DEPLOYING ORACLE SBC IN MICROSOFT AZURE PUBLIC CLOUD WITH ORACLE SESSION ROUTER

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.

Version History

Version	Description of Changes	Date Revision Completed
1.0	Initial Publication	10/24/2019
1.1	• Added Revision Table • Added Architecture Diagram	11/12/2019
1.2	Revised Implementation on SCz9.0	5/15/2022

Table of Contents

1. Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, and end users of the Oracle Enterprise Session Border Controller (E-SBC) and Oracle Session Router (SR). It assumes that the reader is familiar with basic operations of the Oracle Communications Enterprise Session Border Controller, Oracle Communications Session Router, and Azure Cloud Deployments.

2. Document Overview

Vendors manage public clouds using SDN. The SDN controller owns all networking aspects including vNICs, IP addresses, MAC addresses, and so forth. Without the knowledge of the SDN controller, IP addresses cannot be assigned or moved. As a result, the network either drops or ignores GARP traffic. The absence of GARP invalidates the use of traditional HA by the OCSBC in these networks, therefore requiring alternate HA functionality on the OCSBC.

OCSBC supports High Availability (HA) deployments on public clouds using the redundancy mechanisms native to those clouds. Once you configure the cloud to recognize the OCSBC, the REST client on the OCSBC subsequently makes requests to the cloud's Software Defined Networking (SDN) controller for authentication and virtual IP address (VIP) management.

In Microsoft Azure, SBC VM instances are allowed to gain access to these resources which are managed by Active Directory services through the Metadata Instance Data Service. The OCSBC leverages this to give the SBC VM instance permission to change its IP address when deployed in HA.

Due to the limitations in the Azure Cloud redundancy mechanism outlined above, the amount of time necessary for Microsoft Azure Cloud to grant permissions and move the virtual IP addresses from one VM SBC instance to another, (active to standby), is outside of what Oracle Communications considers acceptable for an OCSBC HA deployment.

Understanding the necessity for redundancy in a Unified Communication Environment, we have worked to provide a solution to help minimize the service interruption that may be caused due to the extended amount of time it takes for the Azure cloud to perform a full high availability switchover.

The purpose of this application note is to provide an alternative to HA when deploying the OCSBC in Microsoft Azure Public Cloud Infrastructure by utilizing the Oracle Communications Session Router load balancing functionality. By implementing a pair of OCSR’s in front of a pair of OCSBC’s in Azure, we are able to reduce the amount of production traffic each individual SBC is required to handle. When deployed, this solution will not provide a session stateful redundant pair, but does minimize the amount of traffic potentially impacted and significantly decreases the amount of time for new requests to be processed in case of a fault in the environment.

3. Related Documentation

3.1 Oracle SBC

- Deploying Oracle SBC in Microsoft Azure Public Cloud
- Oracle® Communications Session Border Controller Platform Preparation and Installation Guide
- Oracle® Enterprise Session Border Controller Web GUI User Guide
- Oracle® Enterprise Session Border Controller ACLI Configuration Guide
- Oracle® Enterprise Session Border Controller Release Notes

3.2 Oracle Session Router

- Installation and Platform Preparation Guide
- Configuration Guide
- ACLI Reference Guide

3.3 Microsoft Azure

- Introduction to Azure
- Get started with Azure
- Azure security best practices and patterns

4. Create and Deploy on Azure

You can deploy the Oracle Communications Session Border Controller (OCSBC) and Oracle Communications Session Router (OCSR) on Azure public clouds. The procedure to deploy each VM SBC instance in Azure is outside the scope of this document. For detailed instructions on deploying the OCSBC and OCSR in Microsoft Azure Public Cloud, please refer to ***Deploying Oracle SBC in Microsoft Azure Public Cloud***. This application note continues where the OSBC in Azure Deployment guide leaves off.

Please note: Both the OCSR and OCSBC use the same VHD file and deployment procedure. The product used for each VM instance will be selected through the acli command "setup product" once deployment is complete and you have access to cli through the serial console.

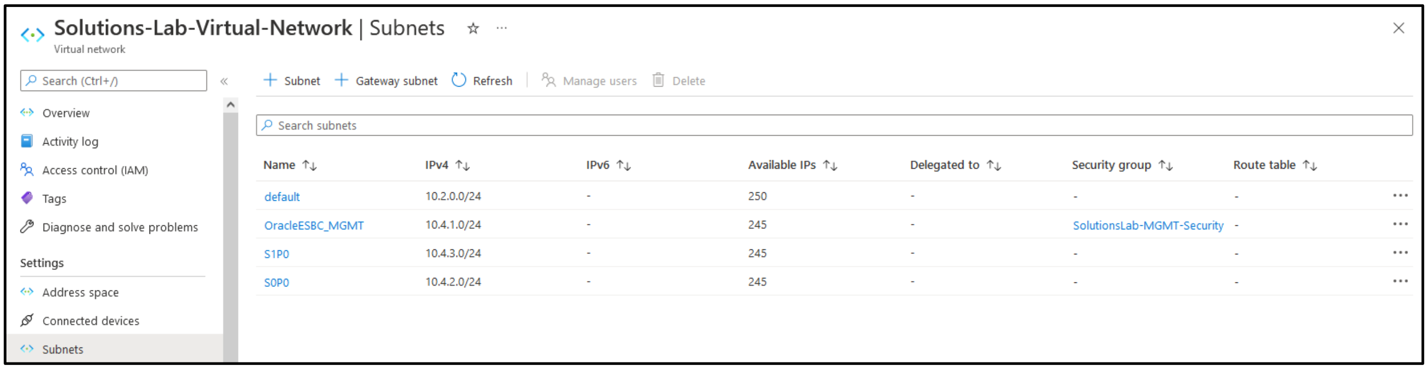
5. Requirements

- Three Oracle Communications VME deployments in Microsoft Azure Cloud, two for OCSBC and one for OCSR.
- If required, virtual public IP's assigned to Media interfaces for each Azure Oracle Communications VME deployed in Azure
  - For our testing, we have assigned Public VIP's to all media interfaces on both the OCSBC and OCSR.

Tip: You can utilize the search bar at the top of the Azure portal to quickly locate any element, resource ordocument during configuration and deployment of the Oracle SBC & Oracle SR in Azure Public Cloud.

6. Architecture

For the purpose of testing this deployment model, we have created three subnets in the Microsoft Azure Public Cloud, and we've deployed four Oracle Communications VME's. All network interfaces configured on the four VME's utilize addressing from these subnets. They are as follows:



Solutions-Lab-Virtual-Network | Subnets ☆ ···

Virtual network

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group ↑↓	Route table ↑↓	
default	10.2.0.0/24	-	250	-	-	-	···
OracleESBC_MGMT	10.4.1.0/24	-	245	-	SolutionsLab-MGMT-Security	-	···
S1P0	10.4.3.0/24	-	245	-	-	-	···
S0P0	10.4.2.0/24	-	245	-	-	-	···

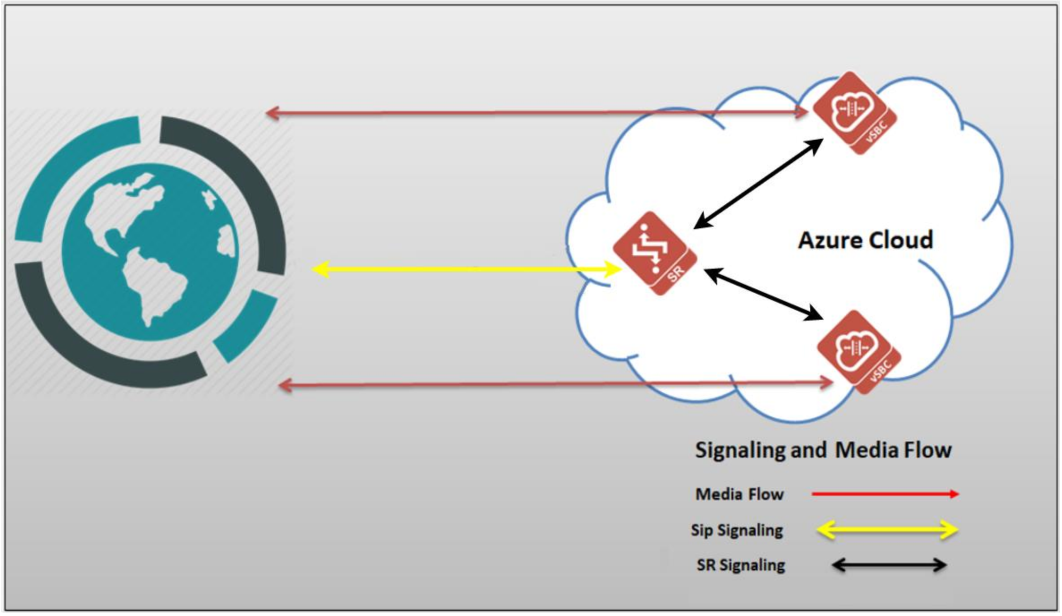
OracleESBC_MGMT - 10.4.1.0/24 is being used for the management interfaces of all three VME's.

The OCSBC and OCSR Network Interfaces are being configured with the following IP addresses:

Interface Label	Azure SR	Azure SBC1	Azure SBC2
S0P0	10.4.2.40	10.4.2.20	10.4.2.30
S1P0	10.4.3.40	10.4.3.20	10.4.3.30

All 6 Network interfaces have been assigned a Public Virtual IP in Azure Cloud.

6.1 Diagram



The following is a configuration example for both the OCSBC and OCSR. This application note assumes a Peering Environment.

7. OCSBC & OCSR Setup and Configuration

7.1 Setup Product and Entitlements

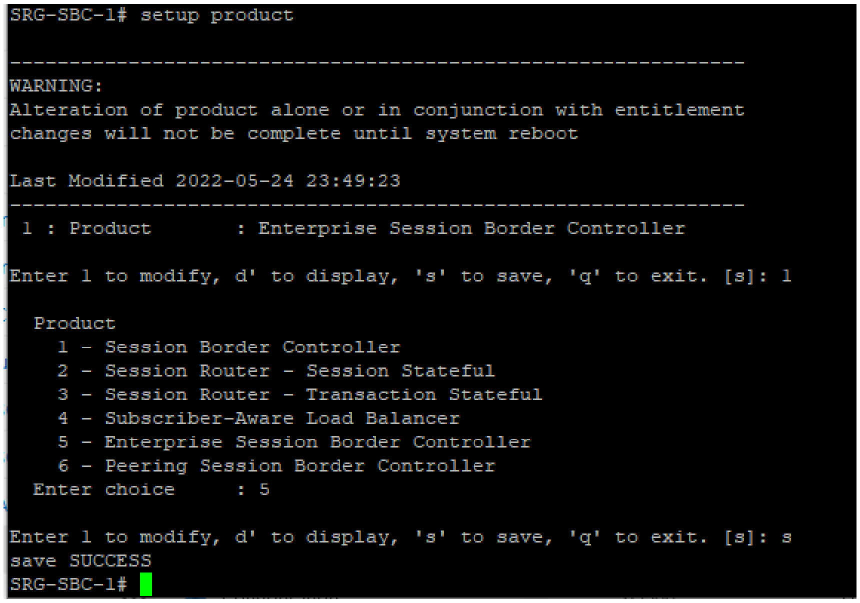
After following the SBC in Azure Deployment Guide referenced above, you should have access to both the SBC/SR Cli through serial console and SSH, passwords have been changed from their defaults, and all media interfaces have assigned mac addresses. We can now move on to selecting the product type, and enabling the features for the three VME's you have successfully deployed.

This procedure will be run on both OCSBC and OCSR deployed in Azure Public Cloud

7.1.1 OCSBC Product Setup

While in enable mode of the ACLI, type:

- setup product
- enter [1] : to modify or add the entry
- Enter Choice: Choose [5] for Enterprise Session Border Controller
- Enter [s] : Saves your product choice

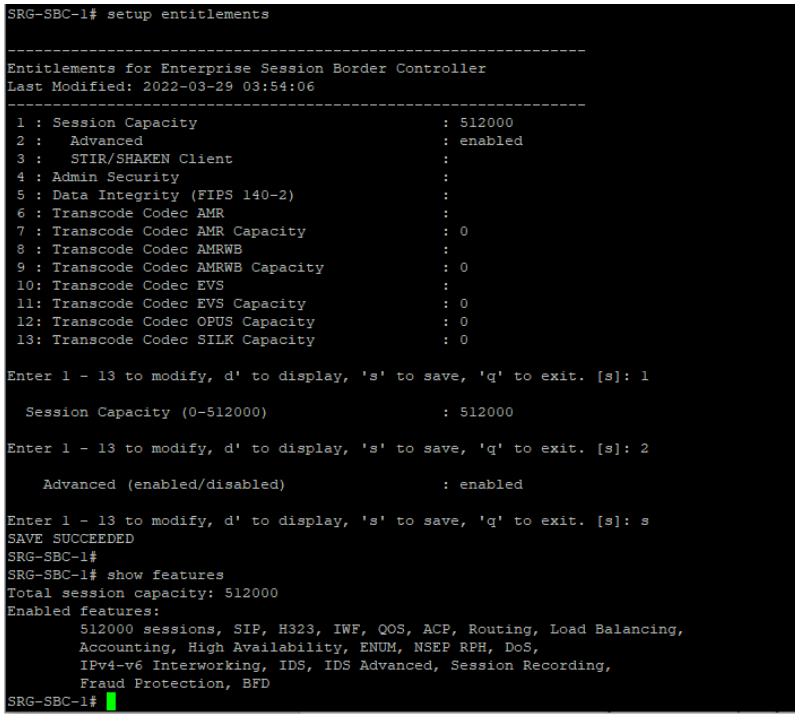


```
SRG-SBC-1# setup product

--------------------------------------------------------------
WARNING:
Alteration of product alone or in conjunction with entitlement
changes will not be complete until system reboot

Last Modified 2022-05-24 23:49:23
--------------------------------------------------------------
 1 : Product       : Enterprise Session Border Controller

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Product
    1 - Session Border Controller
    2 - Session Router - Session Stateful
    3 - Session Router - Transaction Stateful
    4 - Subscriber-Aware Load Balancer
    5 - Enterprise Session Border Controller
    6 - Peering Session Border Controller
  Enter choice     : 5

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
save SUCCESS
SRG-SBC-1#
```

