ORACLE
COMMUNICATIONS

ORACLE

Deploying Oracle Communications SBC in Microsoft Azure Cloud with Oracle Session Router

Technical Application Note

ORACLE

Disclaimer

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

1 Contents

2 Intended Audience

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

3 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.

4 Related Documentation

4.1 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

4.2 Oracle Session Router

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

4.3 Microsoft Azure

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

4.4 Revision History

Version	Date Revised	Description of Changes
1.0	10/24/2019	Initial publication
1.1	11/12/2019	• Added Revision Table • Added Architecture Diagram

5 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.

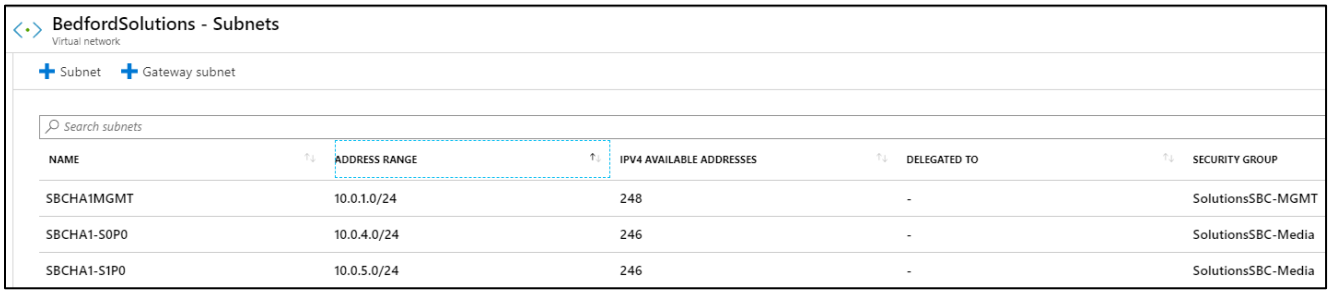
Please note: Both the OCSR and OCSBC use the same VHD file and deployment procedure. The product used for each VM instance will be selected through the acli command "setup product" once deployment is complete and you have access to cli through the serial console.

6 Requirements

- Four Oracle Communications VME deployments in Microsoft Azure Cloud, two for OCSBC and two 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.

7 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:



NAME	ADDRESS RANGE	IPV4 AVAILABLE ADDRESSES	DELEGATED TO	SECURITY GROUP
SBCHA1MGMT	10.0.1.0/24	248	-	SolutionsSBC-MGMT
SBCHA1-S0P0	10.0.4.0/24	246	-	SolutionsSBC-Media
SBCHA1-S1P0	10.0.5.0/24	246	-	SolutionsSBC-Media

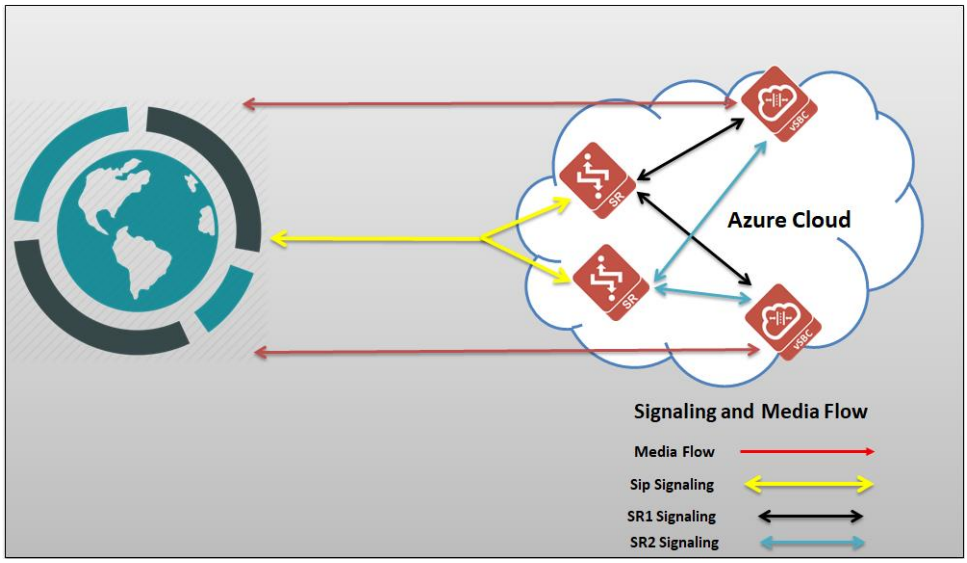
SBCHA1MGMT/10.0.1.0/24 is being used for the management interfaces of all four VME's.

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

Interface Label	Azure SR1	Azure SR2	Azure SBC1	Azure SBC2
S0P0	10.0.4.5	10.0.4.7	10.0.4.4	10.0.4.6
S1P0	10.0.5.5	10.0.5.7	10.0.5.4	10.0.5.6

All 8 Network interfaces have been assigned a Public Virtual IP in Azure Cloud.

7.1.1 Diagram



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

8 OCSBC and OCSR Setup and Configuration

8.1 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 four VME's you have successfully deployed.

