



AT&T IP Flexible Reach Services Including MIS/PNT/AVPN Transports with Oracle Enterprise Session Border Controller, Oracle Enterprise Operations Monitor and Microsoft Skype for Business

Technical Application Note



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

INTEND	ED AUDIENCE	5
DOCUM	ENT OVERVIEW	5
INTROD	UCTION	6
SOFTWA	ARE VERSIONS USED	6
LAB CO	DNFIGURATION	7
PHASE 1	- CONFIGURING THE ORACLE E-SBC	
CONFIG	GURATION	
1.	Login to the Net-Net SD and enter the configuration mode	10
2.	Do the Initial Configuration – Assign the management Interface an IP address	
3.	Configure system element values	
4.	Configure Physical Interface values	12
5.	Configure Global SIP configuration	14
6.	Configure Global Media configuration	
7.	Configure Realms configuration	
8.	Configure SIP signaling configuration	
<i>9</i> .	Configure next-hop signaling elements	
10.	Configure SIP routing	
11. 12	Configure media nandling	20
12. 12	SIP PRACK Interworking and Media Handling	
13.	Configure Sin manipulations and translation rules	2 کے 2 ک
14.	Vorify configuration integrity	20 11
15.	Save and activate your configuration	μ
DUACE 2		
PHASE 2	- CONFIGURING THE SKYPE FOR BUSINESS SERVER	
PHASE 3	8 - CONFIGURING THE ORACLE ENTERPRISE OPERATIONS MONITOR	61
IN SCO	PE	61
OUT OF	F SCOPE	
WHAT	WILL YOU NEED	
EOM -	· GETTING STARTED	
CONFIC	GURING EOM TO DISPLAY ALL LEGS OF A CALL IN A SINGLE REPORT	
TEST SU	MMARY	66
TROUBL	ESHOOTING TOOLS	67
Micro	soft Network Monitor (NetMon)	67
WIRES	HARK	67
Event	VIEWER	67
On thi	E ORACLE E-SBC	67
Exami	NING THE LOG FILES	67
THROU	IGH THE WEB GUI	68
Telne'	Т	68
APPEND	VIX A	69
ACCESS	Accessing the ACLI	
ACLI BASICS		69
Config	CONFIGURATION ELEMENTS	

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 3800/4000 and 6000 series platforms.

Document Overview

This Oracle technical application note outlines the recommended configurations for the Oracle Session Border Controller 3800 series for connecting AT&T's IP Flexible Reach service to Microsoft Skype for Business (SFB) customers. The solution contained within this document has been certified on Oracle's Acme Packet OS ECZ 7.3m1p1.

Microsoft Skype for Business offers the ability to connect to SIP based telephony trunks using an IP communications. This reduces the cost and complexity of extending an enterprise telephony system outside its network borders. Oracle Enterprise Session Border Controllers (E-SBCs) play an important role in SIP trunking as they are used by many ITSPs and some enterprises as part of their SIP trunking infrastructure.

This application note has been prepared as a means of ensuring that AT&T's IP Flexible Reach SIP trunking between Microsoft Skype for Business and Oracle E-SBC are configured in the optimal manner.

It should be noted that while this application note focuses on the optimal configurations for the Oracle SBC in an enterprise Skype for Business environment, the same SBC configuration model can also be used for other enterprise SIP trunking applications with changes to the configuration on the ESBC. In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the Skype for Business associated parameters. Many SBC applications may have additional configuration requirements that are specific to individual customer requirements. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

Introduction

Audience

This is a technical intended for telecommunications engineers with the purpose of configuring the Oracle Enterprise Session Border Controller (E-SBC) and Skype for Business Server. There will be steps that require navigating Microsoft windows Server 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 troubleshotting, if necessary.

Requirements

- Fully functioning Skype for Business Server deployment, including Active Directory and DNS
- A dedicated Mediation Server for the SIP trunking connection
- Microsoft Skype for Business 2015 Version 6.0.93190.0
- Skype for Business 2015 client Version 15.0.4753.1000
- Oracle Enterprise Session Border Controller AP 3820 or any Oracle ESBC appliance or VM edition running Net-Net OS ECZ730m1p1.32.bz. Note: the configuration running on the SBC is backward/forward compatible with any release in the 7.3.0 stream.

Software Versions Used

The following are the software versions used in this testing.

Component	Version
E-SBC	ECZ7.3.0 MR-1 P1 (Build 134)
Oracle Enterprise Operations Monitor	3.3.90.0.0
Microsoft Skype for Business Server 2015	6.0.9319.0

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).

Phase 1 – Configuring the Oracle E-SBC

In this section we describe the steps for configuring a Net-Net E-SBC for use with Skype for Business Server in a SIP trunking scenario.

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 Skype for Business Server. This document covers the setup for the Net-Net E-SBC platforms software SCZ 7.3m1p1 or later. A Net-Net 3800-series (NN3820) 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 Skype for Business Mediation Server
- Signaling and media IP addresses and ports to be used on the Net-Net E-SBC facing Skype for Business and AT&T SIP trunk
- Signaling IP address and port of the next hop network element in the AT&T SIP trunk network
- IP address of the enterprise DNS server

Configuration

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



Plug the slot 0 port 0 (s0p0) interface into your SIP trunk provider (SIP trunk facing) network and the slot 1 port 0 (s1p0) interface into your SFB (SFB mediation 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 **PE11-ATT-Trunk** are parameters which are specific to an individual deployment.

Note: The ACLI is case sensitive.

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.



1. 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
PE11-ATT-Trunk> enable
Password: packet
PE11-ATT-Trunk# configure terminal
PE11-ATT-Trunk (configure)#
```

You are now in the Global Configuration mode.

P 172.18.255.175 - PuTTY	
PE11-ATT-Trunk#	
PE11-ATT-Trunk# conf t	
PE11-ATT-Trunk(configure)#	-

2. Do the 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 PE11-ATT-Trunk#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

```
PE11-ATT-Trunk# (configure) bootparam
'.' = clear field; '-' = go to previous field; g = quit
boot device
                       : eth0
processor number
                       : 0
                        : acmesystem
host name
                       : /boot/nnECZ730m1p1.32.bz--- >location where the
file name
software is loaded on the SBC
inet on ethernet (e) : 172.18.255.175: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)
                        : PE11-ATT-Trunk
startup script (s)
                        :
other (o)
                        :
```

3. Configure system element values

To configure system element values, use the **system-config** command under the system branch. Then enter values appropriate to your environment, including your default gateway IP address for your management Ethernet interface.

```
PE11-ATT-TRUNK(configure)# system
PE11-ATT-TRUNK(system)# system-config
PE11-ATT-TRUNK(system-config)# hostname ATT-trunk-IOT
PE11-ATT-TRUNK(system-config)# description "SFB with ATT SIP Trunking"
PE11-ATT-TRUNK(system-config)# location "Bedford, MA"
PE11-ATT-TRUNK(system-config)# default-gateway 172.18.0.1
PE11-ATT-Trunk(comm-monitor)# state enabled
PE11-ATT-Trunk(monitor-collector)# address 172.18.255.101
PE11-ATT-TRUNK(system-config)# done
```

Once the **system-config** settings have completed and you enter **done**, the Net-Net SBC will output a complete listing of all current settings. This will apply throughout the rest of the configuration and is a

function of the **done** command. Confirm the output reflects the values you just entered as well as any configuration defaults.

system-config	
hostname	ATT-trunk-IOT
process-log-level	DEBUG
comm-monitor	
state	enabled
monitor-collector	
address	
172.18.255.101	
default-gateway	172.18.0.1

4. Configure Physical Interface values

To configure physical Interface values, use the **phy-interface** command under the system branch. To enter the system branch from system-config, you issue the **exit** command then the **phy-interface** command.

You will first configure the slot 0, port 0 interface designated with the name s0p0. This will be the port plugged into your inside (connection to the PSTN gateway) interface.

```
PE11-ATT-TRUNK(system-config)# exit
PE11-ATT-TRUNK(system)# phy-interface
PE11-ATT-TRUNK(phy-interface)# name M00
PE11-ATT-TRUNK(phy-interface)# operation-type media
PE11-ATT-TRUNK(phy-interface)# slot 0
PE11-ATT-TRUNK(phy-interface)# port 0
PE11-ATT-TRUNK(phy-interface)# done
```

Once the **phy-interface** settings have completed for slot 0 port 0 and you enter **done**, the Net-Net SBC will output a complete listing of all current settings. Confirm the output reflects the values you just entered.

phy-interface	
name	M00
operation-type	Media
port	0
slot	0
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
overload-protection	disabled

You will now configure the slot 1 port 0 phy-interface, specifying the appropriate values. This will be the port plugged into your outside (connection to the mediation server) interface.

PE11-ATT-TRUNK(phy-interface)#	name M10
PE11-ATT-TRUNK(phy-interface)#	operation-type media
PE11-ATT-TRUNK(phy-interface)#	slot 1
PE11-ATT-TRUNK(phy-interface)#	port 0
PE11-ATT-TRUNK(phy-interface)#	done
phy-interface	
name	M10
operation-type	Media
port	0
slot	1
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
overload-protection	disabled

6. Configure Network Interface values

To configure Network Interface values, use the **network-interface** command under the system branch. To enter the system branch from **phy-interface**, you issue the **exit** command then the **network-interface** command.

You will first configure the IP characteristics for the M10 interface defined above.