7.1.2 OCSBC Entitlement (feature) Setup

While in enable mode of the ACLI, type

- setup entitlements
- enter [1] : to modify or add system session capacity
- Session Capacity: (this value will vary based on individual requirements)
- Enter [2] : to enabled advanced feature set
- Advanced : enabled
- Enter [s] : Saves your session capacity and enables Advanced feature set on the OCSBC
- show features : verify the session capacity and feature set through the ACLI



```
SRG-SBC-1# setup entitlements

----------------------------------------------------------------
Entitlements for Enterprise Session Border Controller
Last Modified: 2022-03-29 03:54:06
----------------------------------------------------------------
 1 : Session Capacity                              : 512000
 2 :   Advanced                                    : enabled
 3 :   STIR/SHAKEN Client                          :
 4 : Admin Security                                :
 5 : Data Integrity (FIPS 140-2)                   :
 6 : Transcode Codec AMR                           :
 7 : Transcode Codec AMR Capacity                  : 0
 8 : Transcode Codec AMRWB                         :
 9 : Transcode Codec AMRWB Capacity                : 0
 10: Transcode Codec EVS                           :
 11: Transcode Codec EVS Capacity                  : 0
 12: Transcode Codec OPUS Capacity                 : 0
 13: Transcode Codec SILK Capacity                 : 0

Enter 1 - 13 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Session Capacity (0-512000)                      : 512000

Enter 1 - 13 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2

    Advanced (enabled/disabled)                    : enabled

Enter 1 - 13 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
SAVE SUCCEEDED
SRG-SBC-1#
SRG-SBC-1# show features
Total session capacity: 512000
Enabled features:
        512000 sessions, SIP, H323, IWF, QOS, ACP, Routing, Load Balancing,
        Accounting, High Availability, ENUM, NSEP RPH, DoS,
        IPv4-v6 Interworking, IDS, IDS Advanced, Session Recording,
        Fraud Protection, BFD
SRG-SBC-1#
```

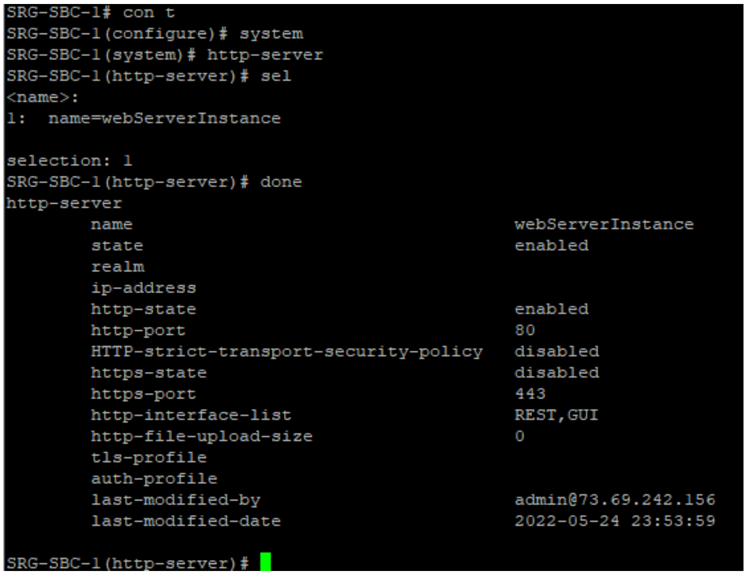
Note: You may also enable additional security features and transcodable codec capacity through entitlements, but that is outside the scope of this document.

7.1.3 OCSBC Web Server Config

To enable access the OCSBC GUI to complete the configuration and setup, you will need to enable the web server config through the ACLI.

ACLI Path: config t→system→http-server

- select : to select the configuration object
- done : to complete the changes made to the configuration object
- Back out of configuration mode, and save and activate the config



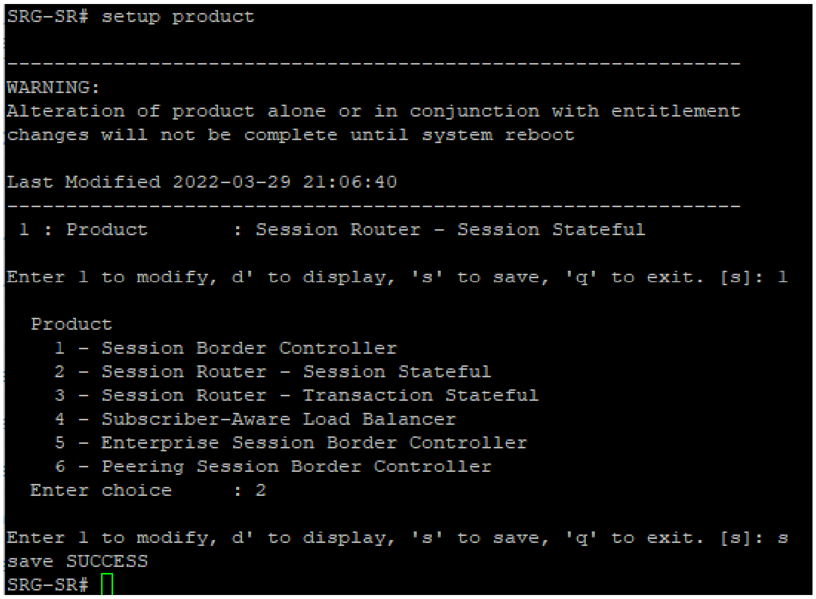
```
SRG-SBC-1# con t
SRG-SBC-1(configure)# system
SRG-SBC-1(system)# http-server
SRG-SBC-1(http-server)# sel
<name>:
1:  name=webServerInstance

selection: 1
SRG-SBC-1(http-server)# done
http-server
        name                                    webServerInstance
        state                                   enabled
        realm
        ip-address
        http-state                              enabled
        http-port                               80
        HTTP-strict-transport-security-policy   disabled
        https-state                             disabled
        https-port                              443
        http-interface-list                     REST,GUI
        http-file-upload-size                   0
        tls-profile
        auth-profile
        last-modified-by                        admin@73.69.242.156
        last-modified-date                      2022-05-24 23:53:59

SRG-SBC-1(http-server)#
```

Note: Configuring access to the OCSBC GUI via secure HTTP is outside the scope of this document. For additional details on how to configure, please refer to the Configuration Guide, accessible from the Related Documents section of this guide.

You will now be able to open a web browser, enter the public IP address (or optional DNS label name if configured) of the management interface and access the GUI on each OCSBC deployed.

7.1.4 OCSR Product Setup

- setup product
- enter [1] : to modify or add the entry
- Enter Choice: Choose [2] for Session Router – Session Stateful
- Enter [s] : Saves your product choice

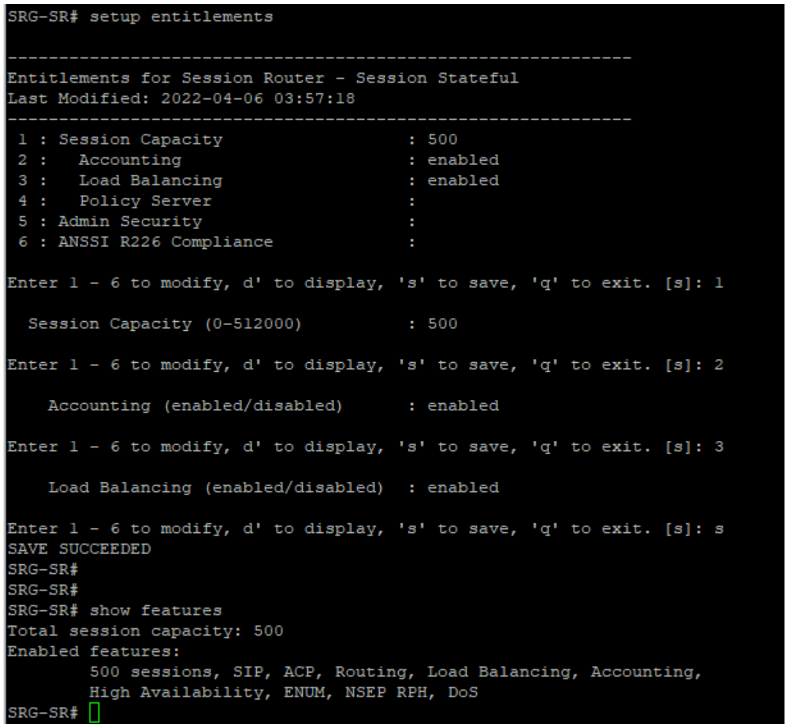


```
SRG-SR# setup product

--------------------------------------------------------------
WARNING:
Alteration of product alone or in conjunction with entitlement
changes will not be complete until system reboot

Last Modified 2022-03-29 21:06:40
--------------------------------------------------------------
 1 : Product       : Session Router - Session Stateful

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Product
    1 - Session Border Controller
    2 - Session Router - Session Stateful
    3 - Session Router - Transaction Stateful
    4 - Subscriber-Aware Load Balancer
    5 - Enterprise Session Border Controller
    6 - Peering Session Border Controller
  Enter choice     : 2

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
save SUCCESS
SRG-SR# 
```

7.1.5 OCSR Entitlement (feature) Setup

While in enable mode of the ACLI, type

- setup entitlements
- enter [1] : to modify or add system session capacity
- Session Capacity: (this value will vary based on individual requirements)
- Enter [2] : to enabled accounting config (optional)
- Enter [3] : to enabled Load Balancing
- Load Balancing: enabled
- Enter [s] : Saves your session capacity and enables Advanced feature set on the OCSBC
- show features : verify the session capacity and feature set through the ACLI



```
SRG-SR# setup entitlements

-------------------------------------------------------------
Entitlements for Session Router - Session Stateful
Last Modified: 2022-04-06 03:57:18
-------------------------------------------------------------
 1 : Session Capacity                    : 500
 2 :   Accounting                        : enabled
 3 :   Load Balancing                    : enabled
 4 :   Policy Server                     :
 5 : Admin Security                      :
 6 : ANSSI R226 Compliance               :

Enter 1 - 6 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Session Capacity (0-512000)            : 500

Enter 1 - 6 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2

    Accounting (enabled/disabled)        : enabled

Enter 1 - 6 to modify, d' to display, 's' to save, 'q' to exit. [s]: 3

    Load Balancing (enabled/disabled)    : enabled

Enter 1 - 6 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
SAVE SUCCEEDED
SRG-SR#
SRG-SR#
SRG-SR# show features
Total session capacity: 500
Enabled features:
        500 sessions, SIP, ACP, Routing, Load Balancing, Accounting,
        High Availability, ENUM, NSEP RPH, DoS
SRG-SR#
```

Note: You may also enable additional security and platform features through entitlements, but those are outside the scope of this document.

The Oracle Communications Session Router does not have an embedded GUI for configuration or management, so there is no web-server-config element that requires enablement on this product.

8. OCSBC Configuration

There are two options available to configure the Oracle Communications Session Border Controller. One is by accessing the ACLI through either SSH or Console. The other is through the OCSBC GUI, accessible via a web browser. For the purposes of this guide, we will be using the OCSBC Web GUI to configure the system.

Once you access the OCSBC GUI via a web browser, at the top, you will see a configuration tab. Click on that tab to access the configuration menu, on the left hand side.

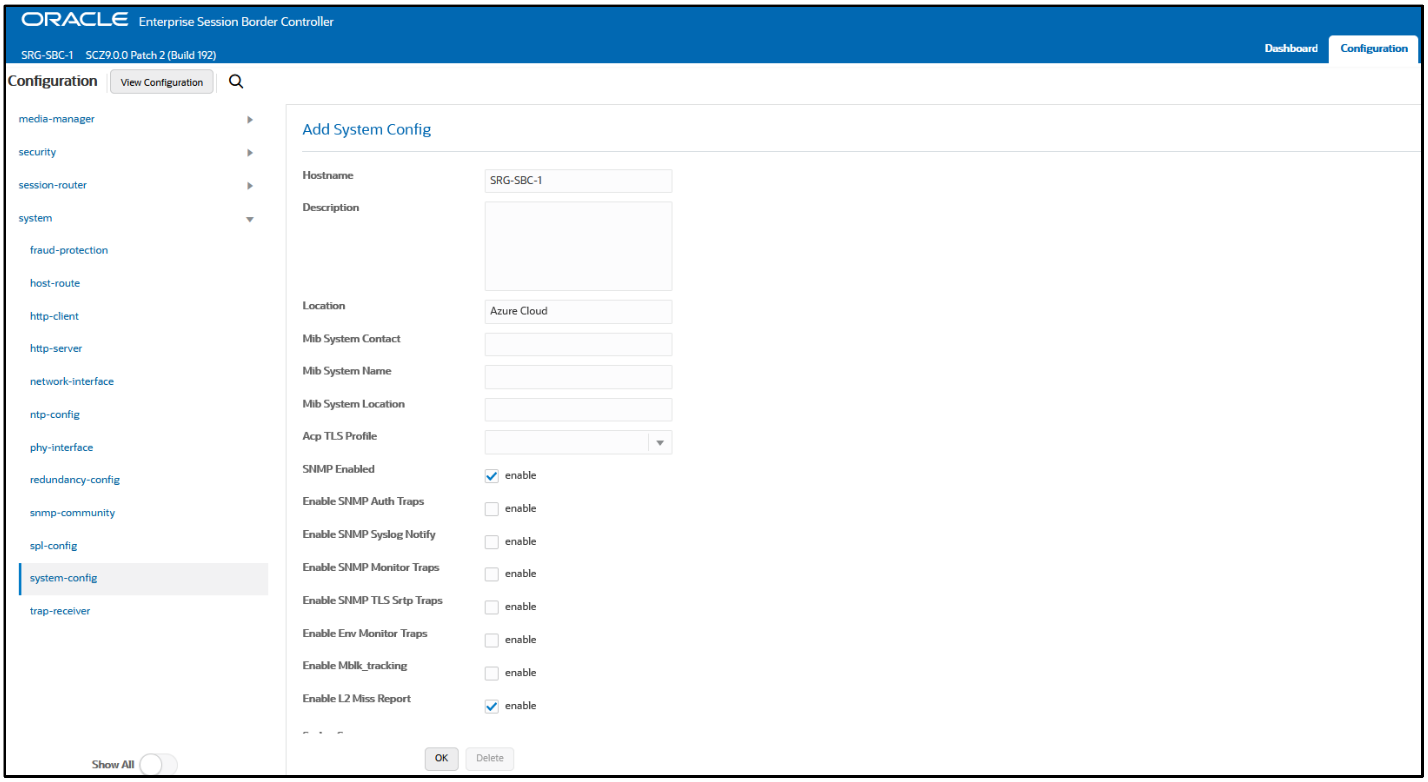
8.1 Global Configuration Elements

8.1.1 System-Config

Path: system➔system-config

The global system config must be enabled by accessing it, and clicking OK, but there are no mandatory configuration changes in this element. Those outlined below are optional.

