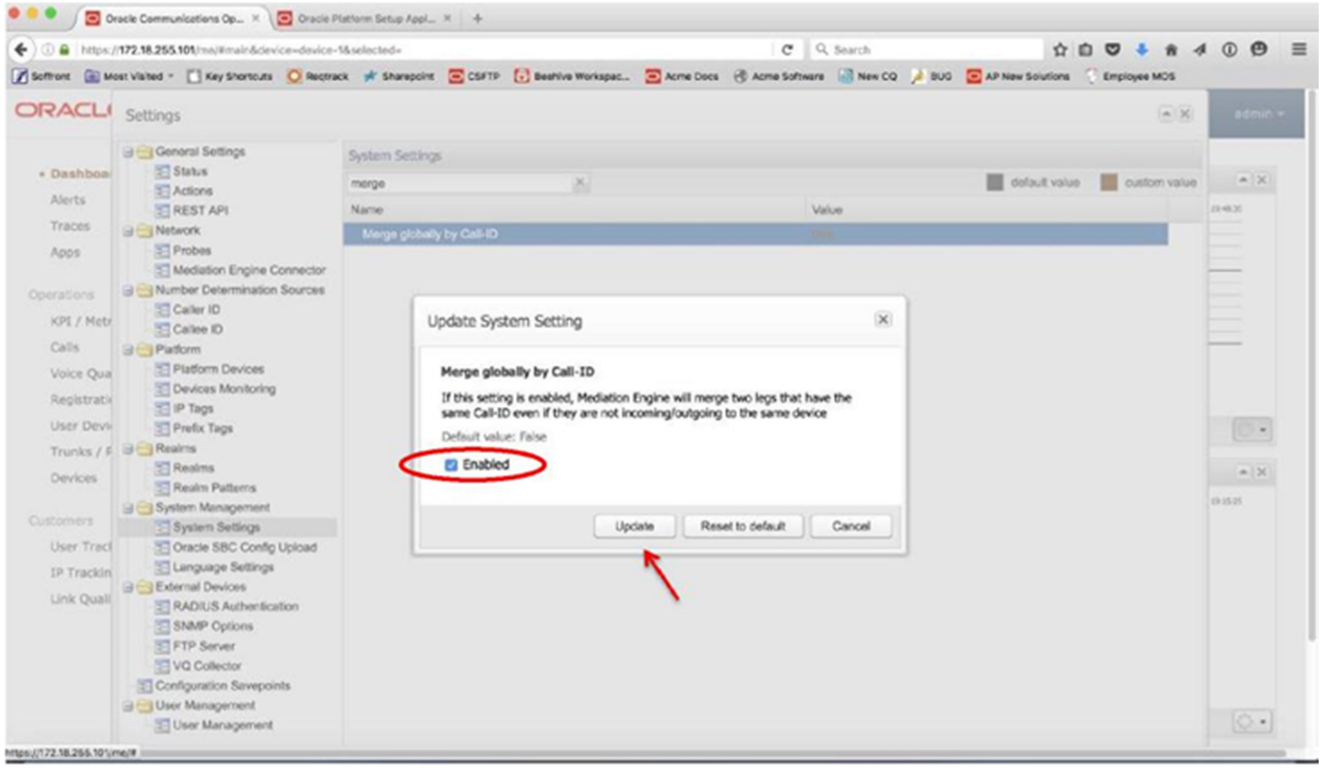
1. Click on the user (admin in this example) in the top right corner, then click on Settings.