```
PE11-ATT-TRUNK(phy-interface) # exit
PE11-ATT-TRUNK(system) # network-interface
PE11-ATT-TRUNK(network-interface) # name s1p0
PE11-ATT-TRUNK (network-interface) # description "Mediation Server-facing
inside interface"
PE11-ATT-TRUNK(network-interface) # hostname attsbc.partnersfb.com
PE11-ATT-TRUNK(network-interface) # ip-address 192.168.4.130
PE11-ATT-TRUNK(network-interface) # netmask 255.255.255.0
PE11-ATT-TRUNK(network-interface) # gateway 192.168.4.1
PE11-ATT-TRUNK (network-interface) # dns-ip-primary 192.168.4.150
PE11-ATT-TRUNK (network-interface) # dns-domain partnersfb.com
PE11-ATT-TRUNK(network-interface) # add-hip-ip 192.168.4.130
PE11-ATT-TRUNK (network-interface) # add-icmp-ip 192.168.4.130
PE11-ATT-TRUNK(network-interface) # done
network-interface
        name
                                        s1p0
```

sub-port-id	0
description	Mediation Server-facing inside
interface	
hostname	attsbc.partnersfb.com
ip-address	192.168.4.130
netmask	255.255.255.0
gateway	192.168.4.1
dns-ip-primary	192.168.4.150
dns-domain	partnersfb.com
hip-ip-list	192.168.4.130
icmp-address	192.168.4.130

You will now configure the slot 0 port 0 subport 0 network-interface, specifying the appropriate values.

<pre>PE11-ATT-TRUNK(network-interface)#</pre>	name s0p0
<pre>PE11-ATT-TRUNK(network-interface)#</pre>	description "ATT gateway-facing inside
interface"	
<pre>PE11-ATT-TRUNK(network-interface)#</pre>	ip-address 155.212.214.181
<pre>PE11-ATT-TRUNK(network-interface)#</pre>	netmask 255.255.255.0
<pre>PE11-ATT-TRUNK(network-interface)#</pre>	gateway 155.212.214.1
<pre>PE11-ATT-TRUNK(network-interface)#</pre>	add-hip-ip 155.212.214.181
<pre>PE11-ATT-TRUNK(network-interface)#</pre>	add-icmp-ip 155.212.214.181
<pre>PE11-ATT-TRUNK(network-interface)#</pre>	done
network-interface	
name	s0p0
sub-port-id	0
description	VoIP gateway-facing inside interface
name	sOpO
ip-address	155.212.214.181
netmask	255.255.255.0
gateway	155.212.214.1
hip-ip-list	155.212.214.181
icmp-address	155.212.214.181

5. Configure Global SIP configuration

To configure the Global SIP values, use the **sip-config** command under the **session-router** branch. To enter the session-router branch from **network-interface**, you issue the **exit** command twice, followed by the **sip-config** command.

PE11-ATT-TRUNK(network-interface)# exit
PE11-ATT-TRUNK(system)# exit
PE11-ATT-TRUNK(configure)# session-router
PE11-ATT-TRUNK(session-router)# sip-config
PE11-ATT-TRUNK(sip-config)# home-realm-id core

PE11-ATT-TRUNK(sip-config)# sip-message-len 6000			
PE11-ATT-TRUNK(sip-config)#options +max-udp-length=0			
PE11-ATT-TRUNK(sip-config) # done			
sip-config			
state	enabled		
home-realm-id	core		
options	max-udp-length=0		
sip-message-len	6000		
refer-src-routing	enabled		

6. Configure Global Media configuration

To configure the Media values, use the media-manager command under the **media-manager** branch. To enter the **media-manager** branch from **sip-config**, you issue the **exit** command twice, followed by the media-manager command twice.

By issuing the select then done commands at this level, you will be creating the **media-manager** element, enabling the media management functions in the Net-Net SBC with the default values.

```
PE11-ATT-TRUNK(sip-config)# exit
PE11-ATT-TRUNK(session-router)# exit
PE11-ATT-TRUNK(configure)# media-manager
PE11-ATT-TRUNK(media-manager)# media-manager
PE11-ATT-TRUNK(media-manager)# state enabled
PE11-ATT-TRUNK(media-manager-config)# done
media-manager
state enabled
```

7. Configure Realms configuration

To configure the realm values, use the **realm-config** command under the **media-manager** branch. To enter the **media-manager** branch from **media-manager-config**, you issue the **exit** command, followed by the **realm-config** command.

You will create two realms:

- The core, which represents the mediation server-facing (inside) network; and
- The trunk-side, which represents the gateway-facing (outside) network.

```
PE11-ATT-TRUNK (media-manager-config) # exit
PE11-ATT-TRUNK (media-manager) # realm-config
PE11-ATT-TRUNK (realm-config) # identifier core
PE11-ATT-TRUNK (realm-config) # description "Mediation Server-facing
(Inside)"
PE11-ATT-TRUNK (realm-config) # network-interfaces s1p0:0
PE11-ATT-TRUNK (realm-config) # mm-in-realm enabled
PE11-ATT-TRUNK (realm-config) # media-sec-policy sdespolicy
```

PE11-ATT-TRUNK(realm-config)#	restricted-latching sdp
PE11-ATT-TRUNK (realm-config)#	refer-call-transfer enabled
PE11-ATT-TRUNK (realm-config)#	codec-policy TrunkCodecs
PE11-ATT-TRUNK (realm-config) #	done
realm-config	
identifier	core
description	Mediation Server-facing
(Inside)	
network-interfaces	s1p0:0
mm-in-realm	enabled
media-sec-policy	sdespolicy
restricted-latching	sdp
refer-call-transfer	enabled
codec-policy	TrunkCodecs
±	

You will now configure the PSTN realm for SIP Trunk side of the SBC, specifying the appropriate values.

<pre>PE11-ATT-TRUNK(realm-config)#</pre>	identifier trunk-side
<pre>PE11-ATT-TRUNK(realm-config)#</pre>	description "Gateway (outside)"
<pre>PE11-ATT-TRUNK(realm-config)#</pre>	<pre>network-interfaces s0p0:0</pre>
<pre>PE11-ATT-TRUNK(realm-config)#</pre>	mm-in-realm enabled
<pre>PE11-ATT-TRUNK(realm-config)#</pre>	media-sec-policy rtponly
<pre>PE11-ATT-TRUNK(realm-config)#</pre>	done
realm-config	
identifier	trunk-side
description	Gateway (outside)
network-interfaces	s0p0:0
mm-in-realm	enabled
media-sec-policy	rtponly

8. Configure SIP signaling configuration

To configure the SIP signaling values, use the **sip-interface** command under the **session-router** branch. To enter the **session-router** branch from **realm-config**, you issue the **exit** command twice, followed by the **sip-interface** command.

Here you will be configuring the IP addresses and TCP ports on which the Net-Net SBC will listen for and transmit SIP messages. These will be the same IP addresses as configured on the associated **network-interface** elements.

```
PE11-ATT-TRUNK(realm-config)# exit
PE11-ATT-TRUNK(media-manager)# exit
```

```
PE11-ATT-TRUNK(configure) # session-router
PE11-ATT-TRUNK(session-router)# sip-interface
PE11-ATT-TRUNK(sip-interface) # realm trunk-side
PE11-ATT-TRUNK(sip-interface) # sip-ports
PE11-ATT-TRUNK(sip-port)# address 155.212.214.181
PE11-ATT-TRUNK(sip-port) # allow-anonymous agents-only
PE11-ATT-TRUNK(sip-port) # done
PE11-ATT-TRUNK(sip-port) # exit
PE11-ATT-TRUNK (sip-interface) # out-manipulationid ChangeforPAIandNAT
PE11-ATT-TRUNK(sip-interface) # rfc2833-payload 100
PE11-ATT-TRUNK(sip-interface) # response-map change183to180
PE11-ATT-TRUNK(sip-interface) # done
sip-interface
                                                 trunk-side
        realm-id
        sip-port
                                                    155.212.214.181
                address
                allow-anonymous
                                                    agents-only
        out-manipulationid
                                                 ChangeforPAIandNAT
        rfc2833-payload
                                                 100
        response-map
                                                 change183to180
```

You will now configure the mediation server-facing SIP interface.

```
PE11-ATT-TRUNK(sip-interface) # realm-id core
PE11-ATT-TRUNK(sip-interface)# description "Mediation Server-Facing
(Inside)"
PE11-ATT-TRUNK(sip-interface) # sip-ports
PE11-ATT-TRUNK(sip-port) # address 192.168.4.130
PE11-ATT-TRUNK(sip-port) # transport-protocol TLS
PE11-ATT-TRUNK(sip-port) # port 5067
PE11-ATT-TRUNK(sip-port) # allow-anonymous agents-only
PE11-ATT-TRUNK(sip-port) # done
sip-port
                                                          192.168.4.130
                address
                                                          5067
                port
                                                          TLS
                transport-protocol
                tls-profile
                                                          core
                allow-anonymous
                                                          agents-only
PE11-ATT-TRUNK(sip-port) # exit
PE11-ATT-TRUNKPE11-ATT-TRUNK(sip-interface) # done
sip-interface
                                        enabled
        state
```

realm-id	core
description	Mediation Server-Facing(Inside)
sip-port	
address	192.168.4.130
port	5067
transport-protocol	TLS
tls-profile	core
allow-anonymous	agents-only

9. Configure next-hop signaling elements

To configure the next-hop signaling elements (i.e., the mediation server and PSTN gateway) you define **session-agents**. Use the **session-agent** command under the **session-router** branch. To enter the **session-agent** branch from **sip-interface**, you issue the **exit** command, followed by the **session-agent** command.

Here you will be configuring the IP addresses and TCP ports to which the Net-Net SBC will send and from which it will expect to receive SIP messages for your next-hop signaling elements.

SFB Gateway specification outlines the need for the SBC to have capability to do DNS load balancing among a pool of mediation servers. This is currently supported by the ESBC via A or SRV records, however not necessarily in a round-robin manner. In this document and testing, the SBC load balances between two mediation servers that are defined in a group (session-group) with round-robin algorithm configured. It is assumed that when using this kind of a configuration at any point another mediation server is added to the pool of servers, it will need to be explicitly configured on the SBC and added to the **session-group** which will be the responsibility of the enterprise network administrator.

We will first configure the PSTN gateway.

```
PE11-ATT-TRUNKPE11-ATT-TRUNK(sip-interface) # exit
PE11-ATT-TRUNK(session-router)#session-agent
PE11-ATT-TRUNK(session-agent)# hostname 207.242.225.210
PE11-ATT-TRUNK(session-agent) # port 5060
PE11-ATT-TRUNK(session-agent) # realm-id trunk-side
PE11-ATT-TRUNK(session-agent) #ping-method OPTIONS;hops=0
PE11-ATT-TRUNK(session-agent) #ping-interval 30
PE11-ATT-TRUNK (session-agent) #in-manipulationid changesendonly
PE11-ATT-TRUNK (session-agent) #rfc2833-payload 100
PE11-ATT-TRUNK(session-agent) # done
session-agent
                                                 207.242.225.210
        hostname
        ip-address
                                                 207.242.225.210
                                                 trunk-side
        realm-id
        description
                                                 ATT
        in-manipulationid
                                                 changesendonly
        rfc2833-payload
                                                 100
        refer-call-transfer
                                                 enabled
```

You will now define the mediation server.

Defining Mediation Server 1

<pre>PE11-ATT-TRUNK(session-agent)#</pre>	hostname medpool.partnersfb.com	
PE11-ATT-TRUNK (session-agent) #	port 5067	
PE11-ATT-TRUNK (session-agent) #	app-protocol <mark>sip</mark>	
PE11-ATT-TRUNK (session-agent) #	transport-method StaticTLS	
PE11-ATT-TRUNK (session-agent) #	realm-id core	
PE11-ATT-TRUNK (session-agent) #	ping-method OPTIONS;hops=0	
PE11-ATT-TRUNK (session-agent) #	ping-interval 30	
PE11-ATT-Trunk(session-agent)#	refer-call-transfer <mark>enabled</mark>	
<pre>PE11-ATT-Trunk(session-agent)#</pre>	out-translationid addplus1	
<pre>PE11-ATT-Trunk(session-agent)#</pre>	out-manipulationid checkFollowMeinDiversion	
<pre>PE11-ATT-Trunk(session-agent)#</pre>	load-balance-dns-query round-robin	
PE11-ATT-TRUNK (session-agent) #	done	
session-agent		
hostname	medpool.partnersfb.com	
port	5067	
transport-method	StaticTLS	
realm-id	core	
ping-method	OPTIONS	
ping-interval	30	
load-balance-dns-query	round-robin	
out-translationid	addplus1	
out-manipulationid	checkFollowMeinDiversion	
refer-call-transfer	enabled	

10. Configure SIP routing

To configure the SIP routing, use the **local-policy** command under the **session-router** branch. To enter the **session-router** branch from **session-agent**, you issue the **exit** command, followed by the **local-policy** command.

We will first configure the route from the gateway to the mediation server.