- Hostname:
- Location:
- When Finished, click the [OK] tab at the bottom of the screen



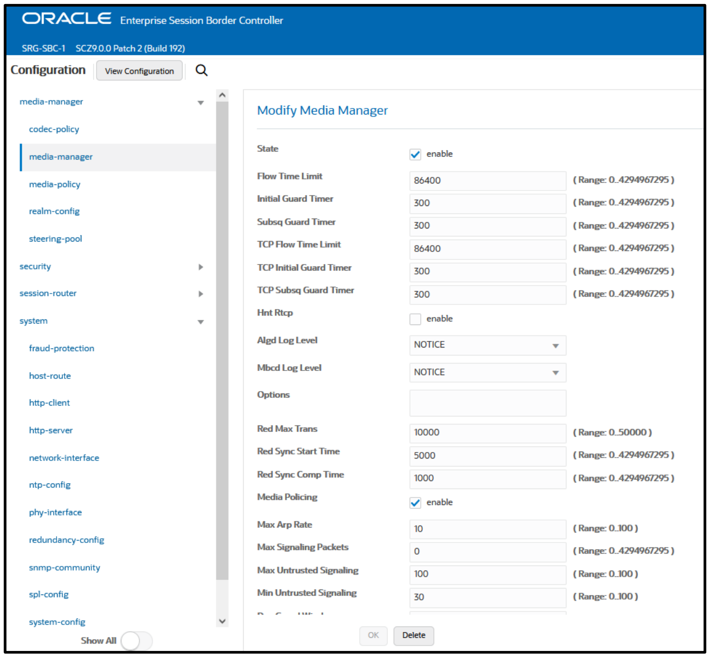
Add System Config

Hostname	SRG-SBC-1
Description	
Location	Azure Cloud
Mib System Contact	
Mib System Name	
Mib System Location	
Acp TLS Profile	
SNMP Enabled	☑ enable
Enable SNMP Auth Traps	☐ enable
Enable SNMP Syslog Notify	☐ enable
Enable SNMP Monitor Traps	☐ enable
Enable SNMP TLS Srtp Traps	☐ enable
Enable Env Monitor Traps	☐ enable
Enable Mblk_tracking	☐ enable
Enable L2 Miss Report	☑ enable

8.1.2 Media Manager

Path: media-manager➔media-manager

There are no required configuration changes to this element, but it must be enabled in order for the SBC to handle media. To enable it, you must access the global element and click “OK” tab at the bottom of the screen:



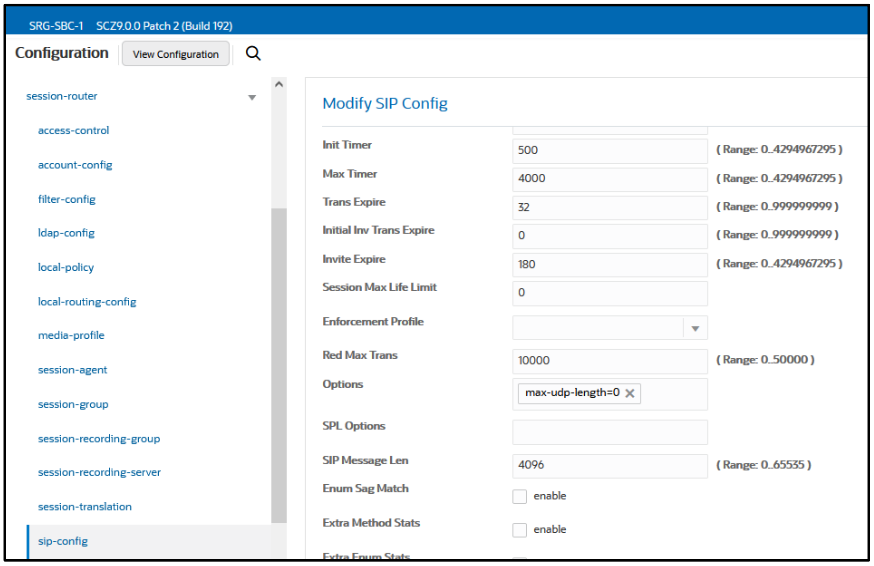
Modify Media Manager

State	☑ enable	
Flow Time Limit	86400	(Range: 0..4294967295)
Initial Guard Timer	300	(Range: 0..4294967295)
Subsq Guard Timer	300	(Range: 0..4294967295)
TCP Flow Time Limit	86400	(Range: 0..4294967295)
TCP Initial Guard Timer	300	(Range: 0..4294967295)
TCP Subsq Guard Timer	300	(Range: 0..4294967295)
Hnt Rtcp	☐ enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	
Options		
Red Max Trans	10000	(Range: 0..50000)
Red Sync Start Time	5000	(Range: 0..4294967295)
Red Sync Comp Time	1000	(Range: 0..4294967295)
Media Policing	☑ enable	
Max Arp Rate	10	(Range: 0..100)
Max Signaling Packets	0	(Range: 0..4294967295)
Max Untrusted Signaling	100	(Range: 0..100)
Min Untrusted Signaling	30	(Range: 0..100)

8.1.3 Sip-Config

Path: session-router➔sip-config

- Under Options, click add
- Configuration dialog box pops up, add “max-udp-length=0” click OK
- Click OK tab at the bottom of the screen



Modify SIP Config

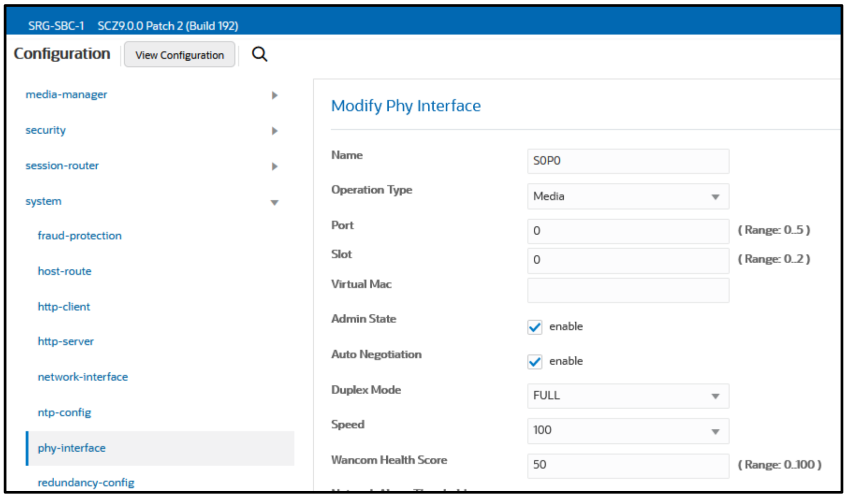
Init Timer	500	(Range: 0..4294967295)
Max Timer	4000	(Range: 0..4294967295)
Trans Expire	32	(Range: 0..999999999)
Initial Inv Trans Expire	0	(Range: 0..999999999)
Invite Expire	180	(Range: 0..4294967295)
Session Max Life Limit	0	
Enforcement Profile		
Red Max Trans	10000	(Range: 0..50000)
Options	max-udp-length=0 ✕	
SPL Options		
SIP Message Len	4096	(Range: 0..65535)
Enum Sag Match	□ enable	
Extra Method Stats	□ enable	
Extra Enum Stats		

8.2 Physical Interfaces

Configure two network interfaces on each OCSBC being deployed, S0P0 and S1P0

Path: system➔phy-interface

- At the top of the screen, click Add
- Name: S0P0
- Operation Type: Media (drop down box)
- Click OK at the bottom

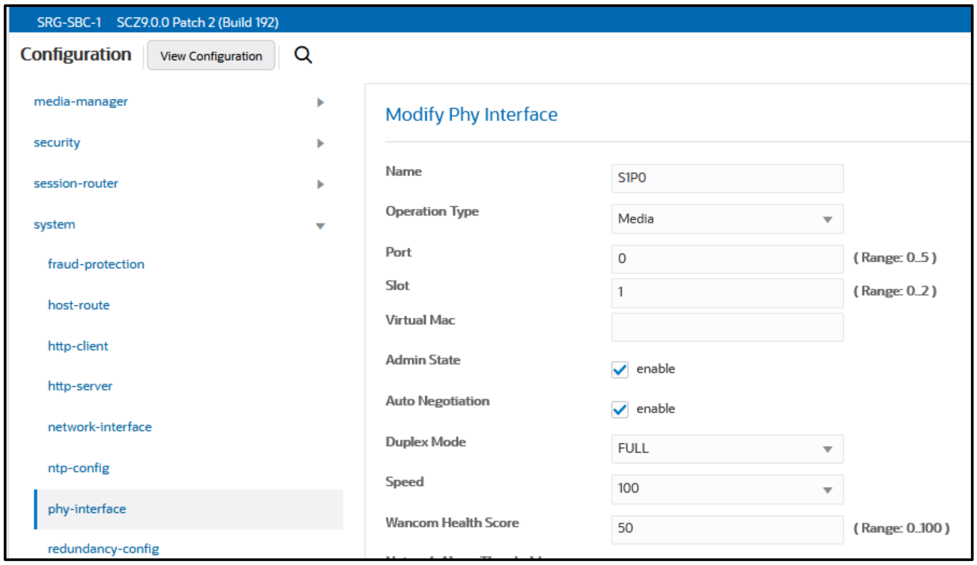


Modify Phy Interface

Name	S0P0	
Operation Type	Media	
Port	0	(Range: 0..5)
Slot	0	(Range: 0..2)
Virtual Mac		
Admin State	☑ enable	
Auto Negotiation	☑ enable	
Duplex Mode	FULL	
Speed	100	
Wancom Health Score	50	(Range: 0..100)

To add a second physical interface, at the top, click Add

- Name: S1P0
- Operation Type: Media (drop down box)
- Slot: [1]
- Click OK at the bottom of the screen



Modify Phy Interface

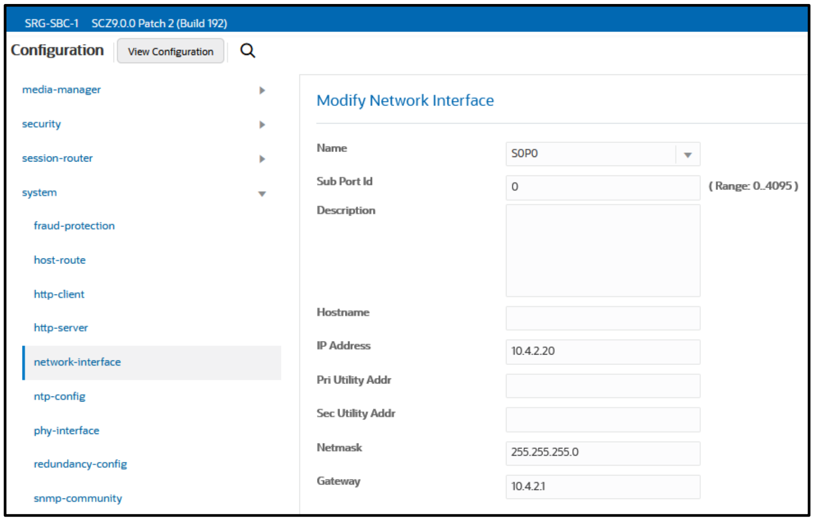
Name	S1P0	
Operation Type	Media	
Port	0	(Range: 0..5)
Slot	1	(Range: 0..2)
Virtual Mac		
Admin State	☑ enable	
Auto Negotiation	☑ enable	
Duplex Mode	FULL	
Speed	100	
Wancom Health Score	50	(Range: 0..100)

8.3 Network Interfaces

Configure two network interfaces on each SBC being deployed, S0P0:0 and S1P0:0

Path: system➔network-interface

- Name: S0P0 (drop down box)
- IP address: (private IP address assigned to S0P0 interface)
- Netmask: (netmask for the assigned network)
- Gateway: (gateway for the network)
- Click OK at the bottom of the screen

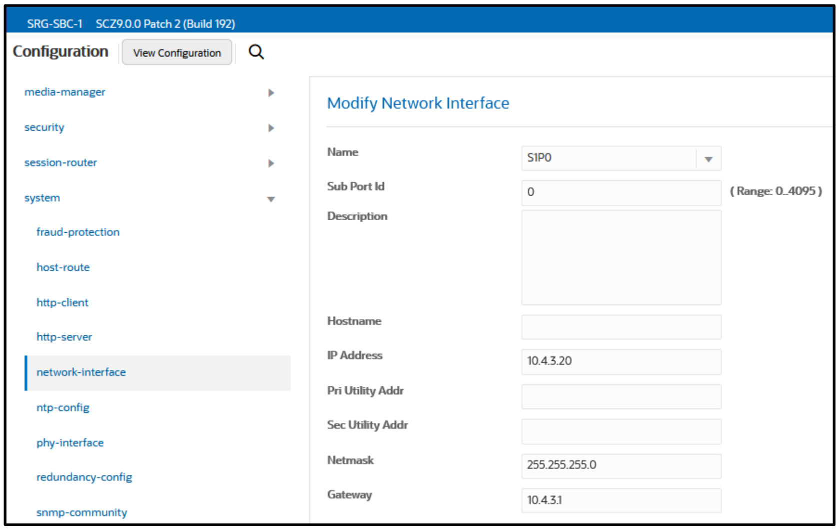


Modify Network Interface

Name	S0P0	
Sub Port Id	0	(Range: 0..4095)
Description		
Hostname		
IP Address	10.4.2.20	
Pri Utility Addr		
Sec Utility Addr		
Netmask	255.255.255.0	
Gateway	10.4.2.1	

To add the second network-interface, click Add at the top of the screen

- Name: S1P0 (drop down box)
- IP Address: (private ip address assigned to S1P0 interface)
- Netmask: (netmask for the assigned network)
- Gateway: (gateway for the network)
- Click OK at the bottom of the screen



Modify Network Interface

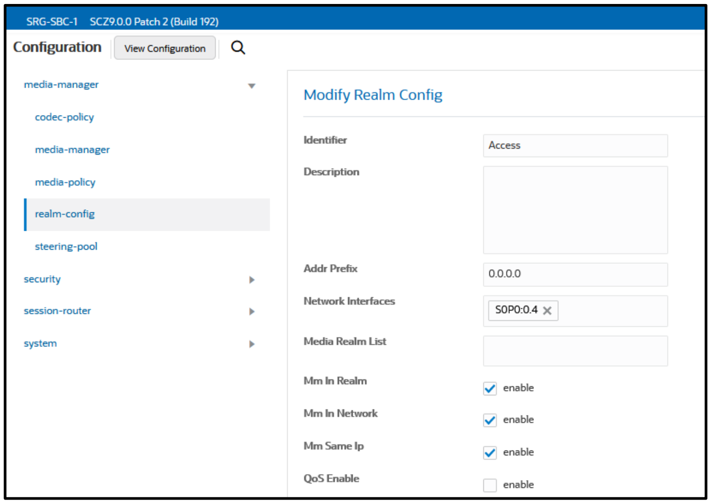
Name	S1P0	
Sub Port Id	0	(Range: 0..4095)
Description		
Hostname		
IP Address	10.4.3.20	
Pri Utility Addr		
Sec Utility Addr		
Netmask	255.255.255.0	
Gateway	10.4.3.1	

8.4 Realm Config

Configure two realms, Access and Core, each assigned to one of the network interfaces configured in prior step.

