

Oracle Enterprise Communications Broker & Oracle Enterprise-Session Border Controller with Microsoft Lync 2013, Avaya Aura 6.3.4 & Cisco Unified Communications Manager 8.6

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

INTENDED AUDIENCE	6
INTRODUCTION	6
ORACLE ENTERPRISE COMMUNICATIONS BROKER OVERVIEW	6
DOCUMENT OVERVIEW	7
Requirements	7
LAB CONFIGURATION	7
PHASE 1 - CONFIGURE THE ECB	9
RUNNING SETUP	
LOGGING IN THE ECB	
CONFIGURING THE ECB	
System Settings	
Configure SIP Interfaces	
Configure Agents	
Configure Dial Plan	
Configure Users	
Configure Routing	
Configure Header manipulation rules	43
Save and activate the configuration	53
PHASE 2 - CONFIGURING THE LYNC 2013 SERVER	56
Adding the ECB as a PSTN gateway	56
CREATING A ROUTE WITHIN THE LYNC SERVER INFRASTRUCTURE	
Additional Steps	73
PHASE 3 - CONFIGURING THE AVAYA SESSION MANAGER	74
Adding the ECB as a SIP Entity	74
CONFIGURING AN ENTITY LINK BETWEEN ECB AND SESSION MANAGER	
CREATING A ROUTING POLICY TO ASSIGN THE APPROPRIATE ROUTING DESTINATION	76
PHASE 4 – CONFIGURING THE CISCO UNIFIED COMMUNICATIONS MANAGER	
CONFIGURING THE SIP TRUNK SECURITY PROFILE	
CONFIGURING THE SIP PROFILE	
CONFIGURING THE TRUNK	
CONFIGURING THE ROUTE PATTERN	



PHASE 5 – CONFIGURING THE ORACLE ENTERPRISE SESSION BORDER CONTROLLER	
IN SCOPE	
OUT OF SCOPE	
WHAT WILL YOU NEED	
CONFIGURING THE ORACLE ENTERPRISE SESSION BORDER CONTROLLER (E-SBC)	
Establish the serial connection and logging in the SBC	
Initial Configuration – Assigning the management Interface an IP address	
Configure System element values	
Configure Physical Interface values	93
Configure Network Interface values	
Configure Global SIP configuration	
Configure Global Media configuration	
Configure Realms	
Configure E-SBC redundancy configuration	
Configure SIP signaling configuration	
Configure Next-hop signaling configuration	
Configure SIP routing	
Configure Media handling	
Configure Sip-manipulations and translation rules	
Configure SIP PRACK Interworking	130
Configuring REFER Handling for Transfers	
Addressing No Ringback tone on Transfers	136
Verify configuration integrity	
Save and activate your configuration	140
INTEROPERABILITY TESTING	141
ΙΝΤΕΩΩΡΕΛΕΙΙ ΤΥ ΡΕΤΙΜΕΕΝ Δυλυλ ΑΝΟ Ι ΥΝΟ	141
INTEDODEDABILITY BETWEEN CUCM AND I VNC	142
INTEROFERABLEITT DET WEEN COCMTAND LTINC	
TEST PLAN & RESULTS	145
TEST PLAN	145
TROUBLESHOOTING TOOLS	
MICROSOFT NETWORK MONITOR (NETMON)	148
WIRFSHARK	148
FVFNTVIFWFR	148
ON THE ORACLE ENTERPRISE COMMUNICATIONS BROKER AND ORACLE ENTERPRISE SESSION BORDER CO	NTROLLER
Resetting the statistical counters, enabling logging and restarting the log files	149



Examining the log files	
Telnet	150
Lync Server Logging Tool	151
APPENDIX A	
NO RING BACK TONE HEARD FOR INBOUND CALLS FROM PSTN TO MS LYNC THROUGH E-SBC	152
Media Bypass	152
Acme Packet Work Around	153
APPENDIX B	
Accessing the ACLI	159
ACLI BASICS	159
CONFIGURATION ELEMENTS	
CREATING AN ELEMENT	163
EDITING AN ELEMENT	163
DELETING AN ELEMENT	164
CONFIGURATION VERSIONS	164
SAVING THE CONFIGURATION	165
ACTIVATING THE CONFIGURATION	166



Intended Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Oracle Enterprise Session Border Controller (E-SBC), Oracle Enterprise Communications Broker (EOM), Lync Mediation Server, Avaya Aura System Manager and Cisco Unified Communications Manager. 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 troubleshooting, if necessary.

Introduction

Oracle Enterprise Communications Broker Overview

The Oracle Enterprise Communications Broker (ECB) is an enterprise-class, core signaling component designed to simplify communications networks. It combines innovative approaches toward dial plan management and SIP topology-aware routing with a purpose-built, intuitive GUI interface. While at its best in signaling environments comprised of products and solutions from multiple vendors, it is useful for consolidating policy enforcement decisions, integrating third-party applications, and managing a network-wide routing topology even in homogenous architectures.





The ECB is typically deployed in the core of a multi-vendor communications network where multiple UC, PBX and service provider trunk interfaces must be interconnected. It normalizes communications between disparate premise-based systems and connects them to service provider networks and hosted applications through E-SBCs.

Document Overview

This technical application note documents the implementation of the Oracle Enterprise Communications Broker in an Enterprise network consisting of multi-vendor Unified Communications platforms - Microsoft Lync 2010/2013, Avaya Aura Session Manager and Cisco Unified Communications Manager - connecting to SIP trunk through an Enterprise Session Border Controller.

Requirements

- Oracle Enterprise Communications Broker
- Oracle Enterprise Session Border Controller
- Microsoft Lync 2010/2013
- Avaya Aura 6.3.4
- Cisco Unified Communications Manager 8.6

Lab Configuration

The following diagram illustrates the lab environment created to facilitate certification testing.





The network architecture consists of two areas. Area 1 represents the Enterprise network and Area 2 is the service provide network. The Enterprise network has ECB at its core connecting together multiple UC platforms. The ECB connects to the E-SBC which provides the enterprise network access to PSTN through the service provider network.

The configuration, validation and troubleshooting of the Area 1 is the focus of this document and will be described in five phases

- Phase 1 Configure the ECB
- Phase 2 Configure Lync 2010/2013 server
- Phase 3 Configure the Avaya Aura System Manager
- Phase 4 Configure the Cisco Unified Communications Manager
- Phase 5 Configure the E-SBC.



Phase 1 – Configure the ECB

The Oracle Enterprise Communications Broker is available either as an appliance or as an application for operation on virtual machines. When running as an appliance, the ECB software is packaged with the Netra Server X3-2 for Oracle and delivered to the end customers. When running as a virtual application, the ECB software can be deployed on any third-party COTS hardware that meets the specified guidelines.

Once the ECB is deployed (in the appliance mode or the application mode) and connected, you can power on the ECB. Software installation of the ECB is required upon first startup. Although the ECB is primarily configured through the GUI, you need to perform the software installation and setup via the CLI.

Connecting to the ECB

The CLI can be accessed through the console connection. If the ECB is appliance based, you can connect to the ECB console using your laptop running a terminal emulator application like PuTTY and an RJ-5 cable. Start the terminal emulator application with the following settings:

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

Power the ECB on. Upon successful boot, the system prompts you to login. The default password for user mode is "acme" and super user mode is "packet".

You can now use the installation wizard to setup your ECB. Using the wizard, you can enable the Web Server, set management access as well as configure high availability and service interface addressing.

Password: acme ORACLE> **enable** Password: packet



Running Setup

The following steps detail the process of using the installation wizard to configure the base setup of the ECB

1. Start the installation wizard by entering the command run setup in super user mode.

ORACLE# run setup

The following displays

```
Thank you for purchasing the Oracle ECB. The following short wizard
will guide you through the initial set-up.
-------
'?' = Help; '.' = Clear; 'q' = Exit
CONFIGURATION
WARNING: Proceeding with wizard will result in existing configuration
being erased.
Erase config and proceed (yes/no) [no] : yes
```

2. Type yes and press Enter

```
Configuration will be backed up as

bkup_setup_wizard_Apr__8_13_25_49_632.gz

'-' = Previous; '?' = Help; '.' = Clear; 'q' = Exit

HIGH AVAILABILITY

This ECB may be a standalone or part of a highly available redundant

pair.

Oracle ECB mode

1 - standalone

2 - high availability

Enter choice [1 - standalone] : 1
```

- 3. Our setup consists of a standalone server. Type 1 and hit Enter
- 4. You will then be asked to configure a unique target name, the ip address, subnet mask and gateway of the management interface of the ECB. Please note at any time during configuration if you would like to keep the default values (values mentioned in []), press Enter.

```
Unique target name of this ECB [primary] :ECB-Oracle
```



```
IP address on management interface [172.30.200.111] : 172.18.255.55
Subnet mask on management interface [255.255.0.0] :
Gateway IP address on management interface [172.18.0.1] :
```

5. You will then see a prompt to configure your sip-interface. This step is required; the system does not allow you to proceed without making a setting. When prompted enter the ip address, subnet mask and gateway ip address of the sip-interface.

```
IP address on SIP interface : 192.168.1.90
Subnet mask on SIP interface [255.255.255.0] :
Gateway IP address on SIP interface :192.168.1.1
```

6. The prompt to setup the system timezone will display

```
SETUP TIMEZONE Setup system timezone (yes/no) [yes] : yes
```

Type your response and press Enter.

7. You will then be asked to enter the number for sessions purchased for the ECB. Type your response and press Enter.

```
LICENSED SESSIONS
Number of licensed sessions
```

```
: 400
```

You will see the following message prompting to save the settings before proceeding to the timezone setup.

```
Enter 1-20 to modify,'d' to display summary,'s' to save,'q' to exit.[s]:
Saving changes and quitting wizard. Are you sure? [y/n]?:
```

8. Type your response and press Enter.

SETUP TIMEZONE Setup system timezone (yes/no) [yes] : yes

The following message displays

```
Deleting configuration
Erase-Cache received, processing.
waiting 1200 for request to finish
Request to 'ERASE-CACHE' has Finished,
Erase-Cache: Completed
Running timezone setup application
Calling tzselect. Use ^D to cancel without save
Please identify a location so that time zone rules can be set
```



```
correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#22
```

Type your response, for example, 2 for Americas and press Enter. The system lists applicable countries in the Americas. Make your selection and press Enter. The system displays applicable time zones. Make your selection. The following message appears

```
The following information has been given:

United States

Eastern Time

Therefore TZ='America/New_York' will be used.

Local time is now: Thu Apr 11 10:13:38 EDT 2014.

Universal Time is now: Thu Apr 11 14:13:38 UTC 2014.

Is the above information OK?

1) Yes

2) No

#?
```

9. Type 1 and then hit Enter. You will be then shown a summary of your settings.



AUTOMATIC CONFIGURATION	
6 : Acquire config from the Primary (yes/no)	: N/A
ECB SETTINGS	
7 : Unique target name of this ECB	: ECB-Oracle
8 : Management interface IP address 172.18.255.55	:
9 : Management interface subnet mask	: 255.255.0.0
10: Management interface gateway IP address	: 172.18.0.1
11: SIP interface VLAN id	: 0
12: SIP interface IP address	: 192.168.1.90
15: SIP interface subnet mask 255.255.255.0	:
16: SIP interface gateway IP address	: 192.168.1.1
PEER CONFIGURATION	
18: Peer target name	: N/A
SETUP TIMEZONE	
19: Setup system timezone (yes/no)	: yes
LICENSED SESSIONS	
20: Number of licensed sessions	: 400
You may access the GUI via http://172.18.255.55:80/ or the acli after reboot.	continue using



Logging in the ECB

You can now access the ECB through the Web GUI. Start an Internet browser and start the GUI using the URL:

http://server ip address/.

The login screen will appear.

* Acme Packet: ECB-Oracle X	
← → C 🗋 172.18.255.55/#Login	☆ ≡
👯 Apps 🖻 My Oracle 🖸 Acme Packet Soluti 🙋 ClearQuest	C Other bookmarks
	🔊 🙆 🙆 🙆 🧶
	•
	ekat Fatannias Communications Dealean
Welcome to Acme Pao	cket Enterprise Communications Broker
Password:	
	Login
	and get
	acme Anacket
	active packet
	· · · · · · · · · · · · · · · · · · ·

Enter your GUI username and password. The default username for the User level is "user" and the default password is "acme. The default username for an Administrator level is "admin", and the default password is "packet".



Configuring the ECB

After logging into the ECB, the **Home** screen will be displayed. The ECB GUI has five tabs across the top – **Home**, **Configuration**, **Monitor and Trace**, **Widgets** and **System**.

The Home tab as shown below contains a configurable dashboard displaying the system statistics.





System Settings

Select the **Configuration** tab. This tab displays the configurable elements in the ECB in two sections – **Service Provisioning** and **System Administration**. Click on the **General** icon under **System Administration**.





Modify System Settings page is displayed.

Modify System settings		
Hostname:	ECB	
Description:		
Location:		
Default gateway IP address:	172.18.0.1	
Enable restart on critical failure:		
Enable SIP monitoring and tracing:		
NTP servers:	Add Edit Delete	
Logging settings		
SNMP settings		
Denial of service settings		
Communications monitoring pro	obe settings	
 High availability settings 		

Expand the Logging settings section.

Modify System settings		
Hostname:	ECB	
Description:		
Location:		
Eocacion.		
Default gateway IP address:	172.18.0.1	
Enable restart on critical failure:		
Enable SIP monitoring and tracing:		
NTP servers:	Add Edit Delete	
<u> </u>		_
 Logging settings 		
SysLog server IP address:	0.0.0.0	
Process log level:	NOTICE	



Process log level is set at **NOTICE**. Change the setting to **DEBUG** by selecting the option from the drop down menu and click **OK**.

NTP servers:	Add Edit Delete	
Logging settings SysLog server IP address:	0.0.0.0	
Process log level:	NOTICE	~
SNMP settings	CRITICAL MINOR	
Denial of service settings	WARNING	
Communications monitoring pro	INFO	
 High availability settings 	TRACE	
\sim	DEBUG	
	OK Back	

Click the **Configuration** button at the top to go to the **Configuration** tab.

You can verify the network interface settings configured through the run setup command by clicking on the **Network** icon under **System Administration**

Modify Network settings		
VLAN id:	0	(Range: 04095)
Network IP address:	192.168.1.90	
Network IP subnet mask:	255.255.255.0	
Network IP gateway address:	192.168.1.1	
DNS server IP address:		
DNS domain:		
Enable ICMP:	√	
Enable gateway hearbeat:		
 High availability settings 		



Configure SIP Interfaces

Click **Configuration** button to go to the **Configuration** tab. Select the **SIP Interface icon** under **System Administration** to make changes to the SIP interface settings configured during initial setup.





Click on the Port tab on the left. You will see the sip port 192.168.1.90 with protocol UDP. Click Edit to change its protocol to TCP.

nterface	SIP ports Search Criteria: All			
ore	Add Edit D	elete		
	Address	Port	Transport	TLS profile
	192.168.1.90	5060	UDP	
	192.168.1.90	5060	UDP	

On the Modify SIP port settings page, select TCP as the transport protocol from the drop-down menu and click OK.

acme packet	ne Configuration Moni	tor and Trace Widgets System	
E Save			
Interface Port	Modify SIP port settin IP address: IP port: Transport protocol: TLS profile:	192.168.1.90 5060 UDP UDP TCP TLS	(Range: 165535)



On the SIP ports page,	click Add to add anoth	er sip port.
------------------------	------------------------	--------------

acme packet	Home Configuration Monitor	and Trace Widgets Sys	tem	
E Save				
Interface Port	SIP ports Search Criteria: All	e		
	Address Add a new item 192.168.1.90	Port ▲ 5060	Transport TCP	TLS profile

Add a sip port with address 192.168.1.90, port 5068 and transport protocol TCP as shown below and click **OK**.

acme packet	ome Configuration Monitor a	nd Trace Widgets System	1	
🗐 <u>S</u> ave				
Interface Port	Add SIP port settings IP address: IP port: Transport protocol: TLS profile:	192.168.1.90 5068 TCP	•	(Range: 165535)



The SIP ports page will be displayed showing the two sip ports we configured.

acme (packet	Home Configuration Mor	itor and Trace Widgets Sys	tem	
E Save				
Interface Port	rface SIP ports Search Criteria: All			
	Add Edit L	Port	Transport	TLS profile
	192.168.1.90	5060	тср	
	192.168.1.90	5068	TCP	

Click on **Configuration** button to back to the **Configuration** tab.

Configure Agents

We will now configure the next hops in our routing paths – the Agents – which in our setup are the Lync Mediation Server, Avaya SM and the E-SBC which connects the ECB to the SIP trunk. Click on **Agents** icon under **Service Provisioning**.





The Agents page will be displayed. Click on the **Add** button. The **Add Agent settings** page is displayed. Add the Lync mediation server by configuring the hostname, ip address and port as shown below.

Add Agent settings			
State:			<u></u>
Hostname:	lync2013med1.acmepacket.net		
IP address:	192.168.2.192		
IP port:	5068		(Range: 065535)
Transport protocol:	StaticTCP	~	
TLS profile:		~	
Description:	Lync 2013 Mediation Server 1		
Source context:		~	
Egress number translation mode:	E164	~	
Number of digits for n digit dialing:	4		(Range: 025)
Prepend prefix on egress:			
Inbound header manipulation:		~	
Outbound header manipulation:		~	
Tags:	Add Edit Delete		
			Ŧ
	OK Back		

Scroll down to enable SIP OPTIONS to monitor agent health locally. Check the **Enable OPTIONS ping** check box and configure the **OPTIONS ping interval** to 30. Click **OK**.

Add Agent settings		
Egress number translation mode:	E164	× ^
Number of digits for n digit dialing:	4	(Range: 025)
Prepend prefix on egress:		
Inbound header manipulation:		▼
Outbound header manipulation:		▼
Tags:	Add Edit Delete	
Enable OPTIONS ping:	×	
OPTIONS ping interval:	30	(Range: 04294967295)
ConstraintsAdvanced		
	OK Back	



You will now see the Lync server listed under **Agents**. Click **Add** to add the second Mediation server from the pool and also enable OPTIONS as shown in the previous step.

Add Agent settings				
State:	•			
Hostname:	lync2013med2.acmepacket.net			
IP address:	192.168.2.193			
IP port:	5068	0	(Range: 065535)	
Transport protocol:	StaticTCP	~		
TLS profile:		~		
Description:	Lync 2013 Mediation Server 2			
Source context:		~		
Egress number translation mode:	E164	~		
Number of digits for n digit dialing:	4	0	(Range: 025)	
Prepend prefix on egress:				
Inbound header manipulation:		~		
Outbound header manipulation:		~		
Tags:	Add Edit Delete			-
	OK Back			

Add another agent with hostname acmepacket.net to route the INVITEs for transfers from Lync and click OK.

Add Agent settings			
State:			Â
Hostname:	acmepacket.net		
IP address:			
IP port:	5068		(Range: 065535)
Transport protocol:	StaticTCP	~	
TLS profile:		~	
Description:	agent for transfers from Lync		
Source context:		~	
Egress number translation mode:	E164	~	
Number of digits for n digit dialing:	4	_	(Range: 025)
Prepend prefix on egress:			
Inbound header manipulation:		~	
Outbound header manipulation:		~	
Tags:	Add Edit Delete		_
	OK Back		·



Next add the two Mediation servers from the Lync 2010 setup using the following settings. In order to monitor agent health locally, please enable OPTIONS as shown in the previous steps.

Add Agent settings		
State:		<u>^</u>
Hostname:	LyncMedSrv1.selab.com	
IP address:	192.168.1.119	
IP port:	5060	(Range: 065535)
Transport protocol:	StaticTCP ~	
TLS profile:	~	
Description:	Lync 2010 Mediation Server 1	
Source context:	· · · · · · · · · · · · · · · · · · ·	
Egress number translation mode:	E164 💙	
Number of digits for n digit dialing:	4	(Range: 025)
Prepend prefix on egress:		
Inbound header manipulation:	~	
Outbound header manipulation:	~	
Tags:	Add Edit Delete	
	OK Back	

State:	۲	<u>^</u>
Hostname:	LyncMedSrv2.selab.com	
IP address:	192.168.1.120	
IP port:	5060	(Range: 065535)
Transport protocol:	StaticTCP 🗸	
TLS profile:	~	
Description:	Lync 2010 Mediation Server 2	1
Source context:	~	
Egress number translation mode:	E164 🗸	
Number of digits for n digit dialing:	4	(Range: 025)
Prepend prefix on egress:		
Inbound header manipulation:	~	
Outbound header manipulation:	~	
Tags:	Add Edit Delete	
	OK Back	



Now add the Avaya Session manager as an agent using the following settings. In our setup, the egress number translation mode for Avaya server was set to no-country code.

Add Agent settings		
State:	s	<u>^</u>
Hostname:	aura.com	
IP address:	10.232.50.102	
IP port:	5060	(Range: 065535)
Transport protocol:	StaticTCP	~
TLS profile:		~
Description:	Avaya Session Manager	
Source context:	· · · · · · · · · · · · · · · · · · ·	
Egress number translation mode:	no-country-code	✓
Number of digits for n digit dialing:	4	(Range: 025)
Prepend prefix on egress:		
Inbound header manipulation:	· · · · · · · · · · · · · · · · · · ·	
Outbound header manipulation:		✓
Tags:	Add Edit Delete	
	OK Back	

Now add the CUCM as an agent using the following settings. In our setup, the egress number translation mode for CUCM is E164no-plus.

Add Agent settings		
State:	s	
Hostname:	172.16.101.39	
IP address:	172.16.101.39	
IP port:	5060	(Range: 065535)
Transport protocol:	StaticTCP	•
TLS profile:		•
Description:	CUCM	
Source context:		-
Egress number translation mode:	E164-no-plus	
Number of digits for n digit dialing:	4	(Range: 025)
Prepend prefix on egress:		7
Inbound header manipulation:		
Outbound header manipulation:		•
Tags:	Add Edit Delete	



Next add the E-SBC which provides the enterprise network access to the SIP trunk and click **OK**.

State:		
Hostname:	192.168.1.130	
IP address:	192.168.1.130	
IP port:	5060	(Range: 065535)
Transport protocol:	StaticTCP	~
TLS profile:		~
Description:	Trunk SBC	
Source context:	NA	~
Egress number translation mode:	E164-no-plus	~
Number of digits for n digit dialing:	4	(Range: 025)
Prepend prefix on egress:		
Inbound header manipulation:		~
Outbound header manipulation:		~
Tags:	Add Edit Delete	

The **Agents page** will be displayed listing the configured agents.