```
PE11-ATT-TRUNK(session-agent)# exit
PE11-ATT-TRUNK(session-router)# local-policy
PE11-ATT-TRUNK(local-policy)# from-address *
PE11-ATT-TRUNK(local-policy)# to-address *
PE11-ATT-TRUNK(local-policy)# source-realm trunk-side
PE11-ATT-TRUNK(local-policy)# policy-attributes
PE11-ATT-TRUNK(local-policy-attributes)#next-hop medpool.partnersfb.com
PE11-ATT-TRUNK(local-policy-attributes)# realm core
PE11-ATT-TRUNK(local-policy-attributes)# done
PE11-ATT-TRUNK(local-policy-attributes)# exit
PE11-ATT-TRUNK(local-policy)# done
```

local-policy	
from-address	*
to-address	*
source-realm	trunk-side
policy-attribute	
next-hop	<pre>medpool.partnersfb.com</pre>
realm	core

We will now configure the route from the mediation server to the gateway.

```
PE11-ATT-TRUNK(local-policy) # from-address *
PE11-ATT-TRUNK(local-policy)# to-address *
PE11-ATT-TRUNK(local-policy) # source-realm core
PE11-ATT-TRUNK(local-policy)# policy-attributes
PE11-ATT-TRUNK(local-policy-attributes)# next-hop 207.242.225.210
PE11-ATT-TRUNK(local-policy-attributes)# realm trunk-side
PE11-ATT-TRUNK(local-policy-attributes)# app-protocol sip
PE11-ATT-TRUNK(local-policy-attributes) # done
PE11-ATT-TRUNK(local-policy-attributes) # exit
PE11-ATT-TRUNK(local-policy) # done
local-policy
        from-address
        to-address
        source-realm
                                                 core
        policy-attribute
                next-hop
                                                         207.242.225.210
                                                         trunk-side
                realm
                app-protocol
                                                         SIP
```

11. Configure media handling

To configure the media handling, use the **steering-pool** command under the **media-manager** branch. To enter the **steering-pool** branch from **local-policy**, you issue the **exit** command twice, followed by the **media-manager** then the **steering-pool** command.

You will use the same IP address for the steering pool as the one used for the SIP interface. Note that the port ranges provide a means of limiting the number of concurrent media sessions within a given realm. For example, assigning 100 ports to a realm would limit it to 50 concurrent bidirectional calls, where two ports are assigned (one port for RTP and second port for RTCP).

```
PE11-ATT-TRUNK(local-policy)# exit
PE11-ATT-TRUNK(session-router)# exit
PE11-ATT-TRUNK(configure)# media-manager
PE11-ATT-TRUNK(media-manager)# steering-pool
PE11-ATT-TRUNK(steering-pool)# ip-address 192.168.4.130
```

```
PE11-ATT-TRUNK(steering-pool)# start-port 20000
PE11-ATT-TRUNK(steering-pool)# end-port 40000
PE11-ATT-TRUNK(steering-pool)# realm-id core
PE11-ATT-TRUNK(steering-pool)# done
steering-pool
ip-address 192.168.4.130
start-port 20000
end-port 40000
realm-id core
```

You will now configure the media handling for the ATT realm.

12. SIP PRACK interworking and Media Handling

SIP PRACK Interworking

In order to establish an early media session for outbound calls, SFB gateway specification mandates the PSTN gateways to offer a reliable provisional response and for inbound calls offer INVITEs with a supported header The SBC can interwork and provide RFC 3262 PRACK interworking towards SFB and it is a mandatory configuration in all Oracle SBC – Microsoft SFB deployments. For this, the following need to be configured:

- Configure option 100rel-interworking on the sip-interface facing mediation server
- Configure a sip-feature to pass the 100rel in supported and require headers
- Configure a manipulation to add a Require:100rel header in incoming SIP INVITE from mediation server and delete the Supported:100rel header

```
PE11-ATT-TRUNK(session-router)# sip-interface
PE11-ATT-Trunk(sip-interface)# sel
<realm-id>:
1: core 192.168.4.130:5067
2: trunk-side 155.212.214.181:5060
selection: 1
PE11-ATT-TRUNK(sip-interface)#options 100rel-interworking
```

Configure Sip-feature to pass Supported and Require headers in SIP messages

```
PE11-ATT-TRUNK (session-router) #sip-feature
PE11-ATT-TRUNK (sip-feature) #name 100rel
PE11-ATT-TRUNK(sip-feature)#realm pstn
PE11-ATT-TRUNK(sip-feature) # support-mode-inbound Pass
PE11-ATT-TRUNK(sip-feature) # require-mode-inbound Pass
PE11-ATT-TRUNK(sip-feature)# proxy-require-mode-inbound Pass
PE11-ATT-TRUNK(sip-feature)# support-mode-outbound Pass
PE11-ATT-TRUNK(sip-feature) # require-mode-outbound Pass
PE11-ATT-TRUNK (sip-feature) # proxy-require-mode-outbound Pass
PE11-ATT-TRUNK(sip-feature)#done
sip-feature
      name
                                      100rel
     realm
                                      pstn
     support-mode-inbound
                                      Pass
     require-mode-inbound
                                      Pass
      proxy-require-mode-inbound
                                      Pass
      support-mode-outbound
                                      Pass
      require-mode-outbound
                                      Pass
      proxy-require-mode-outbound
                                      Pass
```

The manipulation to add Require:100rel header will be configured in the next section.

13. ESBC config for Microsoft Media Bypass feature

In order for Media Bypass to work, both Client and gateway (SBC) need to use the same RTP format, either SRTP (by default) or RTP. In default configuration of MS SFB, SFB client is required to use media encryption, so Media Bypass is mainly when media is encrypted (SRTP) and exchanged between SFB client and PSTN gateway (Net-Net ESBC).

Media Bypass from ESBC's perspective is routing RTP traffic to an endpoint/SFB client on a private routable network directly (instead of RTP going through the mediation server). To enable the SBC to handle the media bypass feature in SFB, you will need to set **restricted-latching** to **sdp** in the core realm (facing mediation server). Select the core realm from the **media-manager --- > realm-config** configuration branch. Note: This setting is recommended irrespective of the media bypass setting.

identifier	core
network-interfaces	s1p0:0
mm-in-realm	enabled
media-sec-policy	sdespolicy
restricted-latching	sdp
refer-call-transfer	enabled
codec-policy	TrunkCodecs

Recently, in some accounts where MS Lync and Oracle SBCs are deployed for enterprise voice and SIP trunk termination to an enterprise, there have been complaints of the PSTN caller hearing a silence when a call is placed from PSTN to a SFB user on the enterprise especially when Media Bypass is enabled on MS SFB The configuration note below aims to explain this scenario briefly, steps taken to rectify this issue and proposed workaround by Acme Packet. The workaround is an interim solution while a permanent solution is being researched and developed by Oracle Communications Engineering.

Media Bypass

As explained earlier in the document, in order for Media Bypass to work, both Client and gateway (SBC) need to use the same RTP format, either SRTP (by default) or RTP. In default configuration of MS SFB, SFB client is required to use media encryption, so Media Bypass is mainly when media is encrypted (SRTP) and exchanged between SFB client and PSTN gateway (E-SBC).

Signaling between mediation server and SBC is a little different (Two 183s with SDP coming from mediation server) when media bypass is enabled on Lync.

The following is the call flow:

After signaling 183 with SDP, SFB never plays any early media and expects gateway (E-SBC) to signal appropriately to the SIP Trunk provider to follow RFC 3960 and play local RBT. The second 183w SDP coming from Mediation server which is forwarded to the SIP trunk and stops the local RBT which was started after 180 Ringing was sent, hence PSTN caller would hear a silence before Lync client answers call.

The solution here is to present 180 ringing (i.e. convert all 183s on lync side to 180 ringing towards SIP trunk and strip the SDP) to trigger RBT in ISUP. The call flow is modified with the help of Oracle Communication's robust Sip Manipulation and Sip Response Map features to the following:



The following header rules needs to be included in the manipulation that is applied on the realm or sip-interface
facing Lync to modify the signaling traffic sent from Lync.

header-rule	
name	delsupported
header-name	Supported
action	delete
comparison-type	case-sensitive
msg-type	request
methods	INVITE
match-value	
new-value	
header-rule	
name	addrequireinINVITE
header-name	Require
action	add
comparison-type	case-sensitive
msg-type	request

	methods	INVITE
	match-value	
		1001
	new-value	luurel
header-	rule	
	name	formod183
	header-name	From
	action	sip-manip
	comparison-type	case-sensitive
	msg-type	any
	methods	
	match-value	
	new-value	Stripsdp183 (the manipulation
Stripsdp183 is a	mentioned below)	

sip-manipulation	
name	Stripsdp183
description	For incoming 183 from Lync, strip SDP
split-headers	
join-headers	
header-rule	
name	check183
header-name	@status-line
action	store
comparison-type	pattern-rule
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	is183
parameter-name	
type	status-code
action	store
match-val-type	any
comparison-typ	e pattern-rule
match-value	183
new-value	
header-rule	
name	delSDP
header-name	Content-Type
action	manipulate
comparison-type	case-insensitive
msg-type methods	any
match-value	\$check183.\$is183
new-value	
element-rule	
name	del183SDP
parameter-name	application/sdp
type	mime
action	delete-element
match-val-tvpe	any
comparison-tvp	e boolean
match-value	
new-value	
header-rule	
name	delContentType

head	der-name	Content-Type
act	ion	manipulate
COM	parison-type	boolean
msg	-type	any
metl	nods	
mate	ch-value	\$check183.\$is183
new	-value	
eler	ment-rule	
	name	delCT
	parameter-name	*
	type	header-param
	action	delete-header
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	

The following sip response map needs to be configured and applied on the sip interface facing ATT.

response-map				
last-modified	-by	admin@1	0.0.	221.18
last-modified	-date	2012-06	-04	11:14:17
name		change1	83to	180
entries				
		183 ->	180	(Ringing)
sip-interface				
state		е	nabl	ed
realm-i	d	A	TT	
descrip	tion			
sip-por	t			
	address			192.20.0.108
	port			5060
	transport-protoc	ol		UDP
	tls-profile			
multi-home-addrs				
allow-anonymous				agents-only
ims-aka-profile				
	••••			
response	-map	ch	ange	183to180

14. Configure Sip-manipulations and translation rules

In order to cater to AT&T's and SFB's call flow standards, we need to configure certain header manipulation rules (HMR). The **sip-manipulation** element can be found under the **session-router** element.

The HMR applied to the signaling towards the trunk performs the following changes:

- The Request-URI is modified to include the ip address and port of the trunk device
- The uri-host portion of the From header is replaced with the FQDN of the trunk, in our case the uri-host is changed to IP Address of the SBC facing the AT&T trunk

- In the Contact header, we have header rules to strip +1 from the uri-user and replace the uri-host and uriport portions with the SBC's local ip and port of the interface facing the trunk.
- In the Route header we remove the +1 from the uri-user.
- For privacy enabled calls, SFB sends the phone number in the From header. It indicates that it is a privacy enabled calls using the 'Privacy:id' header. For such calls, we replace the phone number in the uri-user of the From header with 'anonymous'.

To conform SFB's signaling per the trunk's specification, we modify the messages coming from SFB and also make some changes to messages before they are sent to SFB.

The following changes are applied to the messages coming from SFB:

- We add a 'Require:100rel' header in incoming SIP INVITE from mediation server and delete the 'Supported:100rel' header as mentioned in the SIP PRACK interworking section.
- To enabled ringback on transfers, we replace the 'a=inactive' line in SDP of the INVITEs with 'a=sendonly'. For more information, please refer to the Ring-back tone during Transfers section.

To the messages sent to SFB, the following changes are applied:

- The uri-hosts of the From and To headers are replaced with SBC's local ip and SFB's ip.
- In the From and To headers we remove the +1 from the uri-user, when the uri-user is anonymous.
- At last we have a rule to insert +1 in the uri-user of the Contact header as SFB server is configured for E.164 format.

Here is the list of HMR's used:

- ChangeContact Fixes the contact header offered by SFB before the message is sent to Trunk
- Changeinactosendonly SBC changes SDP from inactive to sendonly on INVITEs for hold (required to trigger audio playback from SIP Trunk)
- Check183 Check the response to INVITE is 183 session progress
- NATting NAT From & To header with correct IP information
- convert183to180 Convert 183 to 180 for triggering early media
- ForEarlyMedia To locally handle PRACK interworking
- Lyncprivacy NAT plus recvonly to inactive
- ChangeforPAIandNAT configured on the trunk side to change the Privacy, Nating

A manipulation, ChangeContact, will need to be configured to change the format of the CONTACT header which will then be referenced in the manipulation that is finally applied to the realm or sip-interface facing AT&T.

The manipulation consists of two header rules – StoreFromnumber and ChangeContact. The StoreFromnumber header rule stores the uri-user-only element in the From header which is then added as the uri-user in the Contact header in the ChangeContact header rule.

sip-manipulation	
name	ChangeContact
description	
split-headers	
join-headers	
header-rule	
name	StoreFromnumber

he	eader-name	From
ac	ction	manipulate
CC	omparison-type	case-sensitive
ms	sg-type	any
me	ethods	
ma	atch-value	
ne	ew-value	
el	ement-rule	
	name	StoreFromnumber_er
	parameter-name	
	type	uri-user-only
	action	store
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	
header-rul	e	
na	ame	ChangeContact
he	eader-name	Contact
ac	ction	manipulate
cc	omparison-type	case-sensitive
ms	sg-type	any
me	ethods	
ma	atch-value	
ne	ew-value	
el	ement-rule	
	name	ChangeContact_er
	parameter-name	
	type	uri-user
	action	add
	match-val-type	any
	comparison-type	case-sensitive
	and the state of the state	
	match-value	
	match-value new-value	

The manipulation ChangeforPAIandNAT is configured on the trunk side to change the Privacy, Nating.

sip-manipulation	
name	ChangeforPAIandNAT
description	Change PAI and NATing
split-headers	
join-headers	
header-rule	
name	forprivacy
header-name	From
action	sip-manip
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	NATting
header-rule	
name	fordiv

header-name From action sip-manip comparison-type case-sensitive msg-type any methods match-value new-value AddDiversion header-rule ForREFER name header-name From action sip-manip comparison-type case-sensitive msg-type any methods match-value changeRefer new-value header-rule ForREFER name header-name From action sip-manip comparison-type case-sensitive msg-type any methods match-value ChangeContact new-value header-rule Refer header name header-name Referred-By action manipulate case-sensitive comparison-type msg-type any methods match-value new-value element-rule referredbyhdr name parameter-name type uri-host action replace match-val-type any comparison-type case-sensitive match-value \$LOCAL IP new-value header-rule name changePrivacy header-name From action sip-manip comparison-type case-sensitive msg-type any methods match-value new-value Check_privacy_header

The sip-manipulation then needs to be applied on the realm or sip-interface or session-agent towards the ATT trunk side. We apply it on the sip-interface here:

```
PE11-ATT-TRUNK(session-router)# sip-interface
PE11-ATT-Trunk(sip-interface)# sel
<realm-id>:
1: core 192.168.4.130:5067
2: trunk-side 155.212.214.181:5060
selection: 2
PE11-ATT-Trunk(sip-interface)# out-manipulationid ChangeforPAIandNAT
PE11-ATT-Trunk(sip-interface)# done
```

In order to complete the calls successfully per AT&T's signaling specifications, we need to configure manipulation rules on the realm facing SFB. The manipulations are mentioned below. The sip-manipulation NATting ensure topology hiding.

sip-manipulation	
name NAT	'ting
description	
split-headers	
join-headers	
header-rule	
name	From
header-name	From
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	From_header
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	То
header-name	То
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	То
parameter-name	

typeuri-hostactionreplacematch-val-typeanycomparison-typecase-sensitivematch-valuematch-valuenew-value\$REMOTE_IP

For simultaneous ringing, the following manipulation is configured

sip-manipulation	
name	ATT-Simulring
description	HMR for simul ring towards Lync
split-headers	
join-headers	
header-rule	
name	getTo
header-name	То
action	store
comparison-type	case-sensitive
msg-type	request
methods	INVITE
match-value	
new-value	
element-rule	
name	getTag
parameter-name	tag
type	header-param
action	store
match-val-type	any
comparison-typ	e pattern-rule
match-value	
new-value	
header-rule	
name	checkHoldSdp
header-name	Content-Type
action	store
comparison-type	boolean
msg-type	request
methods	INVITE
match-value	!\$getTo.\$getTag
new-value	
element-rule	
name	checkIP
parameter-name	application/sdp
type	mime
action	store
match-val-type	any
comparison-typ	e case-sensitive

match-value \Rc=IN IP4 0\.0\.0\b new-value fixSdptest header-name Content-Type action manipulate comparison-type boolean msg-type request methods INVITE match-value \$checkHoldSdp.\$checkIP new-value element-rule replaceIP name parameter-name application/sdp type

mime find-replace-all anv pattern-rule \Rc=IN IP4

 $(0 \ .0 \ .0 \ .0) \ b[[:1:]]$

header-rule

name

new-value

match-value

match-val-type

comparison-type

action

header-rule name header-name action comparison-type msg-type methods match-value new-value element-rule name parameter-name type action match-val-type comparison-type match-value new-value header-rule name header-name action comparison-type msg-type methods match-value new-value element-rule name

\$LOCAL IP

checkmodinactive Content-Type store boolean request INVITE !\$getTo.\$getTag

> checkstate application/sdp mime store any pattern-rule \Ra=inactive\b

fixinactive Content-Type manipulate boolean request INVITE \$checkmodinactive.\$checkstate

replaceAttribute

parameter-name	application/sdp
type	mime
action	find-replace-all
match-val-type	any
comparison-type	pattern-rule
match-value	\Ra=inactive\b
new-value	

The manipulations NATting and ATT-Simulring need to be applied to manipulate the signaling sent to devices in the realm core. Hence the following nested sip-manipulation Lyncprivacy is configured.

sip-manipulat	zion	
name		Lyncprivacy
descr	iption	NAT plus recvonly to inactive
split	-headers	
join-	headers	
heade	er-rule	
	name	doNATforlync
	header-name	From
	action	sip-manip
	comparison-type	case-sensitive
	msg-type	any
	methods	
	match-value	
	new-value	NATting
heade	er-rule	
	name	manipPPreferredIdentity
	header-name	P-Preferred-Identity
	action	manipulate
	comparison-type	case-sensitive
	msg-type	request
	methods	
	match-value	
	new-value	
	element-rule	
	name	PPreferredIdentityURIHost
	parameter-nam	ne
	type	uri-host
	action	replace
	match-val-typ	be any
	comparison-ty	ype case-sensitive
	match-value	
	new-value	\$LOCAL_IP
heade	er-rule	
	name	simulring
	header-name	F.L.
	action	sip-manip
	comparison-type	case-sensitive

msg-type	request	
methods	INVITE	
match-val	ue	
new-value	ATT-Simul	ring

This manipulation is applied on the sip-interface or realm facing SFB.