Path: media-manager➔realm-config

- Identifier: Access
- Network Interfaces: Click Add, in pop up dialog, choose S0P0:0 from drop down
- Mm in Realm: Check box
- Access control trust level: (Recommendation is High for Peering Environment)
- Click OK at the bottom

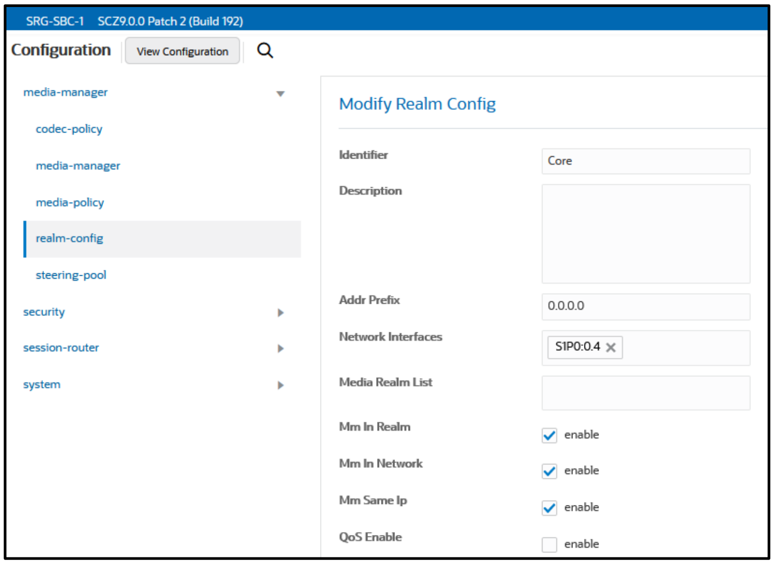


Modify Realm Config

Identifier	Access
Description	
Addr Prefix	0.0.0.0
Network Interfaces	S0P0:4 ✕
Media Realm List	
Mm In Realm	☑ enable
Mm In Network	☑ enable
Mm Same Ip	☑ enable
QoS Enable	□ enable

To add the second realm to the config, click Add at the top of the screen

- Identifier: Core
- Network Interfaces: Click Add, in pop up dialog, choose S1P0:0 from drop down
- Mm in Realm: Check box
- Access control trust level: Select high from drop down box
- Click OK at the bottom



Modify Realm Config

Identifier: Core

Description:

Addr Prefix: 0.0.0.0

Network Interfaces: S1P0:0.4 ✕

Media Realm List:

Mm In Realm: ☑ enable

Mm In Network: ☑ enable

Mm Same Ip: ☑ enable

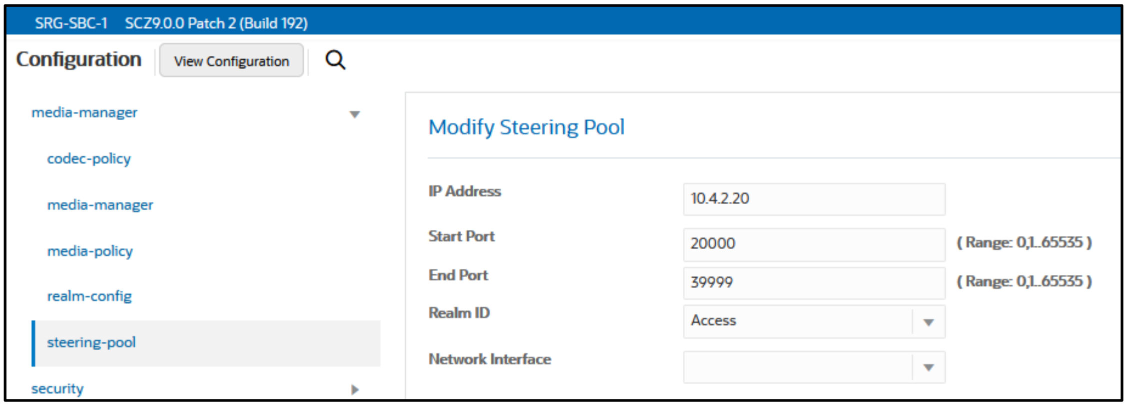
QoS Enable: □ enable

8.5 Steering Pools

Configure two steering pools, one per realm. These are the UDP port ranges the sbc uses for media. Please verify when configuring these port ranges, the Network Security Groups configured and assigned to your network interfaces allow traffic on these ports.

Path: media-manger➔steering-pool

- IP address: (ip used to send and receive media) (in this example, 10.4.2.20)
- Start Port: 20000
- End Port: 39999
- Realm ID: Access (selected from drop down menu)
- Click OK at the bottom



Modify Steering Pool

IP Address: 10.4.2.20

Start Port: 20000 (Range: 0,1..65535)

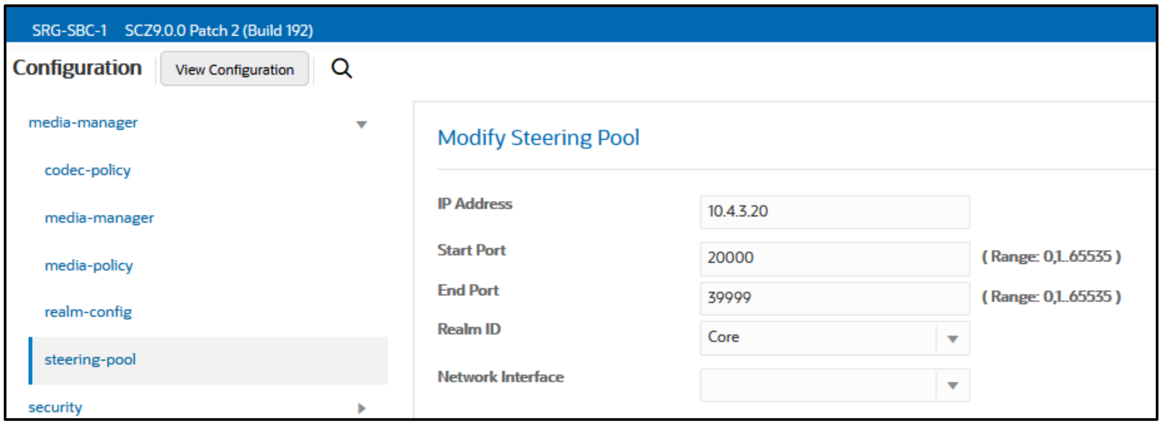
End Port: 39999 (Range: 0,1..65535)

Realm ID: Access

Network Interface:

Add a second Steering pool for the Core Realm. Start by Clicking Add at the top of the screen.

- IP Address: (ip used to send and receive media) (in this example, 10.4.3.20)
- Start Port: 20000
- End Port: 39999
- Realm ID: Core (selected from drop down menu)
- Click OK at the bottom



Modify Steering Pool

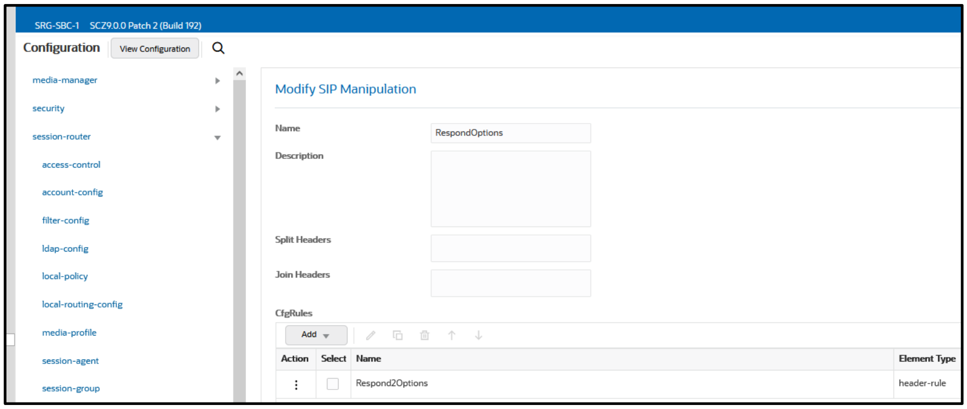
IP Address: 10.4.3.20
Start Port: 20000 (Range: 0,1..65535)
End Port: 39999 (Range: 0,1..65535)
Realm ID: Core
Network Interface:

8.6 Sip Manipulation

The following sip manipulation forces the OCSBC to respond locally to Sip OPTIONS ping being sent by the OCSR.

Path: session-router➔sip-manipulation

- Name: RespondOptions
- CfgRules: Add (dropdown), select header-rule
  Under header rule configuration
  - Name: Resond2Options
  - Header-Name: From
  - Action: Reject
  - Methods: Click Add, then enter OPTIONS
  - New value: 200 OK
- Click OK at the bottom
- Click Back at the bottom



Modify SIP Manipulation

Name: RespondOptions
Description:
Split Headers:
Join Headers:

CfgRules

Action	Select	Name	Element Type
⋮	□	Respond2Options	header-rule

8.7 Sip-Interfaces

Sip interfaces is what the SBC uses to send and receiving signaling packets. Configure one per realm.

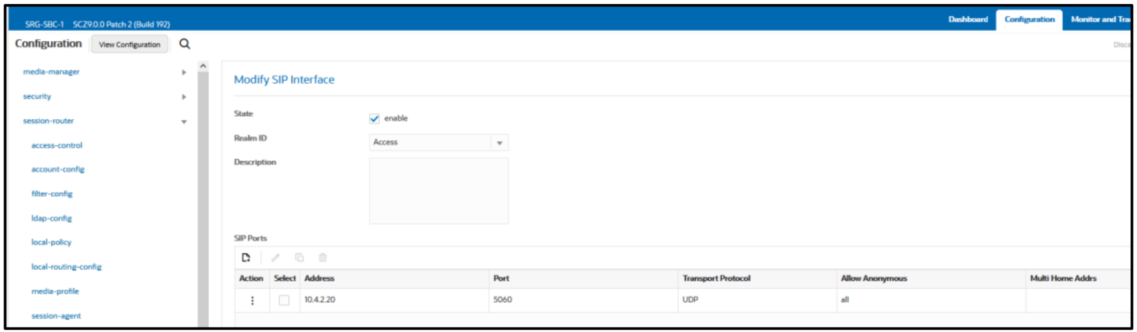
Path: session-router➔sip-interface

- Realm ID: Access (selected from drop down)
- Spl Options: HeaderNatPublicSipIfIp=<PublicIP>,HeaderNatPrivateSipIfIp=<PrivateIP>
- Sip Ports: Click Add

For more information on the necessity of the above Spl Option when deploying the SBC in a public cloud or behind a NAT, please see Appendix A

- The following parameters are found under the Sip Port configuration

  - Address: IP address used to send and receive signaling packets
  - Port: Source and Destination Port for signaling
  - Transport Protocol: Transport used for signaling
  - Allow Anonymous: Agents Only
  - Click OK at the bottom to get back to Sip Interface Config
  - Hit Back at the bottom of the screen



Modify SIP Interface

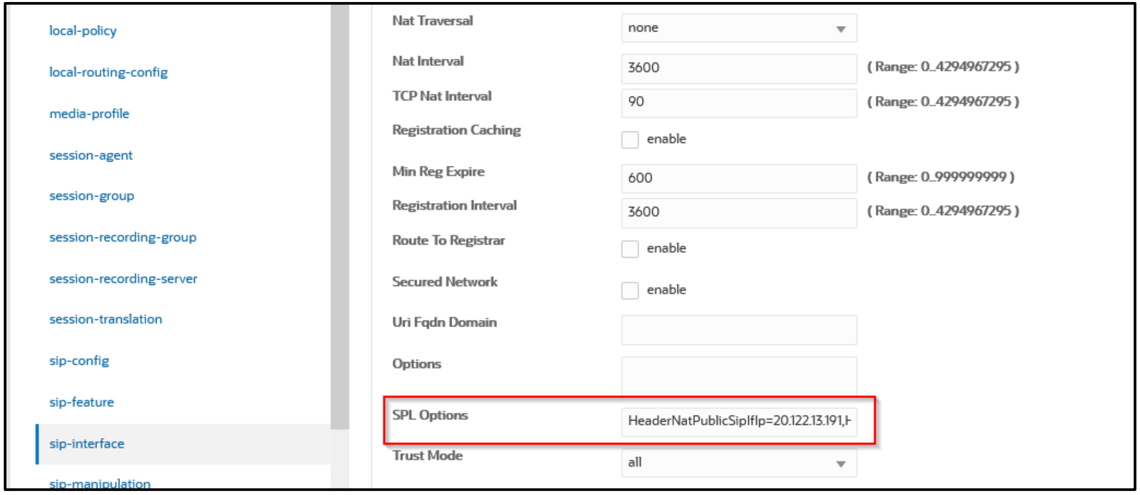
State ☑ enable

Realm ID Access

Description

SIP Ports

Action	Select	Address	Port	Transport Protocol	Allow Anonymous	Multi Home Addrs
⋮	□	10.4.2.20	5060	UDP	all	