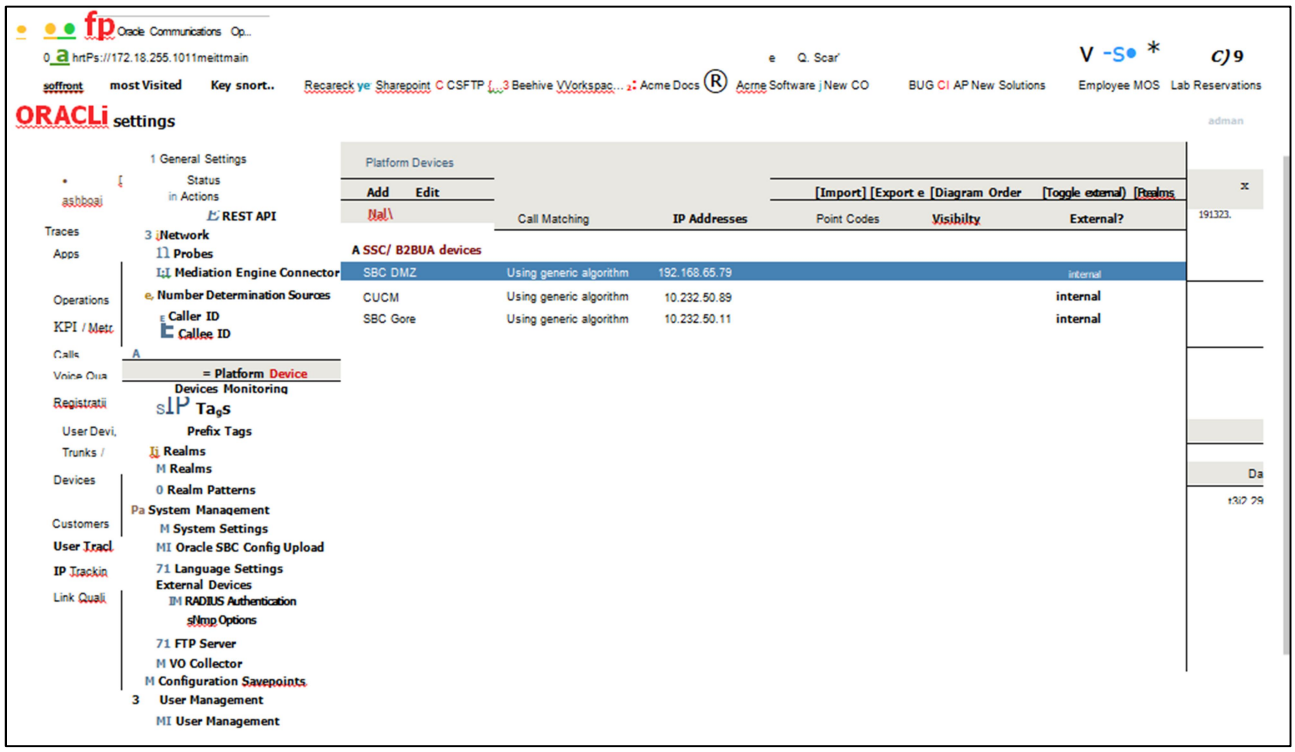
2. Under System Management select System Settings and search for “merge”. Double click on “Merge globally by Call-ID”.



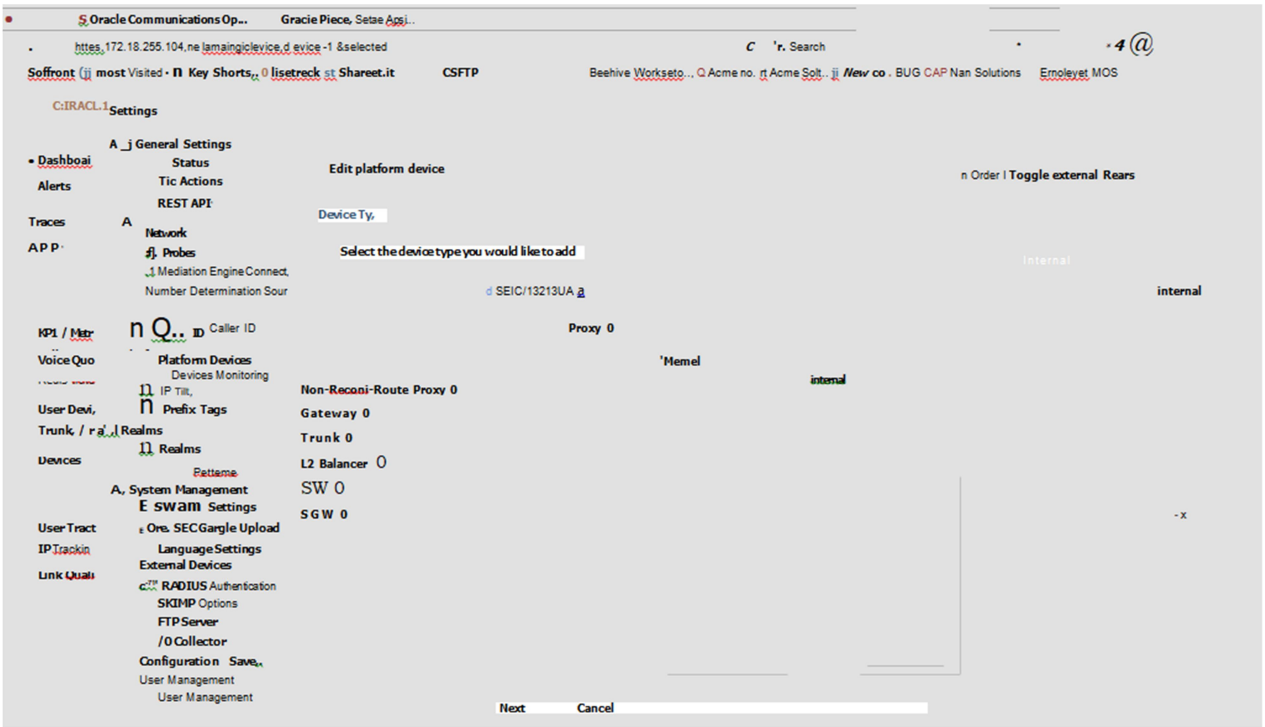
3. Click on the Enabled check box and click Update.