```
PE11-ATT-TRUNK(session-router)# sip-interface
PE11-ATT-Trunk(sip-interface)# sel
<realm-id>:
1: MS-Lync-Peer 192.168.2.130:5068
Note:2: ATT 192.20.0.108:5060
selection: 1
PE11-ATT-Trunk(sip-interface)# out-manipulationid Lyncprivacy
PE11-ATT-Trunk(sip-interface)# done
```

During call transfer to a PSTN party, the transfer completes but the calling party does not hear a ring back tone during the process of transfer. The INVITE Lync sends to the SBC to initiate the transfer contains the SDP attribute, a=inactive which is forwarded to the trunk and as a result of which the SBC cannot play the ring back tone to the original PSTN caller (while call is being transferred). A sendonly attribute is required for MoH and transfer scenarios for the calling party to be able to hear ringback or MoH when it is kept on hold. The SBC is able to signal appropriately towards the SIP trunk by changing the a=inactive SDP attribute in the INVITE to sendonly towards PSTN. This attribute needs to be changed to a=sendrecv when it is sent to AT&T so that the ringback tone or the MOH can be heard.

Sip manipulations are configured to make the necessary changes. The manipulation Changeinactosendonly is configured to change the SDP attribute from a=inactive to a=sendonly in the INVITEs sent to the calling party for transfer.

sip-manipulation		
name		Changeinactosendonly
description		Change inactive to sendonly for pstn tran
split-headers		
join-headers		
header-rule		
name		changeSDP
header-	name	Content-Type
action		manipulate
compari	son-type	case-sensitive
msg-typ	e	request
methods		INVITE
match-v	alue	
new-val	ue	
element	-rule	
	name	inacttosendonly
	parameter-name	application/sdp
	type	mime
	action	find-replace-all
	match-val-type	any
	comparison-type	e pattern-rule

match-value new-value	a=inactive a=sendonly	

Note:

To change the a=sendonly to a=sendrecv before sending the INVITE to AT&T, we have a header rule Changesendonlytosendrecv included in the manipulation Privacy that is applied on the sip-interface facing AT&T.

A nested sip manipulation Forearlymedia is configured to include the header rules mentioned in the section "SIP PRACK interworking and Media Handling" and the manipulation Changeinactosendonly

The manipulation ChangeforPAIandNAT is configured on the trunk side to change the Privacy, Nating.

sip-manipulatio	n			
name		Changefo	orPAIandNAT	
descrip	tion	Change F	PAI and NATing	
split-h	eaders			
join-he	aders			
header-	rule			
	name		forprivacy	
	header-name		From	
	action		sip-manip	
	comparison-type		case-sensitive	
	msg-type		any	
	methods			
	match-value			
	new-value		NATting	
header-	rule			
	name		fordiv	
	header-name		From	
	action		sip-manip	
	comparison-type		case-sensitive	
	msg-type		any	
	methods			
	match-value			
	new-value		AddDiversion	
header-	rule			
	name		ForREFER	
	header-name		From	
	action		sip-manip	
	comparison-type		case-sensitive	
	msg-type		any	
	methods			
	match-value			
	new-value		changeRefer	
header-	rule			
	name		ForREFER	
	header-name		From	
	action		sip-manip	
	comparison-type		case-sensitive	
	msg-type		any	
	methods			
	match-value			
	new-value		ChangeContact	
header-	rule			
	name		Refer_header	
	header-name		Referred-By	

action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	referredbyhdr
paramete	r-name
type	uri-host
action	replace
match-va	l-type any
comparis	on-type case-sensitive
match-va	lue
new-valu	e \$local ip
header-rule	-
name	changePrivacy
header-name	From
action	sip-manip
comparison-type	case-sensitive
msg-type	any
methods	-
match-value	
new-value	Check privacy header

Sip manipulations for checking privacy header.

sip-manipulation		
name	Check_privacy_header	
description	Check for privacy and overwrite FROM	
split-headers		
join-headers		
header-rule		
name	ChechForPrivacy	
header-name	Privacy	
action	manipulate	
comparison-type	case-sensitive	
msg-type	request	
methods	INVITE	
match-value		
new-value		
header-rule		
name	OverwriteFrom	
header-name	From	
action	manipulate	
comparison-type	boolean	
msg-type	request	
methods	INVITE	
match-value	\$ChechForPrivacy	
new-value		
element-rule		
name	OverwriteUser	
parameter-n	ame	
type	uri-user	
	action	find-replace-all
-------------	-----------------	----------------------
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	anonymous
header-rule		4
name		remove P Asserted ID
heade	r-name	P-ASSERTED-IDENTITY
actio	n	delete
compa	rison-type	case-insensitive
msg-t	ype	request
metho	ds	INVITE
match	-value	
new-v	alue	
header-rule		
name		OverwriteFromDisplay
heade	r-name	From
actio	1	manipulate
compa	rison-type	boolean
msg-t	ype	request
metho	ds	INVITE
match	-value	\$ChechForPrivacy
new-v	alue	
eleme	nt-rule	
	name	OverwriteDisplay
	parameter-name	
	type	uri-display
	action	find-replace-all
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	"\"Anonymous\" "
header-rule		
name		add P Asserted ID
heade	r-name	P-Asserted-Identity
actio	ı	add
compa	rison-type	case-sensitive
msg-t	ype	request
metho	ls	INVITE
match	-value	
	-	

Following HMR (checkFollowMeinDiversion) is required when sequential-ring feature is enabled for particular DIDs. In a Sequential ring call flow – a trunk user first calls number 1 – since Sequential ring is enabled for this DID and no answer response was received by the trunk – trunk sends a new INVITE with sendonly in the original SDP offer to the second DID (which is configured as the sequential ring DID). To the SFB's mediation server the second INVITE with sendonly is not an acceptable offer – the mediation server rejects the INVITE if the first INVITE has nothing other than sendrecy. In order to work around this limitation on SFB, following HMR was built.

A header rule adds the text "Follow me" to from header's uri-display if diversion header with follow-me value is present. If the INVITE message doesn't have the Diversion header, the HMR will delete "Follow Me" from uri-display.

Before sending the 200 OK – the SBC checks if the "Follow Me" is present in the uri-display – only if present will add "recvonly" if not, allows the 200 OK without any manipulation.

nar	ne	checkFollowMeinDiversion
de	scription	check for follow me in diversion header
sp	lit-headers	
io	in-headers	
hea	ader-rule	
	name	checkFollowMe
	header-name	Diversion
	action	manipulate
	comparison-type	case-sensitive
	msg-type	request
	methods	TNVTTE
	match-value	
	new-value	
	element-rule	
	name	checkFollowMe er
	parameter-name	e reason
	tvpe	header-param
	action	store
	match-val-tvpe	e any
	comparison-tv	pe case-sensitive
	match-value	follow-me
	new-value	
hea	ader-rule	
	name	addFollowMeFrom
	header-name	From
	action	manipulate
	comparison-type	boolean
	msg-type	request
	methods	INVITE
	match-value	<pre>\$checkFollowMe.\$checkFollowMe_er</pre>
	new-value	
	element-rule	
	name	addFollowMeFrom_er
	parameter-name	e
	type	uri-display
	action	add
	match-val-type	e any
	comparison-typ	pe case-sensitive
	match-value	
_	new-value	"Follow Me"
hea	ader-rule	
	name	checkDiv
	header-name	Diversion
	action	manipulate
	comparison-type	case-sensitive
	msg-type	request
	methods	INVITE
	match-value	
	new-value	
hea	ader-rule	
	name	removeFollowme
	header-name	From
	action	manıpulate

comparison-type boolean msg-type request methods INVITE match-value !\$checkDiv new-value element-rule name removeFollowme er parameter-name uri-display type find-replace-all action match-val-type any comparison-type case-sensitive match-value Follow Me new-value header-rule checkFollowMeFrom200 name header-name From action manipulate comparison-type case-sensitive msg-type reply methods match-value new-value element-rule checkFollowMeFrom200_er name parameter-name uri-display type action store match-val-type any comparison-type case-sensitive match-value Follow Me new-value header-rule addrecvOnly name header-name Content-Type action manipulate boolean comparison-type msg-type reply methods match-value \$checkFollowMeFrom200.\$checkFollowMeFrom200 er new-value element-rule addrecvOnly er name parameter-name application/sdp type mime action find-replace-all match-val-type any comparison-type pattern-rule match-value new-value \$ORIGINAL+\$CRLF+"a=recvonly"

sip-manipu	lation	
na	ame	Forearlymedia
de	escription	
sp	olit-headers	
j¢	oin-headers	
he	eader-rule	
	name	delsupported
	header-name	Supported
	action	delete
	comparison-type	case-sensitiv
	msg-type	request
	methods	INVITE
	match-value	
	new-value	
he	eader-rule	
	name	addreguireinI
	header-name	Require
	action	add
	comparison-type	case-sensitiv
	msa-type	request
	methods	TNVTTE
	match-value	
	new-value	100re]
he	pader-rule	100101
110	name	mod183
	header-name	From
	action	sin-manin
	comparison-type	case-sensitiv
	msa-type	any
	methods	any
	match-walue	
		Stringdn183
he	new value	Scribsdbios
110	name	inactosendonl
	header-name	From
	action	sin-manin
		sip-manip
		case sensitiv
	methods	request
	metrious	
		Changeinagter
h		Changerhactos
116		ChackEallarma
	hander-name	Erom
	accion	sip-manip
	comparison-cype	Case-sensitiv
	msg-type	request
	metrious	
	match-value	
	new-value	CNECKFOLLOW

7e

INVITE ve

- 7e
- LУ ve

sendonly

7e

WMeinDiversion

The sip-interface or realm facing Lync is configured with this manipulation as the in-manipulationid.

```
PE11-ATT-TRUNK(session-router)# sip-interface
PE11-ATT-Trunk(sip-interface)# sel
<realm-id>:
1: core 192.168.4.130:5067
2: trunk-side 155.212.214.181:5060
selection: 1
PE11-ATT-Trunk(sip-interface)# in-manipulationid Forearlymedia
PE11-ATT-Trunk(sip-interface)# done
```

15. Verify configuration integrity

You will verify your configuration referential integrity before saving and activating it with the **verify-config** command. This command is available from Superuser Mode. To enter the Superuser Mode from steering-pool, you issue the exit command three times.

16. Save and activate your configuration

You will now save your configuration with the **save-config** command. This will make it persistent through reboots, but it will not take effect until after you issue the **activate-config** command.