Add Edit Delete						
Hostname	Address	Port	Transport	Agent state		
172.16.101.39	172.16.101.39	5060	StaticTCP	enabled		
192.168.1.130	192.168.1.130	5060	StaticTCP	enabled		
acmepacket.net		5068	StaticTCP	enabled		
aura.com	10.232.50.102	5060	StaticTCP	enabled		
lync2013med1.acmepacket.net	192.168.2.192	5068	StaticTCP	enabled		
lync2013med2.acmepacket.net	192.168.2.193	5068	StaticTCP	enabled		
lyncmedsrv1.selab.com	192.168.1.119	5060	StaticTCP	enabled		
lyncmedsrv2.selab.com	192.168.1.120	5060	StaticTCP	enabled		



Click on **Configuration** button on the top to go back to the **Configuration** tab.

Configure Dial Plan

We will now configure the dialing contexts and dial plans. Dialing-contexts define the system behavior for calls placed to and from either a corporate or geographic focus. Dialing-contexts include multiple dial-patterns, which define the normalization required to most effectively manage diverse signaling structures. Click on the **Dial Plan** icon under **Service Provisioning**.



The Dialing Contexts page shows the default dialing context parents - Corporate and Geographic.

ac	acme packet Home Configuration Monitor and Trace Widgets System							
E	E Save							
Dial	ing contexts							
Ref	fresh Add	Edit Dele	te Upload Dow	nload				
Nan	ne	Geographic location	Description	Country code	Outside line prefix			
	CORPORATE							
	GEOGRAPHIC							



To configure a dialing context, select the Corporate context and click Add.

aci	me (packet	Home	Configura	ation Monitor	and Trace Widg	gets System		
B	E Save							
Diali	ing contexts							
Ref	resh Add	Edit	Delete	Upload Dow	nload			
Nam	ne '	Add a new ite	tion De	scription	Country code	Outside line prefix		
	CORPORATE							
	GEOGRAPHIC							

In the Add Dialing Context page, configure a context with the following details and click OK.

Name:			
	Oracle		
Geographic location:		~	
Description:			
Country code:			
Outside line profix:			
Dial aathaara			
Diai patterns			
Add Edit Del	ete Upload Download	ł	
Remove prefix Pattern	Description	Country code	Replacement prefix



The Dialing Contexts page displays Oracle listed under corporate contexts. We will now configure child contexts under Oracle for our Lync, Avaya and CUCM servers. These can be considered as contexts for the different branches an enterprise has.

Ornda		 Outside line prenx
Uracie		
GEOGRAPHIC		

Select Oracle under the corporate context and click Add.

In the Add Dialing Context window, configure a context named Bedford-Lync and Geographic location as NA. To configure dial patterns, click Add.

Add Dialing context			
Name:	Bedford-Lync		
Geographic location:	NA	~	
Description:			
Country code:			
Outside line prefix:			
Dial patterns			
Add H Edit Delete U	pload Download		
Remove pre Add a new item irn	Description	Country code	Replacement prefix
Remove pre Add a new item irn	Description	Country code	Replacement prefix
Remove pre Add a new item irn	Description	Country code	Replacement prefix
Remove pre Add a new item irn	Description	Country code	Replacement prefix
Remove pre Add a new item irn	Description	Country code	Replacement prefix



Add a dial pattern as shown below to enable 4 digit dialing and click **OK**. If the dialed digits match the pattern 72XX, ECB transforms it to a 10 digit number by adding the prefix 781443.

Add Dialing context / dial pat	ttern
Remove prefix:	
Pattern:	72XX
Description:	
Country code:	
Replacement prefix:	781443
Replacement uri:	
Go to context:	

Add another dial pattern as shown below to match the pattern 73XX and click $\ensuremath{\text{OK}}$.

Add Dialing context / dial patte	rn	
Remove prefix:		
Pattern:	73XX	
Description:		
Country code:		
Replacement prefix:	781443	
Replacement uri:		
Go to context:	×	



The Bedford-Lync dialing context displays the configured dial patterns.

Name: Geographic location: Description:	: [Bedford-Lync NA	~	
Geographic location: Description:	[NA	~	
Description:				
Country code:	l			
Outside line prefix:	L			
Dial patterns	L			
Add Edit	Delete Up	load Download		
Remove prefix	Pattern	Description	Country code	Replacement prefix
	72XX			781443
	73XX			781443
4				

Add another dialing context under Oracle named Burlington-Avaya with the following settings and click OK.

Modify Dialing con	text			
Name:		Burlington-Avaya		
Geographic location	:	NA	~	
Description:				
Country code:				
country code.	L			
Outside line prefix:				
Dial patterns				
Add Edit	Delete Upl	oad Download		
Remove prefix	Pattern	Description	Country code	Replacement prefix
	72XX			781443
	73XX			781443
•				•



Add a dialing context named Braintree-CUCM with the following settings and click **OK**.

	ntext				
Name:		Braintree-CUCM			
Geographic location:		NA		~	
Description :					
Country code:					
Outside line prefixe					
Outside line prenx:					
Dial patterns					
Add Edit	Delete U	pload Download			
Remove prefix	Pattern	Description	Country co	de	Replacement prefix
	73XX				781443
	72XX				704.440

The **Dialing Contexts** page shows the parent context – Oracle and the child contexts.

Dialing contexts								
Refresh Add Edit	Delete Upload	Download						
Name	Geographic location	Description	Country code	Outside line prefix				
CORPORATE								
🔺 Oracle								
Bedford-Lync	NA							
Braintree-CUCM	NA							
Burlington-Avaya	NA							
GEOGRAPHIC								



We need to associate the agents with the contexts within which they reside to assign the dialing rules. Click on the **Configuration** button at the top to go to the **Configuration** tab and click on **Agents**.

On the **Agents** page, select the agent configured for Avaya server and click **Edit**. On the **Modify Agent Settings** page, select Oracle.Burlington-Avaya from **Source context** drop-down menu and click **OK**.

Modify Agent settings			
TI C profile:			
its prome:		~	
Description:			
Source context:		-	
Concern an and an encoded in a standay	EMEA Morocco		
Egress number translation mode:	EMEA.Mozambique		
Number of digits for n digit dialing:	EMEA.Nigeria	(Range: 0	25)
Prepend prefix on egress:	EMEA.SaudiArabia		
Inbound header manipulation:	EMEA.SouthAfrica		
	EMEA.Sudan		
Outbound header manipulation:	EMEA. Tanzania		
Tags:	EMEA.Turkey		
	EMEA.Uganda		
	EMEA.Ukraine		
	EMEA.Yemen		
	NA		
	Oracle		
	Oracle.Bedford-Lync		
	Oracle.Burlington-Avaya	~	
Enable OPTIONS ping:	 Image: A start of the start of		
OPTIONS ping interval:	30	(Range: 0	4294967295)

Next, configure the Lync 2013/2010 mediation servers with the source context – Oracle.Bedford-Lync since the Lync 2010 and Lync 2013 servers have the same dialing rules.

Modify Agent settings		
	ocacie i ci	
TLS profile:		
Description:		
Source context:		-
Egress number translation mode:	EMEA.Morocco	•
Number of digits for p digit dialing:	EMEA.Mozambique	(2
Number of aigles for fragic alaring.	EMEA.Nigeria	(Range: 025)
Prepend prefix on egress:	EMEA.SaudiArabia	
Inbound header manipulation:	EMEA.SouthAfrica	
Outhound beader manipulation:	EMEA.Sudan	
outbound neader manipulation.	EMEA. Tanzania	
Tags:	EMEA.Turkey	
	EMEA.Uganda	
	EMEA.Ukraine	
	EMEA.Yemen	
	NA	
	Oracle	
\sim	Oracle.Bedford-Lync	
	Oracle.Buringcon-Avaya	
Enable OPTIONS ping:	v	
OPTIONS ping interval:	30	(Range: 04294967295)



Finally, configure the CUCM server with the source context - Oracle.Braintree-CUCM.

Source context: Egress number translation mode: Mumber of digits for n digit dialing: Prepend prefix on egress: Inbound header manipulation: Outbound header manipulation: EMEA.SaudiArabia EMEA.SaudiArabia EMEA.SouthAfrica EMEA.SudhAfri	Modify Agent settings	
Cost & English and Cost of Cos	Source context: Egress number translation mode: Number of digits for n digit dialing: Prepend prefix on egress: Inbound header manipulation: Outbound header manipulation: Tags:	EMEA.Mozambique EMEA.Nigeria EMEA.SaudiArabia EMEA.SouthAfrica EMEA.SouthAfrica EMEA.Tanzania EMEA.Turkey EMEA.Uganda EMEA.Yemen NA Oracle.Badford Lync Oracle.Braintree-CUCM

Configure Users

Next we will populate users in the User database. User entries can be added manually or uploaded in a format pre-configured to translate into a user database. Click on the **Users** icon under **Service Provisioning**.





The User entries page will be displayed. Click on Add to start adding users.

acme packet Home Configuration Moni	tor and Trace Widgets Sy	ystem
E Save		
User entries Search Criteria: All		
Add Edit Delete Upload Download		
Number or Add a new item	Dialing context	Agent

The **Add User entries** page will be displayed. You can enter the user numbers in E164 format without the + (17814437383) or a number range (17814437[400-599]) in the **Number** field. Assign the appropriate **Agent** and **Dialing context** and click **OK**.

Add User entries			
Number or pattern:	17814437383	17814437383	
Dialing context:	Oracle.Bedford-Lync	~	
Agent:	LyncMedSrv1.selab.com	~	
Tags:	Add Edit Delete		

Continue adding users as shown above using the corresponding agents and dialing contexts.


The User entries page will list all the users configured. Click Configuration button on the top to go to the Configuration tab

User entries Search Criteria: All		
Add Edit Delete	Upload Download	
Number or pattern	Dialing context	Agent
17814437246	Oracle.Burlington-Avaya	aura.com
17814437247	Oracle.Burlington-Avaya	aura.com
17814437293	Oracle.Braintree-CUCM	172.16.101.39
17814437295	Oracle.Braintree-CUCM	172.16.101.39
17814437383	Oracle.Bedford-Lync	lyncmedsrv1.selab.com
17814437387	Oracle.Bedford-Lync	lync2013med1.acmepacket.net
17814437388	Oracle.Bedford-Lync	lyncmedsrv1.selab.com

Configure Routing

The ECB performs its session routing via the route configuration. Route configuration establishes hop-by-hop paths to signaling endpoints. ECB routing configuration allows the user to specify a route's cost to specify route preference. Cost may or may not be based on monetary considerations. But the reach of an enterprise's network often does allow the user to configure routes that keep session traffic within the enterprise infrastructure rather than incurring cost associated with a service provider.

The ECB allows for a range of route preference criteria to differentiate between routing paths. Criteria include source routing based on the agent or calling number. Target-oriented criteria are also available, allowing the enterprise to designate preferred paths for specific called numbers.

We need not configure a route for the users defined in the user database as the ECB will use their configured agents as next hop to route the calls. Since ECB does not support DNS load balancing as of now, the Lync users are assigned with one mediation server as their agent. To ensure the calls complete if the first mediation server in the pool goes down, we will configure a route to the second agent of the pool with a higher cost. On the **Configuration** tab click on the **Routing** icon under **Service Provisioning**.





On the Routing table page, click Add to add a route.

acme packet	me Configuration	Monitor and Trace	Widgets System	1
E Save				
Routing table Search Criteria: All				
Add Edit Del	ete Upload Down	load		
Source age Add a new item	Calling number	r C	Dest agent	Called number



Add a routing entry for the Lync 2010 user – 17814437383 with the **Route** set to the second mediation server – LyncMedSrv2.selab.com with a cost of 20 and click **OK**.

Add Routing table		
Source agent:	*	
Calling number:	*	
Dest agent:	*	1
Called number:	17814437383	
Route:	LyncMedSrv2.selab.com	
Cost:	20	(Range: 0100)
Description:	Fail over route to Lync 2010 Mediation Server 2	
Tags:	Add Edit Delete	

When the ECB receives a call for 1781437383, it looks up the user DB and finds that this user is associated to LyncMedSrv1.selab.com and routes the call to it. If this agent is down, ECB will find the above entry and route the call to the second agent of the pool – LyncMedSrv2.selab.com.

Similarly add a routing entry for user 17814437387 pointing to lyncmed2.acmepacket.net as its failover route.

Add Routing table		
Source agent:	24c	~
Calling number:	**	
Dest agent:	24c	~
Called number:	17814437387	
Route:	lync2013med2.acmepacket.net	~
Cost:	20	(Range: 0100)
Description:	Fail over route to Lync 2013 Mediation Server	n
Tags:	Add Edit Delete	



For calls being made from the Enterprise to the outside world, we will define routes with the SBC (which connects to the SIP trunk) as the next hop.

In the Add Routing table page, add a route as shown below, routing all calls from the source agent - Lync mediation server – LyncMed1Srv.selab.com to the trunk SBC with cost 10 and click OK.

Add Routing table		
Source agent:	LyncMedSrv1.selab.com	
Calling number:	*	
Dest agent:	*	
Called number:	*	
Route:	192.168.1.130 🗸	
Cost:	10	(Range: 0100)
Description:	Route from LYDC 2010 Med Server 1 to Trunk SBC	
Tags:	Add Edit Delete	-

The cost for these route needs to be higher than 0 so that the ECB does not route the calls for the configured users (like Avaya/Lync users) to the Trunk SBC.

Add similar entries with remaining servers as source agents as shown below.

Add Edit Delete	Upload Download					Search Search Clea
Source agent	Calling number	Dest agent	Called number	Route	Cost	Description
*	*	*	17814437383	lyncmedsrv2.selab.com	20	Fail over route to Lync 2010 Mediation Server 2
*	*	*	17814437387	lync2013med2.acmepacket.net	20	Fail over route to Lync 2013 Mediation Server
172.16.101.39	*	8	*	192.168.1.130	10	Route from Lync 2010 Med Server 1 to Trunk SBC
acmepacket.net	*	8	*	192.168.1.130	10	Route for Transfer INVITEs from Lync 2013 server
aura.com	*	*	*	192.168.1.130	10	Route from Avaya Server to Trunk SBC
lync2013med1.acmepacket.net	*	*	*	192.168.1.130	10	Route from Lync 2013 Med Server 1 to Trunk SBC
lync2013med2.acmepacket.net	*	*	*	192.168.1.130	10	Route from Lync 2013 Med Server 2 to Trunk SBC
lyncmedsrv1.selab.com	*	*	*	192.168.1.130	10	Route from Lync 2010 Med Server 1 to Trunk SBC
lyncmedsrv2.selab.com	*	*	*	192.168.1.130	10	Route from Lync 2010 Med Server 2 to Trunk SBC



To route the INVITEs in case of transfers from Lync 2013, add a route as shown below routing from source agent – acmepacket.net to the trunk SBC and click **OK**.

Add Routing table			
Source agent:	acmepacket.net	~	
Calling number:	- sic		
Dest agent:	*	~	
Called number:	sia		
Route:	192.168.1.130	~	
Cost:	10		(Range: 0100)
Description:	Route for Transfer <u>INVITEs</u> from <u>Lyn</u> 2013 server	ç	
Tags:	Add Edit Delete		



The **Routing Table** page will be displayed listing all the routes added. When you select a specific route, its **Route tree** is displayed at the bottom.

Routing table						
Search Criteria: All						
Add Edit Delete	Upload Download					Search Search Clear
Source agent	Calling number	Dest agent	Called number	Route	Cost	Description
*	*	*	17814437383	lyncmedsrv2.selab.com	20	Fail over route to Lync 2010 Mediation Server 2
*	*	*	17814437387	lync2013med2.acmepacket.net	20	Fail over route to Lync 2013 Mediation Server
172.16.101.39	*	*	*	192.168.1.130	10	Route from Lync 2010 Med Server 1 to Trunk SBC
acmepacket.net	*	*	*	192.168.1.130	10	Route for Transfer INVITEs from Lync 2013 server
aura.com	*	*	*	192.168.1.130	10	Route from Avaya Server to Trunk SBC
lync2013med1.acmepacket.net	*	*	*	192.168.1.130	10	Route from Lync 2013 Med Server 1 to Trunk SBC
lync2013med2.acmepacket.net	*	*	*	192.168.1.130	10	Route from Lync 2013 Med Server 2 to Trunk SBC
lyncmedsrv1.selab.com	*	*	*	192.168.1.130	10	Route from Lync 2010 Med Server 1 to Trunk SBC
lyncmedsrv2.selab.com	*	*	*	192.168.1.130	10	Route from Lync 2010 Med Server 2 to Trunk SBC
Displaying 1 - 9 of 9	Back					
Route tree						
10 - Cost: 10 calling agent: au	ura.com → 192.168.1.	130				
20 – Cost: 20 called number:	$17814437387 \rightarrow $ lync20	13med2.acmepacket.n	iet			
20 — cost: 20 called number:	17814437383 → lyncm	edsrv2.selab.com				

Click on **Configuration** button on the top to go to the **Configuration** tab.



Configure Header manipulation rules

We will now configure header manipulation rules to hide network topology and ensure that the SIP messages sent to all agents cater to their specific signaling standards.

Click on the HMR icon under System Administration on the Configuration tab.



The **SIP manipulation** page is displayed. We need to configure a sip-manipulation to replace the ip-addresses in the From and To headers to hide the network topology. Click Add to add a sip manipulation for this purpose.

acme Anacket					
actice	Home	Configuration	Monitor and Trace	Widgets	System
E Save					
SIP manipulation Search Criteria: All					
Add Edit	Delete	Upload Down	nload		
Name Add a new ite	m				
No objects currently config	ured				



In the Add SIP manipulation page, enter a name and description for the manipulation. In our case, it is called NATting. To add a header-rule, select header-rule from the Add drop down menu under the CfgRules section.

dd SIP manipulation	
Name:	NATting
Description:	HMR for Topology Hiding
Split headers:	Add Edit Delete
Join headers:	
	Add Edit Delete
CfgRules	
Add - Edit Delete Mo	ove up Move down
header-rule	Element type
mime-rule	
mime-isup-rule	

In the Add SIP manipulation / header rule page, add a header-rule From as shown below to manipulate the From header. To configure an element-rule for this From Header-rule, select element-rule from the Add drop down menu under the CfgRules section.

Add SIP manipulation / head	der rule			
Name:	From			
Header name:	From	From		
Action:	manipulate	~		
Comparison type:	case-sensitive	~		
Msg type:	any	~		
Methods:	Add Edit De	lete		
Match value:				
New value:				
CfgRules				
Add - Edit Delete	Move up Move down			



Add an element-rule named From_header to replace the uri-host with ECB's local ip-address (192.168.1.90) as shown below and click **OK**.

Add SIP manipulation / hea	der rule / element rule	5
Name:	From_header	
Parameter name:		
Туре:	uri-host	~
Action:	replace	~
Match val type:	any	~
Comparison type:	case-sensitive	~
Match value:		
New value:	\$LOCAL_IP	

The From header-rule page is displayed. Click **OK** and the NATting sip-manipulation page is displayed. Following the steps explained above configure a header-rule to manipulate the To header as shown below.

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	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$REMOTE_IP

This completes the configuration of the sip-manipulation for topology hiding.



Apply this sip manipulation as an outbound manipulation to the Trunk SBC agent and click OK.

Modify Agent settings			
State:			
Hostname:	192.168.1.130		
IP address:	192.168.1.130		
IP port:	5060		(Range: 065535)
Transport protocol:	StaticTCP	~	
TLS profile:		~	
Description:	Trunk SBC		
Source context:	NA	~	
Egress number translation mode:	E164-no-plus	~]
Number of digits for n digit dialing:	4		(Range: 025)
Prepend prefix on egress:			
Inbound header manipulation:		~	
Outbound header manipulation:	NATting	~	
Tags:	Add Edit Delete		

Next we will configure the manipulations required for the Avaya server. The Avaya setup in our lab uses a FQDN of aura.com. The uri-host portions of the Request-Uri, From and To headers in the SIP messages sent to the Avaya server need to be changed to aura.com. If the INVITE contains a PAI header, we will need to change the uri-host to aura.com. Configure the following manipulation to change the uri-host portion to aura.com. This will be applied as an outbound manipulation to the Avaya server.

sip-manipulation	
name	NATtingavaya
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-bost
	cypc		
	action		replace
	match-val-type		any
	comparison-type		case-sensitive
	match-value		
	new-value		aura.com
header-rule			
		" -	
Itallie		10	
neader-	name	10	
action		manipul	ate
compari	son-type	case-se	nsitive
msg-typ	e	request	
methods			
match-v	alue		
nacen v	20		
ilew-var	ue		
element	-rule		
	name		То
	parameter-name		
	type		uri-host
	action		replace
	match-val-type		any
			ang ang ang itiya
	comparison-cype		Case-Selisitive
	match-value		
	new-value		aura.com
header-rule			
name		Ruri hr	
header-	name	Request	-URI
action		manipul	ate
compari	son-tuno	aaso-so	ngitiwo
Compart	son-cype	Case-se	IISTCIVE
msg-typ	e	any	
methods			
match-v	alue		
new-val	ue		
element	-rule		
	name		Ruri er
	narameter-name		
	parameter name		
	суре		uri-nost
	action		find-replace-all
	match-val-type		any
	comparison-type		case-sensitive
	match-value		
	new-value		aura.com
header-rule			
neader rule		Dei	
name		Fal	
header-	name	P-Asser	tea-identity



action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	Pai header
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	aura.com

The Request-Uri of the INVITEs sent from the Avaya session manager contains the uri-host as aura.com. This causes issues with the routing in ECB when the dialed numbers are not configured as users in userDB. To resolve this issue, we configure a manipulation to replace the aura.com in the RURI with the ip address of the ECB, in our case – 192.168.1.90 and apply in the inbound direction on the Avaya server agent. This HMR is configured as an out-of-dialog manipulation so that it does not affect the INVITEs for hold and transfers.

sip-manipulatior	1		
name		ChangeRURIhost	
descriptior	1		
split-heade	ers		
join-header	s		
header-rule	2		
nam	ie	fixRURI	
hea	der-name	Request-URI	
act	ion	manipulate	
con	nparison-type	case-sensitive	
msc	j-type	out-of-dialog	
met	hods	INVITE	
mat	ch-value		
new	-value		
ele	ement-rule		
	name	updateRURI	
	parameter-name		
	type	uri-host	
	action	replace	
	match-val-type	any	
	comparison-type	pattern-rule	3
	match-value	(.*)\$	
	new-value	192.168.1.90)



Apply NATtingavaya as an outbound manipulation and ChangeRURIhost as an inbound manipulation to the Avaya server agent and click OK.