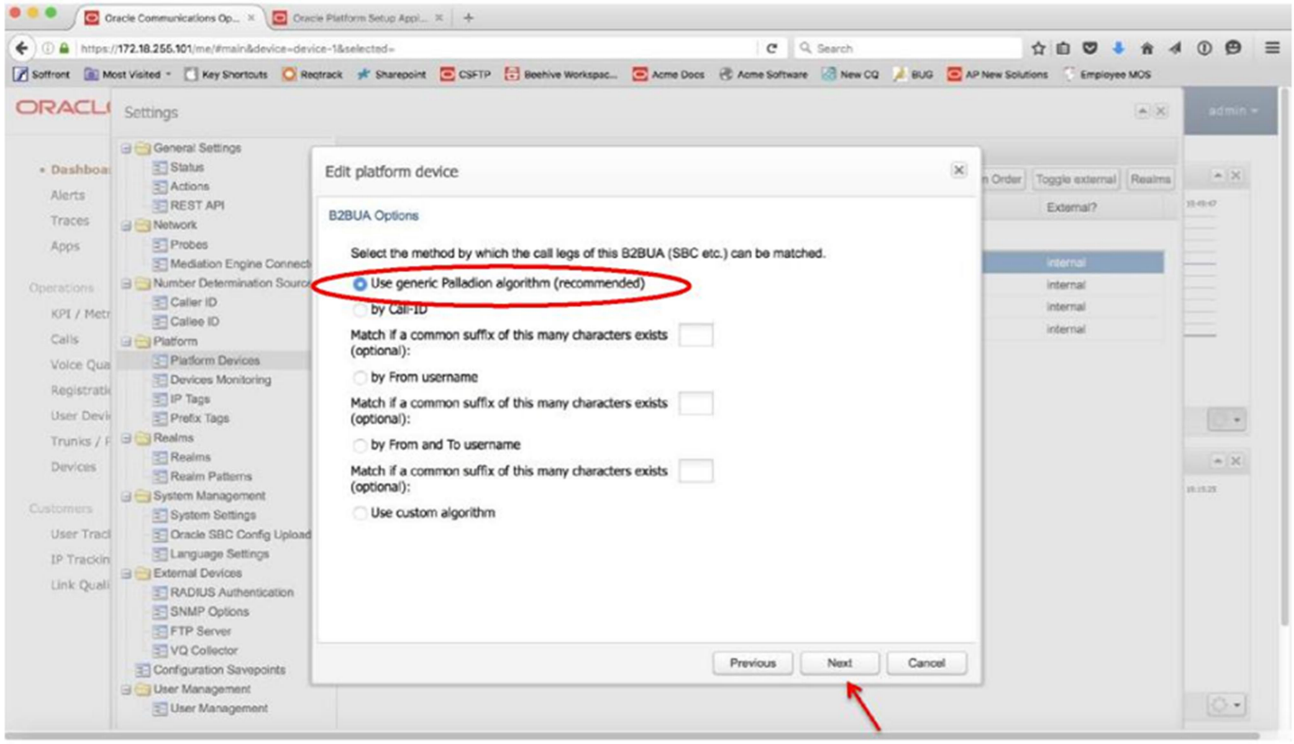
4. Under Platform select Platform Devices. Click Add (or Edit if you've already added a device).