```
PE11-ATT-TRUNK# save-config
checking configuration
Save-Config received, processing.
waiting 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'.
PE11-ATT-TRUNK# activate-config
Activate-Config received, processing.
waiting for request to finish
Setting phy0 on Slot=0, Port=0, MAC=00:08:25:03:FC:43,
VMAC=00:08:25:03:FC:43
Setting phy1 on Slot=1, Port=0, MAC=00:08:25:03:FC:45,
VMAC=00:08:25:03:FC:45
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
```

Phase 2 – Configuring the Skype for Business Server

The enterprise will have a fully functioning Skype for Business Server infrastructure with Enterprise Voice deployed and a Mediation Server dedicated to this installation. If there is no Mediation Server present for this purpose, one will have to be deployed.

There are two parts for configuring Lync Server to operate with the Oracle ESBC:

- Adding the Net-Net SBC as a PSTN gateway to the SFB Server infrastructure
- Creating a route within the SFB Server infrastructure to utilize the SIP trunk connected to the SBC.

To add the PSTN gateway, we will need:

- IP addresses of the external facing NICs of the Mediation Servers
- IP address of the Net-Net SBC external facing port
- Rights to administer Lync Server Topology Builder
- Access to the SFB Server Topology Builder

The following process details the steps to add PSTN gateway

- 1. On the server where the Topology Builder is located start the console.
- 2. From the Start bar, select SFB Server Topology Builder.



3. The Topology Builder window will now be displayed. Select Download Topology from existing deployment.

	Skype for Business Server 2015, Topology Builder	_ 🗆 X
File Action Help	Define a new deployment from the Actions pane	
	Topology Builder	
Weld Serve e C C C C C C C C C C C C C C C C C C	me to Topology Builder. Select the source of the Skype for Business topology document. bownload Topology from existing deployment trieve a copy of the current topology from the Central Management ore and save it as a local file. Use this option if you are editing an isting deployment. been Topology from a local file been an existing Topology Builder file. Use this option if you have work progress. ew Topology eate a blank topology and save it to a local file. Use this option for fining new deployments from scratch. elp OK Cancel	

4. You will then see a screen showing that the current toplogy is being downloaded. Click the Ok button.

Skype	e for Business Server 2015, Topology Builder
File Action Help	
skype for Business Server	Define a new deployment from the Actions pane
	Download Current Topology
Please wai your deple download Download	t while Topology Builder locates a published topology for syment. To cancel this operation, click Cancel. To an existing topology later, in the Actions pane, click Topology.

5. Next you will be prompted to save the topology which you have imported. You should revision the name or number of the topology according to the standards used within the enterprise. Click the Save button

Note: This keeps track of topology changes and, if desired, will allow you to fall back from any changes you make during this installation

19	Skype for Busin	ess Server 2015, Topolo	gy Builder				
5		x					
(©) ⊙ ⊤ ↑]] « 4	(a) → ↑ II ≪ Administrat > Documents → C						
Organize 👻 New folde	Organize 🔻 New folder						
- Envorites	Name	Date modified	Туре				
Desktop	ATT SFB topology.tbxml	3/24/2016 2:40 PM	TBXML Fi				
〕 Downloads	SFB-topology.tbxml	4/15/2016 9:54 AM	TBXML Fi				
Ecent places	topology-4-15-2016.tbxml	6/27/2016 10:57 AM	TBXML Fi				
🖳 This PC							
膧 Desktop							
Documents							
Music							
Pictures							
Videos 🗠			>				
File name: ATT	T SFB topology.tbxml						
Save as type: Top	ology Builder files (*.tbxml)						
A Hide Folders		Save Can	cel				
The Folders							

6. In the upper left hand corner, expand the site in which the PSTN gateway will be added. In our case, the site is labeled **CleanDefaultTopology**. Expand Shared Components. Then click on the **PSTN Gateways**. Right click on PSTN gateways and select **New IP/PSTN Gateway**

Skype for Business Server 20	15, Topology Builder 📃 🗖 🗙
File Action Help	
 Skype for Business Server CleanDefaultTopology Lync Server 2010 Lync Server 2013 Skype for Business Server 2015 Standard Edition Front End Servers Enterprise Edition Front End pools Director pools Mediation pools Persistent Chat pools Edge pools Trusted application servers Shared Components SQL Server stores File stores 	The properties for this item are not available
 PSTN gateways Trunks Office Web App Video gateways SIP Video trunks Branch sites 	Gateway

7. In the **Define New IP/PSTN Gateway** window, enter the IP address of the **SIP interface** of the ESBC in the FQDN text box and click Next.

19	Skype for Business Server 2015, Topology Builder	_	x
File	Action Help Calculate Server 2010 Define New IP/PSTN Gateway		
	Define the PSTN Gateway FQDN		
	Define the fully qualified domain name (FQDN) for the PSTN gateway. FQDN: * attesbc.partnersfb.com		
	4		
	Help Back Next Cancel		
	 Video gateways SIP Video trunks Branch sites 		

8. Select Enable IPv4 in the Define the IP address section and click Next.

19	Skype for Business Server 2015, Topology Builder
File	Action Help
	 Description Description The properties for this item are not available for editing. The properties for this item are not available for editing.
	Define New IP/PSTN Gateway
	Define the IP address
	 Enable IPv4 Use all configured IP addresses. Limit service usage to selected IP addresses. PSTN IP address:
	 Enable IPv6 Use all configured IP addresses. Limit service usage to selected IP addresses. PSTN IP address:
	Help Back Next Cancel

9. In the next section, enter the IP address of the ESBC's SIP interface under Trunk name. Configure the Listening port for IP/PSTN gateway as 5060, TCP as the SIP Transport Protocol, and 5060 as the Associated Mediation Server port, and click Finish.

9		Skype for Business Server 2015, Topology Builder	- 0	x
File	Actio	on Help		
		Lync Server 2010 The properties for this item are not available for editing. Lync Server 2013		
	⊿ [Define New IP/PSTN Gateway		
		Define the root trunk		
		Trunk name: *		
		attesbc.partnersfb.com		
		Listening port for IP/PSTN gateway: * 5067		
	1	SIP Transport Protocol:		
	⊿ [TLS		
	t	Associated Mediation Server:		
		medpool.partnersfb.com Acme		
		Associated Mediation Server port: *		
		5067		
	1	Help Back Finish Cancel		
	Þ	SIP Video trunks		
		Branch sites		

10. In the upper right hand corner of your screen under Actions select Topology then select Publish.

18				Sky	pe	for Business Serv	er 2015, 1	opolo	gy Builder				נ ו	c
File	Actio	n Help												
⊿ [Edit Properties			^	DCTNL C-Assess								
		Topology Delete Help Standard Edition Fro Enterprise Edition Fro Director pools Mediation pools Mediation pools Mediation pools Mediation pools SFBMed1.partners SFBMed2.partners Edge pools Trusted application se Video Interop Server Shared Components SQL Server stores File stores PSTN gateways	fb.co nersft ervers pools	New Open Download Curr Save A Copy Publish Install or upgra Remove Deploy m b.com b.com	rent ade a yme	Topology) P	attesb Use al Not co Root	c.partnersfb.com I configured IPv4 addresses Infigured Trunk attesbc.partnersfb.com	medp	Medi bool.part	ation S	Server .com	
		🖏 attesbc.partnersfb	.com	ı	~	<			ш					>

11. You will now see the Publish Topology window. Click on the Next button.

9	Publish Topology	x
Pub	lish the topology	
In oro publi comp	der for Skype for Business Server 2015 to correctly route messages in your deployment, you must sh your topology. Before you publish the topology, ensure that the following tasks have been pleted:	
• // • // • F • F • C • N • N • N • N	A validation check on the root node did not return any errors. A file share has been created for all file stores that you have configured in this topology. All simple URLs have been defined. For Enterprise Edition Front End pools and Persistent Chat pools and for Monitoring Servers and Archiving Servers: All SQL Server stores are installed and accessible remotely, and firewall exceptions for remote access to SQL Server are configured. For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed. You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role). If you are removing a Front End pool, all users, common area phones, analog devices, application contact objects, and conference directories have been removed from the pool is you are ready to proceed, click Next.	<
H	elp Back Next Cancel	

12. When complete you should see a window from Topology Builder stating that your topology was successfully published. Click the Finish button.

Your topology	was successfully published.		
 ✓ Publishin ✓ Download ✓ Download ✓ Updating ✓ Enabling 	Step g topology ding topology ding global simple URL settings role-based access control (RBAC) roles topology	Status Success Success Success Success Success	View Logs

Creating a route within the Skype for Business infrastructure

In order for the Skype for Business (SFB) clients to utilize the SIP trunking infrastructure that has been put in place, a route will need to be created to allow direction to this egress. Routes specify how SFB handles calls placed by enterprise voice users. When a user places a call, the server, if necessary, normalizes the phone number to the E.164 format and then attempts to match that phone number to a SIP Uniform Resource Identifier (URI). If the server is unable to make a match, it applies outgoing call routing logic based on the number. That logic is defined in the form of a separate voice route for each set of target phone numbers listed in the location profile for a locale. For this document we are only describing how to set up a route. Other aspects which apply to SFB deployments such as dial plans, voice policies, and PSTN usages are not covered.

To add the route we will need:

- Rights to administer the SFB Control Panel
 - Membership in the CS Administrator Active Directory Group
- Access to the SFB Control Panel

The following process details the steps to create the route:

1. From the Start bar, select SFB Control Panel.



You will be prompted for credentials, enter your domain username and password.

2. Once logged in, you will now be at the "Welcome Screen". On the left hand side of the window, click on Voice Routing.

5	Skype for Business Server 2015 Control Panel	_ D ×
Skype for Busine	ess Server	Administrator Sign out 6.0.9319.0 Privacy statement
Home Users Topology IM and Presence Persistent Chat	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING Create voice routing test case information	~
Voice Routing	new 🔻 🥖 Edit 🔻 Action 🔻 Commit 💌	Ð
Response Groups	Name Scope State Normalization rules Description Clobal Global Committed 1 1	
Conferencing Clients		