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

8.1.1 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

```
AzureSBC1# setup product

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

Last Modified 2019-10-02 16:34:39
-----------------------------------------------------------------
 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
AzureSBC1#
```

8.1.2 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

```
AzureSBC1# setup entitlements

----------------------------------------------------------------
Entitlements for Enterprise Session Border Controller
Last Modified: 2019-10-02 16:47:46
----------------------------------------------------------------
 1 : Session Capacity                          : 1000
 2 :   Advanced                                : enabled
 3 : Admin Security                            :
 4 : Data Integrity (FIPS 140-2)               :
 5 : Transcode Codec AMR                       :
 6 : Transcode Codec AMR Capacity              : 0
 7 : Transcode Codec AMRWB                     :
 8 : Transcode Codec AMRWB Capacity            : 0
 9 : Transcode Codec EVS                       :
 10: Transcode Codec EVS Capacity              : 0
 11: Transcode Codec OPUS Capacity             : 0
 12: Transcode Codec SILK Capacity             : 0

Enter 1 - 12 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Session Capacity (0-512000)                  : 1000

Enter 1 - 12 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2

    Advanced (enabled/disabled)                : enabled

Enter 1 - 12 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
SAVE SUCCEEDED
AzureSBC1# show features
Total session capacity: 1000
Enabled features:
        1000 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
```

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

8.1.3 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→web-server-config

- 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

```
AzureSBC1# config t
AzureSBC1(configure)# system
AzureSBC1(system)# web-server-config
AzureSBC1(web-server-config)# select
AzureSBC1(web-server-config)# done
web-server-config
        state                                   enabled
        inactivity-timeout                      5
        http-state                              enabled
        http-port                               80
        https-state                             disabled
        https-port                              443
        http-interface-list                     REST,GUI
        tls-profile
        last-modified-by                        admin@155.212.214.199
        last-modified-date                      2019-10-02 17:01:42

AzureSBC1(web-server-config)# exit
AzureSBC1(system)# exit
AzureSBC1(configure)# done
AzureSBC1# 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'.
AzureSBC1# activate-config
Activate-Config received, processing.
waiting for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
AzureSBC1#
```

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.

8.1.4 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

```
SolutionsSessionRouter# setup product

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

Last Modified 2019-08-19 17:08:57
------------------------------------------------------------
 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
SolutionsSessionRouter#
```

8.1.5 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

```
SolutionsSessionRouter# setup entitlements

------------------------------------------------------------
Entitlements for Session Router - Session Stateful
Last Modified: 2019-10-02 17:20:13
------------------------------------------------------------
 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)          : 1000

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
SolutionsSessionRouter# show features
Total session capacity: 1000
Enabled features:
       1000 sessions, SIP, ACP, Routing, Load Balancing, Accounting,
       High Availability, ENUM, NSEP RPH, DoS
SolutionsSessionRouter#
```

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.

9 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

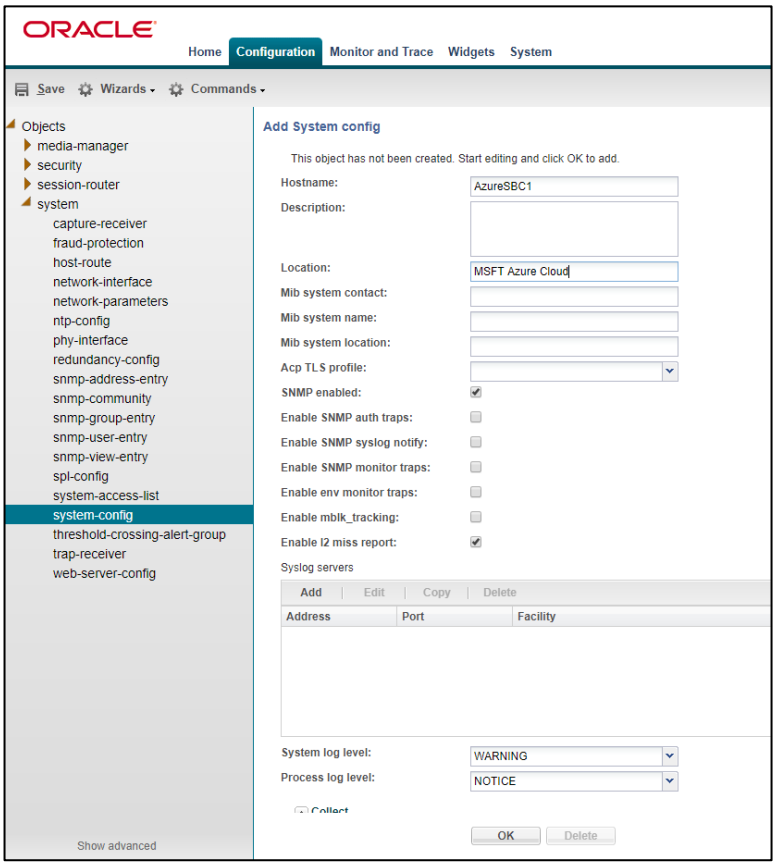
9.1 Global Configuration Elements

9.1.1 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.