State:	•		
Hostname:			1
IP address:	10-232-50-102]
IP port:	5060		(Range: 065535)
Transport protocol:	StaticTCP	~]
TLS profile:		~	
Description:	Avaya Session Manager		
Source context:	Oracle.Burlington-Avaya	~	
Egress number translation mode:	no-country-code	~	
Number of digits for n digit dialing:	4		(Range: 025)
Prepend prefix on egress:			-
Inbound header manipulation:	ChangeRURIhost	~]
Outbound header manipulation:	NATtingavaya	~]
Tags:	Add Edit Delete		

We will now configure manipulations to modify the SIP messages being sent to and received from the Lync server. Lync typically sends mediation server FQDN in the Contact header with no username in the SIP URI which is not acceptable by SIP trunk providers. We configure a manipulation to update the Contact header to include the username appropriately and apply it as an in manipulation on the Lync server.

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
header-name	From
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
element-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-rule			
name		Change	Contact
header	-name	Contact	t
action		manipu	late
compar	ison-type	case-se	ensitive
msg-ty	pe	any	
method	ls		
match-	value		
new-va	lue		
elemen	t-rule		
	name		ChangeContact_er
	parameter-name		
	type		uri-user
	action		add
	match-val-type		any
	comparison-type		case-sensitive
	match-value		
	new-value		
\$StoreFromnumber.\$Stor	eFromnumber er.\$0		

Avaya server sends certain b-lines in the SDP which are not supported by Lync server. We configure the following manipulation to delete these lines from SDP before the messages are being sent out to Lync.

sip-manipulation	
name	Delblines
description	Deleting b-lines from Avaya
split-headers	
join-headers	
header-rule	
name	manipContentType
header-name	Content-Type
action	manipulate
comparison-type	pattern-rule
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	deleteB
parameter-name	application/sdp



type	mime
action	find-replace-all
match-val-type	any
comparison-type	pattern-rule
match-value	$b=CT:.*(\langle n \langle r \rangle)$
new-value	
element-rule	
name	deleteLABEL
parameter-name	application/sdp
type	mime
action	find-replace-all
match-val-type	any
comparison-type	pattern-rule
match-value	$b=AS:.*(\langle n \langle r \rangle)$
new-value	
element-rule	
name	deleteLABEL1
parameter-name	application/sdp
type	mime
action	find-replace-all
match-val-type	any
comparison-type	pattern-rule
match-value	$b=TIAS:.*(\langle n \langle r \rangle n)$
new-value	

A nested manipulation named HMRtowardsLync is configured to include the manipulations –NATting and Delblines and applied in the outbound direction to the Lync server.

sip-manipulation	
name	HMRtowardsLync
description	HMR NAT+deleting the blines
split-headers	
join-headers	
header-rule	
name	donat
header-name	From
action	sip-manip
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	NATting
header-rule	
name	deleteblines
header-name	From
action	sip-manip
comparison-type	case-sensitive



msg-type methods	any
match-value new-value	Delblines

Apply ChangeContact as in inbound manipulation and HMRtowardsLync as an outbound manipulation to all the Lync servers configured as agents.

Modify Agent settings			
State:			
Hostname:	LyncMedSrv1.selab.com		
IP address:	192.168.1.119		
IP port:	5060		(Range: 065535)
Transport protocol:	StaticTCP	~	
TLS profile:		~	
Description:			
Source context:	Oracle.Bedford-Lync	~	
Egress number translation mode:	E164	~	
Number of digits for n digit dialing:	4		(Range: 025)
Prepend prefix on egress:			
Inbound header manipulation:	ChangeContact	~	
Outbound header manipulation:	HMRtowardsLync	~	
Tags:	Add Edit Delete		



Next apply NATting as an outbound manipulation to the CUCM server.

Modify Agent settings			
State:	 Image: A start of the start of		
Hostname:	172.16.101.39		
IP address:	172.16.101.39]
IP port:	5060		(Range: 065535)
Transport protocol:	StaticTCP	~]
TLS profile:		~]
Description:	CUCM		
Source context:	Oracle.Braintree-CUCM	~	
Egress number translation mode:	E164-no-plus	~]
Number of digits for n digit dialing:	4		(Range: 025)
Prepend prefix on egress:]
Inbound header manipulation:		~]
Outbound header manipulation:	NATting	~]
Tags:	Add Edit Delete		

Click Configuration on the top to go back to the Configuration tab.

Save and activate the configuration

We will now save and activate our ECB configuration. Click Save on the top left hand side of the Configuration tab.





🖈 Acme Packet: ECB	×			_	The part in case of the				- 0 X
← → C fi 🗋	172.18.255.55/#								
👯 Apps 🧧 My Oracle	Acme Packet Soluti	🐻 ClearQuest 📌 Sh	arepoint 💮 MOS 🧲	Header Manipulatio T	N Infrastructure qualifi				Dther bookmarks
acme Apacket	Home Configurat	tion Monitor and Tr	ace Widgets Sy	/stem				Welcome: admin	Avotifications Help • Log off
E Save								÷¢⊧ v	/izards • 🚡 Discard 🔍 S <u>e</u> arch
Service Provision Agents System Administ	ning Dial Plan ration	Users Users SIP Interface	Routing ECB Sync	Progree L SIP Registrar	Saving configuration Close LDAP HM	R Security	Accounting	SIMP	Web Server

A progress dialog box will appear showing that the configuration in being saved.

You will be asked to confirm if you would like to activate the configuration. Click Activate.





After the activation is completed, you will see the screen below



Click OK and the ECB configuration is now complete.



Phase 2 - Configuring the Lync 2013 server

The enterprise will have a fully functioning Lync 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 ECB:

- Adding the ECB as a PSTN gateway to the Lync Server infrastructure
- Creating a route within the Lync Server infrastructure to utilize the SIP trunk connected through the ECB.

To add the PSTN gateway, we will need:

- IP addresses of the external facing NICs of the Mediation Servers
- IP address of the sip interface of the ECB
- Rights to administer Lync Server Topology Builder
- Access to the Lync Server Topology Builder

Adding the ECB as a PSTN gateway

The following process details the steps to add the ECB as the PSTN gateway

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





3. The opening screen of the Topology builder will be displayed. Click on the **Cancel** button.



4. The Topology Builder window will now be displayed. Click on Action and select Download Topology.

16	Lyne	c Server 2013, Topology Builder	. 🗆 🗙
File Ac	tion Help		
6	NuM Central Site	nt from the Actions pane	
	Edit Properties		
	New Topology		
_	Open Topology		
	Download Topology		
	Save a copy of To Download complete deployment topolo	ogy from the Central Management store.	
	Publish Topology		
	Install Database		
	Merge Office Communications Server 2007 R2 Topology		
	Remove Deployment		
	Help		



5. You will then see a screen showing that you have successfully imported the topology. Click the **Ok** button.

20	Download Topology
ſ	Downloading topology
	Succeeded
	Downloading global simple URL settings
	Succeeded
	Finished
Ľ	
	OK Cancel
	— K ——

6. 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

20	Save	Topology As		×
🕤 👻 🛞 🕞	« Documents + temp	~ ¢	Search temp	Q
Organize 👻 Ne	w folder		8==	- 0
🔆 Favorites	^ Name	^	Date modified	Type More option
💻 Desktop 鷆 Downloads		No items match	your search.	
强 Recent places	=			
🥽 Libraries				
Documents				
Music				
Pictures				
Videos 📔				
🛤 Computer	~ <			>
File <u>n</u> ame:	Current2			~
Save as type:	Topology Builder files (*.tbx	ml)		~
Hide Folders	L		Save	Cancel



7. You will now see the topology builder screen with the enterprise's topology imported.

10 1	Lync Serve	er 2013,	Topology Builder	_	x
File Action Help					
Lync Server Bedford	SIP domain				•
	Default SIP domain: Additional supported SIP domains:	acmep Not co	acket.net nfigured		
	Simple URLs				•
	Phone access URLs:	Active	Simple URL https://dialin.acmepacket.net		
	Meeting URLs:	Active	Simple URL	SIP domain	
	Administrative access URL:	https://	nttps://meet.acmepacket.net /admin.acmepacket.net	acmepacket.net	
	Central Management Serve	r			•
	Central Management Server:	Active	Front End	Site	
		•	griele isstalaritepercenter	<u></u>	

8. In the upper left hand corner, expand the site in which the PSTN gateway will be added. In our case, the site is **Bedford**. Then click on the **PSTN Gateways**

20	Lync Server 2013, Topology Builder	- • ×
Elle Action Help	The properties for this item are not available for editing.	



9. Right click on PSTN gateways and select New IP/PSTN Gateway.



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

e		Define Nev	v IP/PSTN Ga	teway		×
5	Define the P	STN Gateway F	QDN			
Define the	fully qualified do	main name (FQDN)	for the PSTN gat	teway.		
FQDN: *						
192.168.1	.90					
11.1	-					6. 1
Help				Back	Next	Cancel



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

24	Define New IP/PSTN Gateway
5	Define the IP address
 Enation I 	ole IPv <u>4</u> Jse all configured IP addresses. jimit service usage to selected IP addresses. PSTN JP address:
⊖ Enat	ole IPv <u>6</u> Jse all configured IP addresses. jimit service usage to selected IP addresses. PSTN JP address:
Help	Back Next Cancel

12. In the next section, enter the ip address of the ECB's sip interface under **Trunk name**. Configure the **Listening port for IP/PSTN gateway** as 5068, TCP as the **SIP Transport Protocol** and click **Finish**.

Define New IP/PSTN Gateway	x
Define the root trunk	
Trunk name:*	
192.168.1.90	
Listening port for IP/PSTN gateway: *	
5068	
SIP Transport Protocol:	1
Associated Mediation Server:	'
lync2013med.acmepacket.net Bedford	
Associated Mediation Server port: *	
5068	
Help Back Finish Cancel]



13. The PSTN gateway for the Lync server has been added. It will be listed under PSTN gateways.

Expand the **Mediation Pool** list and click on the Mediation Server to be utilized. In our example the Mediation Server is **Iync2013med.acmepacket.net**.

You will see that the PSTN gateway is associated with the Mediation server.

Lync Server 2013, Topology Builder					
File Action Help					
Lync Server Bedford	General				^
 Lync Server 2010 Lync Server 2013 	FQDN:	lync2013med.	acmepacket.net		
Standard Edition Front End Servers	Associations				
Enterprise Edition Front End pools	Edge pool (for media):	Not associated	1		
Mediation pools	Note: To view the federati	ion route, use the	site property page.		
Inc2013med.acmepacket.net					
Persistent Chat pools	Next hop selection				•
Trusted application servers Shared Components SQL Server stores	Next hop pool:	lync2013std.ar	mepacket.net (Bedford)		
File stores A Comparison procession of the stores of the store	Mediation Server PSTN ga	teway			•
192.168.1.90 Trunks	TLS listening port: TCP listening port:	5067 - 5067 5068 - 5068			
P Office Web Apps Servers Reapch sites	Trunks:	Default	Trunk	Gateway	Site
		<u>192.</u>	168.1.90	<u>192.168.1.90</u>	Bedford
111 > K 111 + 1111 + 111 + 111 + 111 + 111 + 1111 + 111 + 111 + 111 + 11					



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

16			Lync Sen	ver 2013, Topo	ology Builder		x
File A	ction, Help New Server		1				
4	Edit Properties		General				•
	Topology Delete Help Director pools Mediation pools Relync2013med.acm Persistent Chat pools	New Open Downlo Save A (Publish. Install (Merge (Remove	ad Current Topology Copy - Jublish topology to the Centra Office Communications Server	il Mangement st 2007 R2	cmepacket.net		
		rs	Next hop pool: Mediation Server PSTN TLS listening port: TCP listening port:	lync2013sto gateway 5067 - 5067 5068 - 5068	Lacmepacket.net (Bedford)		
	Office Web Apps Servers		Trunks:	Default	Trunk	Gateway	Site
	Branch sites			19	92.168.1.90	<u>192.168.1.90</u>	Bedford
<	101	>	<		ш		>



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

16	Publish Topology	×
F	Publish the topology	
20 10	n order for Lync Server 2013 to correctly route messages in your deployment, you must publish your opology. Before you publish the topology, ensure that the following tasks have been completed:	
	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 control shorts and conference directions have been presented from the seal 	v
٧	When you are ready to proceed, click Next.	
μ	Help Back Next Cancel	

You will now be at a window showing the databases associated with site. Click Next.

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

20	Download Topology
ſ	Downloading topology
	Succeeded
	Downloading global simple URL settings
	Succeeded
	Finished
Ľ	
	OK Cancel

17. You will be at the Topology Builder main window, expand your site and double check that your PSTN entries are correct and that the appropriate Mediation Server has the PSTN gateway associated.



Creating a route within the Lync Server infrastructure

In order for the Lync Server Enterprise Voice 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 Lync Server 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 Lync Server Enterprise Voice deployments such as dial plans, voice policies, and PSTN usages are not covered.

To add the route we will need:

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

The following process details the steps to create the route:

1. From the Start bar, select Lync Server Control Panel.



You will be prompted for credential, 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.



3. The Dial Plan tab in the Voice Routing section will be displayed. On the content area toolbar, click +New.

2	Microsoft Lync Server 2013 Control Panel	×
Lync Server 2013	Administrator 5.0.63004-20 Privecy s	Sign out
🔄 Home	Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Test Voice Routing	
3 Users	Create voice routing test case information	~
Topology IM and Presence	٩	
Persistent Chat	New Zetit Action Commit No Scope State Normalization rules Description	
🗞 Voice Features	Ciobal Global Committed 2	
Response Groups Conferencing		
Clients		
Federation and External Access		
Monitoring and Archiving		
Security		
Configuration		



4. Next you build a Dial Plan and a translation rule for the phone numbers you want this route to handle. You have to create two separate dial plans for US and EMEA.

US Dial-plan	
Match this pattern:	^(\d*)\$
Translation rule: \$1	
International call Dial-pla	in
Match this pattern:	^44(\d{10})\$
Translation rule: +44\$1	
EMEA dial plan	
Match this pattern:	^\+(1\d*)\$
Translation rule: 00\$1	

8	Microsoft Ly	nc Server 2013 Control Panel		
Lync Sonyor 2012			Admin	nistrator Sign o
Lync Server 2015			5.0.8308.420	Privacy stateme
🟠 Home	Dial Plan Voice Policy Route PSTN	I Usage Trunk Configuration Test Voice R	outing	
33 Users	Create voice routing test case informatio	n		~
Topology				
IM and Presence	Edit Dial Plan - Global			
Persistent Chat	✓ OK X Cancel			0
😢 Voice Routing		?		•
& Voice Features	External access prefix:			
🔏 Response Groups		?		
Conferencing	Associated Normalization Rules			
Clients	🕂 New 🖹 Copy 📋 Paste	Select / Show details Remo	ve 🎓 🦊	
Federation and External Access	US dial plan^(\d*)\$	State Pattern to match Committed ^(\d*)\$	Translation pattern \$1	
Monitoring	EMEA dial plan	Committed ^\+(1\d*)\$	00\$1	
and Archiving	International	Committed ^44(\d{10})\$	+44\$1	
Security				
Patwork Configuration	Dialed number to test:			=
		Go	?	•



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

8		Microsoft Lync Server 2013 Control Panel	×
Ly	nc Server 2013	Administrator 5.0.8308.0 Privacy	Sign out statement
-	Home	Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Test Voice Routing	
23.	Users	Create voice routing test case information	×
24	Topology	(C	
Ģ	IM and Presence	٩	
2	Persistent Chat	◆ New / Edit ▼	
C	Voice Routing	State PSTN usage Pattern to match	
S	Voice Features		
22	Response Groups		
ø	Conferencing		
5	Clients		
is.	Federation and External Access		
	Monitoring and Archiving		
-	Security		
Ŷ	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 US route.

OK Cancel		•
ope:		i i
scription		
Build a Pattern to Match		
Build a Pattern to Match — Add the starting digits that you want this route to ha the expression manually by clicking Edit.	ndle, or create	
Build a Pattern to Match Add the starting digits that you want this route to ha the expression manually by clicking Edit. Starting digits for numbers that you want to allow:	ndie, or create	
Build a Pattern to Match Add the starting digits that you want this route to ha the expression manually by clicking Edit. Starting digits for numbers that you want to allow: Type a volid number and then click Add.	ndle, or create	
Build a Pattern to Match Add the starting digits that you want this route to ha the expression manually by clicking Edit. Starting digits for numbers that you want to allow: Type a volid number and then click Add.	Add Exceptions	
Build a Pattern to Match Add the starting digits that you want this route to has the expression manually by clicking Edit. Starting digits for numbers that you want to allow: Type a volid number and then click Add.	Add Exceptions Remove	
Build a Pattern to Match Add the starting digits that you want this route to has the expression manually by clicking Edit. Starting digits for numbers that you want to allow: Type a volid number and then click Add.	Add Exceptions Remove	
Build a Pattern to Match Add the starting digits that you want this route to ha the expression manually by clicking Edit. Starting digits for numbers that you want to allow: Type a volid number and then click Add.	Add Exceptions Remove	



7. Next you build a Pattern Match for the phone numbers you want this route to handle. Click Edit.

¢.	Microsoft Lync Server 2013 Control Panel
Lync Server 2013	Administrator Sign 5.0.8308.420 Privacy statem
🛅 Home	Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Test Voice Routing
👪 Users	Create voice routing test case information
M Topology	
IM and Presence	New Voice Route
Persistent Chat	V X Cancel
🧐 Voice Routing	Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.
📞 Voice Features	Starting digits for numbers that you want to allow:
2 Response Groups	Type a valid number and then click Add. Add
😨 Conferencing	Exceptions
Clients	Remove
Federation and External Access	
Monitoring and Archiving	Match this pattern: "
🔒 Security	
Petwork Configuration	Edit Reset
	Suppress caller ID

8. Enter the pattern for US - ^(\+1[0-9]{10})\$ and click **OK**. To enable 4 digit dial, add the pattern ^(\d{4})\$.

IM and Presence	New Voice Route	
Persistent Chat	✓ OK X Cancel	0
😢 Voice Routing	Add th the ex Type a Regular Expression	^
🌜 Voice Features	Startin Type a regular expression: *	
23 Response Groups	Type a ^((+1[0-9](10))\$	
😨 Conferencing		
Clients	OK Cancel	
Federation and External Access		
Monitoring and Archiving	Match this pattern: *	
Security		
Part Network Configuration	Latt Reset	
	Suppress caller ID	
	Aldenmade selles ID.	· · ·



9. Next you want to associate the Voice Route with the **Trunk** you have just created. Scroll down to **Associated Trunks**, click on the **Add** button.

New Voice Route	
Watch this pattern: * ^(r+1[0-9](10))S Edit Reset	
Suppress caller ID Alternate caller ID:	
Associated trunks:	Add Remove
Associated PSTN Usages	J

10. You will now be at a window showing available Trunks to associate your Voice Route. Click on the PSTN gateway that you just created and then click the **OK** button.

Sele	ect Trunk		(2) 23
			٩
	Service	Site	
	PstnGateway: 192.168.1.90	Bedford	
	PstnGateway:192.168.2.200	Bedford	
		OK K	Cancel



11. 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**.

OK 🛪 Cancel		
ssociated trunks:		
PstnGateway:192.168.1.90	Add	
	Remove	
ssociated PSTN Usages		
osociated i sini osages		
Select Remove	±	
PSTN usage record	Associated voice policies	
Select Remove	Associated voice policies	
Select Remove	Associated voice policies	
Select Remove PSTN usage record	Associated voice policies	
Select Remove PSTN usage record	Associated voice policies	

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

ect PSTN Usage Record		0
		Q
PSTN usage record name	Associated routes	Associated voice policies
Internal		
Local		
Long Distance	ECB	Global
		OK Cancel



13. 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.

OK X Cancel			
ssociated trunks:			
PstnGateway:192.168.1.90	D	Add	
		Remove	
ssociated PSTN Usages			
Select Remove	1 4		
Select Remove PSTN usage record	Associated voice policies		
Select Remove PSTN usage record Long Distance	Associated voice policies Global		
Select Remove PSTN usage record Long Distance	Associated voice policies Global		
Select Remove PSTN usage record Long Distance	Associated voice policies Global		
Select Remove PSTN usage record Long Distance	Associated voice policies Global		
Select Remove PSTN usage record Long Distance	Associated voice policies Global		
Select Remove PSTN usage record Long Distance	Associated voice policies Global		

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

			P		
New / Edit +	The Move up		Action 👻	Commit K	
Name		State	PSTN usage	Review uncommitted changes	atch
ECB		P Uncommitted	Long Distance	Commit all	
				Cancel selected changes	
				Cancel all uncommitted changes	


15. On the Uncommitted Voice Configuration Settings window, click OK.

Unco	mmitted Voice Configuration	on Setting	s		0	23
Ro	utes				^	
	Identity	Action	New value (pattern to match)	Old value (pattern to match)		
	ECB	Modified	2	2		
				ок р с	ancel	

If there are no errors, the new Voice Route has now been successfully created and the state will show as Committed.

Additional Steps

There are other aspects to a Lync Server Enterprise Voice deployment such as

- Site, local, and global dial plans
- Voice Policies
- Assigning Voice Policies to users
- PSTN usage policies

Refer to MSDN technet for relevant information.

Following the same procedure, configure ECB as a PSTN gateway in the Lync 2010 environment.



Phase 3 – Configuring the Avaya Session Manager

The enterprise has a fully functional Avaya Aura System Manager. Configuring the System Manager to operate with ECB consists of three steps –

- Adding the ECB as a SIP Entity
- Configuring an Entity link between ECB and Session Manager
- Creating a Routing policy to assign the appropriate routing destination.

Adding the ECB as a SIP Entity

Log in to the Aura System Manager. Click on Routing under the Elements section.

Users	- Elements	O _o Services
Administrators Directory Synchronization Groups & Roles User Management User Provisioning Rule	Collaboration Environment Communication Manager Communication Server 1000 Conferencing IP Office Meeting Exchange Messaging Presence Routing Session Manager	Backup and Restore Bulk Import and Export Configurations Events Geographic Redundancy Inventory Licenses Replication Reports Scheduler Security Shutdown Shutdown Shutdown Event Management Templates



_

On the **Routing** tab, select **SIP Entities** from the menu on the left side of the screen. Click **New** to add ECB as a SIP entity as shown below and click **Commit**.