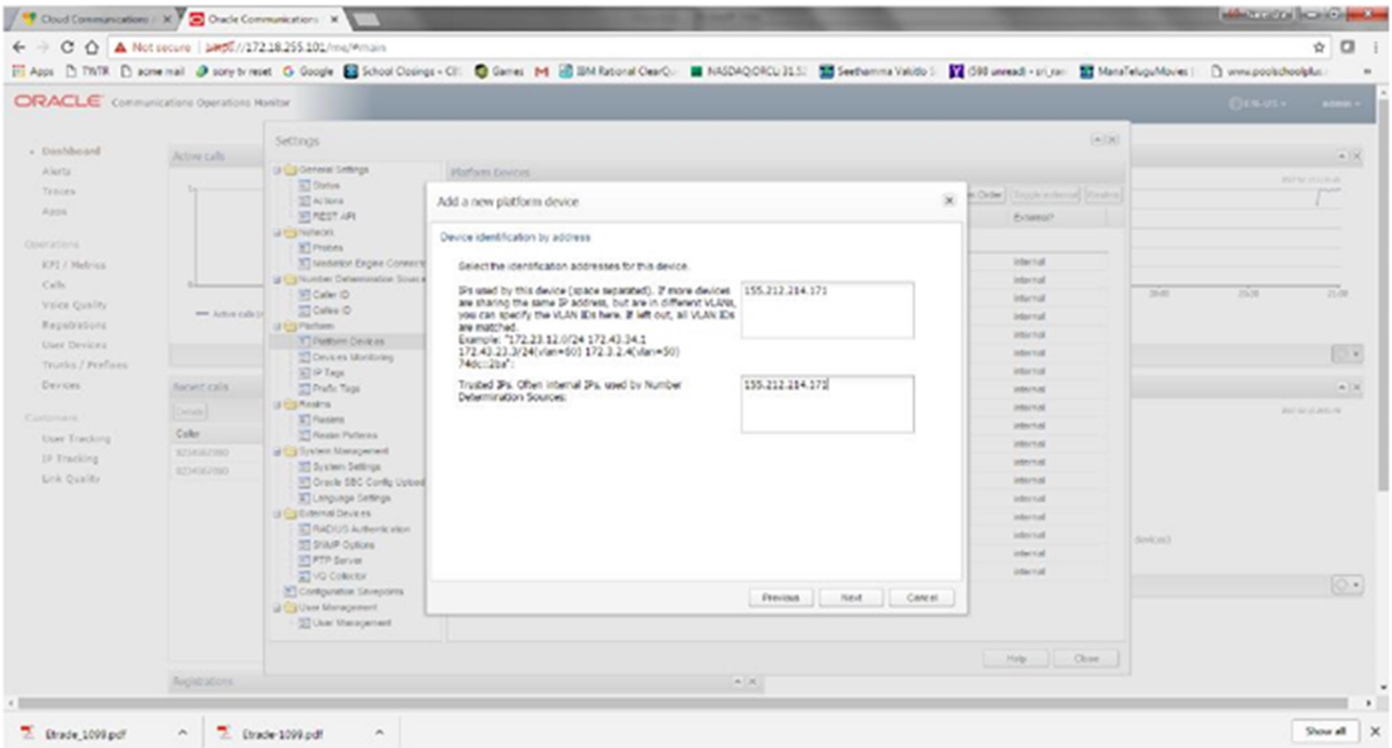
5. Select the SBC/B2BUA radio button regardless of the type of device you're adding, then click Next.



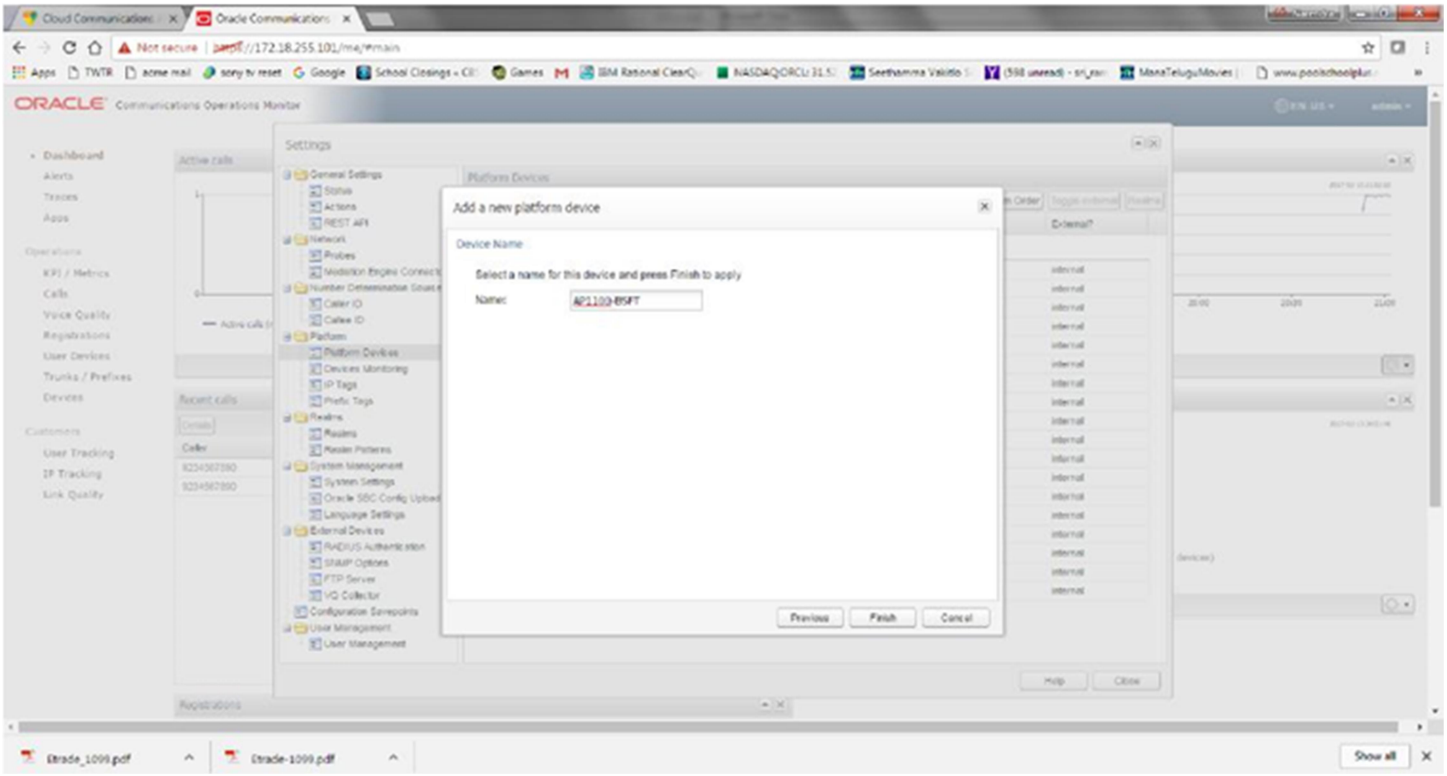
6. Click on the “Use generic Palladion algorithm (recommended)” radio button, then click Next.