Nat Traversal none

Nat Interval 3600 (Range: 0..4294967295)

TCP Nat Interval 90 (Range: 0..4294967295)

Registration Caching □ enable

Min Reg Expire 600 (Range: 0..999999999)

Registration Interval 3600 (Range: 0..4294967295)

Route To Registrar □ enable

Secured Network □ enable

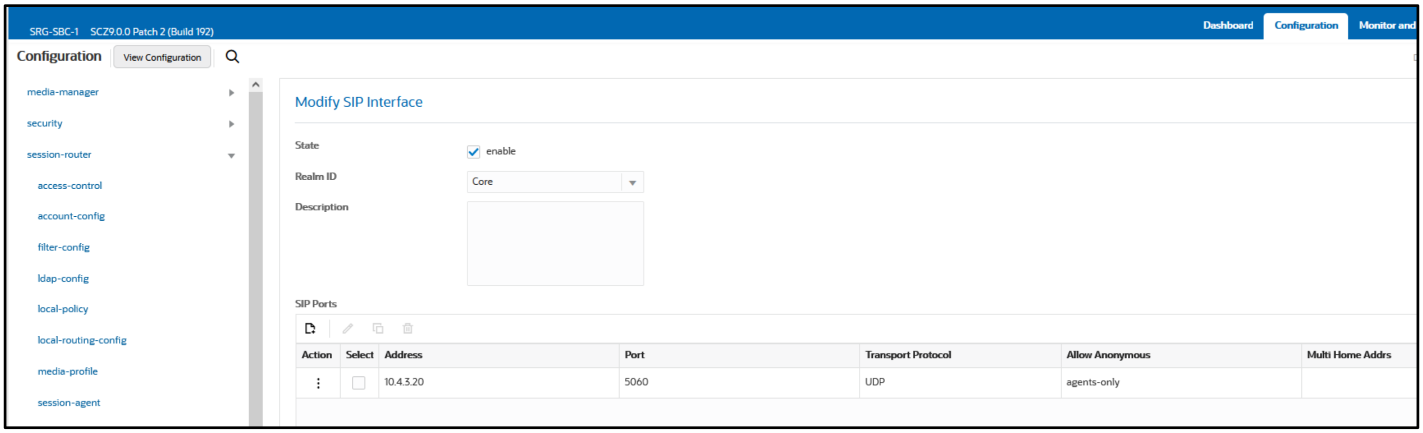
Uri Fqdn Domain

Options

SPL Options HeaderNatPublicSipIfIp=20.122.13.191,H

Trust Mode all

Add a second sip interface for the core realm, makes the necessary changes to allow the “Core” side of the SBC to handle signaling traffic.

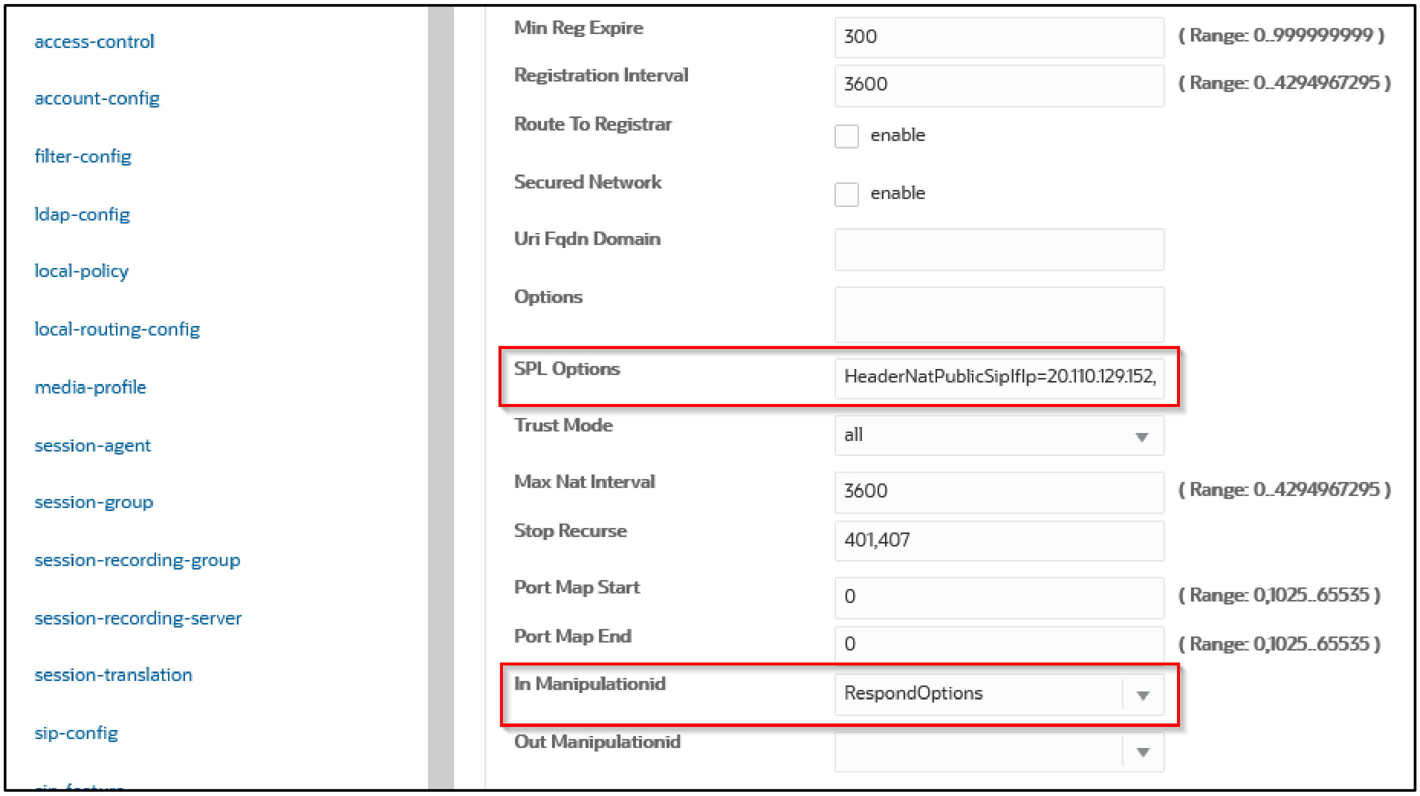


Modify SIP Interface

State	☑ enable
Realm ID	Core
Description	

SIP Ports

Action	Select	Address	Port	Transport Protocol	Allow Anonymous	Multi Home Addrs
⋮	□	10.4.3.20	5060	UDP	agents-only	



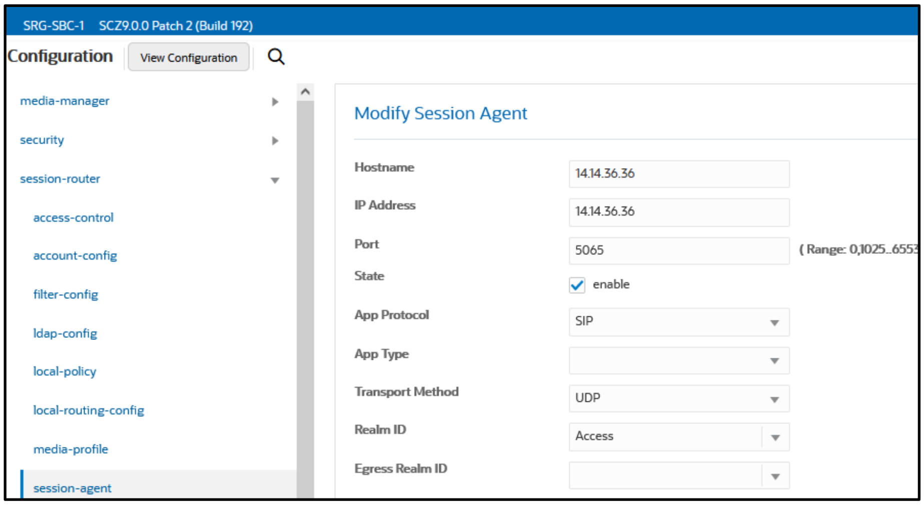
Min Reg Expire	300	(Range: 0..999999999)
Registration Interval	3600	(Range: 0..4294967295)
Route To Registrar	□ enable	
Secured Network	□ enable	
Uri Fqdn Domain		
Options		
SPL Options	HeaderNatPublicSipIfIp=20.110.129.152,	
Trust Mode	all	
Max Nat Interval	3600	(Range: 0..4294967295)
Stop Recurse	401,407	
Port Map Start	0	(Range: 0,1025..65535)
Port Map End	0	(Range: 0,1025..65535)
In Manipulationid	RespondOptions	
Out Manipulationid		

8.8 Session Agent

Session-agents are config elements, which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. Configure two session agents, one for interface on the OCSR's and other for going towards sip-trunk.

Path: session-router➔session-agent

- Hostname: Hostname given to this session agent, can be unique string, or match the configured IP address
- IP address:
- Port Number:
- Transport: Select from Drop down
- Realm ID:



Modify Session Agent

Hostname: 14.14.36.36
IP Address: 14.14.36.36
Port: 5065 (Range: 0,1025..6553
State: ☑ enable
App Protocol: SIP
App Type:
Transport Method: UDP
Realm ID: Access
Egress Realm ID:

Follow the same procedure to create one more session agent for interface configured on the Oracle Session Router. For the purposes of this example config, the required configuration fields will have the following information populated:

OCSR & Sip Interface	Hostname	IP Address	Realm ID
SRG-SR, Private	10.4.3.40	10.4.3.40	Core

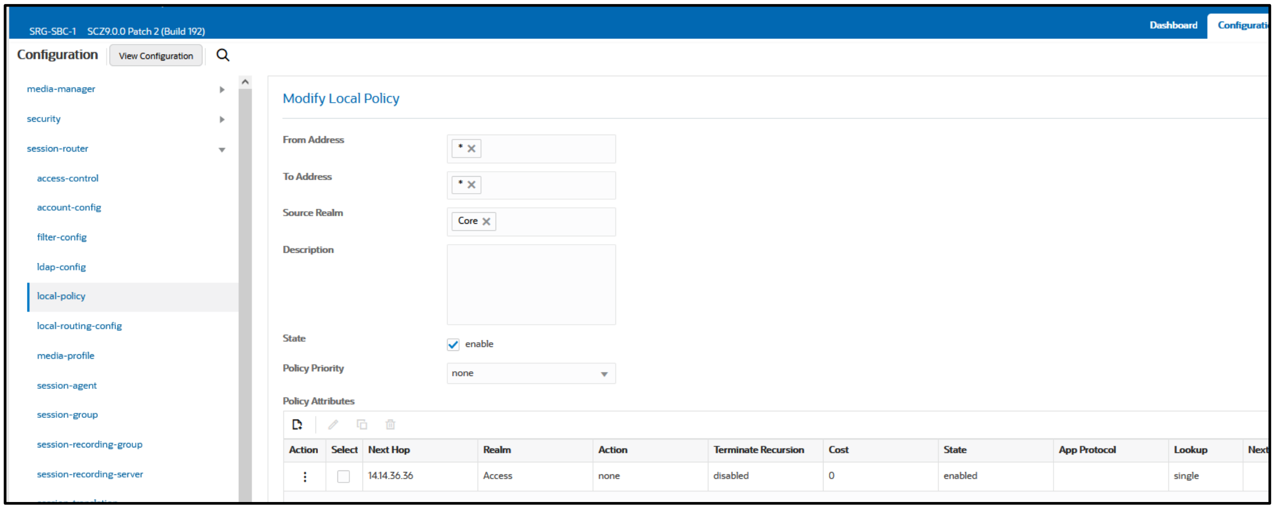
Note: You may need to configure additional session agents, depending on your environments requirements and next hop routing

8.9 Local-Policy

Local policy config allows the SBC to route calls from one end of the network to the other based on routing criteria. Create two local polices to route sip traffic from Access realm to Core realm, and from Core realm to Access Realm.

To configure local-policy, Navigate to Session-Router->local-policy
Path: session-router->local-policy

To route the calls from SR side to SBC side, Use the below local–policy.

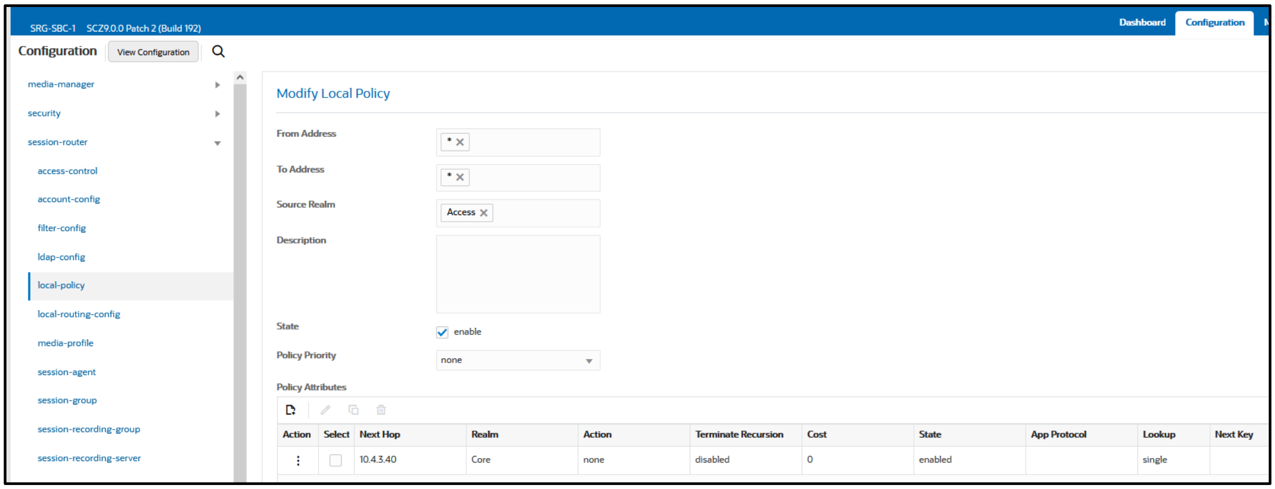


Modify Local Policy

From Address: * ×
To Address: * ×
Source Realm: Core ×
Description:
State: ☑ enable
Policy Priority: none
Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next
⋮	□	14.14.36.36	Access	none	disabled	0	enabled		single	

To route the calls from the SBC side to SR side, Use the below local–policy.