Home Routing ^		
• Routing	Home / Elements / Routing / SIP Enti	ties
Domains		Help ?
Locations	SIP Entity Details	Commit Cancel
Adaptations	General	
SIP Entities	* Name:	acme-ecb
Entity Links	* FQDN or IP Address:	192.168.1.90
Time Ranges	Туре:	SIP Trunk
Routing Policies	Notes:	acme-ecb
Dial Patterns		
Regular Expressions	Adaptation:	\checkmark
Defaults	Location:	acme- Ent Comm Broker
	Time Zone:	America/Fortaleza
	* SIP Timer B/F (in seconds):	4
	Credential name:	
	Call Detail Recording:	none 🔽

Call Detail Recording	none V
Loop Detection Loop Detection Mode	Off
SIP Link Monitoring SIP Link Monitoring	Use Session Manager Configuration
Supports Call Admission Control	
Shared Bandwidth Manager	
Primary Session Manager Bandwidt Association	h
Backup Session Manager Bandwidt Association	h
Entity Links Override Port & Transport with DN SRV Add Remove	S □
2 Items 📚	Filter: Enable
SIP Entity 1 Protocol Port	SIP Entity 2 Port Connection Deny New Service
acme-sm2 V TCP V * 5060	acme-ecb V * 5068 trusted V acme-ecb V * 5068 trusted V
Select : All, None	



Configuring an Entity link between ECB and Session Manager

Select Entity Links from the menu and click on New to add an Entity Link between ECB and SM with the following settings and click Commit.

Н	ome	Routing ×									
۲	Home	/ Elements / Routing) / Entity Links								
	Entity	' Links					Commit	Cancel			
	1 Iten	n I 🍣									F
		Name	SIP Entity 1	Protocol	Port	SIP Entity 2		DNS Override	Port	Connec Polic	tion Y
		* acme-sm_acme-ecb_	* acme-sm 🗸	TCP 🗸	* 5060	* acme-ecb	~		* 5068	trusted	\sim
	<										
	Select	: All, None									

Creating a Routing policy to assign the appropriate routing destination

Select **Routing policies** from the menu and click on **New** to add a routing policy between ECB and SM with the following settings and click **Commit**.

Routing Policy Details Commit Cancel General * Name: Calls to ECB from SM1 Disabled:	Home / Elements / Routing / Routing	Policies			
General * Name: Calls to ECB from SM1 Disabled:	Routing Policy Details				Help ? Commit Cancel
 Name: Calls to ECB from SM1 Disabled: _ Retries: 0 Notes: Calls to ECB from SM1 SIP Entity as Destination Select Name FQDN or IP Address acme-ecb 192.168.1.90 SIP Trunk acme-ecb 192.168.1.90 SIP Trunk acme-ecb 192.168.1.90 Elter: Enable	General				
Disable: Petries: Petries: Notes: Calls to ECB from SM1 SIP Entity as Destination Select Name FQDN or IP Address Type Notes acme-ecb 192.168.1.90 SIP Trunk acme-ecb Time of Day Add Remove View Gaps/Overlaps Litem P	* Name:	Calls to ECB from S	М1		
 Retries: 0 Notes: Calls to ECB from SM1 SIP Entity as Destination Select Name FQDN or IP Address acme-ecb 192.168.1.90 SIP Trunk acme-ecb Time of Day Add Remove View Gaps/Overlaps	Disabled:				
Notes: Calls to ECB from SM1 SIP Entity as Destination Select Type Notes acme-ecb 192.168.1.90 SIP Trunk acme-ecb Time of Day Add Remove View Gaps/Overlaps I Item Time of Day Silter: Enable	* Retries:	0			
SIP Entity as Destination Select Name FQDN or IP Address acme-ecb 192.168.1.90 SIP Trunk acme-ecb Time of Day Add Remove View Gaps/Overlaps Litem Time of Day	Notes:	Calls to ECB from S	м1	7	
FQDN or IP Address Name FQDN or IP Address Type Notes acme-ecb 192.168.1.90 SIP Trunk acme-ecb Time of Day Mathematical Supervision View Gaps/Overlaps 1 Item Time of Day Sip Trunk Sip Trunk					
Select Type Notes name FQDN or IP Address Type Notes acme-ecb 192.168.1.90 SIP Trunk acme-ecb Time of Day Add Remove View Gaps/Overlaps I Item Time of Day	SIP Entity as Destination				
Name FQDN or IP Address Type Notes acme-ecb 192.168.1.90 SIP Trunk acme-ecb Time of Day Add Remove View Gaps/Overlaps	Select				
acme-ecb 192.168.1.90 SIP Trunk acme-ecb Time of Day Add Remove View Gaps/Overlaps	Name FQDN or IP A	ddress	1	Гуре	Notes
Time of Day Add Remove View Gaps/Overlaps Litem Time	acme-ecb 192.168.1.90			SIP Trunk	acme-ecb
1 Itam - 3	Time of Day Add Remove View Gaps/Overlaps				
riter. Ellable	1 Item 🛛 🍣				Filter: Enable
□ Ranking ^ Name Mon Tue Wed Thu Fri Sat Sun Start Time End Time Notes	Ranking A Name Mon Tue V	Wed Thu Fri Sa	t Sun Sta	art Time End T	Fime Notes
0 24/7 🗹 🗹 🗹 🗹 🗹 00:00 23:59 Time Range 24/7	0 24/7 🕅	N N N		00:00 23	:59 Time Range 24/7
Select : All, None	Select : All, None				

r rrei	m 🛛 🍣 👘											Filt	ter: Enable
	Ranking 🔶	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes	
	0	24/7	~	~	~		\checkmark	~	~	00:00	23:59	Time Ran	ge 24/7
elec	t:All, None												
Iter	ms 🍣											Filt	ter: Enable
	Pattern	 Min 	Max	Eme	rgency	Call		SIP Do	main	Originat	ing Location	n	Notes
	765	з	36			Г		-ALL-		-ALL-			
	978	3	11					aura.co	m	acme		Assigned O	riginating l
	×	1	36					-ALL-		-ALL-			
Selec	t : All, None												
Leg Add	ular Expr Remove	essior	15									Fill	ter: Enable
) Iter													

The Avaya System Manager is now configured to operate with ECB.



Phase 4 – Configuring the Cisco Unified Communications Manager

The enterprise will have a fully functioning Cisco Unified Communications Manager deployed. We will now configure it to operate with ECB. This consists of the following steps

- Configuring the SIP Trunk Security profile
- Configuring the SIP profile
- Configure the Trunk
- Configuring the Route Pattern

Configuring the SIP Trunk Security Profile

1. Log into the Cisco Unified CM administration page using the link https://server-ip/.





2. To go to the SIP trunk security profile page, expand the System drop down menu, select SIP Trunk Security Profile under Security.



3. A Non Secure SIP Trunk security profile should be present, if not create one as shown below

SIP Trunk Security Profile Configuration						
🔜 Save 🗙 Delete 🗋 Copy 資 Reset 🧷 Apply Config 🕂 Add New						
Status	Status					
i Status: Ready						
SIP Trunk Security Profile	e Information					
Name*	Non Secure SIP Trunk Profile					
Description	Non Secure SIP Trunk Profile authenticated by null String					
Device Security Mode	Non Secure					
Incoming Transport Type*	TCP+UDP •					
Outgoing Transport Type	TCP -					
Enable Digest Authenticat	tion					
Nonce Validity Time (mins)*	600					
X.509 Subject Name						
Incoming Port*	5060					
Enable Application Level	Authorization					
C Accept Presence Subscrip	otion					
Accept Out-of-Dialog REF	ER**					
Carl Accept Unsolicited Notifica	ation					
Accept Replaces Header						
Transmit Security Status						



Configuring the SIP Profile

1. To go to the SIP Profile page, expand the **Device** drop down menu and select **SIP Profile** from **Device Settings**.

Cisco Unified CM Administration For Cisco Unified Communications Solutions		
System Call Routing Media Resources Advanced Features	Device - Application - User Managem	ent 👻 Bulk Administration 👻 Help 👻
Cisco For Cisco Unified Communications Solutions System Cal Routing Media Resources Advanced Features Cisco Unified CM Administration System version: 8.5.1.10000-26 Licensing Warnings: System version: 8.5.1.10000-26 Licensing Warnings: System is opporting on Demo licenses. Please upload rel Please visit the License Report Page for more details. VHware Installation: 1 vCPU Intel(R) Xeon(R) CPU E5-2 Last Successful Logon: Apr 29, 2014 10:33:11 AM Copyright © 1999 - 2011 Cisco Systems, Inc. All rights reserved. This product contains cryptographic features and is subject to United syporters, distributors and users are responsible for compliance with a summary of U.S. laws governing Cisco cryptographic products may for information about Cisco Unified Communications Manager please for Cisco Technical Support please visit our Technical Support web s	Device Application User Managem CTI Row Point Gatekreper Gateway Phone Trunk Remote Destination Device Settings 6400 @ 2.50GHz, disk 1: 160GE States and local country laws governing U.S. and local country laws. By using y be found at our <u>Export Compliance P</u> visit our <u>Unified Communications Syst</u> ite.	ent Buik Administration Help Device Defaults Firmware Load Information Default Device Profile Device Profile Phone Button Template Softley Template Softley Template Softley Template Softley Template Softley Template Common Device Configuration Common Phone Profile Remote Destination Profile Remote Destination Profile Remote Destination Profile Reature Control Policy
		Recording Profile SIP Normalization Script

2. The **Find and List SIP Profiles** page will display the default SIP profile. Click on the **Copy** button to create a new SIP profile.

Find and List SIP	Profiles		
Add New	Select All 🔛 Clear All 💥 Delete Selected		
_ Status			
1 records four	nd		
SIP Profile (1 -	1 of 1)		Rows per Page 50 👻
Find SIP Profile wh	ere Name 🗸 begins with 🗸	Find Clear Filter	
	Name *	Description	Copy
	Standard SIP Profile	Default SIP Profile	
Add New Sel	ect All Clear All Delete Selected		N,



3. Add a new SIP profile with the following settings. It is same as the default profile but includes PRACK support.

SIP Profile Information		
Name*	SIP Profile for PRACK	
Description	SID Profile for DRACK	
Default MTP Telephony Event Pauload Tupe*		
	101	
Resource Priority Namespace List	< None >	▼
Early Offer for G.Clear Calls	Disabled	▼
Redirect by Application		
🗖 Disable Early Media on 180		
🔲 Outgoing T.38 INVITE include audio mline	2	
Enable ANAT		
🔲 Require SDP Inactive Exchange for Mid-C	all Media Change	
	-	
- Parameters used in Phone		-
Timer Invite Expires (seconds)*	180	
Timer Register Delta (seconds)*	5	
Timer Register Expires (seconds)*	3600	
Timer T1 (msec)*	500	
Timer T2 (msec)*	4000	
Retry INVITE*	6	
Retry Non-INVITE*	10	
Start Media Port*	16294	
	10001	
Start Media Port [*]	16384	
Stop Media Port [*]	32766	
Stop Media Port* Call Pickup URI*	32766 ×-cisco-serviceuri-pickup	
Stop Media Port* Call Pickup URI* Call Pickup Group Other URI*	32766 ×-cisco-serviceuri-pickup ×-cisco-serviceuri-opickup	
Stop Media Port* Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI*	32766 x-cisco-serviceuri-pickup x-cisco-serviceuri-opickup x-cisco-serviceuri-gpickup	
Stop Media Port [*] Call Pickup URI [*] Call Pickup Group Other URI [*] Call Pickup Group URI [*] Meet Me Service URI [*]	32766 ×-cisco-serviceuri-pickup ×-cisco-serviceuri-opickup ×-cisco-serviceuri-gpickup ×-cisco-serviceuri-meetme	
Stop Media Port* Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info*	32766 x-cisco-serviceuri-pickup x-cisco-serviceuri-opickup x-cisco-serviceuri-gpickup x-cisco-serviceuri-meetme None	•
Stop Media Port* Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info* DTMF DB Level*	32766 x-cisco-serviceuri-pickup x-cisco-serviceuri-opickup x-cisco-serviceuri-gpickup x-cisco-serviceuri-meetme None Nominal	•
Stop Media Port* Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info* DTMF DB Level* Call Hold Ring Back*	32766 x-cisco-serviceuri-pickup x-cisco-serviceuri-opickup x-cisco-serviceuri-gpickup x-cisco-serviceuri-meetme None None Nominal Off	•
Stop Media Port Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info DTMF DB Level* Call Hold Ring Back* Anonymous Call Block	32766 x-cisco-serviceuri-pickup x-cisco-serviceuri-opickup x-cisco-serviceuri-gpickup x-cisco-serviceuri-meetme None None Nominal Off Off	
Stop Media Port Call Pickup URI Call Pickup Group Other URI Call Pickup Group URI Meet Me Service URI User Info DTMF DB Level Call Hold Ring Back Anonymous Call Block Caller ID Blocking	32766 x-cisco-serviceuri-pickup x-cisco-serviceuri-opickup x-cisco-serviceuri-gpickup x-cisco-serviceuri-meetme None Nominal Off Off Off	
Stop Media Port Call Pickup URI Call Pickup Group Other URI Call Pickup Group URI Meet Me Service URI User Info DTMF DB Level Call Hold Ring Back Anonymous Call Block Caller ID Blocking Do Not Disturb Control	32766 x-disco-serviceuri-pickup x-disco-serviceuri-opickup x-disco-serviceuri-gpickup x-disco-serviceuri-meetme None None Nominal Off Off Off User Disc block	
Stop Media Port Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info* DTMF DB Level* Call Hold Ring Back Anonymous Call Block Caller ID Blocking Do Not Disturb Control Telnet Level for 7940 and 7960	32766 x-cisco-serviceuri-pickup x-dsco-serviceuri-opickup x-cisco-serviceuri-gpickup x-cisco-serviceuri-meetme None None Nominal Off Off Off User Disabled 100	
Stop Media Port Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info* DTMF DB Level* Call Hold Ring Back* Anonymous Call Block Caller ID Blocking* Do Not Disturb Control Telnet Level for 7940 and 7960* Timer Silveribe Expires (seconds)	32766 x-disco-serviceuri-pickup x-disco-serviceuri-opickup x-disco-serviceuri-gpickup x-disco-serviceuri-meetme None None Nominal Off Off Off User Disabled 120	
Stop Media Port Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info* DTMF DB Level* Call Hold Ring Back* Anonymous Call Block Caller ID Blocking* Do Not Disturb Control Telnet Level for 7940 and 7960* Timer Keep Alive Expires (seconds)* Timer Subscribe Expires (seconds)*	32766 x-disco-serviceuri-pickup x-disco-serviceuri-opickup x-disco-serviceuri-gpickup x-disco-serviceuri-meetme None None Nominal Off Off Off User Disabled 120 -	
Stop Media Port Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info* DTMF DB Level* Call Hold Ring Back* Anonymous Call Block* Caller ID Blocking* Do Not Disturb Control Telnet Level for 7940 and 7960* Timer Keep Alive Expires (seconds)* Timer Subscribe Expires (seconds)*	32766 x-dsco-serviceuri-pickup x-dsco-serviceuri-opickup x-dsco-serviceuri-gpickup x-dsco-serviceuri-meetme None None Nominal off off Off User Disabled 120 5	
Stop Media Port Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info* DTMF DB Level* Call Hold Ring Back* Anonymous Call Block Caller ID Blocking* Do Not Disturb Control Telnet Level for 7940 and 7960* Timer Keep Alive Expires (seconds)* Timer Subscribe Expires (seconds)* Timer Subscribe Delta (seconds)* Maximum Redirections*	32766 x-dsco-serviceuri-pickup x-dsco-serviceuri-opickup x-dsco-serviceuri-gpickup x-dsco-serviceuri-meetme None None Nominal off off off Off User Disabled 120 5 70	
Stop Media Port Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info* DTMF DB Level* Call Hold Ring Back Anonymous Call Block Caller ID Blocking Do Not Disturb Control Telnet Level for 7940 and 7960* Timer Keep Alive Expires (seconds)* Timer Subscribe Expires (seconds)* Timer Subscribe Delta (seconds)* Maximum Redirections*	32766 x-dsco-serviceuri-pickup x-dsco-serviceuri-opickup x-dsco-serviceuri-gpickup x-dsco-serviceuri-meetme None None Nominal off off Off Off User Disabled 120 5 70 15000	
Stop Media Port Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info* DTMF DB Level* Call Hold Ring Back Anonymous Call Block Caller ID Blocking Do Not Disturb Control Telnet Level for 7940 and 7960* Timer Keep Alive Expires (seconds)* Timer Subscribe Expires (seconds)* Timer Subscribe Delta (seconds)* Maximum Redirections* Off Hook To First Digit Timer (milliseconds)* Call Forward URI*	32766 x-dsco-serviceuri-pickup x-dsco-serviceuri-opickup x-dsco-serviceuri-gpickup x-dsco-serviceuri-meetme None None None Noninal off off Off Off User Disabled 120 5 70 15000 x-dsco-serviceuri-dwall	
Stop Media Port Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info* DTMF DB Level* Call Hold Ring Back Anonymous Call Block Caller ID Blocking Do Not Disturb Control Telnet Level for 7940 and 7960* Timer Subscribe Expires (seconds)* Timer Subscribe Expires (seconds)* Timer Subscribe Delta (seconds)* Maximum Redirections* Off Hook To First Digit Timer (milliseconds)* Call Forward URI*	32766 x-dsco-serviceuri-pickup x-dsco-serviceuri-opickup x-dsco-serviceuri-gpickup x-dsco-serviceuri-meetme None None None Nominal off off Off Off User Disabled 120 5 70 15000 x-dsco-serviceuri-dwall x-dsco-serviceuri-dwall	
Stop Media Port* Call Pickup URI* Call Pickup Group Other URI* Call Pickup Group URI* Meet Me Service URI* User Info* DTMF DB Level* Call Hold Ring Back* Anonymous Call Block* Caller ID Blocking* Do Not Disturb Control* Telnet Level for 7940 and 7960* Timer Subscribe Expires (seconds)* Timer Subscribe Expires (seconds)* Timer Subscribe Delta (seconds)* Maximum Redirections* Off Hook To First Digit Timer (milliseconds)* Call Forward URI* Speed Dial (Abbreviated Dial) URI*	32766 x-dsco-serviceuri-pickup x-dsco-serviceuri-opickup x-dsco-serviceuri-meetme None None Nominal off off Off User Disabled 120 5 70 15000 x-dsco-serviceuri-dwdall x-dsco-serviceuri-abbrdial	



RFC 2543 Hold			
🔽 Semi Attended Transfer			
Enable VAD			
Stutter Message Waiting			
_ Trunk Specific Configuration			
Reroute Incoming Request to new Trunk based on*	Never	▼	
RSVP Over SIP*	Local RSVP	▼	
Fall back to local RSVP			
SIP Rel1XX Options*	Send PRACK for all 1×× Messages	ges 🗸	
🔲 Deliver Conference Bridge Identifier			
Early Offer support for voice and video calls (insert MTP if needed)			
Send send-receive SDP in mid-call INVITE			
SIP OPTIONS Ping			
Enable OPTIONS Ping to monitor destination st	atus for Trunks with Service Type "N	e "None (Default)"	
Ping Interval for In-service and Partially In-service	Trunks (seconds) [*] 60		
Ping Interval for Out-of-service Trunks (seconds)*	120		
Ping Retry Timer (milliseconds)*	500		
Ping Retry Count*	6		
- Save Delete Copy Reset Apply C	onfig Add New		

Configuring the Trunk

1. To go to the Trunks page, select **Trunk** from the **Device** drop down menu.

System Call Routing Media Resources Advanced Features	Device Application User Management Buk Administration Help
Find and List Gateway	CTI Route Point
r Add New	Gatekeeper
	O ateway Phone
Lateways	Trunk N inter Find Clear Silter
	Remote Destination
No active que	Device Settings the options above.
Add New	