7. Enter the device’s IP address in both fields, then click Next.



8. Enter a name for the device and click Finish.



9. Repeat for all other devices in the call flow. Enter each side of the SBC (inside and outside) separately. You don't necessarily need to define the access client's information.
10. On the Dashboard, under Recent Calls, make sure the Auto Refresh is set to something other than Off.
11. Make a call. After the call is finished, the call will show up under Recent Calls with 2 or more segments if the call only traverses the SBC once, or with 4 or more segments if the call traverses the SBC twice. Double click on the call.
12. The call will show up with all segments. Click on the PDF button to generate a report.
13. Click on the Create button.
14. Choose to either save the file or open it.
15. View the Call Report in Acrobat Reader or another program. The report will show all segments of the call.

Test Summary

A comprehensive test plan was executed per Broadcloud and call flows. For a copy of full test report, please contact your Oracle Sales account team.

Broadcloud Session Border Controller Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
Basic	Call Origination	Yes	
	Call Termination	Yes	
	Session Audit	Yes	
	Session Timer	Yes	
	Ringback	Yes	
	Forked Dialog	Yes	
	181 Call Being Forwarded	Yes	
	DTMF – Inband	Yes	
	DTMF – RFC 2833	Yes	
	DTMF – DTMF Relay	Yes	
Broadcloud Services	Third-Party Call Control – Basic	Yes	
	Third-Party Call Control – Advanced	Yes	
	Diversion Header	Yes	
	History-Info Header	Yes	
Access Device Services – Call Control Services	Call Waiting	Yes	
	Call Hold	Yes	
	Call Transfer	Yes	
	Local Conference	Yes	
	Call Forwarding	Yes	
Access Device Services – Registration and Authentication	Registration – Register Authentication	Yes	
	Registration – Maximum Registration	Yes	
	Registration – Minimum Registration	Yes	
	Authentication – Invite Authentication	Yes	
	Authentication – Re-Invite or Update Authentication	Yes	
	Authentication – Refer Authentication	Yes	
	Authentication – Access Device Authenticating Broadcloud	Yes	
	SIP Trunk GIN Registration – Call to PBX User	Yes	
	SIP Trunk GIN Registration – Call from PBX User	Yes	
	SIP Trunk Pilot Registration – Pilot Register	Yes	
	SIP Trunk Pilot Registration – Call to PBX User	Yes	
	SIP Trunk Pilot Registration – Call from PBX User	Yes	
	Surrogate Registration – Pilot Register	Yes	
	Surrogate Registration – Call to PBX User	Yes	

Broadcloud Session Border Controller Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
	Surrogate Registration – Call from PBX User	Yes	
	Maximum Monitored Users	Yes	
Redundancy	DNS SRV Lookup	Yes	
	Register Failover/Failback	Yes	
	Invite Failover/Failback	Yes	
	Bye Failover	Yes	
Remote Survivability	Register	Yes	
	Local Calls – Without Subscriber Data	Yes	Except extension calling
	PSTN Calls – Without Subscriber Data	Yes	

Software Versions Used

The following are the software versions used in this testing.

Component	Version
E-SBC	ECZ7.5.0 P3
Oracle Operations Monitor	3.3.90.0.0
Broadcloud	R21.sp1
Polycom Phones	VVX 600

Troubleshooting Tools

If you find that you are not able to complete calls or have problems with the test cases, there are a few tools available for Oracle E-SBC like logging and tracing which may be of assistance. In this section we will provide a list of tools which you can use to aid in troubleshooting any issues you may encounter.

Wireshark

Wireshark is a network protocol analyzer which is freely downloadable from

www.wireshark.org.

