



Configuring the Oracle SBC hosted on Azure Cloud with Microsoft Teams Direct Routing

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.

Revision History

Version	Description of Changes	Date Revision Completed
1.0	Added MSTeams specific configuration on Azure Cloud and SBC.	10-10-2019

Table of Contents

Introduction	
Configuring the SBC	5
Deploying Oracle SBC on the Azure Cloud	7
Configuring the Azure Cloud to support Direct Routing	7
Network Security configuration	7
Network Security Group for Media Interfaces	7
Create Network Interfaces on Azure cloud	
Create virtual Network	
Creating Public IP	
Creating network interfaces	
Attaching network interfaces to the Oracle SBC	
About Microsoft Teams Direct Routing	
Planning Direct Routing	
Licensing Requirements	
DNS Requirements	
SBC Domain Names	
Public trusted certificate for the SBC	
SBC configuration	
Interface Mapping	
System-Config in SBC	
Deploying SBC behind Azure NATing	

Introduction

This document describes how to connect the Oracle SBC in Azure cloud to Microsoft Teams Direct Routing environment. This paper is intended for IT or telephony professionals.

Configuring the SBC

Like the on-premises SBC, the VMSBC can also be connected to the Microsoft Teams Direct Routing. Here the platform is called as VME.



Figure :1: Signaling & media flow with media-bypass disabled

There are several connection entities on the picture:

- Enterprise network consisting of Teams client
- SBC on Azure Cloud
- Microsoft Teams Direct Routing Interface
- PSTN trunk from a 3rd party provider

These instructions cover configuration steps between the Oracle SBC and Microsoft Teams Direct Routing Interface. The interconnection of other entities, such as connection of the PSTN trunk, 3rd Party PBX and/or analog devices are not covered in this instruction. The details of such connection are available in other instructions produced by the vendors of respective components.

Deploying Oracle SBC on the Azure Cloud

This document assumes that Oracle SBC is up and running in the Azure cloud. If the customer is looking to deploy a new SBC on the Azure cloud, please follow the documentation here.

https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/OCSBC-Deployed-In-Azure.pdf

Configuring the Azure Cloud to support Direct Routing

To support direct routing on Azure cloud, the following configuration changes are required to the Oracle SBC instance running on the Azure cloud

- Network security configuration
- Network Interfaces with a static public IP
- Attaching network interfaces to the Oracle SBC

Network Security configuration

Network Security Group for Media Interfaces

Create network security group for media interfaces. Here we will be creating two network security groups.

- Towards MS Teams
- Towards PSTN

Microsoft Azure	\wp Search resources, services, and docs (G+/)	\geq	Ŗ	Û	<u>ين</u>	?	\odot	g
	« Home > New > Network security group > Create network security group							
+ Create a resource	Create network security g \Box \times							
🛧 Home								
🛅 Dashboard	* Name TowardsTeams							
∃ All services	* Subscription							
+ FAVORITES	Microsoft Azure Enterprise - SBC							
All resources	* Resource group							
😭 Resource groups	MSTeams V							
🔕 App Services	Create new							
Function App	(US) East US							
👼 SQL databases								
🞾 Azure Cosmos DB								
<u> </u> Virtual machines								
💠 Load balancers								
Storage accounts								

From Azure's navigation list on the left side of the portal, click Create a resource, Networking, Network Security Group Configure the following for the Media Interface Network Security Group:

- Name
- Resource Group
- Location
- Click Create

Note: The Resource group and location should be the same used in deploying the Oracle SBC in Azure.

The following TCP/UDP protocols and/or ports should be opened for the Media Interface NSG "TowardsTeams"

Inbound Rules for network interface facing Teams

The below table shows the ports to be opened for Non-Media bypass Configuration.

Source	Source Port Range	Destination	Destination Port	Protocol
			Range	
Any	*	Any	5061	TCP
Any	*	Any	53	*
Any	49152-53247	Any	10000-20000*	UDP
Any	*	Any	123	UDP

Here 10000-20000* specifies the steering pool configured on the SBC.(i.e the media port range of the SBC) The ports 49152-53247 are defined as per Microsoft documentation for non-media bypass configuration For more information on the ports to be configured for non-media bypass configuration, please click on the link below.. <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-ports</u>

Please use the table below for Media bypass configuration

Source	Source Port Range	Destination	Destination Port Range	Protocol
Any	*	Any	5061	ТСР
Any	*	Any	53	*
Any	50000-50019	Any	10000-20000*	UDP
Any	*	Any	123	UDP

Similarly,10000-20000* specifies the steering pool configured on the SBC.

The ports 49152-53247 are defined as per Microsoft documentation for media bypass configuration For more information on the ports to be configured for media bypass configuration, please click on the link below. https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan-media-bypass