2. Add a trunk with the following settings and click **Save**.

Trunk Configuration	Related Links: Back To Find/List 🚽	Go
🔚 Save 🗙 Delete 🏻 Reset 🕂 Add New		
i Status: Ready		
∟ ⊢ Device Information ────		E
Product:	SIP Trunk	
Device Protocol: Truck Service Tuce	SIP None(Default)	
Device Name*	FCB	
Description	ECP	
Device Pool*	Default	
Common Device Configuration	< None >	
Call Classification*	Use System Default	
Media Resource Group List	< None >	
Location*	Hub None	
AAR Group	<pre></pre>	
Tunneled Protocol*	None	
QSIG Variant*	No Changes	
ASN.1 ROSE OID Encoding*	No Changes	
Packet Capture Mode*	Batch Processing Mode 🗸	
Packet Capture Duration	0	
Media Termination Point Required		
Retry Video Call as Audio		
Dath Replacement Support		-
Trunk Configuration	Related Links: Back To Find/List 🗸	Go
Trunk Configuration	Related Links: Back To Find/List 🚽	Go
Trunk Configuration Save Delete Save Delete Reset Add New	Related Links: Back To Find/List 🚽	Go ^
Fast Representent Support Trunk Configuration Save Delete Save Delete Watery Video Call as Audio Path Replacement Support	Related Links: Back To Find/List 🚽	Go
Trunk Configuration Save Delete Path Reset Delete Add New Restry Video Call as Audio Path Replacement Support Transmit UTF-8 for Calling Party Name	Related Links: Back To Find/List 🚽	Go
Trunk Configuration Save Colling Path Replacement Support Add New Restry Video Call as Audio Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU	Related Links: Back To Find/List 🚽	Go
Trunk Configuration Save Delete Path Reset Delete Add New Restry Video Call as Audio Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port	Related Links: Back To Find/List 🚽	Go
Trunk Configuration Resty Video Call as Audio Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS	Related Links: Back To Find/List	Go
Trunk Configuration Resty Video Call as Audio Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Turffe on This Turk Secure*	Related Links: Back To Find/List	Go
Trunk Configuration Save Delete Reset Add New Retry Video Call as Audio Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Traffic on This Trunk Secure* Route Class Signaling Enabled*	Related Links: Back To Find/List	and
Trunk Configuration Save Delete Delete Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 for Calling Party Name Transmit UTF-8 hames in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Traffic on This Trunk Secure* Route Class Signaling Enabled* Use Trusted Relay Point*	Related Links: Back To Find/List needs to be configured in the network to provide end to end security. Failure to do so will expose keys When using both sRTP and TLS Default	and
Trunk Configuration Save Delete Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Traffic on This Trunk Secure* Route Class Signaling Enabled* Use Trusted Relay Point*	Related Links: Back To Find/List needs to be configured in the network to provide end to end security. Failure to do so will expose keys When using both sRTP and TLS Pefault V	and
Trunk Configuration Save Delete Path Replacement Support Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Traffic on This Trunk Secure* Route Class Signaling Enabled* Use Trusted Relay Point*	Related Links: Back To Find/List needs to be configured in the network to provide end to end security. Failure to do so will expose keys When using both sRTP and TLS v Default v	and
Trunk Configuration Save Delete Delete Path Replacement Support Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Traffic on This Trunk Secure* Route Class Signaling Enabled* Use Trusted Relay Point* PSTN Access Run On All Active Unified CM Nodes	Related Links: Back To Find/List needs to be configured in the network to provide end to end security. Failure to do so will expose keys When using both sRTP and TLS v Default v	and
Trunk Configuration Save Delete Delete Path Replacement Support Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Traffic on This Trunk Secure* Route Class Signaling Enable4* Use Trusted Relay Point* PSTN Access Intercompany Media Engine (IME) E 164 Transformation Profile	Related Links: Back To Find/List needs to be configured in the network to provide end to end security. Failure to do so will expose keys When using both sRTP and TLS Default Default	and
Trunk Configuration Save Delete Delete Path Replacement Support Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Traffic on This Trunk Secure* Route Class Signaling Enabled* Use Trusted Relay Point* PSTN Access Run On All Active Unified CM Nodes	Related Links: Back To Find/List	and
Trunk Configuration Save Delete Delete Path Replacement Support Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Traffic on This Trunk Secure* Route Class Signaling Enable4* Use Trusted Relay Point* PSTN Access Intercompany Media Engine (IME) E.164 Transformation Profile < None > Multilevel Precedence and Preemption (MLPP) Information	Related Links: Back To Find/List	and
Trunk Configuration Save Delete Delete Path Replacement Support Add New Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Traffic on This Trunk Secure* Route Class Signaling Enable4* Use Trusted Relay Point* PSTN Access Run On All Active Unified CM Nodes Intercompany Media Engine (IME) E.164 Transformation Profile < None > Multilevel Precedence and Preemption (MLPP) Information MLPP Domain < None >	Related Links: Back To Find/List	and
Trunk Configuration Save Delete Delete Path Replacement Support Add New Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Traffic on This Trunk Secure* Route Class Signaling Enable* Use Trusted Relay Point*	Related Links: Back To Find/List	and
Trunk Configuration Save Delete Delete Path Replacement Support Path Replacement Support Transmit UTF-8 for Calling Party Name Transmit UTF-8 for Calling Party Name Transmit UTF-8 Names in QSIG APDU Unattended Port SRTP Allowed - When this flag is checked, Encrypted TLS other information. Consider Traffic on This Trunk Secure* Route Class Signaling Enable4* Use Trusted Relay Point* PSTN Access Run On All Active Unified CM Nodes Intercompany Media Engine (IME) E.164 Transformation Profile < None > Multilevel Precedence and Preemption (MLPP) Information MLPP Domain < None > Call Routing Information // Remote-Party-Id	Related Links: Back To Find/List	and E
Trunk Configuration	Related Links: Back To Find/List	and



Image: Series in the series of t
Call Routing Information Remote-Party:Id Remote-Party:Id Remote-Party:Id Remote-Party:Id Remote-Party:Id Remote-Party:Id Remote-Party:Id Remote-Party:Id Parseted-Type* Default Significant Digits* Connected Inse Presentation* Default Calling Search Space K to administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Othervise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned. Incoming Calling Party Settings Number Type Prefix Default Connected Party Transformation CSS
Remote-Party-Id Arsented-Identity Arsented-Identity Arsented-Identity Arsented-Identity Default Calling Search Space Knone > AR Calling Search Space Knone > Knone > Calling Search Space Knone > Called Party Transformation CSS Knone > Called Party Transformation CSS Knone > Called Party Transformation CSS
Asserted-identity Arsserted-identity Arsserted-identity Arsserted-identity Arsserted-identity Sip Privacy* Default Ibound Calls Connected Into ID Presentation* Default Connected Name Presentation* Default Redirecting Diversion Header Delivery - Inbound Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix a stigned. Iclear Prefix Dit Caller Prefix Settings Incoming Number Default Incoming Number Default Incoming Number Default Connected Party Transformation CSS Outbound Calls Connected Party Transformation CSS Connected Party Transformation CSS
Asserted Type* Default SIP Privay* Default SIP Privay* Default Significant Digits* Connected Line 1D Presentation* Default Connected Line 1D Presentation* Default Connected Name Presentation* Default Connected Name Presentation* Default Connected Name Presentation* Default Connected Pains Space ARR Calling Search Space ARR Calling Search Space ARR Calling Search Space ARR Calling Party Settings If the advince the prefix to Default this indicates call processing uill use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix to Default this indicates call processing uill use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, Lear Prefix Settings If the advince Type Prefix Settings Lincoming Number Default Connected Party Settings Connected Party Transformation CSS Context Party Transformation CSS Context Party Transformation CSS V use Device Pool Called Party Transformation CSS
SIP Privacy* Default Incoming Calling Search Space AR Calling Search Space AR Calling Search Space AR Calling Search Space Cear Prefix Contexted Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, Cear Prefix Contexted Party Settings Incoming Number Prefix Contexted Party Settings Contexted Party Settings Connected Party Transformation CSS < kone > Contexted Party Transforma
Inbound Calls Significant Digits* All Connected Name Dresentation* Default Calling Search Space < None > Calling Search Space < None > Prefix DN Redireding Diversion Header Delivery - Inbound Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is amply in which care there is no prefix astigned. Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is amply in which care there is no prefix astigned. Incoming Number Default Clear Prefix Statip Digit Number Type Prefix Statip Digit Calling Search Space Use Device Peol CSS Number Type Prefix Statip Digit Calling Search Space Icent Peol Statip Strest Default Called Party Transformation CSS None > Icent Peol Called Party Transformation CSS Outbo
Significant Digits* All Connected Line ID Presentation* Default Connected Name Presentation* Default Connected Name Presentation* Default Calling Search Space AR Calling Search Space AR Calling Search Space None > Prefix DN Redurecting Diversion Header Delivery - Inbound Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned. Incoming Calling Party Settings Number Type Prefix Strip Digits Calling Search Space Use Device Pool/Service Pool CSS Incoming Number Default Connected Party Transformation CSS Connected Party Transformation CSS Connected Party Transformation CSS Contourd Calls Called Party Transformation CSS Connected Party Transformation CSS Contourd Called Party Transformation CSS Connected Par
Connected Line ID Presentation* Default Connected Name Presentation* Default Calling Search Space < None > Calling Search Space < None > Prefix DN Redirecting Diversion Header Delivery - Inbound Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned. Incoming Calling Party Settings Incoming Number Type Default Prefix Connected Party Settings Connected Party Settings Connected Party Settings Connected Party Settings Connected Party Transformation CSS Connected Party Transformation CSS Vubbound Calls Called Party Transformation CSS Vub Device Pool Called Party Transformation CSS
Connected Name Presentation* Default Calling Search Space < None > AAR Calling Search Space < None > Prefix DN Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, Incoming Calling Party Settings Incoming Rumber Type Prefix Strip Digits Calling Search Space Very Perfix Strip Digits Connected Party Settings Connected Party Settings Connected Party Settings Connected Party Transformation CSS Outbound Calls Called Party Transformation CSS Vue Device Pool Called Party Transformation CSS
Calling Search Space < None > ARR Calling Search Space < None > Prefix DN Redirecting Diversion Header Delivery - Inbound Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned. Liear Prefix Settings Default Clear Prefix Settings Default Incoming Number Default O Save Delete Presix Connected Party Settings Connected Party Settings Connected Party Transformation CSS Outbound Calls Called Party Transformation CSS < None > Vuse Device Pool Called Party Transformation CSS
AAR Calling Search Space Prefix DN Redirecting Diversion Header Delivery - Inbound Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned. Clear Prefix Settings Default Prefix Settings Incoming Number Default O Related Links: Back To Find/List Go Save the Reset the Add New Connected Party Settings Connected Party Transformation CSS Number CSS Outbound Calls Called Party Transformation CSS None >
Prefix DN ■ Redirecting Diversion Header Delivery - Inbound Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned. Clear Prefix Settings Number Type Prefix Stip Digits Calling Search Space Use Device Pool CSS Incoming Number Default Incoming Number Image: Connected Party Settings Connected Party Settings Connected Party Transformation CSS None > Image: Connected Party Transformation CSS Outbound Calls Culled Party Transformation CSS None > Image: Connected Party Transformation CSS
Redirecting Diversion Header Delivery - Inbound Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned. It was a state prefix unless the field is empty in which case there is no prefix assigned. Incoming Number Type Prefix State Type Prefix Stave Connected Party Transformation CSS < None > Connected Party Transformation CSS < None > Outbound Calls Colled Party Transformation CSS < None > Called Party Transformation CSS < None > W use Device Pool Called Party Transformation CSS
Incoming Calling Party Settings If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned. Clear Prefix Settings Default Prefix Settings Number Type Prefix Strip Digits Calling Search Space Use Device Pool CSS Incoming Number Default None > Incoming Party Settings Connected Party Settings Connected Party Settings Connected Party Transformation CSS None > Suve Service Pool Connected Party Transformation CSS Colled Party Transformation CSS None > Suve Service Pool Called Party Transformation CSS Value Device Pool Cal
If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned. Clear Prefix Settings Default Prefix Settings Number Type Prefix Strip Digits Calling Search Space Use Device Pool CSS Incoming Number Default < None > runk Configuration Related Links: Back To Find/List Go Save Connected Party Settings Connected Party Settings Connected Party Transformation CSS < None > Vuse Device Pool Connected Party Transformation CSS Dutbound Calls Called Party Transformation CSS < None > W Use Device Pool Called Party Transformation CSS
The additing address the prefix one prefix as the prefix as the field is empty in which case there is no prefix assigned. Clear Prefix Settings Default Prefix Settings Number Type Prefix Strip Digits Calling Search Space Use Device Pool CSS Incoming Number Default Oefault Related Links: Back To Find/List Go Save Connected Party Settings Connected Party Transformation CSS Outbound Calls Called Party Transformation CSS < None > Vuse Device Pool Called Party Transformation CSS
Clear Prefix Settings Number Type Prefix Strip Digits Calling Search Space Use Device Pool CSS Incoming Number Default 0 < None > Image: Connected Links: Back To Find/List Go Save Connected Party Settings Connected Party Transformation CSS < None > Use Device Pool Connected Party Transformation CSS
Number Type Prefix Strip Digits Calling Search Space Use Device Pool CSS Incoming Number Default Image: Constant Space Image: Constant Space Image: Constant Space Save Connected Party Settings Connected Party Transformation CSS < None > Image: Connected Party Transformation CSS Outbound Calls Called Party Transformation CSS < None > Image: Connected Party Transformation CSS Image: Connected Party Transformation CSS
Incoming Number Default Compared And New Connected Party Settings Connected Party Transformation CSS < None > Connected Party Transformation CSS Outbound Calls Called Party Transformation CSS < None > Called Party Transformation CSS <
runk Configuration Related Links: Back To Find/List Go Save Delete Reset Add New Connected Party Settings Connected Party Transformation CSS < None > Vuse Device Pool Connected Party Transformation CSS Outbound Calls Called Party Transformation CSS < None > W Use Device Pool Connected Party Transformation CSS
Prince Related Links: Back To Find/List Go Save Delete Reset Add New Connected Party Settings Connected Party Transformation CSS < None > Vuse Device Pool Connected Party Transformation CSS Outbound Calls Called Party Transformation CSS < None > W Use Device Pool Connected Party Transformation CSS
Connected Party Settings Connected Party Transformation CSS < None > Image: Connected Party Transformation CSS < None > Outbound Calls Colled Party Transformation CSS < None > Image: Connected Party Transformation CSS Outbound Calls Image: Connected Party Transformation CSS Image: Connected Party Transformation CSS Image: Connected Party Transformation CSS Image: Connected Party Transformation CSS Image: Connected Party Transformation CSS Image: Connected Party Transformation CSS Image: Connected Party Transformation CSS Image: Connected Party Transformation CSS
Save X Delete Yest Add New Connected Party Settings Connected Party Transformation CSS < None > ✓ Use Device Pool Connected Party Transformation CSS Outbound Calls Called Party Transformation CSS < None > ✓ Use Device Pool Called Party Transformation CSS
Save X Delete Y Reset Add New Connected Party Settings Connected Party Transformation CSS < None > ✓ Use Device Pool Connected Party Transformation CSS Dutbound Calls
Connected Party Settings Connected Party Transformation CSS < None > Use Device Pool Connected Party Transformation CSS Dutbound Calls Called Party Transformation CSS < None > W Use Device Pool Called Party Transformation CSS
Connected Party Transformation CSS < None > Vuse Device Pool Connected Party Transformation CSS Dutbound Calls Called Party Transformation CSS < None > V Use Device Pool Called Party Transformation CSS
Use Device Pool Connected Party Transformation CSS Outbound Calls Called Party Transformation CSS < None > Image: Use Device Pool Called Party Transformation CSS
Outbound Calls Called Party Transformation CSS < None > Image: Called Party Transformation CSS
Called Party Transformation CSS < None > V Use Device Pool Called Party Transformation CSS
Called Party Transformation CSS < None > V Use Device Pool Called Party Transformation CSS
Use Device Pool Called Party Transformation CSS
El ose bevice Poli called Party Halistofiniation cos
Calling Party Transformation CSS < None >
Colling Party Selection* Originator
Calling Line ID Presentation Default
Calling Name Presentation Default
Caller ID DN
Caller Name



Trunk Configuration	Related Links: Back To Find/List 🛛 🗸 Go
🔚 Save 🗶 Delete 💁 Reset 🕂 Add New	
SIP Information	· · · · · · · · · · · · · · · · · · ·
r Destination	
Destination Address is an SBV	
Destination Address Destination Address IPv6 Destination Port	
1* 192.168.1.90 5068	
MTP Preferred Originating Codec* 711ulaw	
Presence Group * Standard Presence group +	
SIP Trunk Security Profile* Non Secure SIP Trunk Profile 🗸	
Rerouting Calling Search Space < None >	
Out-Of-Dialog Refer Calling Search Space < None >	
SUBSCRIBE Calling Search Space < None >	
SIP Profile * SIP Profile for PRACK	
DTMF Signaling Method* No Preference -	
Normalization Script	
Normalization Script < None > +	
Enable Trace	
Parameter Name Parameter Value	
	E
Geolocation Configuration	
Geolocation < None >	
Geolocation Filter < None >	
Send Geolocation Information	-



Configuring the Route Pattern

1. To go to the Route pattern page, click on Call Routing and select Route Pattern from the Route/Hunt drop down menu.

System 💌	Call Routing K Media Resources	• A	dvanced Features + Device +	▼ Application ▼ User Management ▼ Bulk Administration ▼ Help ▼
Find and	AAR Group			
Add N	Dial Rules	• [
	Route Filter			
[Status -	Route/Hunt K	•	Route Group	
(i) 0 re-	SIP Route Pattern		Route List	
	Intercom	• 🛙	Route Pattern	N
SIP Rou	Class of Control	• T		Rows per Page 50
Find SIP I	Client Matter Codes	- 11	Line Group	Find Clear Filter 🔶 👄
	Forced Authorization Codes	- 11	Hunt List	ir your search criteria using the options above.
C	Translation Pattern	- 11	Hunt Pilot	
Add Ne	Call Park	T		
	Directed Call Park	- 1		
	Call Pickup Group	- 1		
	Directory Number	- 1		
	Meet-Me Number/Pattern	- 1		
	Dial Plan Installer	- 1		
	Route Plan Report	- 1		
	Transformation	·		
	Mobility	·		
	Logical Dedition Dation			

2. In our setup, users dial 8 to dial out. Add a route pattern with the following settings and associate it with the trunk configured in the previous step.

Save Delete Copy Add New Pattern Definition Route Pattern* Route Pattern Route Pattern* Route Filter Callers* Default Route Class* Default Gateway/Route List* ECB Route Option Block this pattern Block this pattern Block this pattern Block this pattern Call Classification* OffNet Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Use Calling Party's External Phone Number Mask Calling Party's External Phone Number Mask Prefix Digits (Outgoing Calls)	t 🚽 Go	Related Links: Back To Find/List 👻		e Pattern Configuration	Route
Pattern Definition Route Pattern* Route Pattern* Route Pattern* Numbering Plan* NANP Numbering Plan* NANP Route Filter < None > Route Filter < None > Persource Priority Namespace Network Domain None > Route Class* Default Gateway/Route List* Coll Classification* OffNet Block this pattern No Error Call Classification* OffNet Allow Device Override V Provide Outside Dial Tone Allow Device Coverride V Provide Outside Dial Tone Allow Device Override V Provide Outside Dial Tone <td< th=""><th></th><th></th><th>NI</th><th>Save 🗙 Delete 📄 Copy 👍 Add New</th><th>🔒 s.</th></td<>			NI	Save 🗙 Delete 📄 Copy 👍 Add New	🔒 s.
Route Pattern* 8.@ Route Partition < None > Description Koute to SP Numbering Plan* NNP Route Fliter < None > MLPP Precedence* Default Route Class* Default Route Class* Default Gateway/Route List* ECB Route Option @ Route this pattern Block this pattern No Error Call Classification* OffNet Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority Require Forced Authorization Code Authorization Level* 0 Calling Party Transformations Sub Colling Party's External Phone Number Mask Calling Party Transform Mask Prefix Digits (Outgoing Calls)				em Definition	_ Patte
Route Partition < None > Description Route to SP Numbering Plan* NANP Route Filter < None > MLPP Precedence* Default Route Class* Default Route Option © Route this pattern Block this pattern No Error Call Classification* OffNet Allow Device Override Provide Outside Dial Tone Allow Device Override Provide Outside Dial Tone Allow Device Coverride Orovide Outside Dial Tone Allow Tevere Class Hatter Code Calling Party Transform Mask Calling Party Transform Mask Prefix Digits (Outgoing Calls)			8.@	te Pattern*	Route
Description Route to SP Numbering Plan* NANP Route Filter < None > Route Class* Oefault Route Class* Default Gateway/Route List* ECB Route Option © Route this pattern Block this pattern © Block this pattern Call Classification* OffNet Allow Device Override Provide Outside Dial Tone Authorization Level* 0 Calling Party Transform Mask Calling Party Transform Mask Prefix Digits (Outgoing Calls)			< None >	te Partition	Route
Numbering Plan* NANP Route Filter < None > MLPP Precedence* Default Resource Priority Namespace Network Domain < None > Route Class* Default Gateway/Route List* ECB Route Option ® Route this pattern Block this pattern Block this pattern No Error Call Classification* OffNet Allow Device Override Provide Outside Dial Tone Authorization Level* 0 0 Outside Dial Tone Use Calling Party Transform Mask Calling Party Transform Mask Prefix Digits (Outgoing Calls)			Route to SP	cription	Descr
Route Filter < None > MLPP Precedence* Default Resource Priority Namespace Network Domain < None > Route Class* Default Gateway/Route List* ECB Route Option ® Route this pattern Block this pattern Block this pattern Call Classification* OffNet Allow Device Override Provide Outside Dial Tone Allow Device Override Provide Outside Dial Tone Allow Device Override Provide Outside Dial Tone Allow Device Override 0 Calling Party Transformations			NANP	bering Plan*	Numb
MLPP Precedence* Default Resource Priority Namespace Network Domain < None > Route Class* Default Callessification* OffNet Block this pattern Block this patter			< None >	te Filter	Route
Resource Priority Namespace Network Domain < None > Route Class* Default Gateway/Route List* ECB Route Option © Route this pattern © Block this pattern © Block this pattern © Block this pattern No Error Call Classification* OffNet @ Allow Device Override Provide Outside Dial Tone Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority Require Forced Authorization Code Authorization Level* 0 Require Client Matter Code Calling Party Transform Mask Prefix Digits (Outgoing Calls)			Default 🗸	P Precedence*	MLPP
Route Class* Gateway/Route List* ECB Route Option Image: Require Forced Authorization Code Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority Require Forced Authorization Code Authorization Level* Image: Require Client Matter Code Calling Party Transform Mask Prefix Digits (Outgoing Calls)			None >	ource Priority Namespace Network Domain	Reso
Gateway/Route List* ECB (Edit) Route Option			Default 👻	te Class*	Route
Route Option Route this pattern Block this pattern No Error Call Classification* OffNet Provide Outside Dial Tone Allow Override OffNet Outside Outside Dial Tone Outside Outside Dial Tone Outside Outside Dial Tone <td></td> <td>(Edit)</td> <td>ECB 🗸</td> <td>eway/Route List*</td> <td>Gatev</td>		(Edit)	ECB 🗸	eway/Route List*	Gatev
Block this pattern No Error Call Classification* OffNet Glock this pattern No Error Call Classification* OffNet Glock duthorization Code Authorization Level* O Require Client Matter Code Calling Party Transformations Gling Party Transform Mask Prefix Digits (Outgoing Calls)			Route this pattern	te Option	Route
Call Classification* OffNet Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority Require Forced Authorization Code Authorization Level* Require Client Matter Code Calling Party Transformations Use Calling Party's External Phone Number Mask Calling Party Transform Mask Prefix Digits (Outgoing Calls)		-	Block this pattern No Error		
Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority Require Forced Authorization Code Authorization Level* Require Client Matter Code Calling Party Transformations Calling Party Transform Mask Calling Party Transform Mask Prefix Digits (Outgoing Calls)			▼	Classification* OffNet	Call C
			Dial Tope Allow Overlap Sending Urgent Priori		E Al
Authorization Level*				aquire Forced Authorization Code	
				orization Level*	Autho
Calling Party Transformations Use Calling Party's External Phone Number Mask Calling Party Transform Mask Prefix Digits (Outgoing Calls)					
Calling Party Transformations Use Calling Party's External Phone Number Mask Calling Party Transform Mask Prefix Digits (Outgoing Calls)				Require Client Matter Code	
Use Calling Party's External Phone Number Mask Calling Party Transform Mask Prefix Digits (Outgoing Calls)				ng Party Transformations	Callin
Calling Party Transform Mask Prefix Digits (Outgoing Calls)			er Mask	Jse Calling Party's External Phone Number	🔲 U:
Prefix Digits (Outgoing Calls)				ing Party Transform Mask	Callin
				ix Digits (Outgoing Calls)	Prefix
Calling Line ID Presentation* Default				ing Line ID Presentation* Default	Callin



Save Delete Colling Line ID Presentation Default Calling Party Number Type Cisco CallManager Calling Party Numbering Plan* Cisco CallManager Connected Party Transformations Connected Name Presentation* Default Called Party Transformations Default Called Party Transformations Default Called Party Transformations	
Prenx Digits (outgoing Cails) Calling Line ID Presentation* Default Calling Name Presentation* Default Calling Party Number Type* Cisco CallManager Calling Party Numbering Plan* Cisco CallManager Connected Party Transformations Connected Line ID Presentation* Default Connected Name Presentation* Default Called Party Transformations Connected Name Presentation* Default Called Party Transformations Discard Digits PreDot Called Party Transform Mask Prefix Digits (Outgoing Calls)	
Calling Line ID Presentation* Default Calling Name Presentation* Default Calling Party Number Type* Cisco CallManager Calling Party Numbering Plan* Cisco CallManager Connected Party Transformations Connected Line ID Presentation* Default Connected Name Presentation* Default Connected Name Presentation* Default Connected Name Presentation Discard Digits Called Party Transformations Discard Digits Called Party Transform Mask Prefix Digits (Outgoing Calls)	
Calling Name Presentation* Default Calling Party Number Type* Cisco CallManager Calling Party Numbering Plan* Cisco CallManager Connected Party Transformations Connected Line ID Presentation* Default Connected Name Presentation* Default Connected Name Presentation Discard Digits PreDot Called Party Transform Mask Prefix Digits (Outgoing Calls)	
Calling Party Number Type* Cisco CallManager Calling Party Numbering Plan* Cisco CallManager Connected Party Transformations Connected Line ID Presentation* Default Connected Name Presentation* Default Connected Name Presentation* Discard Digits PreDot Called Party Transform Mask Prefix Digits (Outgoing Calls)	
Calling Party Numbering Plan* Cisco CallManager	
Connected Party Transformations Connected Line ID Presentation Default Connected Name Presentation Default Called Party Transformations Discard Digits PreDot Called Party Transform Mask Prefix Digits (Outgoing Calls)	
Connected Line ID Presentation* Default Connected Name Presentation* Default Called Party Transformations Discard Digits PreDot Called Party Transform Mask Prefix Digits (Outgoing Calls)	_
Connected Name Presentation* Default Called Party Transformations Discard Digits PreDot Called Party Transform Mask Prefix Digits (Outgoing Calls)	
Called Party Transformations Discard Digits Called Party Transform Mask Prefix Digits (Outgoing Calls)	
Discard Digits PreDot Called Party Transform Mask Prefix Digits (Outgoing Calls)	
Called Party Transform Mask Prefix Digits (Outgoing Calls)	
Prefix Digits (Outgoing Calls)	
Called Party Number Type" Cisco CallManager 🚽	
Called Party Numbering Plan* Cisco CallManager 🗸	
r ISDN Network-Specific Facilities Information Element	
Network Service Protocol Not Selected	=
Carrier Identification Code	
Network Service Service Parameter Name Service Parameter Value	
Not Selected	
- Save Delete Copy Add New	

The CUCM configuration is now complete.