On the Oracle E-SBC

The Oracle SBC provide a rich set of statistical counters available from the CLI, as well as log file output with configurable detail. The follow sections detail enabling, adjusting and accessing those interfaces.

Resetting the statistical counters, enabling logging and restarting the log files. At the console:

```
oraclesbc1# reset sipd
oraclesbc1# notify sipd debug
oraclesbc1#
enabled SIP Debugging
oraclesbc1# notify all rotate-logs
```

Examining the log files

Note: You will FTP to the management interface of the ESBC or SBC with the username user and user mode password (the default is “acme”).

```
C:\Documents and Settings\user>ftp 192.168.5.24
Connected to 192.168.85.55.
220 oraclesbc1FTP server (VxWorks 6.4) ready.
User (192.168.85.55:(none)): user
331 Password required for user.
Password: acme
230 User user logged in.
ftp> cd /ramdrv/logs
250 CWD command successful.
ftp> get sipmsg.log
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/sipmsg.log' (3353
bytes).
226 Transfer complete.
ftp: 3447 bytes received in 0.00Seconds 3447000.00Kbytes/sec.
ftp> get log.sipd
200 PORT command successful.
```

```
150 Opening ASCII mode data connection for '/ramdrv/logs/log.sipd' (204681
bytes).
226 Transfer complete.
ftp: 206823 bytes received in 0.11Seconds 1897.46Kbytes/sec.
ftp> bye
221 Goodbye.
```

You may now examine the log files with the text editor of your choice.

Through the Web GUI

You can also check the display results of filtered SIP session data from the Oracle E-SBC and ESBC, and provide traces in a common log format for local viewing or for exporting to your PC. Please check the "Monitor and Trace SIP Messages" section (page 140) of the E-SBC Web GUI User Guide available at http://docs.oracle.com/cd/E56581_01/index.htm. For the ESBC, see the "Monitor and Trace" section (page 95) of the User's Guide available at http://docs.oracle.com/cd/E55725_01/index.htm.

Telnet

Since we are working within an architecture which uses bound TCP listening ports for functionality, the simplest form of troubleshooting can be seeing if the devices are listening on a particular port, as well as confirming that the there is nothing blocking them such as firewalls. Ensure that you have a TELNET client available on a workstation.

Appendix A

BroadCloud Parameter	Description
<OUTBOUND PROXY>	The BroadCloud Outbound Proxy value is found on the BroadCloud MySite Trunk Group configuration page under the 'Trunk Group Settings' section.
<SIP USER>	The BroadCloud SIP User value is found on the BroadCloud MySite Trunk Group configuration page under the 'Device Settings for Authentication' section.
<SIP PASSWORD>	The BroadCloud SIP Password is found on the BroadCloud My Trunk Group configuration page under the 'Device Settings for Authentication' section.
<REGISTER DOMAIN>	The BroadCloud Register Domain is found on the BroadCloud MySite Trunk Group configuration page under the 'Trunk Group Settings' section.
<SIP USER>	The BroadCloud SIP User value is found on the BroadCloud MySite Trunk Group configuration page under the 'Device Settings for Authentication' section.
<SIP PASSWORD>	The BroadCloud SIP Password is found on the BroadCloud My Trunk Group configuration page under the 'Device Settings for Authentication' section.

Appendix B

Accessing the ACLI

Access to the ACLI is provided by:

- The serial console connection;
- TELNET, which is enabled by default but may be disabled; and
- SSH.

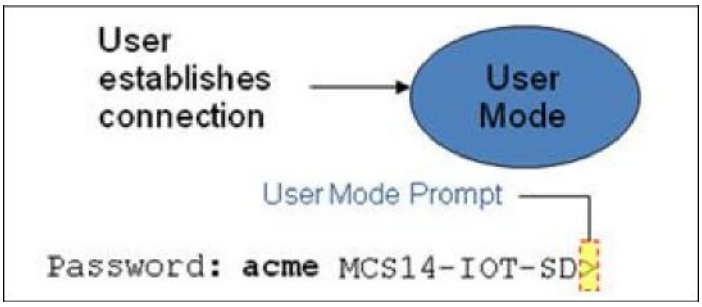
Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) interface on the SBC.

ACLI Basics

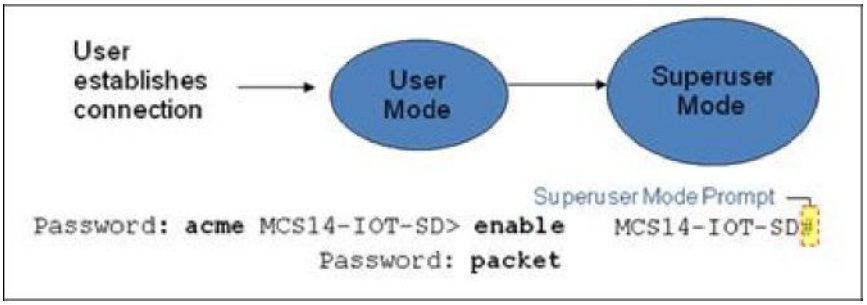
There are two password protected modes of operation within the ACLI, User mode and Superuser mode.