SRG-SBC-1 SCZ9.0.0 Patch 2 (Build 192)

Modify Local Policy

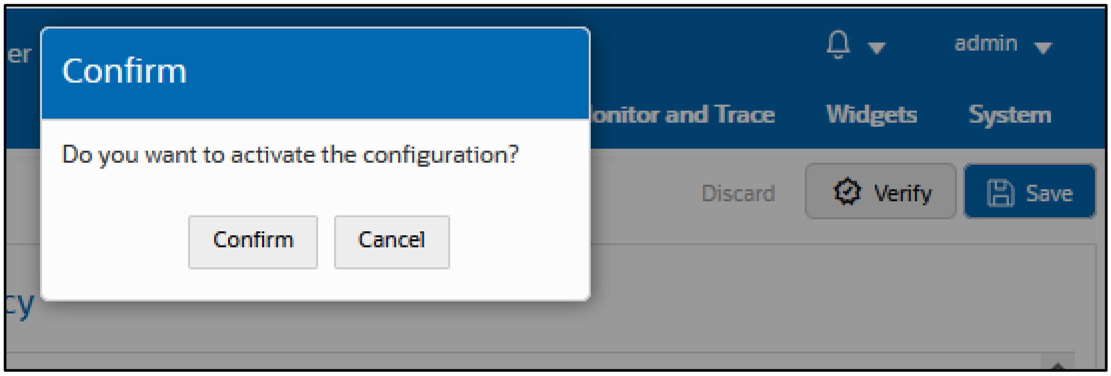
From Address	* ✕
To Address	* ✕
Source Realm	Access ✕
Description	
State	☑ enable
Policy Priority	none

Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
⋮	□	10.4.3.40	Core	none	disabled	0	enabled		single	

8.10 Save and Activate

At this point, we have completed the OCSBC basic configuration. On the top left of the screen, click Save, then Activate.



Confirm

Do you want to activate the configuration?

Now proceed with setting up and configuring a second OCSBC required for this deployment model!

9. OCSR Configuration

Oracle Communications Session Router provides high-performance SIP routing with scalable routing policies that increase overall network capacity and reduce costs. It plays a central role in Oracle's open session routing (OSR) architecture and helps customers build a scalable, next-generation signaling core for SIP-based services

In this deployment, the OCSR will be utilized to distribute SIP traffic evenly to multiple OCSBC's. This traffic distribution decreases the amount of production traffic a single OCSBC is required to handle, thus eliminating the impact in the event of a service disruption.

As mentioned previously in this application note, the Oracle Communication Session Router does not have a GUI we can utilize for configuration like the Oracle Communications Session Border Controller, so we must configure this device through the ACLI interface, which can be access via a SSH remote session, or through the Azure serial console.

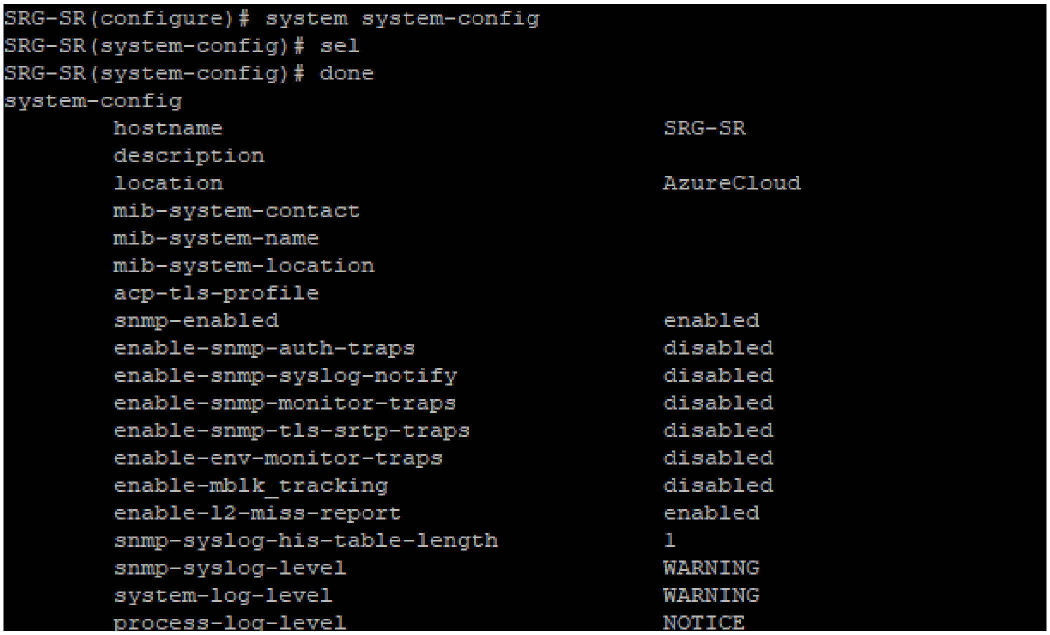
As we go through the steps to configure the OCSR, please remember that each element needs to be "selected" in the ACLI for additions or changes to be made. This is accomplished by typing "select" after entering the object by following the ACLI path outlined at the beginning of each element heading below.

9.1 Global Configuration Elements

9.1.1 System Config

ACLI Path: config t➔system➔system-config

The system configuration element must be enabled, although there are no necessary changes required. It's enabled by selecting it, and then issuing a "done".



```
SRG-SR(configure)# system system-config
SRG-SR(system-config)# sel
SRG-SR(system-config)# done
system-config
        hostname                                SRG-SR
        description
        location                                AzureCloud
        mib-system-contact
        mib-system-name
        mib-system-location
        acp-tls-profile
        snmp-enabled                            enabled
        enable-snmp-auth-traps                  disabled
        enable-snmp-syslog-notify               disabled
        enable-snmp-monitor-traps               disabled
        enable-snmp-tls-srtp-traps              disabled
        enable-env-monitor-traps                disabled
        enable-mblk_tracking                    disabled
        enable-l2-miss-report                   enabled
        snmp-syslog-his-table-length            1
        snmp-syslog-level                       WARNING
        system-log-level                        WARNING
        process-log-level                       NOTICE
```

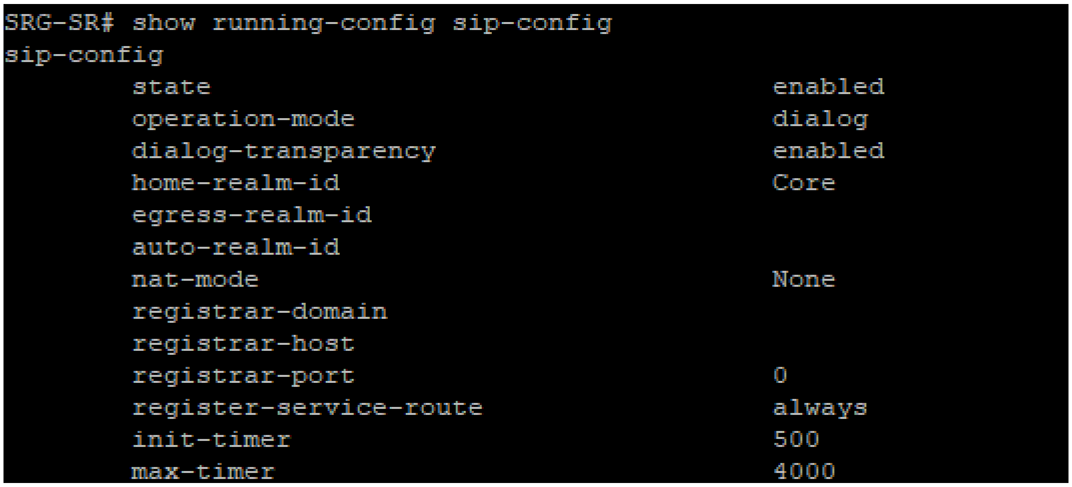
9.1.2 Sip Config

ACLI Path: config t➔session-router➔sip-config

Similar to the system config above, this must be enabled by selecting it, and issuing the “done” command. There are no required configuration changes from the default values.

We do however recommend assigning a value to the home realm ID, so if you have pre planned your realm identifiers, you can enter at this time. If not, you can enter a value in this parameter at any time in the future.

The home realm ID will be the realm the SBC uses to source a packet if there are no other options available through other configuration elements.



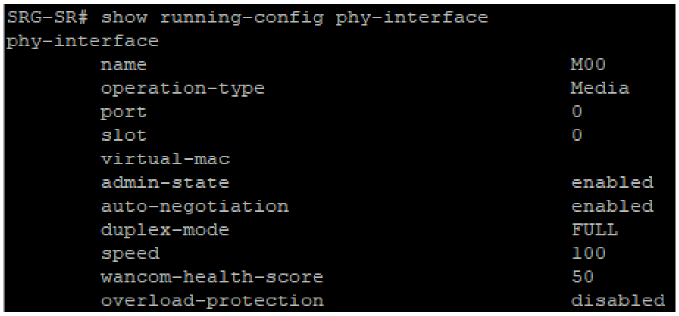
```
SRG-SR# show running-config sip-config
sip-config
        state                                   enabled
        operation-mode                          dialog
        dialog-transparency                     enabled
        home-realm-id                           Core
        egress-realm-id
        auto-realm-id
        nat-mode                                None
        registrar-domain
        registrar-host
        registrar-port                          0
        register-service-route                  always
        init-timer                              500
        max-timer                               4000
```

9.2 Physical Interfaces

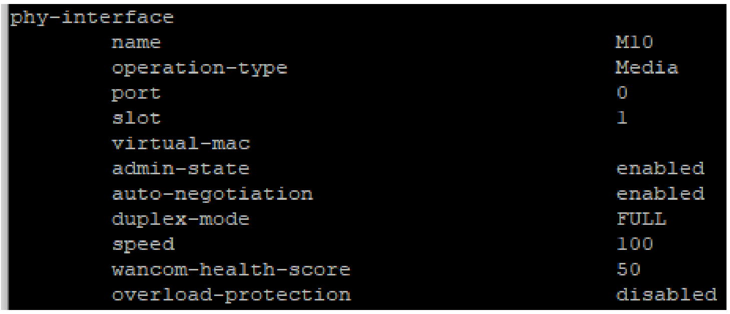
Configure two Physical Interfaces on each OCSR being setup

ACLI Path: config t➔system➔phy-interface

- Name
- Operation Type
- Slot
- Port



```
SRG-SR# show running-config phy-interface
phy-interface
        name                                    M00
        operation-type                          Media
        port                                    0
        slot                                    0
        virtual-mac
        admin-state                             enabled
        auto-negotiation                        enabled
        duplex-mode                             FULL
        speed                                   100
        wancom-health-score                     50
        overload-protection                     disabled
```

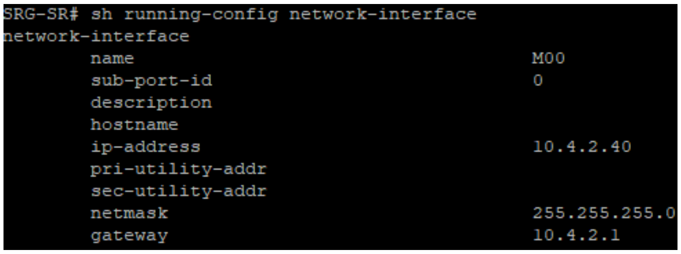


```
phy-interface
        name                                    M10
        operation-type                          Media
        port                                    0
        slot                                    1
        virtual-mac
        admin-state                             enabled
        auto-negotiation                        enabled
        duplex-mode                             FULL
        speed                                   100
        wancom-health-score                     50
        overload-protection                     disabled
```

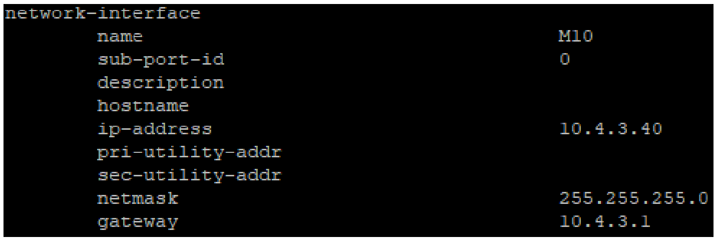
9.3 Network Interfaces

Configure two network interfaces, each associated with a physical interface already configured.