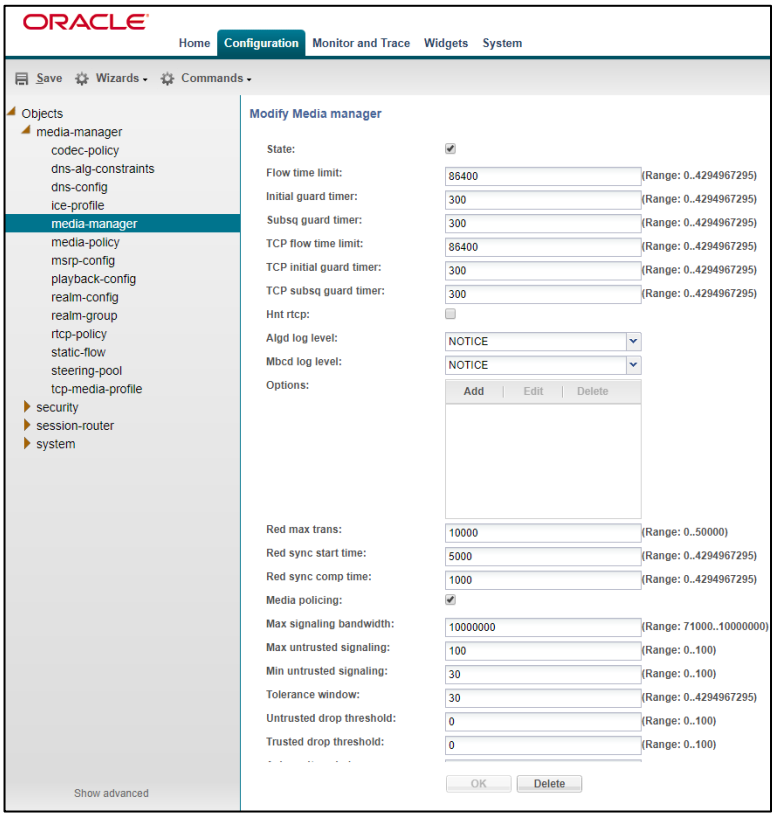
- Hostname:
- Location:
- When Finished, click the [OK] tab at the bottom of the screen



9.1.2 Media Manger

Path: media-manager➔media-manager

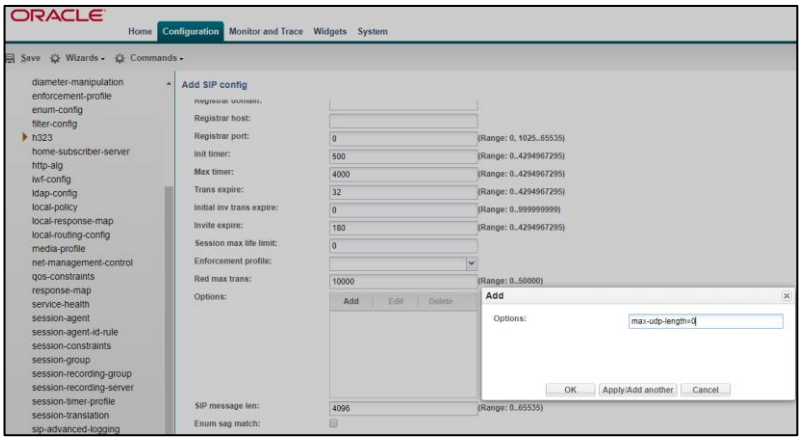
There are no required configuration changes to this element, but it must be enabled in order for the SBC to handle media. To enable it, you must access the global element and click "OK" tab at the bottom of the screen:



9.1.3 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

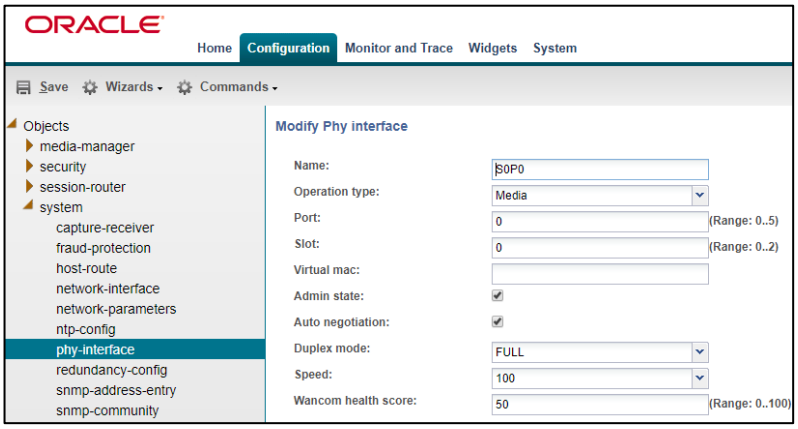


9.2 Physical Interfaces

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

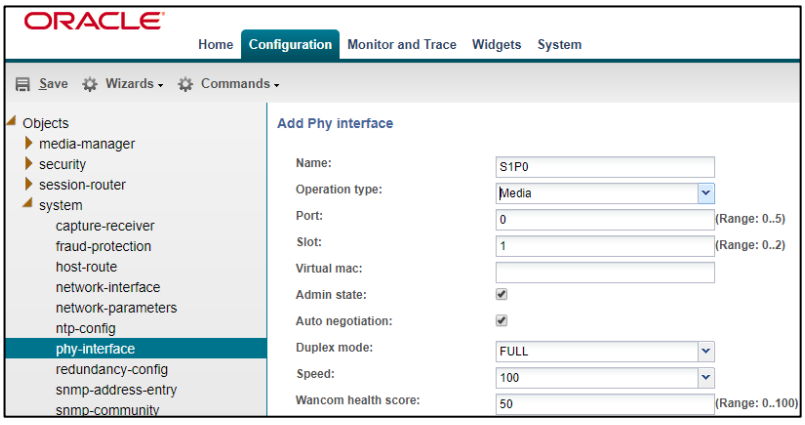
Path: system➔phy-interface

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



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

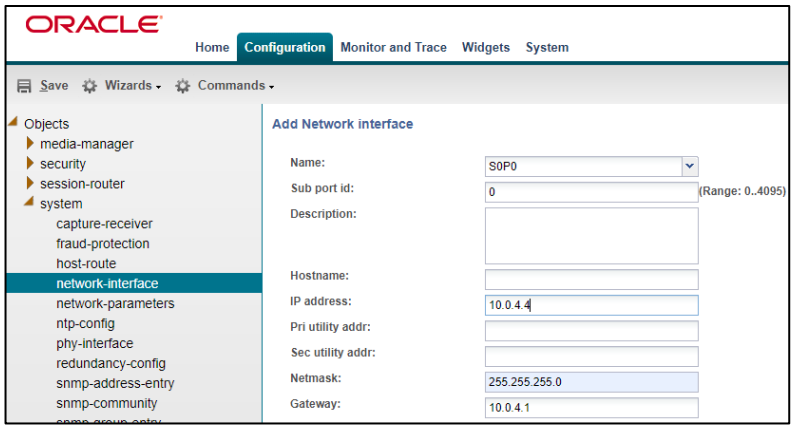


9.3 Network Interfaces

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

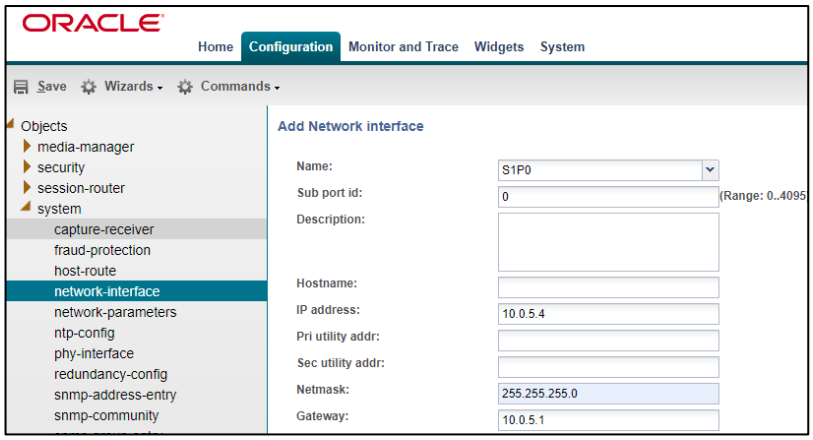
Path: system➔network-interface

- 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



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

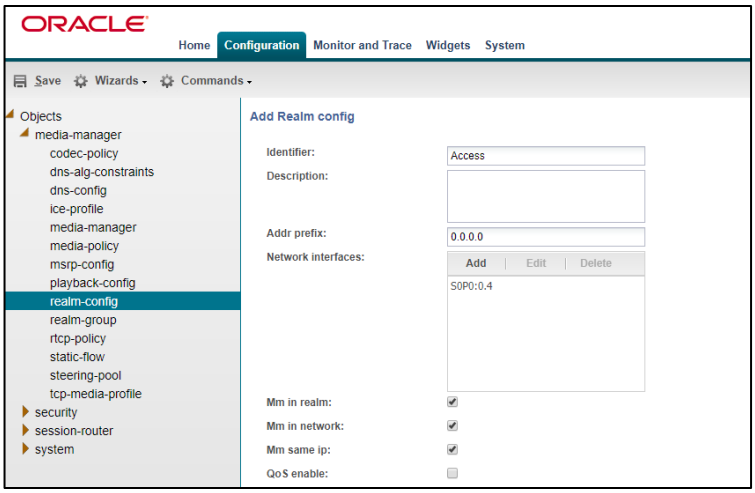


9.4 Realm Config

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

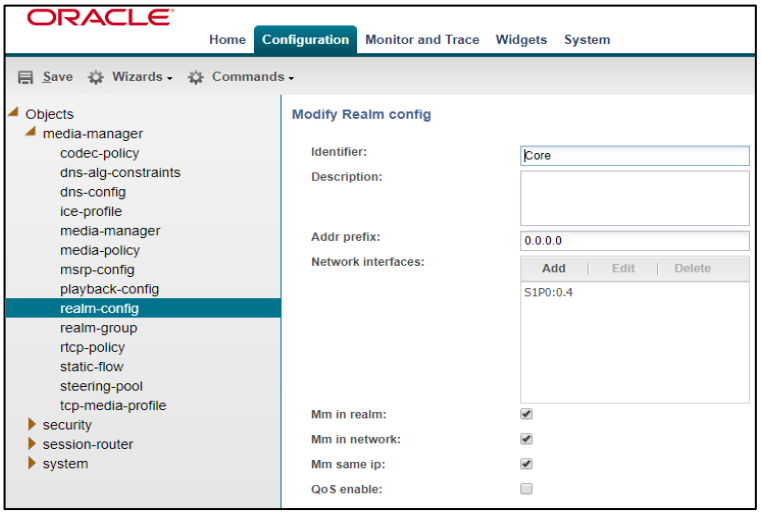
Path: media-manager➔realm-config

- 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



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

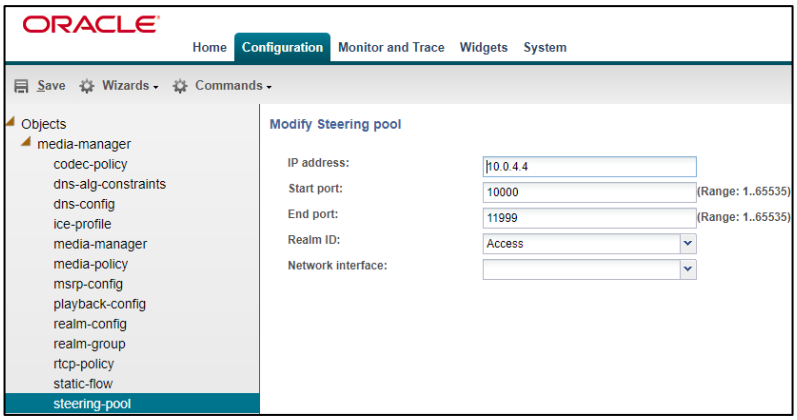


9.5 Steering Pools

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.