Phase 5 – Configuring the Oracle Enterprise Session Border Controller

In this section we describe the steps for configuring an Oracle Enterprise Session Border Controller (E-SBC), formally known as an Acme Packet Net-Net Enterprise Session Director (E-SBC), for use with the Oracle Enterprise Communications Broker in a SIP trunking scenario.

In Scope

The following step-by-step guide configuring the E-SBC assumes that this is a newly deployed device dedicated to a single customer. If the enterprise currently has the E-SBC deployed and is adding ECB, then please see the appendix for a better understanding of the Acme Packet Command Line Interface (ACLI).

Note that Oracle offers several models of E-SBC. This document covers the setup for the Acme Packet 3820 and Acme Packet 4500 platform series running Net-Net OS ECX 6.2.0 or later. If instructions are needed for other E-SBC models, please contact your Oracle representative.

Out of Scope

- Configuration of Network management including SNMP and RADIUS; and
- Redundancy configuration

What will you need

- Serial Console cross over cable with RJ-45 connector
- Terminal emulation application such as PuTTY or HyperTerm
- Passwords for the User and Superuser modes on the E-SBC
- IP address to be assigned to management interface (Wancom0) of the E-SBC the Wancom0 management interface must be connected and configured to a management network separate from the service interfaces. Otherwise the E-SBC is subject to ARP overlap issues, loss of system access when the network is down, and compromising DDoS protection. Oracle does not support E-SBC configurations with management and media/service interfaces on the same subnet.
- IP address of the ECB
- IP address to be used for the E-SBC internal and external facing ports (Service Interfaces)
- IP address of the next hop gateway in the SIP trunk provider network



Configuring the Oracle Enterprise Session Border Controller (E-SBC)

Once the 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 outside (gateway facing) network and the slot 0 port 1 (s1p0) interface into your inside (mediation server-facing) network. Once connected, perform 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 **ORACLE-SBC** are parameters which are specific to an individual deployment. **Note:** The ACLI is case sensitive.

Establish the serial connection and logging in the SBC

Confirm the E-SBC is powered off and connect one end of a straight-through Ethernet cable to the front console port (which is active by default) on the E-SBC and the other end to console adapter that ships with the E-SBC, connect the console adapter (a DB-9 adapter) to the DB-9 port on 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

Power on the E-SBC and confirm that you see the following output from the bootup sequence.





Enter the following commands to login to the E-SBC and move to the configuration mode. Note that the default E-SBC password is "acme" and the default super user password is "packet".



You are now in the global configuration mode.

Initial Configuration – Assigning the management Interface an IP address

To assign an IP address, one has to configure the bootparams on the E-SBC by going to

Oracle-SBC# 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

```
Oracle-SBC#(configure)bootparam

'.' = clear field; '-' = go to previous field; q = quit

boot device : eth0

processor number : 0

host name : acmesystem

file name : /code/images/nnECX640m2.tar--- >location where

the software is loaded on the SBC

inet on ethernet (e) : 172.18.255.52:ffffff80 --- > 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) : ORACLE-SBC
startup script (s) :
other (o) :
```

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.

```
ORACLE-SBC(configure)# system
ORACLE-SBC(system)# system-config
ORACLE-SBC(system-config)# hostname ORACLE-SBC
ORACLE-SBC(system-config)# description "SBC for SIP Trunking"
ORACLE-SBC(system-config)# location "Bedford, MA"
ORACLE-SBC(system-config)# default-gateway 172.18.0.1
ORACLE-SBC(system-config)# done
```

Once the **system-config** settings have completed and you enter **done**, the E-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.

config	
hostname	
description	SBC for SIP Trunking
location	Bedford, MA
mib-system-contact	
mib-system-name	
mib-system-location	
snmp-enabled	enabled
enable-snmp-auth-traps	disabled
enable-snmp-syslog-notify	disabled
enable-snmp-monitor-traps	disabled
enable-env-monitor-traps	disabled
<pre>snmp-syslog-his-table-length</pre>	1
snmp-syslog-level	WARNING
system-log-level	WARNING
	<pre>config hostname description location mib-system-contact mib-system-name mib-system-location snmp-enabled enable-snmp-auth-traps enable-snmp-syslog-notify enable-snmp-monitor-traps enable-env-monitor-traps snmp-syslog-his-table-length snmp-syslog-level system-log-level</pre>



process-log-level	DEBUG
process-log-ip-address	0.0.0
process-log-port	0
collect	
sample-interval	5
push-interval	15
boot-state	disabled
start-time	now
end-time	never
red-collect-state	disabled
red-max-trans	1000
red-sync-start-time	5000
red-sync-comp-time	1000
push-success-trap-state	e disabled
call-trace	disabled
internal-trace	disabled
log-filter	all
default-gateway	172.18.0.1
restart	enabled
exceptions	
telnet-timeout	0
console-timeout	0
remote-control	enabled
cli-audit-trail	enabled
link-redundancy-state	disabled
source-routing	disabled
cli-more	disabled
terminal-height	24
debug-timeout	0
trap-event-lifetime	0
default-v6-gateway	::
ipv6-signaling-mtu	1500
ipv4-signaling-mtu	1500
cleanup-time-of-day	00:00
snmp-engine-id-suffix	
snmp-agent-mode	v1v2
comm-monitor	
state	disabled
qos-enable	enabled
sbc-grp-id	0
tls-profile	



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 outside (connection to the trunk) interface.

```
ORACLE-SBC(system-config) # exit
ORACLE-SBC(system) # phy-interface
ORACLE-SBC(phy-interface) # name M00
ORACLE-SBC(phy-interface) # operation-type media
ORACLE-SBC(phy-interface) # slot 0
ORACLE-SBC(phy-interface) # port 0
ORACLE-SBC(phy-interface) # done
```

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

phy-in	terface	
	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 inside (connection to the ECB) interface.

```
ORACLE-SBC (phy-interface) # name M10

ORACLE-SBC (phy-interface) # operation-type media

ORACLE-SBC (phy-interface) # slot 1

ORACLE-SBC (phy-interface) # port 0

ORACLE-SBC (phy-interface) # done

phy-interface

name M10

operation-type Media

port 0
```

	Contraction of the local distance of the loc	A second se Second second sec second second sec	1000

slot	1
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
overload-protection	disabled

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

```
ORACLE-SBC (phy-interface) # exit
ORACLE-SBC(system) # network-interface
ORACLE-SBC(network-interface) # name s1p0
ORACLE-SBC(network-interface) # description "ECB-facing inside interface"
ORACLE-SBC(network-interface) # ip-address 192.168.1.130
ORACLE-SBC(network-interface) # netmask 255.255.255.0
ORACLE-SBC(network-interface)# gateway 192.168.1.1
ORACLE-SBC(network-interface) # pri-utility-addr 192.168.1.131
ORACLE-SBC(network-interface) # sec-utility-addr 192.168.1.132
ORACLE-SBC(network-interface) # add-hip-ip 192.168.1.130
ORACLE-SBC(network-interface)# add-icmp-ip 192.168.1.130
ORACLE-SBC (network-interface) # done
network-interface
                                       s1p0
       name
                                       0
        sub-port-id
                                       ECB-facing inside interface
        description
        hostname
                                      192.168.1.130
        ip-address
        pri-utility-addr
                                      192.168.1.131
        sec-utility-addr
                                      192.168.1.132
                                       255.255.255.0
        netmask
        gateway
                                       192.168.1.1
        sec-gateway
        gw-heartbeat
                                               disabled
                state
                                               0
                heartbeat
```



retry-count	0	
retry-timeout	1	
health-score	0	
dns-ip-primary		
dns-ip-backup1		
dns-ip-backup2		
dns-domain		
dns-timeout	11	
hip-ip-list	192.168.1.130	
ftp-address		
icmp-address	192.168.1.130	
snmp-address		
telnet-address		
ssh-address		

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

```
ORACLE-SBC(network-interface) # name s0p0
ORACLE-SBC(network-interface)# description "VoIP gateway-facing outside
interface"
ORACLE-SBC(network-interface) # ip-address 192.20.0.108
ORACLE-SBC(network-interface) # netmask 255.255.255.0
ORACLE-SBC(network-interface) # gateway 192.20.0.1
ORACLE-SBC(network-interface) # pri-utility-addr 192.20.0.109
ORACLE-SBC(network-interface) # sec-utility-addr 192.20.0.110
ORACLE-SBC(network-interface) # dns-ip-primary 8.8.8.8
ORACLE-SBC(network-interface) # dns-ip-backup1 8.8.4.4
ORACLE-SBC(network-interface) # dns-domain tsengr.com
ORACLE-SBC(network-interface) # add-hip-ip 192.20.0.108
ORACLE-SBC(network-interface) # add-icmp-ip 192.20.0.108
ORACLE-SBC (network-interface) # done
network-interface
                                        s0p0
         name
        sub-port-id
                                        0
        description
                                        VoIP gateway-facing outside
interface
        hostname
        ip-address
                                       192.20.0.108
                                       192.20.0.109
        pri-utility-addr
        sec-utility-addr
                                      192.20.0.110
                                       255.255.255.0
        netmask
                                       192.20.0.1
        gateway
```



sec-gateway	
gw-heartbeat	
state	disabled
heartbeat	0
retry-count	0
retry-timeout	1
health-score	0
dns-ip-primary	8.8.8
dns-ip-backup1	8.8.4.4
dns-ip-backup2	
dns-domain	tsengr.com
dns-timeout	11
hip-ip-list	192.20.0.108
ftp-address	
icmp-address	192.20.0.108
snmp-address	
telnet-address	
ssh-address	

You will now configure the wancom1 and wancom2 for redundancy, specifying the appropriate values.

```
ORACLE-SBC(network-interface) # name wancom1
ORACLE-SBC(network-interface)# netmask 255.255.255.252
ORACLE-SBC(network-interface) # pri-utility-addr 169.254.1.1
ORACLE-SBC(network-interface) # sec-utility-addr 169.254.1.2
ORACLE-SBC(network-interface) # done
network-interface
                                     wancoml
       name
       sub-port-id
                                     0
       description
       hostname
       ip-address
       pri-utility-addr 169.254.1.1
       sec-utility-addr
                                   169.254.1.2
                                   255.255.255.252
       netmask
       gateway
       sec-gateway
       gw-heartbeat
              state
                                             disabled
               heartbeat
                                             0
              retry-count
                                             0
```



retry-timeout	1	
health-score	0	
dns-ip-primary		
dns-ip-backup1		
dns-ip-backup2		
dns-domain		
dns-timeout	11	
hip-ip-list		
ftp-address		
icmp-address		
snmp-address		
telnet-address		
ssh-address		
ORACLE-SBC (network-interface) #	name wancom2	
ORACLE-SBC (network-interface) #	netmask 255.255.255.252	
ORACLE-SBC (network-interface) #	pri-utility-addr 169.254.2.1	
ORACLE-SBC (network-interface) #	sec-utility-addr 169.254.2.2	
ORACLE-SBC (network-interface) #	done	
network-interface		
name	wancom2	
sub-port-id	0	
description		
hostname		
ip-address		
pri-utility-addr	169.254.2.1	
sec-utility-addr	169.254.2.2	
netmask	255.255.255.252	
gateway		
sec-gateway		
gw-heartbeat		
state	disabled	
heartbeat	0	
retry-count	0	
retry-timeout	1	
health-score	0	
dns-ip-primary		
dns-ip-backup1		
dns-ip-backup2		
dns-domain		



dns-timeout	11
hip-ip-list	
ftp-address	
icmp-address	
snmp-address	
telnet-address	
ssh-address	

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.

ORACLE-S	ORACLE-SBC(network-interface) # exit			
ORACLE-SBC(system)# exit				
ORACLE-S	SBC(configure)# session-router			
ORACLE-S	SBC(session-router)# sip-config			
ORACLE-S	<pre>SBC(sip-config) # operation-mode</pre>	dialog		
ORACLE-S	SBC(sip-config)# done			
sip-con:	fig			
	state	enabled		
	operation-mode	dialog		
	dialog-transparency	enabled		
	home-realm-id			
	egress-realm-id			
	nat-mode	None		
	registrar-domain			
	registrar-host			
	registrar-port	0		
	register-service-route	always		
	init-timer	500		
	max-timer	4000		
	trans-expire	32		
	invite-expire	180		
	inactive-dynamic-conn	32		
	enforcement-profile			
	pac-method			
	pac-interval	10		
	pac-strategy	PropDist		
	pac-load-weight	1		



pac-session-weight	1
pac-route-weight	1
pac-callid-lifetime	600
pac-user-lifetime	3600
red-sip-port	1988
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
add-reason-header	disabled
sip-message-len	4096
enum-sag-match	disabled
extra-method-stats	disabled
rph-feature	disabled
nsep-user-sessions-rate	0
nsep-sa-sessions-rate	0
registration-cache-limit	0
register-use-to-for-lp	disabled
refer-src-routing	disabled
add-ucid-header	disabled
proxy-sub-events	
pass-gruu-contact	disabled
sag-lookup-on-redirect	disabled
set-disconnect-time-on-bye	disabled

Configure Global Media configuration

To configure the Media values, use the **media-manager** command under the media-manager branch. To enter the mediamanager 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 E-SBC with the default values.

ORACLE-SBC(sip-config)# exit		
ORACLE-SBC (session-router) # exit		
ORACLE-SBC(configure)# media-manager		
ORACLE-SBC(media-manager) # media-manager		
ORACLE-SBC (media-manager) # select		
ORACLE-SBC(media-manager-config) # done		
media-manager		
state enabled		
latching enabled		



flow-time-limit	86400
initial-guard-timer	300
subsq-guard-timer	300
tcp-flow-time-limit	86400
tcp-initial-guard-timer	300
tcp-subsq-guard-timer	300
tcp-number-of-ports-per-flow	2
hnt-rtcp	disabled
algd-log-level	NOTICE
mbcd-log-level	NOTICE
red-flow-port	1985
red-mgcp-port	1986
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
media-policing	enabled
max-signaling-bandwidth	1000000
max-untrusted-signaling	100
min-untrusted-signaling	30
app-signaling-bandwidth	0
tolerance-window	30
rtcp-rate-limit	0
trap-on-demote-to-deny	disabled
min-media-allocation	2000
min-trusted-allocation	4000
deny-allocation	64000
anonymous-sdp	disabled
arp-msg-bandwidth	32000
fragment-msg-bandwidth	0
rfc2833-timestamp	disabled
default-2833-duration	100
rfc2833-end-pkts-only-for-non-s	sig enabled
translate-non-rfc2833-event	disabled
media-supervision-traps	disabled
dnsalg-server-failover	disabled

Configure Realms

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 ECB- Peer, which represents the ECB-facing (inside) network; and
- The SIP-trunk, which represents the gateway-facing (outside) network.

```
ORACLE-SBC (media-manager-config) # exit
ORACLE-SBC (media-manager) # realm-config
ORACLE-SBC(realm-config) # identifier ECB-Peer
ORACLE-SBC (realm-config) # description "ECB-facing (Inside)"
ORACLE-SBC(realm-config)# network-interfaces s1p0:0
ORACLE-SBC(realm-config) # done
realm-config
       identifier
                                    ECB-Peer
       description
                                    ECB-facing(Inside)
                                     0.0.0.0
       addr-prefix
       network-interfaces
                                     s1p0:0
       mm-in-realm
                                    enabled
                                    enabled
       mm-in-network
       mm-same-ip
                                    enabled
                                   enabled
disabled
       mm-in-system
       bw-cac-non-mm
       msm-release
                                    disabled
       qos-enable
                                    disabled
       generate-UDP-checksum disabled
       max-bandwidth
                                     0
       fallback-bandwidth
                                    0
                                    0
       max-priority-bandwidth
       max-latency
                                    0
       max-jitter
                                    0
       max-packet-loss
                                     0
                                     0
       observ-window-size
       parent-realm
       dns-realm
       media-policy
       media-sec-policy
       in-translationid
       out-translationid
       in-manipulationid
       out-manipulationid
       manipulation-string
```



manipulation-pattern	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
cac-failure-threshold	0
untrust-cac-failure-threshold	0
ext-policy-svr	
diam-e2-address-realm	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
codec-manip-in-network	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled

1			
	/		

stun-server-ip	0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled

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

<pre>ORACLE-SBC(realm-config)# identifier S</pre>	IP-trunk				
ORACLE-SBC(realm-config) # description	"Gateway(Outside)"				
ORACLE-SBC(realm-config)# network-interfaces s0p0:0					
ORACLE-SBC(realm-config)# done					
realm-config					
identifier	SIP-trunk				
description	Gateway(Outside)				
addr-prefix	0.0.0				
network-interfaces					
	s0p0:0				
mm-in-realm	enabled				
mm-in-network	enabled				
mm-same-ip	enabled				
mm-in-system	enabled				
bw-cac-non-mm	disabled				
msm-release	disabled				
qos-enable	disabled				
generate-UDP-checksum	disabled				
max-bandwidth	0				
fallback-bandwidth	0				
max-priority-bandwidth	0				
max-latency	0				
max-jitter	0				
max-packet-loss	0				
observ-window-size	0				
parent-realm					
dns-realm					
media-policy					



media-sec-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
cac-failure-threshold	0
untrust-cac-failure-threshold	0
ext-policy-svr	
diam-e2-address-realm	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled

codec-manip-in-network	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled

Configure E-SBC redundancy configuration

To configure the E-SBC redundancy configuration, use the **redundancy-config** command under **system** element.

```
ORACLE-SBC (realm-config) # exit
ORACLE-SBC (media-manager) # exit
ORACLE-SBC (configure) # system
ORACLE-SBC(system) # redundancy
ORACLE-SBC(redundancy) # state enabled
ORACLE-SBC (redundancy) # peer
ORACLE-SBC(rdncy-peer) # name Oracle-SBC
ORACLE-SBC(rdncy-peer) # state enabled
ORACLE-SBC(rdncy-peer) # type Primary
ORACLE-SBC (rdncy-peer) # destination
ORACLE-SBC(rdncy-peer-dest)# address 169.254.1.1:9090
ORACLE-SBC(rdncy-peer-dest) # network-interface wancom1:0
ORACLE-SBC(rdncy-peer-dest) # done
destination
                                   169.254.1.1:9090
   address
    network-interface
                                   wancom1:0
ORACLE-SBC(rdncy-peer-dest)# address 169.254.2.1:9090
ORACLE-SBC(rdncy-peer-dest) # network-interface wancom2:0
ORACLE-SBC(rdncy-peer-dest) # done
destination
    address
                                   169.254.2.1:9090
    network-interface
                                   wancom2:0
```