When you establish a connection to the SBC, the prompt for the User mode password appears. The default password is acme.

User mode consists of a restricted set of basic monitoring commands and is identified by the greater than sign (>) in the system prompt after the target name. You cannot perform configuration and maintenance from this mode.



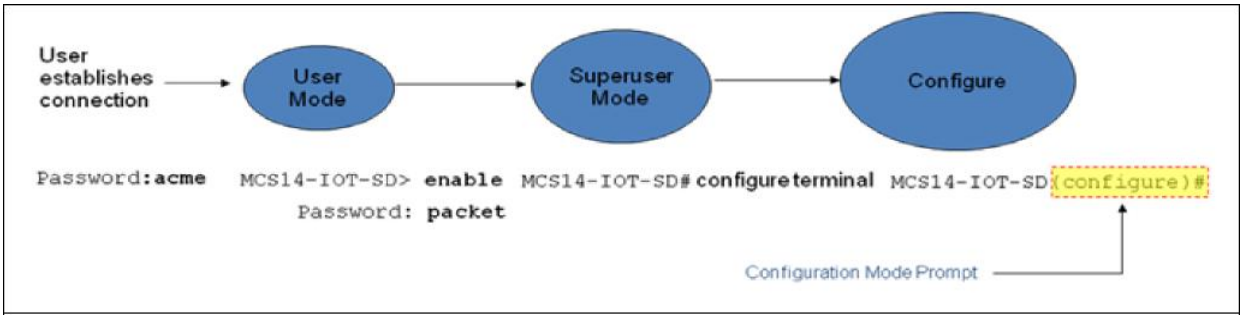
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command in the User mode.



From the Superuser mode, you can perform monitoring and administrative tasks; however you cannot configure any elements. To return to User mode, issue the exit command.

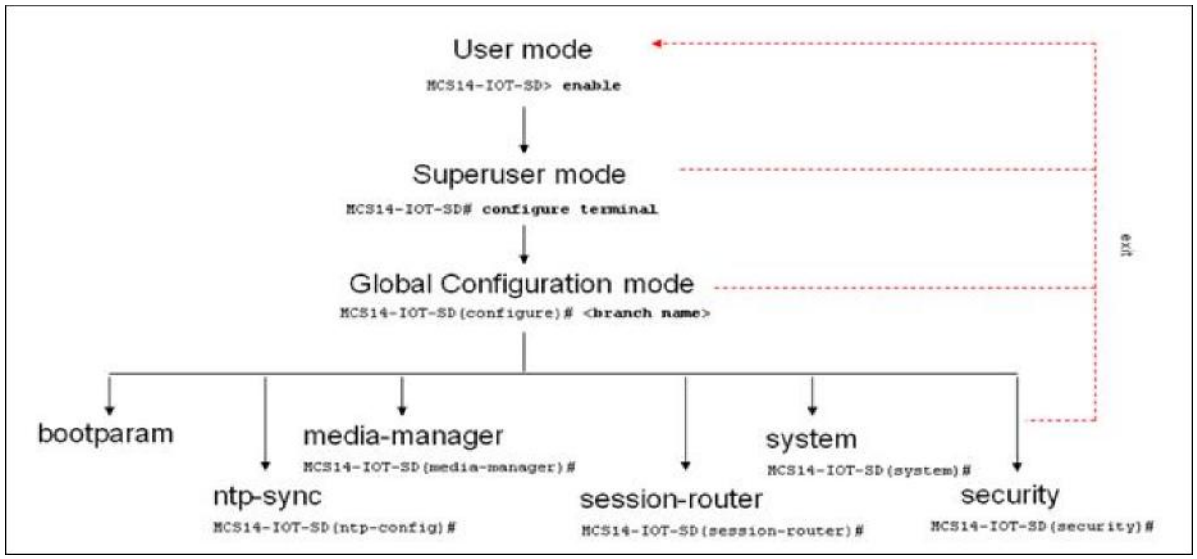
You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the configure terminal command in the Superuser mode.

Configuration mode is identified by the word configure in parenthesis followed by the pound sign (#) in the prompt after the target name, for example, oraclesbc1(configure)#. To return to the Superuser mode, issue the exit command.



In the configuration mode, there are six configuration branches:

- bootparam;
- ntp-sync;
- media-manager;
- session-router;
- system; and
- security.



The ntp-sync and bootparams branches are flat branches (i.e., they do not have elements inside the branches). The rest of the branches have several elements under each of the branches.

The bootparam branch provides access to SBC boot parameters.