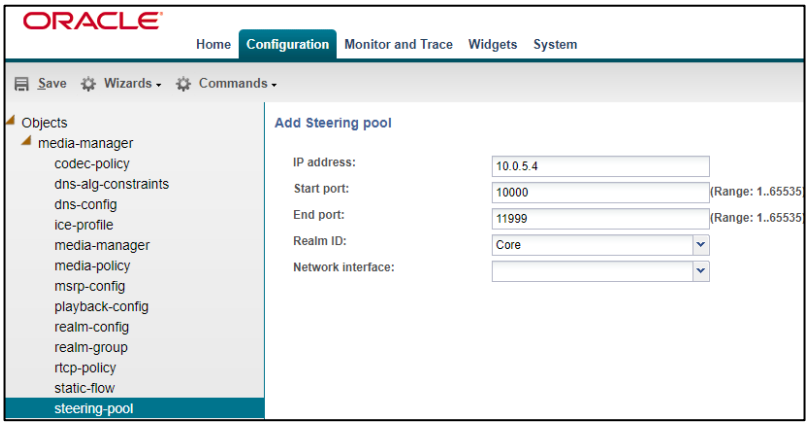
Path: media-manger➔steering-pool

- IP address: (ip used to send and receive media) (in this example, 10.0.4.5)
- Start Port: 10000
- End Port: 11999
- Realm ID: Access (selected from drop down menu)
- Click OK at the bottom



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, 10.0.5.4)
- Start Port: 10000
- End Port: 11999
- Realm ID: Core (selected from drop down menu)
- Click OK at the bottom

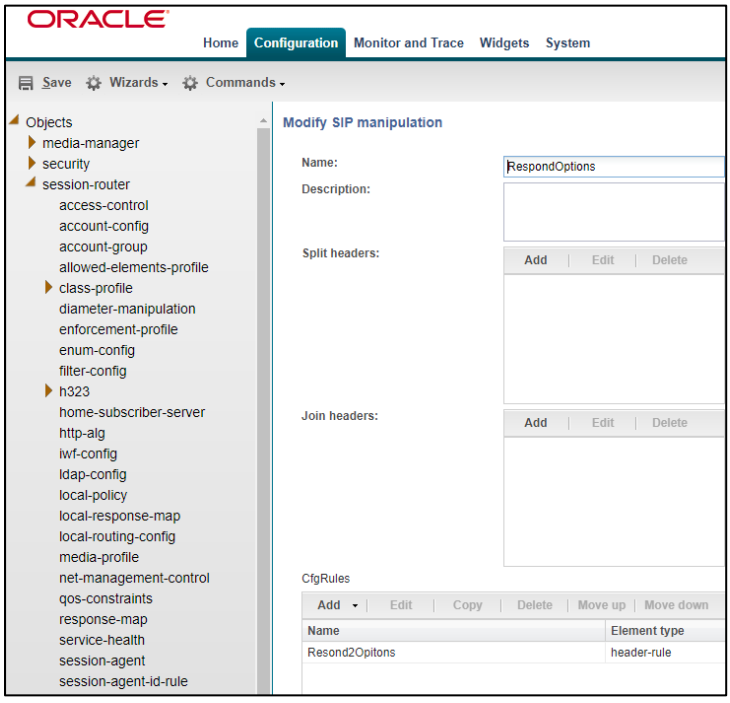


9.6 Sip Manipulation

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



9.7 Sip-Interfaces

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

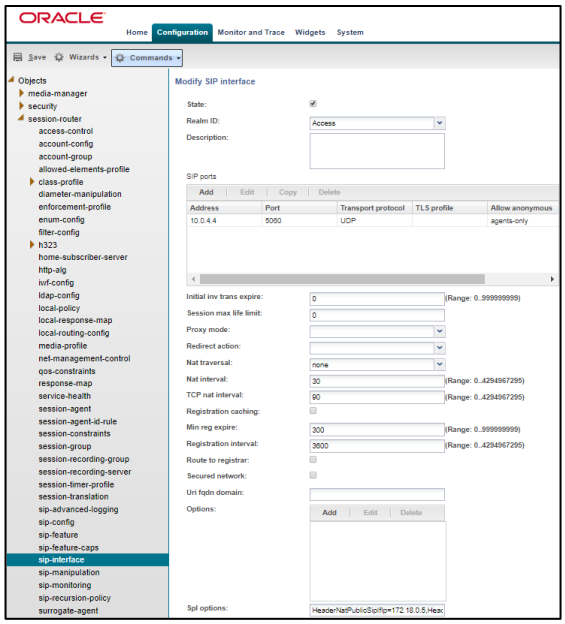
Path: session-router➔sip-interface

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

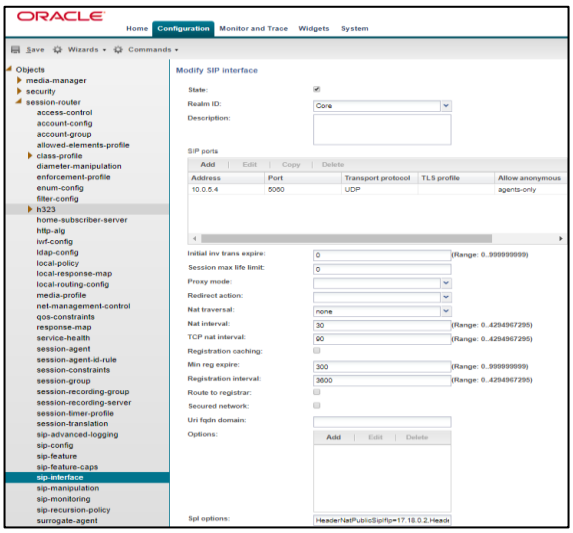
For more information on the necessity of the above Spl Option when deploying the SBC in a public cloud or behind a NAT, please see Appendix A

-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



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.