Federation and External Access		
Monitoring and Archiving		
Network Configuration		

3. The Dial Plan tab in the Voice Routing section will be displayed. Select the Global dial plan. On the content area toolbar, click Edit

C Skype for Business Server 2015 Control Panel	
S Skype for Business Server 60.9319.0	ninistrator Sign out) Privacy statement
Home DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING Users Topology Create voice routing test case information	~
Persistent Chat	
Voice Routing New Edit Action Commit Operation Description Voice Features Name Scope State Normalization rules Description	0
Response Groups Global Global Committed 1 Conferencing Clients	
Federation and External Access	
Monitoring and Archiving	
Network Configuration	

4. Next you build a Dial Plan and a translation rule for the phone numbers you want this route to handle.

	Skype for	Business Server 2015 Control Pane	el	
Skype for Busir	ness Server			Administrator Sign ou 6.0.9319.0 Privacy statemer
Home	DIAL PLAN VOICE POLICY ROUTE	PSTN USAGE TRUNK CONFIGURATIC	DN TEST VOICE ROUTING	
Users Topology	Create voice routing test case infor	mation		~
IM and Presence Persistent Chat	Edit Dial Plan - Global			
Voice Routing	V X X Cancel			
Voice Features	Associated Normalization Rules	(?)		
lesponse Groups	🗣 New 🖹 Copy 📋 Paste 🛸	Select 🧪 Show details Remove	↑ ↓	
Conferencing	Normalization rule	State Pattern to match	Translation pattern	
lients	Keep All	Committed ^(\d*)\$	\$1	^
ederation and	ATT Call Fwd activation	Committed ^(*72\d*)\$	\$1	
xternal Access	ATT Call Forward deactivation	Committed ^(*73)\$	\$1	
Ionitoring	ATT Call forward busy activation	Committed ^(*90\d*)\$	\$1	
nd Archiving	ATT CFB deactivation	Committed ^(*91)\$	\$1	
ecurity	ATT CFRNA activation	Committed ^(*92\d*)\$	\$1	
letwork	ATT CFRNA deactivation	Committed ^(*93)\$	\$1	
coniguration	ATT CF not reachableactivation	Committed ^(*94\d*)\$	\$1	
	ATT CF not reachable	Committed ^(*95)\$	\$1	-
	Dialed number to test:			
		60	?	

5. On the top row of the tabs, select Route. On the content area toolbar, click +New.

Skype for Busir	ness Server							
Home	DIAL PLAN	VOICE POLICY	ROUTE	PSTN USAGE	TRUNK CO	NFIGURATION	TEST VOICE ROUTI	NG
Users								
Topology	Create vo	ice routing test	case infor	mation				
IM and Presence								
Persistent Chat						P		
Voice Routing		A				5		
Voice Features	New New	Edit 🔻 🍸	Nove up	State PSTN	Action V	Commit Pa	ttern to match	
Response Groups								
Conferencing								
Clients								
Federation and External Access								
Monitoring and Archiving								
Security								
Network Configuration								

6. On the New Voice Route page, in the Name field, enter the name you have selected for the Route. In our example, it is labeled "route1". Leave the Match this pattern field as .* so all numbers will be matched.

Skype for Bus	iness Server
lome	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING
Jsers	
opology	Create voice routing test case information
v and Presence	
ersistent Chat	New Voice Route
oice Routing	
oice Features	Scope: Name: *
esponse Groups	route1
onferencing	Description:
ients	
ederation and dernal Access	Build a Pattern to Match Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.
Ionitoring	Starting digits for numbers that you want to allow:
na Archiving	Type a valid number and then click Add. Add
ecurity	Exceptions
etwork onfiguration	Remove
	Match this pattern: *
	*

7. Next you want to associate the Voice Route with the Trunk you have just created. Scroll down to Associated Trunks and add the ATT trunk. You can now see that you have associated your trunk with the route you created. An appropriate PSTN usage record will need to be assigned as well. In our example, we use one that was already created in the enterprise. Click on the Select button under Associated PSTN Usages

6	Skype for Business Server 2015 Control Panel	_ D X
Skype for Busin	iess Server	Administrator Sign_out 6.0.9319.0 Privacy statement
Home Users Topology	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING Create voice routing test case information	•
IM and Presence Persistent Chat	Edit Voice Route - LocalRoute	0
Voice Routing Voice Features Response Groups	Edit Reset 🕐	1
Conferencing Clients Federation and External Access	Suppress caller ID Alternate caller ID: Associated trunks:	
Monitoring and Archiving Security	PstnGateway:attesbc.partnersf Add Remove	
Network Configuration	Associated PSTN Usages Select Remove PSTN usage record Long Distance Global	Ţ

8. In the Select PSTN Usage Record window displayed, select the appropriate PSTN Usage Record and click OK.

5	S	kype for Business Server 2015 Control Panel		_ □ ×
Skype for Busine	ess Server			Administrator Sign out 6.0.9319.0 Privacy statement
Home	DIAL PLAN VOICE POLICY	ROUTE PSTN USAGE TRUNK CONFIGURATION	TEST VOICE ROUTING	
Users				
Topology	Create voice routing test	case information		*
IM and Presence				
Persistent Chat		٩		
Voice Routing				0
Voice Features	✓ Edit ▼ Action ▼ C	commit	Policies	U
Response Groups	Internal	Committed	Policies	
Conferencing	Local	Committed		
Clients	Long Distance	Committed LocalRoute	Global	
Federation and External Access				
Monitoring and Archiving				
Security				
Network Configuration				

9. You will now see the Associated PSTN Usages which you have added. Click the OK button at the top of the New Voice Route screen.

5	Skype for Business Server 2015 Control Panel	
Skype for Busin	ness Server	Administrator Sign out 6.0.9319.0 Privacy statement
Home	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING	
Users Topology	Create voice routing test case information	~
IM and Presence Persistent Chat	Edit Voice Route - LocalRoute	
Voice Routing	V OK Cancel	•
Voice Features	Alternate caller ID:	
Response Groups	Associated trunks:	
Conferencing	PstnGateway:attsbc.partnersfb Add	
Clients	Remove	
Federation and External Access		
Monitoring and Archiving	Associated PSTN Usages	
Security	Select Remove 👚 🦊	
Network Configuration	PSTN usage record Associated voice policies Long Distance Global	
		•

10. You will now be at the Routes page showing route1. Click the Commit drop-down menu, and then Commit All.



Phase 3 – 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.

	5.101/me/#main&device=device-1&	selected=		C Q Se	arch	合自 🛡 🕹	↑ 4 0 9
offront 🔯 Most Visited =	Key Shortcuts 🧿 Regtrack	📌 Sharepoint 🧧 CSFTP 📑 Be	ehive Workspac 🧧 Acme Doc	🛞 Acme Software	🗿 New CQ 🌛 BUG 🧧 AP N	lew Solutions 😗 Employee	MOS
RACLE Comm	nunications Operations Monito	Dr.					
• Dashboard	Active calls		۲	× Registered user	5	\sim	My Profile Settings
Alerts Traces Apps	1		2016-04-05 19:47:36	10 9- 8- 7-			About the product
erations KPI / Metrics			l.	6. 5. 4. 3. 2.			Setup Logout
Calls Voice Quality	0 17:00 — Active calls (minu	18:00 Ite average)	<u> </u>	17:00	18:00 red users (minute average)	19:00	
Registrations User Devices Trunks / Prefixes			Q	•			.
Registrations User Devices Trunks / Prefixes Devices	Recent calls			User Device Dis	tribution		• ×
Registrations User Devices Trunks / Prefixes Devices stomers	Recent calls Details Caller	Callee	Call time Seg	User Device Dis	tribution Caco-CP9971/9.4.2 (16.7 %)		2016-04-05 19:15:25
Registrations User Devices Trunks / Prefixes Devices stomers User Tracking	Recent calls Details Caller 7322162709	Callee 7322162720	Call time Seg 6°368ms 4	User Device Dis	tribution Case-CP99719.42 (16.7.9)		2016 04 05 19:15:25
Registrations User Devices Trunks / Prefixes Devices stomers User Tracking IP Tracking Link Quality	Recent calls Details Caller 7322162709 7322162709	Callee 7322162720 7322162720 7322162720	Call time Seg 6"366ms 4 8"551ms 2	User Device Dis	tribution Case-CP99719.42 (16.7 %)		2016-04-05 19:15:25
Registrations User Devices Trunks / Prefixes Devices Istomers User Tracking IP Tracking Link Quality	Recent calls Details Caller 7322162709 7322162709 7322162709 7322162709	Callee 7322162720 7322162720 7322162720 7322162720	Call time Seg 6"368ms 4 8"551ms 2 8"544ms 2 5"568ms 4	User Device Dis	tribution Cases C19971/9.42 (16.7 %)	Cheep-CP7821/10.2.1 (8	2016 04 05 19:15:25 33.3 %)
Registrations User Devices Trunks / Prefixes Devices ustomers User Tracking IP Tracking Link Quality	Calls 7322162709 7322162709 7322162709 7322162709	Callee 7322162720 7322162720 7322162720 7322162720	Call time Seg 6"366ms 4 8"551ms 2 8"54ms 2 5"568ms 4	V User Device Dis	tribution Case-CP9719.42 (16.7 %) User devices (12 reg	Cisco-CP7821/10.2.1 (8 gistrations on 2 devices)	2016-04-05 19:15:25 333 %)

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

🗊 🔒 https://	/172.18.255.101/me/#main&device=device-	1&selected=		C	Q. Search	☆ 自 ♥ ↓ 俞 ∢	
ffront 🔯 Mo	est Visited 👻 🚺 Key Shortcuts 🛛 🔯 Reqtra	ck 📌 Sharepoint 🧧	CSFTP 🛃 Beehive Workspac	Acme Docs 🛞 Acme Soft	ware 🔯 New CQ 🌛 BU	G 🧧 AP New Solutions 🍸 Employee MOS	
RACLI	Settings						admin =
	🖃 🔄 General Settings	System Settings					
Dashboa	- El Status	marra	×			default value	- X
Alerts	E Actions	merge	<u>^</u>				(
-	E REST API	Name			Value		19:48:14
Traces	Carl Carl Network	Merge globally by	Call-ID				
Apps	E Probes						
	Mediation Engine Connector	· · · · ·					
erations	Number Determination Sources	· · · ·					
KPI / Metr	Caller ID						
Calla	E Callee ID						
Calls	E E Platform						
Voice Qua	Platform Devices						
Registratic	Devices Monitoring						
User Devi	Profix Tags						(20) m
							Count •
Trunks / F	Bealms						(2)(2)
Devices	Bealm Patterns						× ×
							19:15:25
stomers	System Settings						
User Tracl	Config Upload						
IP Trackin	E Language Settings						
IF TRUCKIN	🖃 😋 External Devices						
Link Quali	E RADIUS Authentication						
	SNMP Options						
	FTP Server						
	E VQ Collector						
	Configuration Savepoints						
	🖃 😋 User Management						(d)
	🔄 🔄 User Management						Q.•

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

(i) 🔒 https:/	/172.18.255.101/me/#main&device=device-	&selected=		C Q	Search		自 🛡 🦊 🏫 🛷	09
Soffront 💼 Me	ost Visited - 📋 Key Shortcuts [Reqtra	k 📌 Sharepoint	CSFTP 📴 Beehive Workspac	Acme Docs 🛞 Acme Software	🗃 New CQ 🍌 BUG	AP New Solutions	Employee MOS	
RACL	Settings						*	admir
Dashboar Alerts Traces Apps Deerations KPI / Metr Calls	General Settings Status Actions REST API Network Probes Mediation Engine Connector Mumber Determination Sources Caller ID Caller ID Platform Platform Devices	System Setting: merge Name Merge globally	r by Call-ID pdate System Setting	Valu	JO N	default value	custom value	* X 19-46.35
Voice Qua Registratie User Devie Trunks / F Devices ustomers	Platform Devices Prags Prefix Tags Prefix Tags Realms Realms Realm Patterns System Management System Settings	<	Merge globally by Call-ID If this setting is enabled, Mediation same Call-ID even if they are not in Default value: False Enabled	Engine will merge two legs that have coming/outgoing to the same device date Reset to default	Cancel			() + * X 19:15.25