The ntp-sync branch provides access to ntp server configuration commands for synchronizing the SBC time and date.

The security branch provides access to security configuration.

The system branch provides access to basic configuration elements as system-config, snmp-community, redundancy, physical interfaces, network interfaces, etc.

The session-router branch provides access to signaling and routing related elements, including H323-config, sip-config, iwf-config, local-policy, sip-manipulation, session-agent, etc.

The media-manager branch provides access to media-related elements, including realms, steering pools, dns-config, media-manager, and so forth.

You will use media-manager, session-router, and system branches for most of your working configuration.

Configuration Elements

The configuration branches contain the configuration elements. Each configurable object is referred to as an element. Each element consists of a number of configurable parameters.

Some elements are single-instance elements, meaning that there is only one of that type of the element - for example, the global system configuration and redundancy configuration.

Some elements are multiple-instance elements. There may be one or more of the elements of any given type. For example, physical and network interfaces.

Some elements (both single and multiple instance) have sub-elements. For example:

- SIP-ports - are children of the sip-interface element
- peers – are children of the redundancy element
- destinations – are children of the peer element

Creating an Element

1. To create a single-instance element, you go to the appropriate level in the ACLI path and enter its parameters. There is no need to specify a unique identifier property because a single-instance element is a global element and there is only one instance of this element.
2. When creating a multiple-instance element, you must specify a unique identifier for each instance of the element.
3. It is important to check the parameters of the element you are configuring before committing the changes. You do this by issuing the show command before issuing the done command. The parameters that you did not configure are filled with either default values or left empty.
4. On completion, you must issue the done command. The done command causes the configuration to be echoed to the screen and commits the changes to the volatile memory. It is a good idea to review this output to ensure that your configurations are correct.
5. Issue the exit command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the SBC reboots, your configurations will be lost.

Editing an Element

The procedure of editing an element is similar to creating an element, except that you must select the element that you will edit before editing it.

6. Enter the element that you will edit at the correct level of the ACLI path.
7. Select the element that you will edit, and view it before editing it.
8. The select command loads the element to the volatile memory for editing. The show command
9. allows you to view the element to ensure that it is the right one that you want to edit.
10. Once you are sure that the element you selected is the right one for editing, edit the parameter one by one. The new value you provide will overwrite the old value.
11. It is important to check the properties of the element you are configuring before committing it to the volatile memory. You do this by issuing the show command before issuing the done command.
12. On completion, you must issue the done command.
13. Issue the exit command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the SBC reboots, your configurations will be lost.

Deleting an Element

The no command deletes an element from the configuration in editing.
To delete a single-instance element,

14. Enter the no command from within the path for that specific element
15. Issue the exit command.

To delete a multiple-instance element,

16. Enter the no command from within the path for that particular element. The key field prompt, such as <name>:<sub-port-id>, appears.
17. Use the <Enter> key to display a list of the existing configured elements.
18. Enter the number corresponding to the element you wish to delete.
19. Issue the select command to view the list of elements to confirm that the element was removed.

Note that the configuration changes at this point are not permanently saved yet. If the SBC reboots, your configurations will be lost.

Configuration Versions

At any time, three versions of the configuration can exist on the SBC: the edited configuration, the saved configuration, and the running configuration.

- The edited configuration – this is the version that you are making changes to. This version of the
- configuration is stored in the SBC's volatile memory and will be lost on a reboot.
- To view the editing configuration, issue the show configuration command.
- The saved configuration – on issuing the save-config command, the edited configuration is copied into the non-volatile memory on the SBC and becomes the saved configuration. Because the saved configuration has not been activated yet, the changes in the configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded, not the saved configuration.
- The running configuration is the saved then activated configuration. On issuing the activate-config command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration. Although most of the configurations can take effect once being activated without reboot, some configurations require a reboot for the changes to take effect.
- To view the running configuration, issue command show running-config.

Saving the Configuration

The save-config command stores the edited configuration persistently.
Because the saved configuration has not been activated yet, changes in configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded. At this stage, the saved configuration is different from the running configuration.
Because the saved configuration is stored in non-volatile memory, it can be accessed and activated at later time.
Upon issuing the save-config command, the SBC displays a reminder on screen stating that you must use the activate-config command if you want the configurations to be updated.

```
oraclesbc1 # save-config
Save-Config received, processing.
waiting 1200 for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
oraclesbc1 #
```

Activating the Configuration

On issuing the activate-config command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration. Some configuration changes are service affecting when activated. For these configurations, the SBC warns that the change could have an impact on service with the configuration elements that will potentially be service affecting. You may decide whether or not to continue with applying these changes immediately or to apply them at a later time.

```
oraclesbc1# activate-config
Activate-Config received, processing.
waiting 120000 for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
oraclesbc1#
```

ORACLE

CONNECT WITH U S

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services