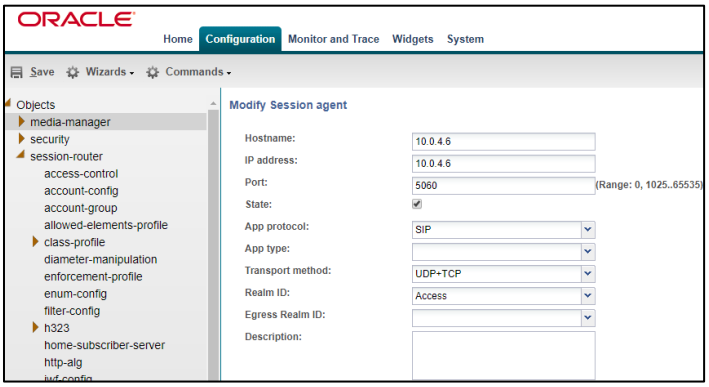


9.8 Session Agent

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 four session agents, one for each interface on the two OCSR's.

Path: session-router➔session-agent

- Hostname: Hostname given to this session agent, can be unique string, or match the configured IP address
- IP address:
- Transport: Select from Drop down
- In manipulationid: Choose from Drop Down Menu
- Realm ID:



Follow the same procedure to create three more session agents so you will have one session agent for each 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
Azure SR1, Private	10.0.5.6	10.0.5.6	Core
Azure SR2 Public	10.0.4.7	10.0.4.7	Access
Azure SR 2 Private	10.0.5.7	10.0.5.7	Core

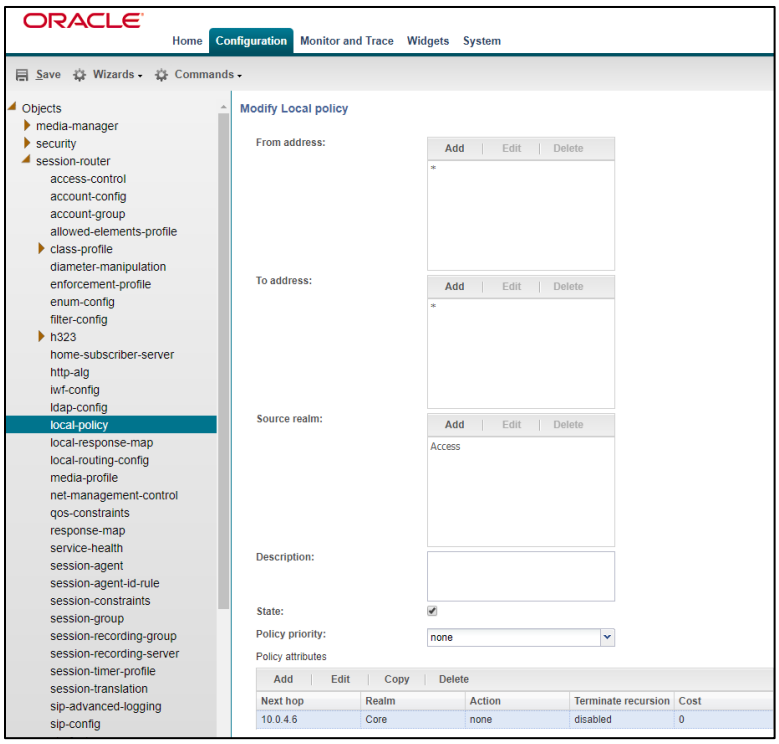
Note: You may need to configure additional session agents, depending on your environments requirements and next hop routing

9.9 Local Policy

Local policy config allows for 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

Path: session-router➔local-policy

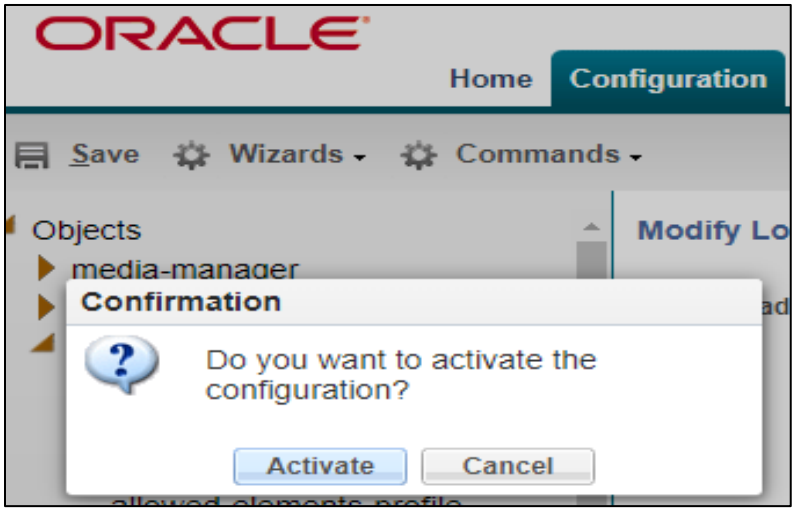
- From Address:
- To Address:
- Source Realm:
- Policy attributes: Click on Add
- Next hop:
- Realm:



Create a second local policy to route traffic from the Core Realm, to the Access realm by changing the source realm and realm under policy attribute, as well as choosing the correct next hop.