ORACLE-SBC (rdncy-peer-dest) # exit ORACLE-SBC (rdncy-peer) # done peer Oracle-SBC name state enabled type Primary destination address 169.254.1.1:9090 network-interface wancom1:0 destination address 169.254.2.1:9090 wancom2:0 network-interface ORACLE-SBC(rdncy-peer) # name SN1Secondary ORACLE-SBC(rdncy-peer) # state enabled ORACLE-SBC(rdncy-peer) # type Secondary ORACLE-SBC(rdncy-peer) # destination ORACLE-SBC(rdncy-peer-dest) # address 169.254.1.2:9090 ORACLE-SBC(rdncy-peer-dest) # network-interface wancom1:0 ORACLE-SBC(rdncy-peer-dest) # done destination address 169.254.1.2:9090 network-interface wancom1:0 ORACLE-SBC(rdncy-peer-dest)# address 169.254.2.2:9090 ORACLE-SBC(rdncy-peer-dest) # network-interface wancom2:0 ORACLE-SBC(rdncy-peer-dest) # done destination 169.254.2.2:9090 address network-interface wancom2:0 ORACLE-SBC (rdncy-peer-dest) # exit ORACLE-SBC(rdncy-peer) # done peer SN1Secondary name enabled state type Secondary destination 169.254.1.2:9090 address network-interface wancom1:0 destination address 169.254.2.2:9090 network-interface wancom2:0 ORACLE-SBC(rdncy-peer) # exit



ORACLE-SBC (redundancy) # done						
redundancy-config						
st	tate		enabled			
lc	log-level		INFO			
he	ealth-threshold	l	75			
en	emergency-threshold		50			
pc	ort		9090			
ac	dvertisement-ti	.me	500			
pe	ercent-drift		210			
in	nitial-time		1250			
be	ecoming-standby	-time	180000			
be	ecoming-active-	time	100			
cf	fg-port		1987			
cf	fg-max-trans		10000			
cf	fg-sync-start-t	ime	5000			
cf	fg-sync-comp-ti	.me	1000			
ga	ateway-heartbea	at-interval	10			
ga	ateway-heartbea	t-retry	3			
ga	ateway-heartbea	t-timeout	1			
ga	ateway-heartbea	t-health	1			
m∈	media-if-peercheck-time		0			
pe	eer					
	name			SN1Secor	ndary	
	state			enabled		
	type		Secondary		су	
	destination					
		address			169.254.1.2:9090	
		network-interfa	.ce		wancom1:0	
	destinat	ion				
		address			169.254.2.2:9090	
	network-interfac		.ce		wancom2:0	
pe	eer					
	name			Oracle-S	SBC	
	state			enabled		
	type			Primary		
	destinat	ion				
		address			169.254.1.1:9090	
		network-interface			wancom1:0	
	destinat	destination				
		address			169.254.2.1:9090	
	network-interface			wancom2:0		



ORACLE-SBC (redundancy) # exit

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 E-SBC will listen for and transmit SIP messages. These will be the same IP addresses as configured on the associated network-interface elements.

```
ORACLE-SBC (realm-config) # exit
ORACLE-SBC (media-manager) # exit
ORACLE-SBC(configure) # session-router
ORACLE-SBC(session-router) # sip-interface
ORACLE-SBC(sip-interface) # realm SIP-trunk
ORACLE-SBC(sip-interface) # description "SIP Trunk-facing (Outside)"
ORACLE-SBC (sip-interface) # sip-ports
ORACLE-SBC(sip-port) # address 192.20.0.108
ORACLE-SBC(sip-port) # done
sip-port
address
                               192.20.0.108
port
                               5060
                              UDP
transport-protocol
tls-profile
allow-anonymous
                              all
ims-aka-profile
ORACLE-SBC(sip-port) # exit
ORACLE-SBC(sip-interface) # done
sip-interface
       state
                                       enabled
       realm-id
                                       SIP-trunk
        description
                                     SIP Trunk-facing (Outside)
        sip-port
                                               192.20.0.108
               address
                                               5060
               port
               transport-protocol
                                               UDP
               tls-profile
               allow-anonymous
                                               all
               ims-aka-profile
        carriers
```


trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
options	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
${\tt charging-function-address-mode}$	pass



ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	

You will now configure the ECB-facing SIP interface.

ORACLE-SBC(sip-interface) # realm-id ECB-Peer					
<pre>ORACLE-SBC(sip-interface)# description "ECB-Facing(Inside)"</pre>					
ORACLE-SBC(sip-interface) # sip	p-ports				
ORACLE-SBC(sip-port)# address	192.168.1.130				
ORACLE-SBC(sip-port) # transpor	rt-protocol TCP				
ORACLE-SBC(sip-port) # done					
sip-port					
address	192.168.1.130				
port	5060				
transport-protocol	TCP				
tls-profile					
allow-anonymous	all				
ims-aka-profile					
ORACLE-SBC(sip-port) # exit					
ORACLE-SBCORACLE-SBC(sip-inter	rface)# done				
sip-interface					
state	enabled				
realm-id	ECB-Peer				
description	ECB-Facing(Inside)				
sip-port					



address	192.168.1.130
port	5060
transport-protocol	TCP
tls-profile	
allow-anonymous	all
ims-aka-profile	
carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0



untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	

Configure Next-hop signaling configuration

To configure the next-hop signaling elements (i.e., the ECB and PSTN gateway) you define session-agents. Use the **session-agent** command under the session-router branch. To enter the session-router 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 E-SBC will send and from which it will expect to receive SIP messages for your next-hop signaling elements.

We will first configure the PSTN gateway.

```
ORACLE-SBCORACLE-SBC(sip-interface) # exit
ORACLE-SBC(session-router) # hostname 10.10.1.8
ORACLE-SBC(session-router) # ip-address 10.10.1.8
ORACLE-SBC(session-router) # port 5060
ORACLE-SBC(session-router) # realm-id SIP-trunk
ORACLE-SBC(session-router) # done
```



session-	agent	
	hostname	10.10.1.8
	ip-address	10.10.1.8
	port	5060
	state	enabled
	app-protocol	SIP
	app-type	
	transport-method	UDP
	realm-id	SIP-trunk
	egress-realm-id	
	description	
	carriers	
	allow-next-hop-lp	enabled
	constraints	disabled
	max-sessions	0
	max-inbound-sessions	0
	max-outbound-sessions	0
	max-burst-rate	0
	max-inbound-burst-rate	0
	max-outbound-burst-rate	0
	max-sustain-rate	0
	max-inbound-sustain-rate	0
	max-outbound-sustain-rate	0
	min-seizures	5
	min-asr	0
	time-to-resume	0
	ttr-no-response	0
	in-service-period	0
	burst-rate-window	0
	sustain-rate-window	0
	req-uri-carrier-mode	None
	proxy-mode	
	redirect-action	
	loose-routing	enabled
	send-media-session	enabled
	response-map	
	ping-method	
	ping-interval	0
	ping-send-mode	keep-alive
	ping-all-addresses	disabled
	ping-in-service-response-codes	



out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	

We will now configure the ECB as the second session agent.

ORACLE-SBC(session-router)# ip-address 192.168.1.90
ORACLE-SBC(session-router) # port 5060
ORACLE-SBC(session-router)
ORACLE-SBC(session-router) # transport-method <pre>StaticTCP</pre>
ORACLE-SBC(session-router)
<pre>Oracle-SBC(session-agent)# refer-call-transfer enabled</pre>
ORACLE-SBC(session-router)# done



session	-agent	
	hostname	
	ip-address	192.168.1.90
	port	5060
	state	enabled
	app-protocol	SIP
	app-type	
	transport-method	StaticTCP
	realm-id	ECB-Peer
	egress-realm-id	
	description	
	carriers	
	allow-next-hop-lp	enabled
	constraints	disabled
	max-sessions	0
	max-inbound-sessions	0
	max-outbound-sessions	0
	max-burst-rate	0
	max-inbound-burst-rate	0
	max-outbound-burst-rate	0
	max-sustain-rate	0
	max-inbound-sustain-rate	0
	max-outbound-sustain-rate	0
	min-seizures	5
	min-asr	0
	time-to-resume	0
	ttr-no-response	0
	in-service-period	0
	burst-rate-window	0
	sustain-rate-window	0
	req-uri-carrier-mode	None
	proxy-mode	
	redirect-action	
	loose-routing	enabled
	send-media-session	enabled
	response-map	
	ping-method	OPTIONS;hops=0
	ping-interval	30
	ping-send-mode	keep-alive
	ping-all-addresses	disabled



ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	enabled
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	

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 ECB.



ORACLE-SBC(session-agent) # exit ORACLE-SBC (session-router) # local-policy ORACLE-SBC(local-policy) # from-address * ORACLE-SBC(local-policy) # to-address * ORACLE-SBC(local-policy) # source-realm SIP-trunk ORACLE-SBC (local-policy) # policy-attributes ORACLE-SBC(local-policy-attributes)#next-hop 192.168.1.90 ORACLE-SBC(local-policy-attributes)# realm ECB-Peer ORACLE-SBC(local-policy-attributes)# app-protocol sip ORACLE-SBC(local-policy-attributes) # done policy-attribute next-hop 192.168.1.90 ECB-Peer realm action none terminate-recursion disabled carrier 0000 start-time 2400 end-time days-of-week U-S cost 0 SIP app-protocol state enabled methods media-profiles lookup single next-key disabled eloc-str-lkup eloc-str-match ORACLE-SBC(local-policy-attributes) # exit ORACLE-SBC (local-policy) # done local-policy from-address to-address source-realm SIP-trunk description activate-time N/A



deactiva	ate-time	N/A	
state		enabled	
policy-p	priority	none	
policy-a	attribute		
	next-hop		192.168.1.90
	realm		ECB-Peer
	action		none
	terminate-recursion		disabled
	carrier		
	start-time		0000
	end-time		2400
	days-of-week		U-S
	cost		0
	app-protocol		SIP
	state		enabled
	methods		
	media-profiles		
	lookup		single
	next-key		
	eloc-str-lkup		disabled
	eloc-str-match		

We will first configure the route from the ECB to the gateway.

```
ORACLE-SBC(local-policy)# from-address *
ORACLE-SBC(local-policy)# to-address *
ORACLE-SBC(local-policy) # source-realm ECB-Peer
ORACLE-SBC(local-policy)# policy-attributes
ORACLE-SBC(local-policy-attributes)# next-hop 10.10.1.8
ORACLE-SBC(local-policy-attributes) # realm SIP-trunk
ORACLE-SBC(local-policy-attributes)# app-protocol sip
ORACLE-SBC(local-policy-attributes)# done
policy-attribute
                                     10.10.1.8
      next-hop
      realm
                                    SIP-trunk
       action
                                     none
       terminate-recursion
                                     disabled
      carrier
       start-time
                                     0000
       end-time
                                     2400
       days-of-week
                                     U-S
```



cost	(C	
app-protoc	ol	SIP	
state	e	enabled	
methods			
media-prof.	iles		
lookup	S	single	
next-key	next-key		
eloc-str-l	kup d	disabled	
eloc-str-m	atch		
ORACLE-SBC (local-)	policy-attributes)# ex	kit	
onnenn ppe (rocar)	porrey) « done		
local-policy			
from-addre	ess		
		*	
to-addres:	S		
		*	
source-rea	alm		
		ECB-Peer	
descriptio	on		
activate-	time	N/A	
deactivate	e-time	N/A	
state		enabled	
policy-pr	iority	none	
last-modi:	fied-by	admin@17	2.41.0.11
last-modi:	fied-date	2012-03-	06 11:43:03
policy-at	tribute		10 10 1 0
ne	ext-hop		
r	ea⊥m		SIP-trunk
a	ction .		none
te	erminate-recursion		disabled
C	arrier		0000
S	tart-time		0000
ei	na-time		2400
da	ays-oi-week		0-5
C			0
aj	pp-protocol		
S	tate		enabled
me	etnoas		
me	edia-profiles		



lookup	single	
next-key		
eloc-str-lkup	disabled	
eloc-str-match		

We will need a route to handle call transfer and refer scenarios (local refer handling by the E-SBC) when Lync client 1 refers/transfers the call to Lync Client 2.

local-policy	
from-address	
	*
to-address	
	192.168.1.90
source-realm	
	SIP-trunk
description	For referred party header
activate-time	N/A
deactivate-time	N/A
state	enabled
policy-priority	none
last-modified-by	admin@console
last-modified-date	2012-02-28 13:05:51
policy-attribute	
next-hop	192.168.1.90
realm	ECB-Peer
action	replace-uri
terminate-recursion	disabled
carriers	
start-time	0000
end-time	2400
days-of-week	U-S
cost	0
app-protocol	SIP
state	enabled
methods	
media-profiles	
lookup	single
next-key	
eloc-str-lkup	disabled
eloc-str-match	



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 per unidirectional media stream).

```
ORACLE-SBC(local-policy) # exit
ORACLE-SBC (session-router) # exit
ORACLE-SBC(configure) # media-manager
ORACLE-SBC (media-manager) # steering-pool
ORACLE-SBC(steering-pool) # ip-address 192.168.1.130
ORACLE-SBC(steering-pool) # start-port 30000
ORACLE-SBC(steering-pool) # end-port 40000
ORACLE-SBC(steering-pool) # realm-id ECB-Peer
ORACLE-SBC(steering-pool)# network-interface s1p0:0
ORACLE-SBC(steering-pool) # done
steering-pool
       ip-address
                                      192.168.1.130
                                       30000
       start-port
        end-port
                                       40000
        realm-id
                                       ECB-Peer
       network-interface
                                       s1p0:0
```

You will now configure the media handling for the pstn realm

```
ORACLE-SBC(steering-pool)# ip-address 192.20.0.108
ORACLE-SBC(steering-pool) # start-port 40000
ORACLE-SBC(steering-pool) # end-port 50000
ORACLE-SBC(steering-pool) # realm-id SIP-trunk
ORACLE-SBC(steering-pool) # network-interface s0p0:0
ORACLE-SBC(steering-pool) # done
steering-pool
       ip-address
                                       192.20.0.108
       start-port
                                       40000
       end-port
                                       50000
        realm-id
                                       SIP-trunk
        network-interface
                                       s0p0:0
```



Configure Sip-manipulations and translation rules

To ensure that the E-SBC is doing topology hiding and replacing host-portions in SIP URIs of From and To headers, a sip manipulation will need to be created and configured as the out-manipulation id on the sip-interface.

The sip-manipulation element can be found under the session-router element.

sip-manipu	lation		
name		NATting	
descr	iption		
split	-headers		
join-	headers		
heade	r-rule		
	name	From	
	header-name	From	
	action	manipu	late
	comparison-type	case-s	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
heade	er-rule		
	name	То	
	header-name	To .	
	action	manipu	late
	comparison-type	case-s	sensitive
	msg-type	reques	st
	methods		
	match-value		
	new-value		
	element-rule		_
	name		То
	parameter-name		
	type		uri-host
	action		replace
	match-val-type		any
	comparison-type		case-sensitive
	match-value		
	new-value		SREMOTE_IP



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

```
ORACLE-SBC(session-router)# sip-interface
Oracle-SBC(sip-interface) # sel
<realm-id>:
1: ECB-Peer 192.168.1.130:5060
2: SIP-trunk 192.20.0.108:5060
selection: 2
Oracle-SBC(sip-interface)# out-manipulationid NATting
Oracle-SBC(sip-interface)# done
sip-interface
                                    enabled
       state
       realm-id
                                    SIP-trunk
                                  SIP Trunk-facing (Outside)
       description
       sip-port
              address
                                           192.20.0.108
              port
                                           5060
              transport-protocol
                                           UDP
              tls-profile
              allow-anonymous
                                          all
              ims-aka-profile
       carriers
       trans-expire
                                    0
                                    0
       invite-expire
       max-redirect-contacts
                                  0
       proxy-mode
       redirect-action
                                  none
none
       contact-mode
       nat-traversal
                                  30
       nat-interval
       tcp-nat-interval
                                  90
       registration-caching disabled
       min-reg-expire
                                    300
       registration-interval 3600
       route-to-registrar
                                  disabled
       secured-network
                                  disabled
       teluri-scheme
                                   disabled
       uri-fqdn-domain
       options
```



trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	NATting
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
${\tt charging-function-address-mode}$	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	



```
ORACLE-SBC(session-router)# sip-interface
Oracle-SBC(sip-interface) # sel
<realm-id>:
1: ECB-Peer 192.168.1.130:5060
2: SIP-trunk 192.20.0.108:5060
selection: 1
Oracle-SBC(sip-interface) # out-manipulationid NATting
Oracle-SBC(sip-interface) # done
sip-interface
                                   enabled
       state
       realm-id
                                   ECB-Peer
       description
                                   ECB-Facing(Inside)
       sip-port
                                           192.168.1.130
              address
                                            5060
              port
              transport-protocol
                                           TCP
              tls-profile
              allow-anonymous
                                           all
              ims-aka-profile
       carriers
       trans-expire
                                    0
                                   0
       invite-expire
       max-redirect-contacts
                                   0
       proxy-mode
       redirect-action
       contact-mode
                                   none
       nat-traversal
                                   none
       nat-interval
                                    30
       tcp-nat-interval
                                    90
                                 disabled
       registration-caching
       min-reg-expire
                                   300
       registration-interval
                                  3600
disabled
       route-to-registrar
       secured-network
                                    disabled
       teluri-scheme
                                   disabled
       uri-fqdn-domain
       trust-mode
                                    all
       max-nat-interval
                                    3600
```



nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401.407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	NATting
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	



Lync does send E164 numbers in the To and From headers whereas the trunk does not accept E164 numbers. Hence we need a translation rule on the E-SBC to translate the E164 phone numbers into a regular one by stripping off the +1 from the phone numbers. The translation rule then needs to be added on the session-translation which then gets called from the trunk session-agent.

```
Oracle-SBC(sip-interface) # exit
Oracle-SBC(session-router)# translation-rules
Oracle-SBC(translation-rules)# id stripplus1
Oracle-SBC(translation-rules)# type delete
Oracle-SBC(translation-rules)# delete-string +1
Oracle-SBC(translation-rules) # done
translation-rules
       id
                                      stripplus1
                                      delete
       type
       add-string
                                      0
       add-index
       delete-string
                                      +1
                                      0
       delete-index
Oracle-SBC(translation-rules) # exit
Oracle-SBC(session-router)# session-translation
Oracle-SBC(session-translation)# id stripplus1
Oracle-SBC(session-translation)# rules-calling stripplus1
Oracle-SBC(session-translation)# rules-called stripplus1
Oracle-SBC(session-translation) # done
session-translation
       id
                                      stripplus1
       rules-calling
                                     stripplus1
       rules-called
                                     stripplus1
       last-modified-by
                                      admin@console
        last-modified-date
                                      2012-01-26 18:28:59
Oracle-SBC(session-translation) # exit
Oracle-SBC(session-router)# session-agent
Oracle-SBC(session-agent) # sel
<hostname>:
1: 10.10.1.8
                            realm=SIP-trunk
2: 192.168.1.130
                          realm=ECB-Lync-Peer ip=192.168.1.130
```



selection: 1			
Oracle-SBC(session-agent) # out-translationid stripplus1			
Oracle-SBC (session-agent) # done			
session-agent			
hostname	10.10.1.8		
ip-address	10.10.1.8		
port	5060		
state	enabled		
app-protocol	SIP		
app-type			
transport-method	UDP		
realm-id	SIP-trunk		
egress-realm-id			
description			
carriers			
allow-next-hop-lp	enabled		
constraints	disabled		
max-sessions	0		
max-inbound-sessions	0		
max-outbound-sessions	0		
max-burst-rate	0		
max-inbound-burst-rate	0		
max-outbound-burst-rate	0		
max-sustain-rate	0		
max-inbound-sustain-rate	0		
max-outbound-sustain-rate	0		
min-seizures	5		
min-asr	0		
time-to-resume	0		
ttr-no-response	0		
in-service-period	0		
burst-rate-window	0		
sustain-rate-window	0		
req-uri-carrier-mode	None		
proxy-mode			
redirect-action			
loose-routing	enabled		
send-media-session	enabled		
response-map			



ping-method	
ping-interval	0
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	stripplus1
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	NATting
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	



Configure SIP PRACK Interworking

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

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

```
ORACLE-SBC(session-router) # sip-interface
Oracle-SBC(sip-interface) # sel
<realm-id>:
1: ECB-Peer 192.168.1.130:5060
2: SIP-trunk 192.20.0.108:5060
selection: 1
Oracle-SBC(sip-interface) # options 100rel-interworking
Oracle-SBC(sip-interface) # done
sip-interface
                                   enabled
       state
       realm-id
                                    ECB-Peer
                                   ECB-Facing(Inside)
       description
       sip-port
              address
                                            192.168.1.130
                                            5060
              port
              transport-protocol
                                            TCP
              tls-profile
             allow-anonymous
                                            all
              ims-aka-profile
       carriers
                                    0
       trans-expire
                                    0
       invite-expire
       max-redirect-contacts 0
       proxy-mode
       redirect-action
```



contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
options	100rel-interworking
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	NATting
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101



rfc2833-mode	transparent	
constraint-name		
response-map		
local-response-map		
ims-aka-feature	disabled	
enforcement-profile		
route-unauthorized-cal	ls	
tcp-keepalive	none	
add-sdp-invite	disabled	
add-sdp-profiles		
sip-profile		
sip-isup-profile		

Configure Sip-feature to pass Supported and Require headers in SIP messages. The sip-feature element can be found under session-router.