- Name
- Sub-port-id
- IP-address
- netmask
- gateway



```
SRG-SR# sh running-config network-interface
network-interface
        name                                            M00
        sub-port-id                                     0
        description
        hostname
        ip-address                                      10.4.2.40
        pri-utility-addr
        sec-utility-addr
        netmask                                         255.255.255.0
        gateway                                         10.4.2.1
```



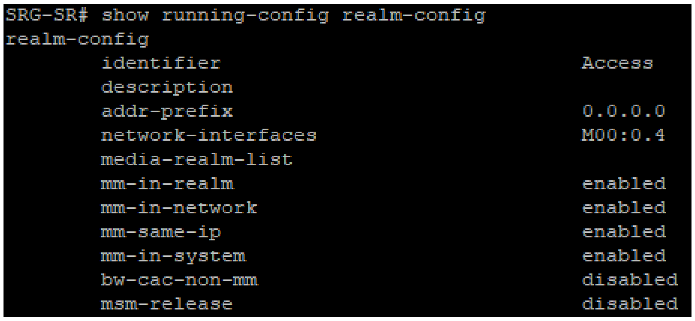
```
network-interface
        name                                            M10
        sub-port-id                                     0
        description
        hostname
        ip-address                                      10.4.3.40
        pri-utility-addr
        sec-utility-addr
        netmask                                         255.255.255.0
        gateway                                         10.4.3.1
```

9.4 Realm Config

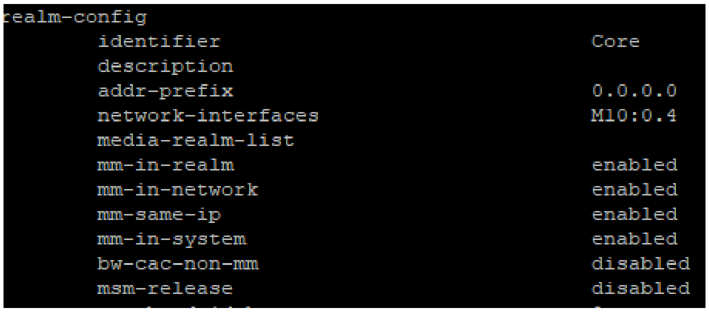
Configure two realms, Access and Core, each assigned to one of the network interfaces configured in prior step.

Navigate to realm-config under media-manager and configure a realm as shown below.
ACLI Path: config t->media-manger->realm-config

In the below case, Realm name is given as Access & Core. Please set the Access Control Trust Level as high for these realms.



```
SRG-SR# show running-config realm-config
realm-config
        identifier                                      Access
        description
        addr-prefix                                     0.0.0.0
        network-interfaces                              M00:0.4
        media-realm-list
        mm-in-realm                                     enabled
        mm-in-network                                   enabled
        mm-same-ip                                      enabled
        mm-in-system                                    enabled
        bw-cac-non-mm                                   disabled
        msm-release                                     disabled
```



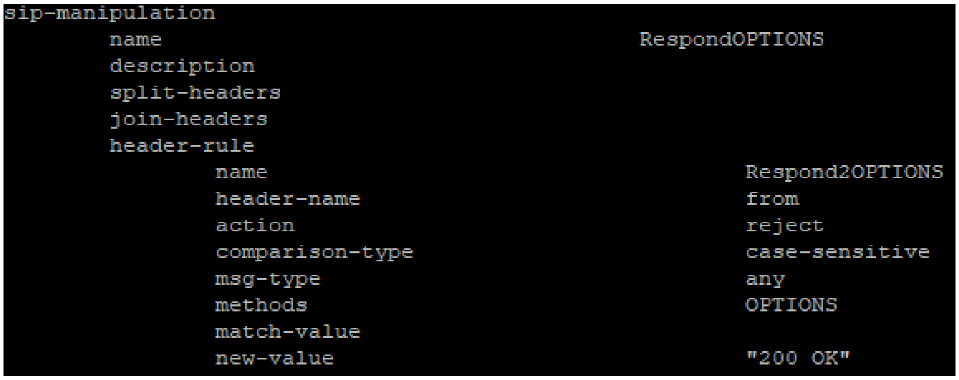
```
realm-config
        identifier                                      Core
        description
        addr-prefix                                     0.0.0.0
        network-interfaces                              M10:0.4
        media-realm-list
        mm-in-realm                                     enabled
        mm-in-network                                   enabled
        mm-same-ip                                      enabled
        mm-in-system                                    enabled
        bw-cac-non-mm                                   disabled
        msm-release                                     disabled
```

9.5 Sip Manipulation

The default behavior of the OCSR is to proxy, or route all Sip request to their configured next hop. This includes Options Request, which are widely used to monitor the reachability of next hop sip stacks. To force the OCSR to respond locally to OPTIONS requests it is receiving from session agents, we must implement the following sip manipulation. Once this manipulation is configured, it needs to be assigned as the in-manipulation ID to either session agents or sip interfaces.

ACLI Path: config t➔session-router➔sip-manipulation

- Name
- Header-rule
  - Name
  - Header-name
  - Action
  - Methods
  - New-value



```
sip-manipulation
        name                                    RespondOPTIONS
        description
        split-headers
        join-headers
        header-rule
                name                                    Respond2OPTIONS
                header-name                             from
                action                                  reject
                comparison-type                         case-sensitive
                msg-type                                any
                methods                                 OPTIONS
                match-value
                new-value                               "200 OK"
```

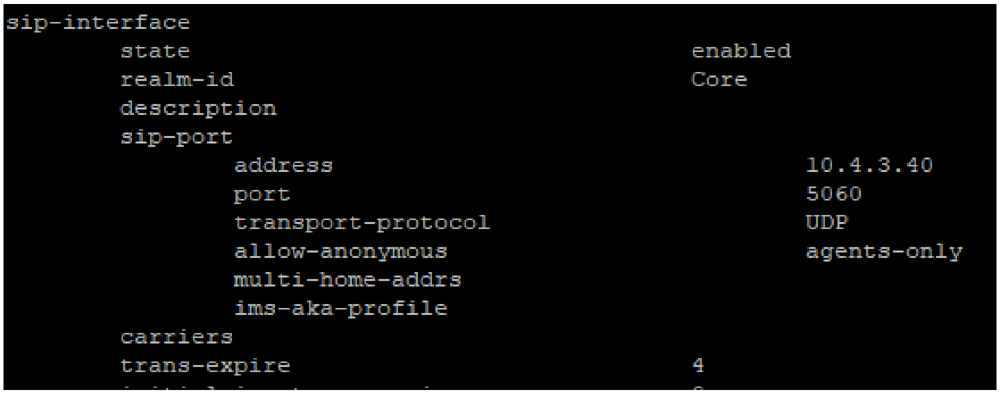
Your setup may require an additional sip manipulation to be applied as an out manipulation if the OCSR has Azure Public VIP's assigned to public facing interfaces. If this is a requirement in your environment, please refer to Appendix B.

9.6 Sip-Interfaces

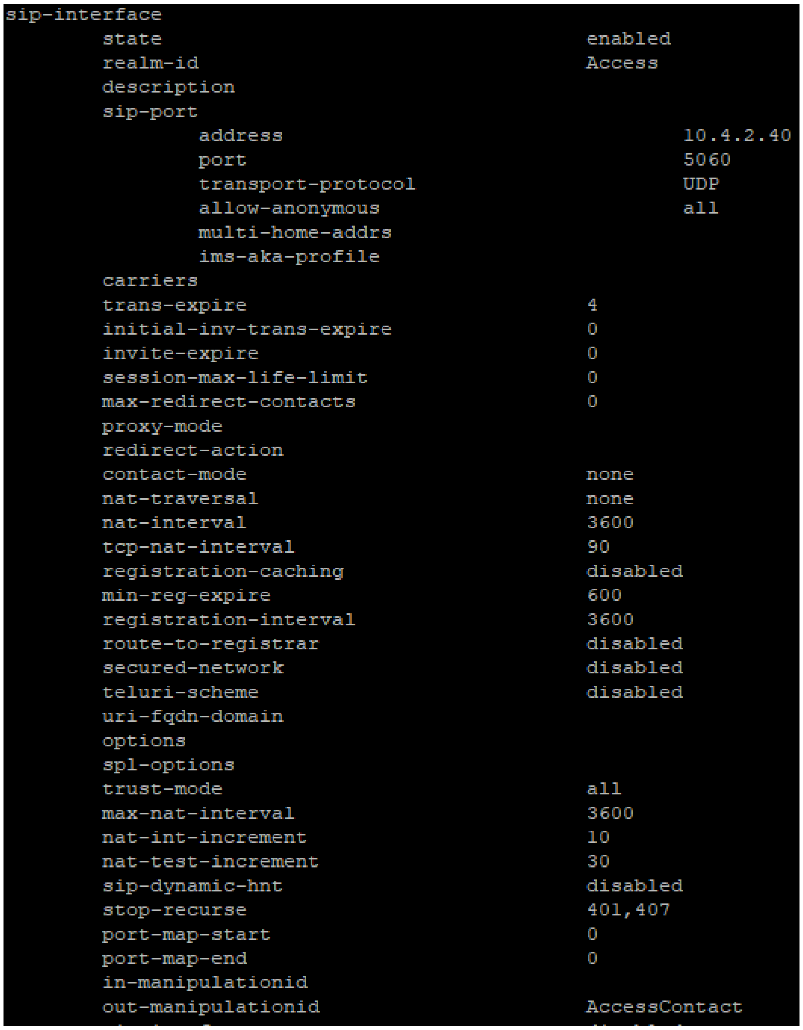
Sip interfaces is what the SBC uses to send and receiving signaling packets. Configure one per realm.

Path: session-router➔sip-interface

- Realm ID
- Trans-expire
- Sip-port
  - Address
  - Next-hop
  - Port
  - Transport protocol
  - Allow-anonymous



```
sip-interface
        state                                   enabled
        realm-id                                Core
        description
        sip-port
                address                                 10.4.3.40
                port                                    5060
                transport-protocol                      UDP
                allow-anonymous                         agents-only
                multi-home-addrs
                ims-aka-profile
        carriers
        trans-expire                            4
```



```
sip-interface
        state                                   enabled
        realm-id                                Access
        description
        sip-port
                address                                 10.4.2.40
                port                                    5060
                transport-protocol                      UDP
                allow-anonymous                         all
                multi-home-addrs
                ims-aka-profile
        carriers
        trans-expire                            4
        initial-inv-trans-expire                0
        invite-expire                           0
        session-max-life-limit                  0
        max-redirect-contacts                   0
        proxy-mode
        redirect-action
        contact-mode                            none
        nat-traversal                           none
        nat-interval                            3600
        tcp-nat-interval                        90
        registration-caching                    disabled
        min-reg-expire                          600
        registration-interval                   3600
        route-to-registrar                      disabled
        secured-network                         disabled
        teluri-scheme                           disabled
        uri-fqdn-domain
        options
        spl-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                      AccessContact
```

The trans expire value has been changed from its default value of 0 (32 seconds), to 4 seconds. This value is used for timers B, D, F, H and J as defined in RFC 3261. This is the amount of time the OCSR will wait for a response for a sip request it has generated. Decreasing this value, in combination with other configured parameters, allows us to significantly reduce the amount of time it takes for the OCSR to detect a possible fault with the next hop route, allowing it to quickly recurse to the next best routing option.

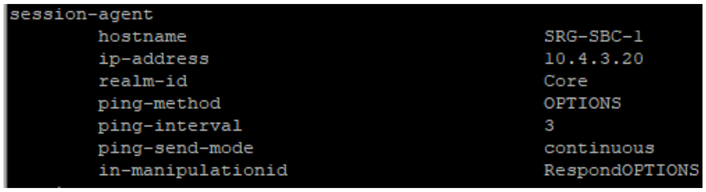
9.7 Session Agents

In the test setup, we have configured three session agents. The two of which session agents correspond with configured interface on the OCSBC's and one is pointing towards public element. Additional session agents may be required for connections to public elements.

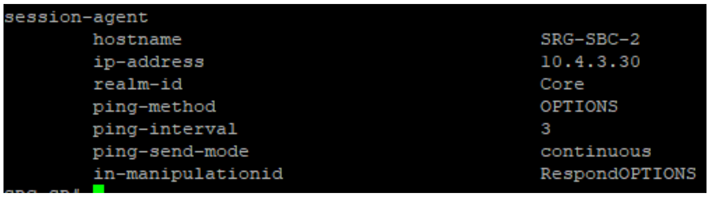
Pay close attention to the ping method, ping interval, and ping send mode configurations on the session agents configured for the OCSBC's. These configuration parameters, along with the trans expire value discussed above, work in conjunction to constantly monitor the health of the OCSBC sip stack.

ACLI Path: config t➔session-router➔session-agent

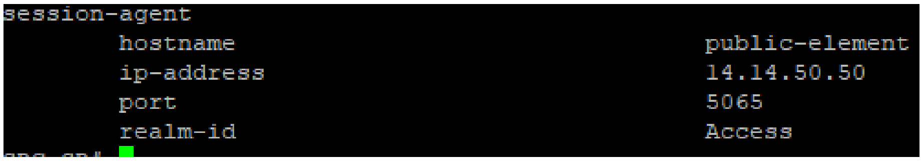
- Hostname
- IP address
- Realm ID
- Port
- Transport-protocol
- Ping-method
- Ping-interval
- Ping-send-mode
- In-manipulationid



```
session-agent
        hostname                                SRG-SBC-1
        ip-address                              10.4.3.20
        realm-id                                Core
        ping-method                             OPTIONS
        ping-interval                           3
        ping-send-mode                          continuous
        in-manipulationid                       RespondOPTIONS
```



```
session-agent
        hostname                                SRG-SBC-2
        ip-address                              10.4.3.30
        realm-id                                Core
        ping-method                             OPTIONS
        ping-interval                           3
        ping-send-mode                          continuous
        in-manipulationid                       RespondOPTIONS
```



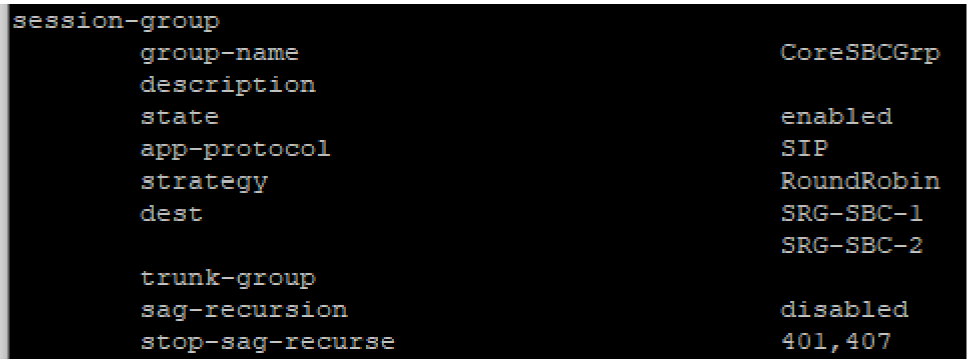
```
session-agent
        hostname                                public-element
        ip-address                              14.14.50.50
        port                                    5065
        realm-id                                Access
```

9.8 Session Group

Configure one session groups on OCSR. This is the load balancing functionality that allows traffic to be distributed evenly to each of the session agents (OCSBC's) configured in group. This also allows the SR to recurse if there is no response from the next hop.