9.10 Save and Activate

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



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

10 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.

10.1 Global Configuration Elements

10.1.1 System Config

ACLI Path: config t➔system➔system-config

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

```
system-config
      hostname                    AzureSR1
      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-env-monitor-traps    disabled
      enable-mblk_tracking        disabled
      enable-l2-miss-report       enabled
```

10.1.2 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.

```
sip-config
      state                    enabled
      operation-mode             dialog
      dialog-transparency         enabled
      home-realm-id              Private
      egress-realm-id
      auto-realm-id
      nat-mode                 None
      registrar-domain
      registrar-host
      registrar-port           0
      register-service-route       always
```

10.2 Physical Interfaces

Configure two Physical Interfaces on each OCSR being setup

ACLI Path: config t➔system➔phy-interface

- Name
- Operation Type
- Slot
- Port

```
phy-interface
      name                     s0p0
      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                     s1p0
      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
```

10.3 Network Interfaces

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

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

network-interface		network-interface	
name	s0p0	name	s1p0
sub-port-id	0	sub-port-id	0
description		description	
hostname		hostname	
ip-address	10.0.4.5	ip-address	10.0.5.5
pri-utility-addr		pri-utility-addr	
sec-utility-addr		sec-utility-addr	
netmask	255.255.255.0	netmask	255.255.255.0
gateway	10.0.4.1	gateway	10.0.5.1

10.4 Realm Config

10.4.1 Nested Realms

Nested Realms is a Oracle SR feature that supports hierarchical realm groups. One or more realms may be nested within higher order realms. Realms and sub-realms may be created for media and bandwidth management purposes.

In our setup, we have four realms configured. Public and Private realms are parent realms, and directly interface with the outside world. Core-OCSBC-S0P0 and Core-OCSBC-S1P0 directly interface with the OCSBC's

To enable this feature, configure both parent and child realms

- Identifier
- Network-interface
- Parent realm (assigned the parent to the child realms only)

realm-config		realm-config	
identifier	Public	identifier	Private
description		description	
addr-prefix	0.0.0.0	addr-prefix	0.0.0.0
network-interfaces	s0p0:0	network-interfaces	s1p0:0
mm-in-realm	disabled	mm-in-realm	disabled
mm-in-network	enabled	mm-in-network	enabled
mm-same-ip	enabled	mm-same-ip	enabled
mm-in-system	enabled	mm-in-system	enabled
bw-cac-non-mm	disabled	bw-cac-non-mm	disabled
msm-release	disabled	msm-release	disabled
parent-realm		parent-realm	

```
realm-config
    identifier                  Core-OCSBC-S0P0
    description
    addr-prefix                 0.0.0.0
    network-interfaces            s0p0:0
    mm-in-realm                 disabled
    mm-in-network                 enabled
    mm-same-ip                  enabled
    mm-in-system                  enabled
    bw-cac-non-mm                   disabled
    msm-release                 disabled
    parent-realm                Public
```

```
realm-config
    identifier                  Core-OCSBC-S1P0
    description
    addr-prefix                 0.0.0.0
    network-interfaces            s1p0:0
    mm-in-realm                 disabled
    mm-in-network                 enabled
    mm-same-ip                  enabled
    mm-in-system                  enabled
    bw-cac-non-mm                   disabled
    msm-release                 disabled
    parent-realm                Private
```

10.5 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.

10.6 Sip-Interface

Sip interfaces are used by the OCSR to send and receiving signaling packets. In this nested realms config, we will be configuring one sip interface per Parent Realm.

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

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

```
sip-interface
    state                 enabled
    realm-id              Public
    description
    sip-port
        address                 10.0.4.5
        port                    5065
        transport-protocol      UDP
        allow-anonymous         agents-only
        multi-home-addrs
        ims-aka-profile
    sip-port
        address                 10.0.4.5
        port                    5065
        transport-protocol      TCP
        allow-anonymous         agents-only
    carriers
    trans-expire            4
```

```
sip-interface
    state                 enabled
    realm-id              Private
    description
    sip-port
        address                 10.0.5.5
        port                    5065
        transport-protocol      UDP
        allow-anonymous         agents-only
        multi-home-addrs
        ims-aka-profile
    sip-port
        address                 10.0.5.5
        port                    5065
        transport-protocol      TCP
        allow-anonymous         agents-only
    carriers
    trans-expire            4
```

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.