User Tracl IP Trackin Link Quali	Coracle SBC Config Upload Coracle SBC Config Upload E Language Settings RADUS Authentication SNMP Options FTP Server VQ Collector Configuration Savepoints User Management User Management							0.

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

(i) 🔒 https://	/172.18.255.101/me/#main			C	Q. Search		☆ 自 ☑ ↓ 余 4	
offront in Ma	net Visited a 🗖 Kay Shortquite 🧿 Reatra	ok 🛃 Sharanoint 🔽 CSE		Acmo Door 🖉 Acmo Soft	twara 🔊 Now CO 🤞 F		utions	Lab Record
Mont i Mo	st visited . D key siloi teats 💟 keytia			Actile Docs Of Actile Sold	wale 👩 New Cor 🍌 L			Lab Reservat
RACL	Settings							admir
-	🗟 🚔 General Settings	Distance Devices						
Dachboar		Platform Devices						
Dasiibuai		Add Edit Delete			Import Export	- Diagram Order	Toggle external Realms	
Alerts	E REST API	Name	Call Matching	IP Addresses	Point Codes	Visibility	External?	+19 13:23:18
Traces	🖃 🚞 Network							
Apps	- E Probes	☐ SBC/B2BUA devices						
	E Mediation Engine Connector	SBC DMZ	Using generic algorithm	192.168.65.79			internal	<u> </u>
erations	Number Determination Sources	CUCM	Using generic algorithm	10.232.50.89			internal	
KPI / Metr	E Caller ID	SBC Core	Using generic algorithm	10.232.50.11			internal	
	Callee ID							
Calls								
Voice Qua	= Platform Devices							
Registratic	Devices Monitoring							
User Devi								100
Trupke / F								24
TTUTIKS / P	Realms							
Devices	E Realm Patterns							
	🖃 🚖 System Management							19 13:21:29
stomers	System Settings							
User Tracl	- E Oracle SBC Config Upload							
IP Trackin	E Language Settings							
Link Quali	External Devices							
LIIK Quai	RADIUS Authentication							
	SNMP Options							
	FTP Server							
	VQ Collector							
	Configuration Savepoints							
								1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

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

https://	/172.18.255.101/me/#main&device=devi	ce-1&selected= C Q Search		☆ 自 ♥ ◀	A 4	00
ront 🔯 Mo	ost Visited - 🚺 Key Shortcuts 🧿 Red	atrack 📌 Sharepoint 🧧 CSFTP 🚦 Beehive Workspac 🧧 Acme Docs 🛞 Acme Software 🔠 New CQ 🌛 BUG 🧧	AP New Solu	tions 💮 Employe	e MOS	
ACL	Settings					admin
Dashboa Alerts	General Settings	Edit platform device	n Order	Toggle external	Realms	* X
Traces	REST API	Device Type		External?		19:49:32
Apps	Probes	Select the device type you would like to add		Internal		
	Number Determination Source Caller ID	SBC/B2BUA		internal		
Calls	Callee ID	Non-Record-Route Proxy		internal		
/oice Qua	Platform Devices	Gateway 🕕				
Registratio	E IP Tags	L2 Balancer				1000
runks / F	Calms	STP 0				(agente
Devices	Realms	SGW 🕕				* ×
omers	System Management					19(15:25
lser Tracl	Cracle SBC Config Upload					
ink Quali	External Devices RADIUS Authentication SNMP Options FTP Server					
	VQ Collector	Next Cancel)			
	User Management	`\				0.

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

Here Mark Valed • Mey Photoxs • Registrat. • Sharepoit • CSTP • Behvio Workspac. • A none Dox • A none Software • New CQ • BUG • AP New Software • Cemployee MOS Settings • Bething * Settings • Settings • Order * Toggie external * Realmant • Order * Toggie external * Realmant Alorts • A thirds • Bething * Settings • Settings • Order * Toggie external * Realmant • Order * Toggie external * Realmant • Order * Toggie external * Realmant Alorts • A thirds • Bething * Settings • Settings • Order * Toggie external * Realmant • Order * Toggie external * Realmant Probase • Method K • Bething * Settings • Setternal * Realmant • Settings • Setternal * Settings	🗊 🔒 https://	/172.18.255.101/me/#main&device=devic	-1&selected=				C	Q, Search			☆自♥	+	n 4	1 1	ø
Settings Edit platform device E	ffront 💿 Mo	ost Visited - 📋 Key Shortcuts 🚺 Req	rack 📌 Sharepoint	CSFTP	Beehive Works	spac 🧿 Acme Dor	s 🛞 Acme Softw	vare 🏼 🗿 New CQ	🏄 BUG 🧧 A	P New Solut	ions 💮 Emp	ployee M	IOS		
Dashbook Status Edit platform device Image: Construction of the status Image: Construction of the status Aterso Status Edit platform device Image: Construction of the status Image: Construction o	ACLI	Settings												a.	
S FTP Server Vo Collector Configuration Savepoints Outriguration Savepoints Outriguration Savepoints Outriguration Savepoints	Dashboar Alerts Traces Apps Frations KPI / Metr Calls Voice Qua Registratic User Devir Trunks / F Devices tomers User Trackin Link Quali	General Settings Status Actions REST API Network Probes Mediation Engine Connect Mediation Engine Connect Caller ID Caller ID Caller ID Platform Sealms Realms Realms Realms System Management System Settings Oracle SBC Config Upload Language Settings Caller JD/Submit Config Upload Submit Settings Cancel SBC Config Upload Language Settings SNMP Options	Edit platform de B2BUA Options Select the me Use generi by Call-ID Match if a con (optional): by From u Match if a con (optional): Use custor	thod by whit c Palladion nmon suffix sername nmon suffix nd To usern nmon suffix n algorithm	ich the call legs o algorithm (recon c of this many cha ame c of this many cha name c of this many cha n	of this B2BUA (SBC nmended) aracters exists aracters exists	etc.) can be ma	tched.	×	n Order	Toggle exter External? internal internal internal	mai F	Realms	13:49:47	• ×
		VQ Collector Configuration Savepoints					Previous	Next	Cancel						

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

🛈 🔒 https://	/172.18.255.101/me/#main	C Q Search	合自 🛡 🕹 🎓 👌	
offront 💿 Mo	ost Visited 👻 🚺 Key Shortcuts 🛛 🔘 Red	ztrack 🗚 Sharepoint 🧧 CSFTP 🗧 Beehive Workspac 🧧 Acme Docs 🛞 Acme Software 🎯 New CQ 🍌 BUG 🧧 A	P New Solutions 🍧 Employee MOS 📝	Lab Reservati
RACL	Settings			admin
Dashboa	General Settings	Edit platform device	n Order Toggle external Realms	
Alerts	REST API	Device identification by address	External?	19 13:42:33
Apps	Probes	Select the identification addresses for this device.	internal	
	Number Determination Source	IPs used by this device (space separated). If more devices 192.168.65.79 are sharing the same IP address, but are in different VLANs.	internal	
KPI / Metr	Callee ID	you can specify the VLAN IDs here. If left out, all VLAN IDs are matched.	internal	
Calls Voice Qua	Platform	Example: "172.23.12.0/24 172.43.34.1 172.43.23.3/24(vlan=60) 172.3.2.4(vlan=50) 74dc::2ba":		
Registratic	Devices Monitoring	Trusted IPs. Often internal IPs, used by Number 192.168.65.79		
User Devi	E Prefix Tags			
Trunks / F	Realms			
	System Management			ŀ-19 13:21:29
User Track	System Settings			
IP Trackin	E Language Settings			
Link Quali	External Devices ADJUS Authentication SNMP Options FTP Server			
	VQ Collector Configuration Savepoints	Previous Next Cancel		
	User Management			

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

1) 🔒 https://	/172.18.255.101/me/#main&device=devic	ce-1&selected=	G	Q, Search		☆ 自 ♥ ♣ ♠ ⋪	0 9
ffront 🔯 Mo	st Visited * 📋 Key Shortcuts [Rec	track 📌 Sharepoint 🧧 CSFTP 📑 Beehive Workspac 🥃 Ac	me Docs 🛞 Acme Softw	vare 🕕 New CQ 🌛 BUG		New Solutions 💮 Employee MOS	
RACLI	Settings						admin
Dashboar	General Settings	Edit platform device			×	n Order	* ×
Traces	REST API	Device Name				External?	19:50:13
Apps	Probes	Select a name for this device and press Finish to apply				internal	
	Carter Source	Name: SBC DMZ				internal	
KPI / Metr	Caller ID					internal	
Calls	Callee ID					internal	
Voice Qua	Platform Devices						
Registratic	Devices Monitoring						
User Devi	Prefix Tags						10 -
Trunks / F	🖃 🚰 Realms						
Devices	Realms						* X
	System Management						19:13:32
User Tracl	Oracle SBC Config Upload						
IP Trackin	E Language Settings						
Link Quali	🖃 😁 External Devices						
ann gaun	SNMP Options						
	FTP Server						
	VQ Collector		Previous	Finish Cano	el		
	User Management		(
	User Management			`			0.*

- 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 ATT test specifications and call flows. For a copy of full test report, please contact your Oracle Sales account team.

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 Windows Server, Lync/SFB Server, and the Oracle ESBC and 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.

Microsoft Network Monitor (NetMon)

NetMon is a network protocol analyzer which is freely downloadable from Microsoft. It can be found at www.microsoft.com/downloads. NetMon could be installed on the Lync Server mediation server, the Lync Server Standard Edition server, or Enterprise Edition front end server.

Wireshark

Wireshark is also a network protocol analyzer which is freely downloadable from www.wireshark.org. Wireshark could be installed on the Lync/SFB Server mediation server, the Lync/SFB Server Standard Edition server, or MCS Enterprise Edition front end server.

Eventviewer

There are several locations in the event viewer where you can find valuable information to aid in troubleshooting issues with your deployment.

With the requirement that there is a completely functioning Lync and/or SFB Server with Enterprise Voice deployment in place, there are only a few areas in which one would use the Event Viewer for troubleshooting:

- The Enterprise Voice client;
- The Lync/SFB Server Front End server;
- A Lync/SFB Server Standard Edition Server; and
- A Lync/SFB Server Mediation Server.

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.

All devices tested in this document will listen on TCP port 5060 for SIP signaling. In our example we are listening on 5060 on the PSTN facing NIC. Tests may include:

- Client to pool server: telnet <servername> 5060
- Pool server to Mediation Server: telnet <servername> 5060

Appendix A

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.

- 1. Enter the element that you will edit at the correct level of the ACLI path.
- 2. Select the element that you will edit, and view it before editing it. The select command loads the element to the volatile memory for editing. The show command allows you to view the element to ensure that it is the right one that you want to edit.
- 3. 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.

- 4. 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.
- 5. On completion, you must issue the done command.
- 6. 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,

- 1. Enter the no command from within the path for that specific element
- 2. Issue the exit command.

To delete a multiple-instance element,

- 1. Enter the no command from within the path for that particular element. The key field prompt, such as <name>:<sub-port-id>, appears.
- 2. Use the <Enter> key to display a list of the existing configured elements.
- 3. Enter the number corresponding to the element you wish to delete.
- 4. 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 activateconfig 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.





B blogs.oracle.com/oracle f facebook.com/oracle twitter.com/oracle oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0916