ACLI Path: config t➔session-router➔session-group

- Group-name
- Strategy
- Dest (for multiple destinations, surround the entries with ", with a space in between…i.e "SRG-SBC-1 SRG-SBC-2"
- Sag-recursion



```
session-group
        group-name                              CoreSBCGrp
        description
        state                                   enabled
        app-protocol                            SIP
        strategy                                RoundRobin
        dest                                    SRG-SBC-1
                                                SRG-SBC-2
        trunk-group
        sag-recursion                           disabled
        stop-sag-recurse                        401,407
```

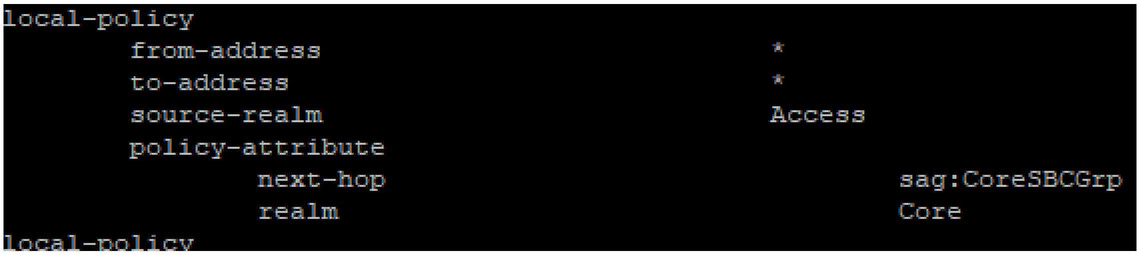
9.9 Local-Policy

Local policy configuration on the OCSR will route all incoming traffic to the already configured session group.

ACLI Path: config t➔session-router➔local-policy

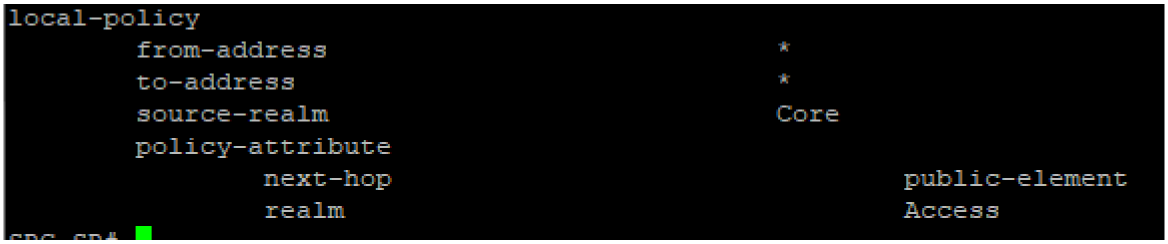
- From-address
- To-address
- Source-realm
- Policy-attribute
  - Next-hop
  - realm

To route the calls from SR side to SBC side, Use the below local–policy.



```
local-policy
        from-address                            *
        to-address                              *
        source-realm                            Access
        policy-attribute
                next-hop                                sag:CoreSBCGrp
                realm                                   Core
local-policy
```

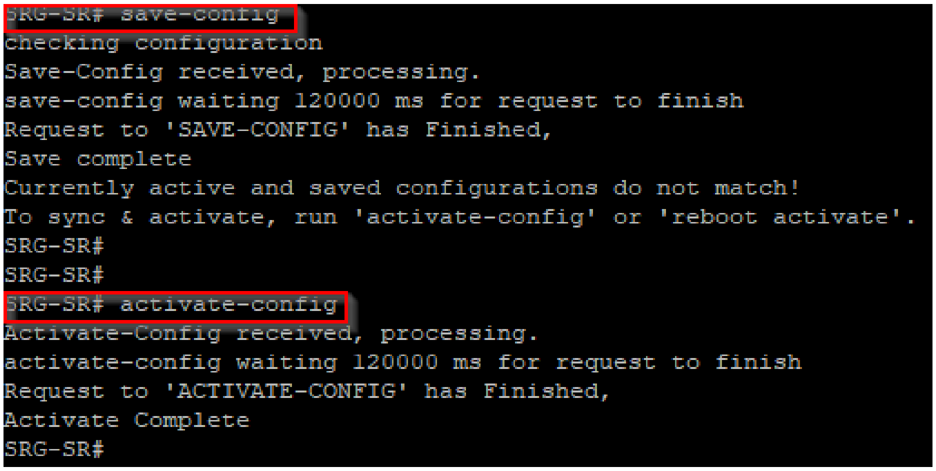
To route the calls from SBC side to SR side, Use the below local–policy.



```
local-policy
        from-address                            *
        to-address                              *
        source-realm                            Core
        policy-attribute
                next-hop                                public-element
                realm                                   Access
SRG-SR#
```

9.10 Save and Activate

At this point, the OCSR configuration is completed. Back out of configuration mode, and perform a save/activate



```
SRG-SR# save-config
checking configuration
Save-Config received, processing.
save-config waiting 120000 ms 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'.
SRG-SR#
SRG-SR#
SRG-SR# activate-config
Activate-Config received, processing.
activate-config waiting 120000 ms for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
SRG-SR#
```

10. Appendix A

10.1 SBC Deployment behind Azure NAT

This SPL-configuration is necessary for SBC deployed in Cloud Environments.

Use the Support for SBC behind NAT SPL plug-in for deploying the Oracle® Enterprise Session Border Controller (E-SBC) on the private network side of a Network Address Translation (NAT) device. The Support for SBC behind NAT SPL plug-in changes information in SIP messages to hide the end point located inside the private network. The specific information that the Support for SBC Behind NAT SPL plug-in changes depends on the direction of the call, for example, from the NAT device to the E-SBC or from the E-SBC to the NAT device. Configure the Support for SBC behind NAT SPL plug-in for each SIP interface that is connected to a NAT device. One public-private address pair is required for each SIP interface that uses the SPL plug-in, as follows.

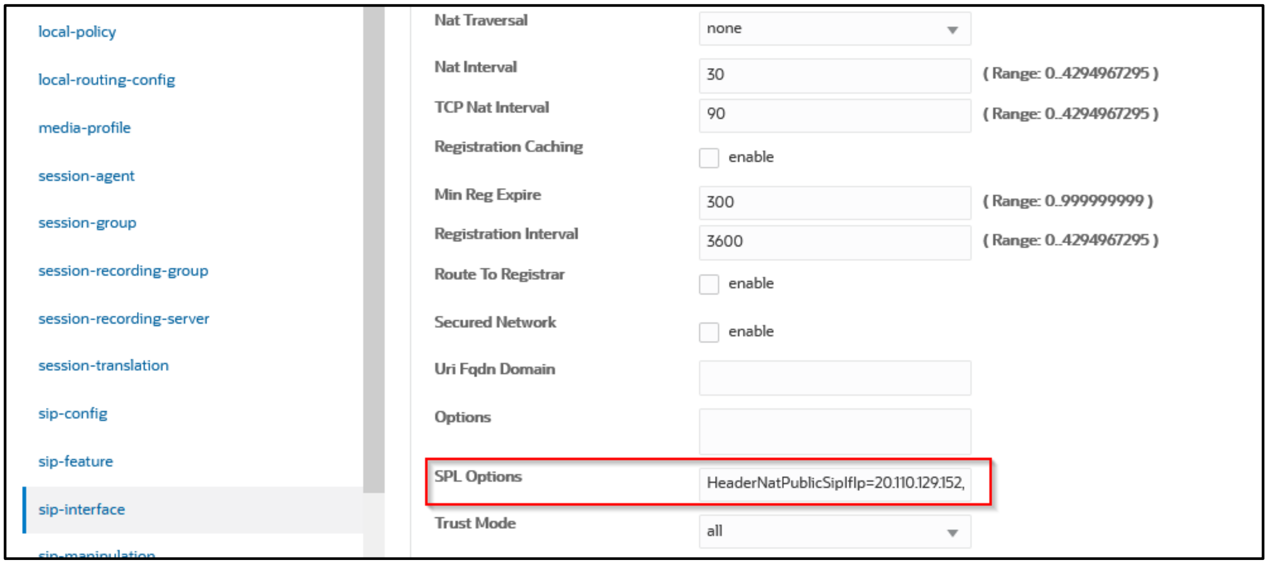
• The private IP address must be the same as the SIP Interface IP address.

• The public IP address must be the public IP address of the NAT device. (Azure Public VIP assigned to Network Interface)

To configure SBC behind NAT SPL Plug, using the GUI:

Path: session-router->sip-interface->spl-options

HeaderNatPublicSipIfIp=<Azure Public VIP >,HeaderNatPrivateSipIfIp=<private sip interface IP>



Nat Traversal: none

Nat Interval: 30 (Range: 0..4294967295)

TCP Nat Interval: 90 (Range: 0..4294967295)

Registration Caching: □ enable

Min Reg Expire: 300 (Range: 0..999999999)

Registration Interval: 3600 (Range: 0..4294967295)

Route To Registrar: □ enable

Secured Network: □ enable

Uri Fqdn Domain:

Options:

SPL Options: HeaderNatPublicSipIfIp=20.110.129.152,

Trust Mode: all

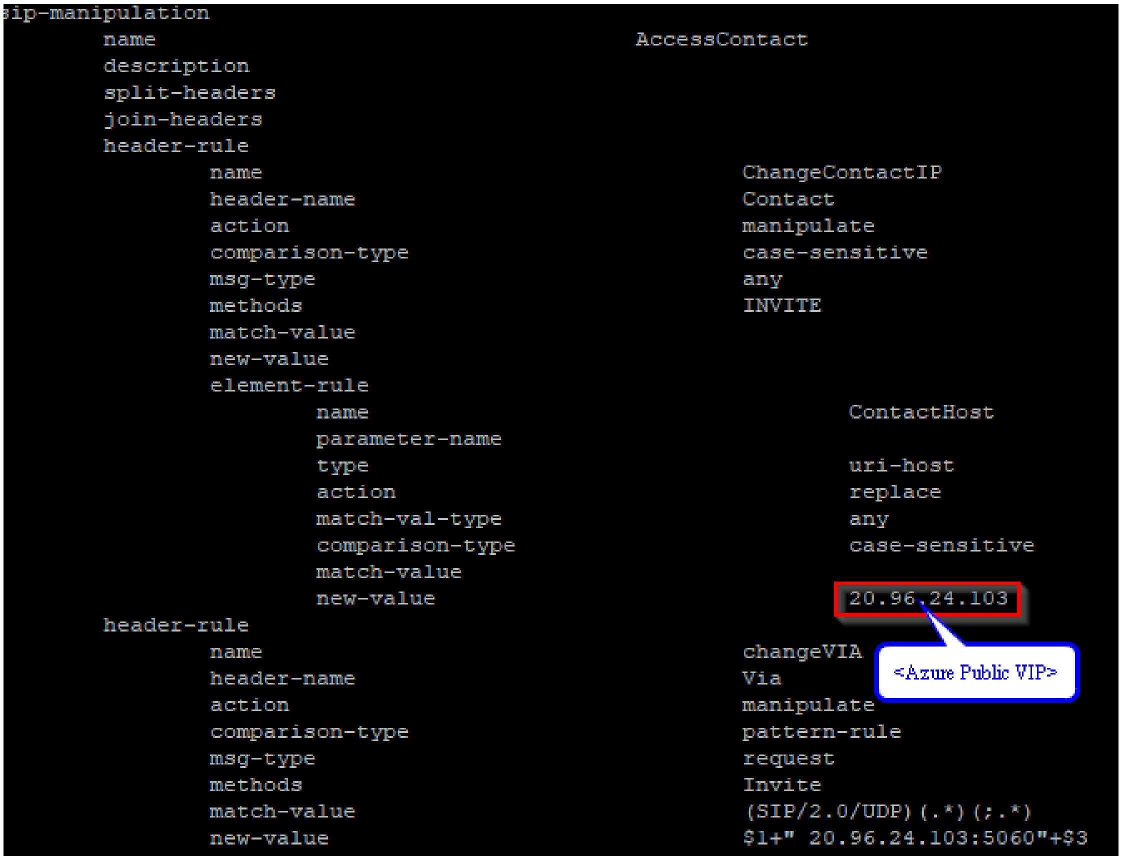
11. Appendix B

11.1 OCSR Sip Manipulation to Change Private IP when deployed in Public Cloud

The Oracle Communications Session Router does not have support for the SPL Option outlined in Appendix A above. For this reason, it may be necessary to add an additional sip manipulation to the OCSR configuration to change the private IP addresses in Sip Messages to the assigned Azure Public VIP. This will allow the OCSR to communicate with session agents and endpoints located in the public realm.
The example below is changing the host uri in the Contact Header to the Azure public VIP assigned to the Network Interface as well as Via part.
This would be applied as an out-manipulation ID on the session agent, realm or sip-interface facing a public network.

ACLI Path: config t➔session-router➔sip-manipulation

- Name
- Header-rule
  - Name
  - Header-name
  - Action
  - Element-rule
    - Name
    - Type
    - Action
    - Match-value
    - New-value



```
sip-manipulation
        name                                     AccessContact
        description
        split-headers
        join-headers
        header-rule
                name                                     ChangeContactIP
                header-name                              Contact
                action                                   manipulate
                comparison-type                          case-sensitive
                msg-type                                 any
                methods                                  INVITE
                match-value
                new-value
                element-rule
                        name                                     ContactHost
                        parameter-name
                        type                                     uri-host
                        action                                   replace
                        match-val-type                           any
                        comparison-type                          case-sensitive
                        match-value
                        new-value                                20.96.24.103
        header-rule
                name                                     changeVIA
                header-name                              Via
                action                                   manipulate
                comparison-type                          pattern-rule
                msg-type                                 request
                methods                                  Invite
                match-value                              (SIP/2.0/UDP)(.*)(;.*)
                new-value                                $1+" 20.96.24.103:5060"+$3
```

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/Oracle/
- twitter.com/Oracle
- oracle.com

Integrated Cloud Applications & Platform Services