10.7 Session Agents

In the test setup, we have configured four session agents. The four session agents correspond with each configured interface on the OCSBC's. 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 AzureSBC1S0P0 ip-address 10.0.4.4 port 5065 transport-method UDP+TCP realm-id Core-OCSBC-S0P0 ping-method OPTIONS ping-interval 3 ping-send-mode continuous in-manipulationid RespondOPTIONS	session-agent hostname AzureSBC1S1P0 ip-address 10.0.5.4 port 5065 transport-method UDP+TCP realm-id Core-OCSBC-S1P0 ping-method OPTIONS ping-interval 3 ping-send-mode continuous in-manipulationid RespondOPTIONS
session-agent hostname AzureSBC2S0P0 ip-address 10.0.4.7 port 5065 transport-method UDP+TCP realm-id Core-OCSBC-S0P0 ping-method OPTIONS ping-interval 3 ping-send-mode continuous in-manipulationid RespondOPTIONS	session-agent hostname AzureSBC2S1P0 ip-address 10.0.5.7 port 5065 transport-method UDP+TCP realm-id Core-OCSBC-S1P0 ping-method OPTIONS ping-interval 3 ping-send-mode continuous in-manipulationid RespondOPTIONS

10.8 Session Group

Configure two session groups on each OCSR. This is the load balancing functionality that allows traffic to be distributed evenly to each of the session agents (OCSBC's) configured in each 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…ie "AzureSBC1S0P0 AzureSBC2S0P0"
- Sag-recursion

```
session-group
    group-name                  SBCS0P0
    description
    state                     enabled
    app-protocol                SIP
    strategy                  RoundRobin
    dest                      AzureSBC1S0P0
                              AzureSBC2S0P0
    trunk-group
    sag-recursion               disabled
    stop-sag-recurse            401,407
    sip-recursion-policy
```

```
session-group
    group-name                  SBCS1P0
    description
    state                     enabled
    app-protocol                SIP
    strategy                  RoundRobin
    dest                      AzureSBC1S1P0
                              AzureSBC2S1P0
    trunk-group
    sag-recursion               disabled
    stop-sag-recurse            401,407
    sip-recursion-policy
```

10.9 Local Policy

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

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

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

```
local-policy
    from-address                *
    to-address                  *
    source-realm                Public
    policy-attribute
        next-hop                SAG:SBCS0P0
        realm                   Core-OCSBC-S0P0
```

```
local-policy
    from-address                *
    to-address                  *
    source-realm                Private
    policy-attribute
        next-hop                SAG:SBCS1P0
        realm                   Core-OCSBC-S1P0
```

10.10 Save and Activate

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

```
AzureSR1# 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'.
AzureSR1# activate-config
Activate-Config received, processing.
waiting for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
AzureSR1#
```

11 Appendix A

11.1 SBC Deployment Behind Azure NAT

This SPL-configuration is a must 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.

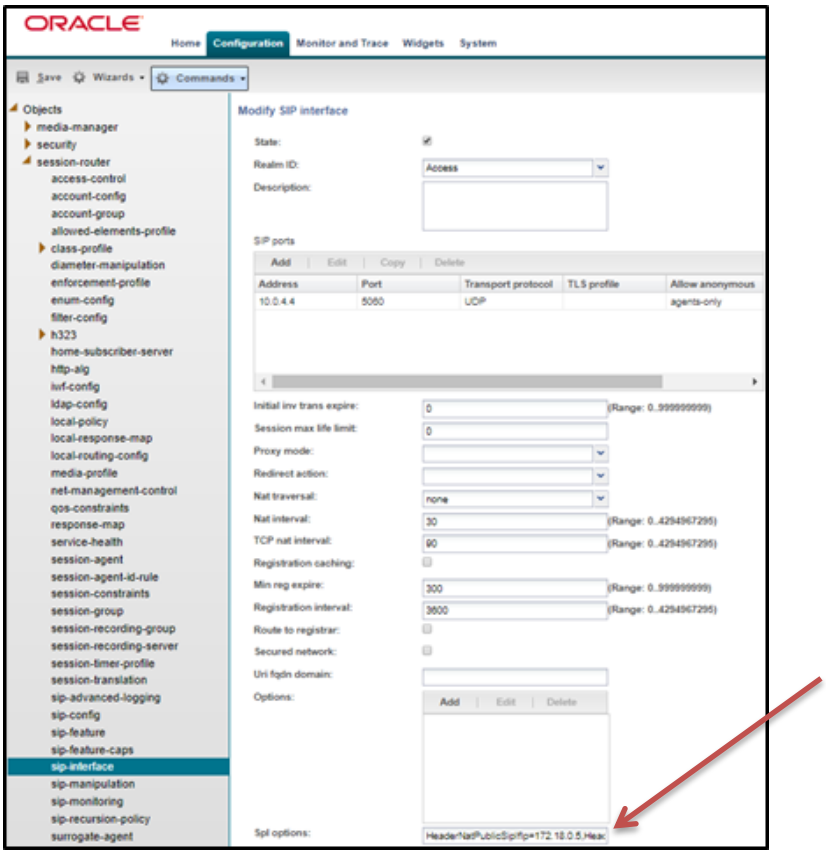
• The private IP address must be the same as the SIP Interface IP address.

• The public IP address must be the public IP address of the NAT device. (Azure Pulic 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>



12 Appendix B

12.1 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.
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                    ChangeContactHost
    description
    split-headers
    join-headers
    header-rule
        name                ChangeContactIP
        header-name         Contact
        action              manipulate
        comparison-type     case-sensitive
        msg-type            any
        methods
        match-value
        new-value
        element-rule
            name            ChangeContactS0P0
            parameter-name
            type            uri-host
            action          replace
            match-val-type  any
            comparison-type case-sensitive
            match-value     10.0.4.6
            new-value       <Azure Public VIP>
        element-rule
            name            ChangeContactS1P0
            parameter-name
            type            uri-host
            action          replace
            match-val-type  any
            comparison-type case-sensitive
            match-value     10.0.5.6
            new-value       <Azure Public VIP>
```

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