ORACLE-SBC (session-router) #sip-feature		
ORACLE-SBC(sip-feature)#name 100rel		
ORACLE-SBC(sip-feature) #realm pstn		
ORACLE-SBC(sip-feature) # support-mode	-inbound Pass	
ORACLE-SBC(sip-feature) # require-mode	-inbound Pass	
ORACLE-SBC(sip-feature) # proxy-requir	e-mode-inbound Pass	
ORACLE-SBC(sip-feature) # support-mode	-outbound Pass	
ORACLE-SBC(sip-feature) # require-mode	-outbound Pass	
ORACLE-SBC(sip-feature) # proxy-requir	e-mode-outbound Pass	
ORACLE-SBC(sip-feature)# done		
sip-feature		
name	100rel	
realm	SIP-Trunk	
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	



Configure the sip-manipulation For early media to delete the Supported header and add the Required header and apply it as an inmanipulation in the interface facing ECB.

sip-manipulation	
name Forearlymedia	
description	
split-headers	
join-headers	
header-rule	
name	delsupported
header-name	Supported
action	delete
comparison-type	case-sensitive
msg-type	request
methods	T NA T.I.F.
match-value	
new-value	
neader-rule	
header-name	Boguiro
	nequire
comparison-type	case-sensitive
msg-type	request
methods	TNVTTE
new-value	100rel
	100101
ORACLE-SBC (session-router) # sip-interfa	ace
Oracle-SBC(sip-interface) # sel	
<realm-id>.</realm-id>	
$1 \cdot \text{FCB-Peer} 192 168 1 130 \cdot 5060$	
1. ECB-reel 192.100.1.130.3000	
2: SIP-trunk 192.20.0.108:5060	
selection: 1	
<pre>Oracle-SBC(sip-interface)# in-manipula</pre>	tionid Forearlymedia
Oracle-SBC(sip-interface)# done	
sip-interface	
state	enabled
realm-id	ECB-Peer
description	ECB-Facing (Inside)
sin-nort	202 100103 (100100)
orb-borc	102 160 1 120
address	192.108.1.130



port	5060
transport-protocol	TCP
tls-profile	
allow-anonymous	all
ims-aka-profile	
carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	Forearlymedia
out-manipulationid	NATting
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0



network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
${\tt charging-function-address-mode}$	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	

Configuring REFER Handling for Transfers

Lync Server authorizes transfers of all Lync initiated calls whether it is Lync to Lync or Lync to PSTN. The E-SBC provides REFER handling by terminating the REFER from Lync and generating an INVITE for the referred party back towards the Lync Mediation server. Lync then process the INVITE, authorizes the call transfer and sends either a new INVITE (for calls transferred to PSTN) to the E-SBC or transfers call internally to the transferred Lync client

To handle the call transfer and refer scenarios – when Lync client 1 refers/transfers the call to Lync Client 2 or to a party on the PSTN, we will need a route to the ECB.

local-policy	
from-address	*
to-address	192.168.1.90
source-realm	Trunk
description	For referred party
activate-time	
deactivate-time	
state	enabled
policy-priority	none



192.168.1.90
ECB-Peer
replace-uri
disabled
0000
2400
U-S
0
enabled
SIP
single
-
disabled

Addressing No Ringback tone on Transfers

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 E-SBC to initiate the transfer contains the SDP attribute, a=inactive which is forwarded to the trunk and as a result of which the E-SBC cannot play the ring back tone to the original PSTN caller (while call is being transferred). A send only 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 E-SBC is able to signal appropriately towards the SIP trunk by changing the a=inactive SDP attribute in the INVITE to sendonly towards PSTN.

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 transfer
split-headers	
join-headers	
header-rule	
name	changeSDP
header-name	Content-Type
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	INVITE
match-value	
new-value	



element-rule	
name	inacttosendonly
parameter-name	application/sdp
type	mime
action	find-replace-all
match-val-type	any
comparison-type	pattern-rule
match-value	a=inactive
new-value	a=sendonly

The above manipulation is applied as a nested manip in the manipulation – Forearlymedia that is applied inbound on the sip-interface facing ECB.

sip-manipulation	
name	Forearlymedia
description	
split-headers	
join-headers	
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	
new-value	100rel
header-rule	
name	inactosendonly
header-name	From
action	sip-manip
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	Changeinactosendonly



We utilize the local playback feature of the E-SBC to play ring back tone during transfers. The ringback tone is played based on REFER. You must upload a file containing to /code/media on the E-SBC for the media you want played. This file must be raw media binary containing data for the desired codec. A separate file is required for each different codec type, even if the media itself is the same.

The playback configuration is defined listing the media files that you want to play. The playback-config element is configured under media-manager.

playback-config	
name	transferrbt
entry	
encoding	PCMU
filename	US ringbackPCMU.raw
bytes-per-sec	8000

The playback options can be applied to realms, sip-interfaces or session agents using the spl-options command.

```
ORACLE-SBC(session-router)# sip-interface
Oracle-SBC(sip-interface) # sel
<realm-id>:
1: ECB-Peer 192.168.1.130:5060
2: SIP-trunk 192.20.0.108:5060
selection: 1
Oracle-SBC(sip-interface) # spl-options playback-on-refer="transferrbt"
Oracle-SBC(sip-interface) # done
sip-interface
                                    enabled
       state
       realm-id
                                     ECB-Peer
       description
                                    ECB-Facing(Inside)
       sip-port
                                              192.168.1.130
               address
               port
                                              5060
               transport-protocol
                                              TCP
               tls-profile
               allow-anonymous
                                              all
               ims-aka-profile
       carriers
                                      0
       trans-expire
                                      0
       invite-expire
                                      0
       max-redirect-contacts
       proxy-mode
        redirect-action
       contact-mode
                                      none
```



nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
options	100rel-interworking
spl-options	playback-on-refer="transferrbt"
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	NATting
manipulation-string	-
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	-
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	



```
route-unauthorized-calls

tcp-keepalive none

add-sdp-invite disabled

add-sdp-profiles

sip-profile

sip-isup-profile
```

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 session-agent, you issue the exit command three times.

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.

```
ORACLE-SBC# 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'.
ORACLE-SBC# 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 phyl 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
```

E-SBC configuration is now complete.

Interoperability testing

Interoperability between Avaya and Lync

The following observations were made during testing -

- In versions prior to the 6.2 release, Avaya SM uses INVITEs for session refreshes. These INVITEs do not include SDP. This
 results in an interoperability issue with Microsoft Lync when media bypass is enabled as it does not accept INVITEs without
 SDP.
- In releases 6.2 and later, UPDATE message can be used for session refresh, to enable UPDATEs from the Avaya SM instead of the INVITEs without SDP, the signaling group was configured as follows

change signaling-group 2	Page 1 of	2
SIGNAL	ING GROUP	
Group Number: 2 Group Typ	e: sip	
IMS Enabled? n Transport Method	: tcp	
IP Video? n	Enforce SIPS URI for SRTP?	n
Peer Detection Enabled? y Peer Server	r: SM	
Prepend '+' to Outgoing Calling/Alerting/Diver	rting/Connected Public Numbers?	У
Remove '+' from Incoming Called/Calling/Alertir	ng/Diverting/Connected Numbers?	V
Near-end Node Name: procr	Far-end Node Name: acme-sm	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain: aura.com		
	Bypass If IP Threshold Exceeded?	n
Incoming Dialog Loopbacks:	RFC 3389 Comfort Noise?	n
elininate		
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections?	n
DTMF over IP: rtp-payload Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? IP Audio Hairpinning?	n y



- With UPDATEs enabled, the calls flows for hold and resume were as follows:
 - When Avaya server places a call on hold during the inbound calls, the call flow does not include INVITE messages to signal the hold and resume. It utilizes the UPDATE messages.
 - When Avaya server performs a call hold and resume during the outbound calls, it sends INVITE message to signal the hold and resume.
- For lync initiated transfers, Avaya does not support REFER from Lync. The Refer-To in the REFER from Lync does not contain the uri-user. Avaya sends a 403 Forbidden (Refer-to user is null) error.
 - In Lync environments with REFER enabled, the calls will need to be sent through the E-SBC to the ECB for REFER termination on the E-SBC.
 - o Or Lync needs to be reconfigured to use INVITEs for transfer scenarios.

Interoperability between CUCM and Lync

During an inbound call from Lync, when CUCM performs a call hold and resume, CUCM sends an INVITE without SDP. When media bypass is enabled on Lync, the mediation server does not accept INVITEs without SDP and responds with *488 GatewayCall is not in Connected State*. As a result the hold and resume fails. To resolve this issue we either have to insert SDP or disable media bypass. To insert SDP, the call will need to be placed through a E-SBC.

When media bypass is disabled, Lync accepts the INVITE when it is sent without SDP. However, during call resume, the INVITE sent from CUCM contains SDP without the telephone event. Lync responds with the error *488 Invalid SDP: Gateway ParseSdpOffer Error: No DTMF support on Gateway side.*

To resolve this issue, we configure a sip-manipulation to add the SDP line for telephone event if it does not exist before forwarding the INVITE to Lync.

sip-manipulation	
name	fixSDP
description	To bypass the 488 due to missing DTMF from CUCM during hold
split-headers	
join-headers	
header-rule	
name	Checkfordtmf
header-name	Content-type
action	store
comparison-type	case-sensitive
msg-type	any
methods	INVITE
match-value	
new-value	
element-rule	
name	Checkdtmfexists
parameter-name	application/sdp
type	mime
action	store
match-val-type	any



comparison-typ	pe case-sensitive
match-value	(a=rtpmap:101 telephone-event/8000)
new-value	
header-rule	
name	AddPtime10
header-name	Content-Type
action	manipulate
comparison-type	boolean
msg-type	any
methods	INVITE
match-value	!\$Checkfordtmf.\$Checkdtmfexists
new-value	
element-rule	
name	Adddtmf
parameter-name	application/sdp
type	mime
action	find-replace-all
match-val-type	e any
comparison-typ	pe pattern-rule
match-value	(*)
new-value	<pre>\$0+"a=rtpmap:101 telephone-event/8000"+\$CRLF+"a=fmtp:101 0-15"+\$CRLF</pre>
header-rule	
name	Modifymline
header-name	From
action	sip-manip
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	Modmline
last-modified-by	Web@
last-modified-date	2014-07-23 15:43:00

This manipulation is then nested into the HMR, HMRtowardsLync that is applied in the outbound directions towards the Lync servers.

sip-manipulation	
name	HMRtowardsLync
description	HMR NAT+deleting the blines+addDTMF
split-headers	
join-headers	
header-rule	
name	donat
header-name	From
action	sip-manip
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	NATting
header-rule	
name	deleteblines



	header-name	From
	action	sip-manip
	comparison-type	case-sensitive
	msg-type	any
	methods	
	match-value	
	new-value	Delblines
header-rule		
	name	adddtmflines
	header-name	From
	action	sip-manip
	comparison-type	case-sensitive
	msg-type	any
	methods	INVITE
	match-value	
	new-value	fixSDP

Please note that when CUCM calls Lync and the call is placed on hold by Lync, the issue mentioned above does not occur.

In Lync environments with media bypass and REFER enabled, the calls will need to be sent through the E-SBC to the ECB to utilize the add-sdp-profile and REFER termination features of the E-SBC.
Test Plan & Results

Test Plan

The testing was done with TCP/RTP. Lync 2010 and Lync 2013 servers are two different environments independent of each other. Lync 2010 has media bypass and refer enabled. Lync 2013 setup has media bypass and refer disabled.

The test plan consisted of the following test cases.

Test case	Result	Notes
Basic inbound and Outbound calls		
PSTN calls Lync 2010	Pass	
PSTN calls Lync 2013	Pass	
PSTN calls Avaya	Pass	
PSTN calls CUCM	Pass	
Lync 2013 calls CUCM	Pass	
Lync 2013 calls Avaya	Pass	
Lync 2013 calls PSTN	Pass	
CUCM calls Avaya	Pass	
CUCM calls PSTN	Pass	
CUCM calls Lync 2010	Pass	
CUCM calls Lync 2013	Pass	
Lync 2010 calls CUCM	Pass	
Lync 2010 calls Avaya	Pass	
Lync 2010 calls PSTN	Pass	
Avaya calls PSTN	Pass	
Avaya calls Lync 2010	Pass	
Avaya calls Lync 2013	Pass	
Avaya calls CUCM	Pass	
Back up route (replicating the SAG in ECB)		
PSTN calls Lync 2010 (home agent med1 paused)	Pass	



4 digit dialing		
Lync 2010 calls Avaya	Pass	
Lync 2010 calls CUCM	Pass	
CUCM calls Avaya	Pass	
CUCM calls Lync 2010	Pass	
Avaya calls Lync 2010	Pass	
Avaya calls CUCM	Pass	
Transfers		
PSTN calls Lync 2010 and Lync transfers to PSTN	Pass	
PSTN calls Lync 2013 and Lync transfers to PSTN	Pass	
PSTN calls CUCM and CUCM transfers to PSTN	Pass	The transfer was successful but the calling number displayed to the second PSTN party is that of Cisco phone and not the Original PSTN party
PSTN calls Lync 2010 and Lync transfers to CUCM using 4 digit dial	Pass	
PSTN calls Avaya and Avaya transfers to Lync using 4 digit dial	Pass	
PSTN calls Avaya and Avaya transfers to Lync 2013 using 10 digits	Pass	
PSTN calls Lync 2013 and Lync transfers to CUCM using 10 digit dial	Pass	
Lync 2013 calls Lync 2010 and transfers to CUCM	Pass	
Lync 2013 calls CUCM(10 digit) and CUCM transfers to Lync 2010 (4 digit) - no media bypass on Lync 2013	Pass	The transfer was successful but the calling number displayed to the second PSTN party is that of Cisco phone and not the Original PSTN party
Lync calls Avaya and transfer to CUCM (refer disabled)	Pass	Transfer works with refer disabled
CUCM calls Avaya and Avaya transfers to Lync	Pass	
CUCM calls Lync 2013 and Lync transfers to Lync 2010 (refer disabled)	Pass	
CUCM calls Avaya and CUCM transfers to Lync	Pass	
CUCM calls Avaya and CUCM transfers to PSTN	Pass	
Avaya calls Lync and transfers to CUCM	Pass	



Call Hold/Resume		
PSTN calls Lync and Lync places call on hold	Pass	
PSTN call Avaya and Avaya places call on hold	Pass	
PSTN calls CUCM and CUCM places call on hold	Pass	
Lync 2013 calls Avaya and Lync places call on hold	Pass	
Lync 2013 calls Avaya and Avaya places call on hold	Pass	
Lync 2013 calls CUCM and CUCM places call on hold	Pass	During the call hold process, one of the re- invites with sdp from CUCM does not contain a lines for DTMF support to which Lync responds with a 488 DTMF not supported. To overcome this issue we have an HMR towards Lync to add the a lines for DTMF in SDP if not present
CUCM calls Lync 2010 and CUCM places the call on hold	Pass	
Avaya calls Lync 2013 and Avaya places the call on hold	Pass	
Lync 2010 calls Avaya and Avaya places the call on hold	Pass	
CUCM calls Avaya and CUCM places the call on hold	Pass	
Avaya calls PSTN and Avaya places the call on hold	Pass	
Avaya calls CUCM and Avaya places the call on hold	Pass	



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 Server, and the E-SBC like logging and tracing which may be of assistance. In this section we will provide a list of tools which you can use to aid in troubleshooting any issues you may encounter.

Since we are concerned with communication between the Lync Server mediation server and the E-SBC we will focus on the troubleshooting tools to use between those devices if calls are not working or tests are not passing.

Microsoft Network Monitor (NetMon)

NetMon is a network protocol analyzer which is freely downloadable from Microsoft. It can be found at <u>www.microsoft.com/downloads</u>. 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 <u>www.wireshark.org</u>. Wireshark could be installed on the Lync Server mediation server, the Lync 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 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 Server Front End server;
- A Lync Server Standard Edition Server; and
- A Lync Server Mediation Server.



On the Oracle Enterprise Communications Broker and Oracle Enterprise Session Border Controller

The Oracle Enterprise Session Border Controller and Oracle Enterprise Communications Broker provide a rich set of statistical counters available from the ACLI, 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 E-SBC Console:

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

Examining the log files

Note: You will FTP to the management interface of the E-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 ORACLE-SBCFTP 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.

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 as well as on the Lync Server mediation server.

The Lync Server mediation server will listen on TCP port 5067 by default for SIP signaling. In our example we are listening on 5060 on the PSTN facing NIC. From the Standard Edition pool or Enterprise Edition pool the Mediation Server would be listening on port 5061. Tests may include:

- Client to pool server: telnet <servername> 5061
- Pool server to Mediation Server: telnet <servername> 5061



Lync Server Logging Tool

The Lync Server 2013 Logging Tool provides internal traces and messaging between different Lync Server 2013 elements like Front-end, Mediation server, Lync Clients, etc. File name is OCSReskit.msi. Once installed, it can be accessed from any one of the Lync Server servers by running Start/Microsoft Lync Server 2013/Lync Server Logging Tool.

Lync Server 2013 Logging Tool			
Logging Options Components Level Clent Version Filter F CLSCommon F CLSController V CLSController V CLSFormat F Coshotrollering V Coshotrollering V Coshotrollering V Coshotrollering V Coshotrollering V Coshotrollering V DataMCU DataMCU DataMCUURIn Time Bags DeviceUpdateHttpHandler V Dialin V Dix TF Dialin Dix HybridConfig IIMFilter ImMou IncomingFederation Infrastructure V	Giliatal Errors Girors Varnings nformation /erbose VI E_COMPONENT PROTOCOL E_CONNECTION E_DIAG Flags	obal Options Log File Options Type Maximum Size: © Circular 20 O Sequential Append to log file New File Display only Filter Options Enabled Enabled Edit Clear Include Filters Exclude Filters	
Log File Folder: C:\Windows\Tracing Browse			
Start Logging View Log Files An	nalyze Log Files Advance	ed Options Exit Help	
No active log session. Check the components you wish to log in the list on the left. For each checked component, configure the log level and flags for that component. Click Start Logging button to start logging the checked components with the configured level and flags.			

Appendix A

No Ring Back Tone heard for inbound calls from PSTN to MS Lync through E-SBC

Recently, in some accounts where MS Lync and E-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 Lync user on the enterprise especially when Media Bypass is enabled on MS Lync

The configuration note below aims to explain this scenario briefly, steps taken to rectify this issue and proposed workaround by Oracle. The workaround is an interim solution while a permanent solution is being researched and developed by Oracle Engineering

Media Bypass

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

Signaling between mediation server and E-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





Note that after signaling 183 with SDP, Lync 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.

Acme Packet Work Around

The interim solution is to present 180 ringing (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's robust Sip Manipulation and Sip Response Map features to the following:





sip-manipulatio	n		
name		Stripsdp183	
descrip	tion	For incoming 183 from Lync,	
strip SDP			
split-h	eaders		
join-he	aders		
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-type	pattern-rule	
	match-value	183	
	new-value		
header-	rule		
	name	delSDP	
	header-name	Content-Type	
	action	manıpulate	
	comparison-type	case-insensitive	
	msg-type	any	
	methods		
	match-value	\$check183.\$is183	
	new-value		
	element-rule	1 1100000	
	name	dell83SDP	
	parameter-name	application/sdp	
	type	mime	
	action	delete-element	
	match-val-type	any	
	comparison-type	DOOLEAN	
	match-value		
hoods	new-value		
neader-	TUTE	dol Contont Turno	
	hander-name		
	neauer-name	content-Type	
	action	manipulate	

A sip manipulation, Stripsdp183, is configured to delete the SDP from the 183 messages.

125.00 - 0.000	2.5 12 20 20 20 20 20 20 20 20 20 20 20 20 20	

comparison-type	boolean
msg-type	any
methods	
match-value	\$check183.\$is183
new-value	
element-rule	
name	delCT
parameter-name	*
type	header-param
action	delete-header
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	

The above manipulation is applied as a nested manip in the manipulation – Forearlymedia that is applied inbound on the sipinterface facing ECB.

sip-manipulation	
name	Forearlymedia
description	
split-headers	
join-headers	
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	
new-value	100rel
header-rule	
name	inactosendonly
header-name	From
action	sip-manip
comparison-type	case-sensitive



msg-type	request
methods	
match-value	
new-value	Changeinactosendonly
header-rule	
name	mod183
header-name	From
action	sip-manip
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	Stripsdp183

A sip response map is configured to change the 183s to 180 and applied on the sip-interface facing the trunk.

response-map			
name		change1	83to180
entries			
	recv-code		183
	xmit-code		180
	reason		Ringing
	method register-response-expi	res	
ORACLE-SBC (sess: Oracle-SBC (sip-: <realm-id>: 1: ECB-Peer 192 2: SIP-trunk 192</realm-id>	ion-router)# sip-interf interface)# sel 2.168.1.130:5060 2.20.0.108:5060	ace	
<pre>selection: 1 Oracle-SBC(sip-interface) # response-map change183to180 Oracle-SBC(sip-interface) # done</pre>			
sip-interface			
state		enabled	
realm-io	d	ECB-Peer	
descrip	tion	ECB-Facing(Insid	e)
sip-por	t		
	address	192.168.	1.130



port	5060
transport-protocol	TCP
tls-profile	
allow-anonymous	all
ims-aka-profile	
carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
options	100rel-interworking
spl-options	playback-on-refer="transferrbt"
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	NATting
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass



${\tt charging-function-address-mode}$	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	change183to180
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	

Appendix B

Accessing the ACLI

Access to the ACLI is provided by:

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

Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) interface on the E-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 E-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, **ORACLE-SBC(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 E-SBC boot parameters. Key boot parameters include:

- boot device The global management port, usually eth0
- file name The boot path and the image file.
- inet on ethernet The IP address and subnet mask (in hex) of the management port of the SD.



- host inet -The IP address of external server where image file resides.
- user and ftp password Used to boot from the external FTP server.
- gateway inet The gateway IP address for reaching the external server, if the server is located in a different network.

```
'.' = clear field; '-' = go to previous field; g = guit
boot device
processor number
                       : eth0
                       : 0
host name
                        .
file name : /tffs0/nnSCX620.gz
inet on ethernet (e) : 10.0.3.11:ffff0000
inet on backplane (b) :
                       : 10.0.3.100
host inet (h)
gateway inet (g)
user (u)
                       : 10.0.0.1
                        : anonymous
ftp password (pw) (blank = rsh) : anonymous
flags (f) : 0x8
target name (tn)
                       : MCS14-IOT-SD
startup script (s)
                       . .
other (o)
```

The ntp-sync branch provides access to ntp server configuration commands for synchronizing the E-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, mediamanager, 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 E-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.



- 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 E-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,

- 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 E-SBC reboots, your configurations will be lost.

Configuration Versions

At any time, three versions of the configuration can exist on the E-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 E-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 nonvolatile memory on the SBC and becomes the saved configuration. Because the saved configuration has not been activated yet, the changes in the configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded, not the saved configuration.
- The **running configuration** is the saved then activated configuration. On issuing the **activate-config** command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration. Although most of the configurations can take effect once being activated without reboot, some configurations require a reboot for the changes to take effect. To view the running configuration, issue command show **running-config**.

Saving the Configuration

The **save-config** command stores the edited configuration persistently.

Because the saved configuration has not been activated yet, changes in configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded. At this stage, the saved configuration is different from the running configuration.

Because the saved configuration is stored in non-volatile memory, it can be accessed and activated at later time.

Upon issuing the **save-config** command, the E-SBC displays a reminder on screen stating that you must use the **activate-config** command if you want the configurations to be updated.

```
MCS14-IOT-SD# 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'.
MCS14-IOT-SD#
```



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 E-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.

MCS14-IOT-SD# activate-config Activate-Config received, processing. waiting 120000 for request to finish Request to 'ACTIVATE-CONFIG' has Finished, Activate Complete MCS14-IOT-SD#



Oracle Corporation World Headquarters 500 Oracle Parkway Redwood Shores, CA 94065 U.S.A.

Worldwide Inquiries: Phone: +1.650.506.7000 Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Copyright © 2013, 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. 0113

Hardware and Software, Engineered to Work Together