Pagis			
Basic	 		
Source n		Î	
Any	~		
Source port ranges			
*			
Destination A			
Any	~	1	
Destination port ranges			
5061,53,123	✓	7	
Protocol		-	
Any TCP UDP ICMP			
Action			
Action			
Allow Deny			
Allow Deny		-	
Allow Deny		•	
Allow Deny		•	
Allow Deny Construct Construction Constructi	>	•	
Allow Deny Allow Deny Add inbound security rule TowardsTeams Basic	>	Ŧ	
Allow Deny Priority Add inbound security rule TowardsTeams Basic 61,53,123	>	•	
Allow Deny C Priority Add inbound security rule TowardsTeams Basic 61,53,123 otocol	>	Ţ	
Allow Deny Allow Deny Allow Deny Add inbound security rule TowardsTeams Basic 61,53,123 otocol Any TCP UDP ICMP	 >	•	
Allow Deny Contract C	>	•	
Allow Deny Allow Deny Allow Deny Add inbound security rule TowardsTeams Basic 61,53,123 otocol Any TCP UDP ICMP ttion Allow Deny	>		
Allow Deny Allow Deny Allow Deny Add inbound security rule TowardsTeams Basic 61,53,123 otocol Any TCP UDP ICMP ction Allow Deny iority	, ,	•	
Allow Deny Allow Deny Allow Deny Add inbound security rule TowardsTeams Basic 61,53,123 otocol Any TCP UDP ICMP ction Allow Deny iority 0	>	Ţ	
Allow Deny Allow Deny Allow Deny Add inbound security rule TowardsTeams Basic 61,53,123 otocol Any TCP UDP ICMP ttion Nlow Deny iority 0 ame PTLS	→ →	•	
Allow Deny Allow Deny Allow Deny Contract Contre	> ~	Ţ	
Allow Deny Allow Deny Allow Deny Add inbound security rule TowardsTeams Basic 61,53,123 otocol Any TCP UDP ICMP ttion Allow Deny iority O ame PTLS cription	→ →	Ţ	
Allow Deny Allow Deny Allow Deny Contract Contre	 ✓ ✓ ✓ 	Ţ	

Refer the above tables and create inbound media rule according to your environment. Note: Set priority as 110 for the media rules.

Outbound Rules for network interface facing Teams

The below table shows the ports to be opened for Non-Media bypass Configuration.

Source	Source Port Range	Destination	Destination Port Range	Protocol
Any	5061	Any	*	ТСР
Any	53	Any	*	*
Any	10000-20000*	Any	49152-53247	UDP
any	123	Any	*	UDP

Here 10000-20000* specifies the steering pool configured on the SBC.(i.e the media port range of the SBC) The ports 49152-53247 are defined as per Microsoft documentation for non-media bypass configuration For more information on the ports to be configured for non-media bypass configuration, please click on the link below. <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-ports</u>

Please use the table below for Media bypass configuration

Source	Source Port Range	Destination	Destination Port	Protocol
			Range	
Any	5061	Any	*	ТСР
Any	53	Any	*	*
Any	10000-20000*	Any	50000-50019	UDP
Any	123	Any	*	UDP

Similarly,10000-20000* specifies the steering pool configured on the SBC.

The ports 49152-53247 are defined as per Microsoft documentation for media bypass configuration For more information on the ports to be configured for media bypass configuration, please click on the link below. <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan-media-bypass</u>

Add outbound security rule TowardsTeams	>
🗲 Basic	
* Source @	
Any	~
* Source port ranges 🚯	
5061,53,123	~
* Destination 🕦	
Any	\checkmark
* Destination port ranges 🚯	
*	
* Protocol	
Any TCP UDP ICMP	
* Action	
Allow Deny	

Add outbound security rule				
🗲 Basic				
* Protocol				
Any TCP UDP ICMP				
* Action				
Allow Deny				
* Priority 🚯				
100				
* Name				
SIP_TLS	✓			
Description				

Refer the above tables and create outbound media rule according to your environment. Note: Set priority as 110 for the media rules.

Inbound Rules for network interface facing PSTN

For the NSG "TowardsPSTN", create the following inbound rules.

Please note, the port matrix below is an example only. The ports opened during installation should depend on the environment needs and user preferences.

Source	Source Port Range	Destination	Destination Port Range	Protocol
Any	*	Any	5060	UDP
Any	*	Any	53	*
Any	*	Any	1719	UDP
Any	*	Any	123	UDP
Any	*	Any	1720	UDP
Any	*	Any	20000-30000*	UDP

Here 20000-30000 is the steering pool for PSTN side configured on SBC.

Refer the above tables and create inbound media rule according to your environment. Note: Set priority as 110 for the media rules.

Outbound Rules for network interface facing PSTN

For the NSG "TowardsPSTN", create the following outbound rules.

Source	Source Port Range	Destination	Destination Port	Protocol
			Range	
Any	5060	Any	*	UDP
Any	53	Any	*	*
Any	1719	Any	*	UDP
Any	123	Any	*	UDP
Any	1720	Any	*	UDP
Any	20000-30000*	Any	*	UDP

Here 20000-30000 is the steering pool for PSTN side configured on SBC.

Add outbound security rule		
🗲 Basic		
* Source 🕦		
Any	~	
Source port ranges 🚯		
5060,53,1719,123,1720		
* Destination 🚯		
Any	~	
* Destination port ranges 🚯		
*	~	
* Protocol		
Any TCP UDP ICMP		
* Action		
Allow Deny		
* Driority @	-	

	Add outbound	security r	ule	
🗲 Basi	с			
Action	v Deny			
* Priorit	y O			
100				
* Name				
SIP_ou	tb			~
Descript	tion			

Refer the above tables and create outbound media rule according to your environment. Note: Set priority as 110 for the media rules.

Create Network Interfaces on Azure cloud

For MS Teams deployment, we have to create two network interfaces

- S0P0-Facing the PSTN trunk
- S0P1-Facing the MS Teams

Before creating the network interface ,create virtual networks to be associated with network interfaces.

Create virtual Network

Provide the following information in the designated fields:

- Virtual Network Name
- Address Space: (below example is Azure provided)
- Subscription
- Resource Group (created above)
- Location (same as Resource Group location)

Microsoft Azure	✓ Search resources, services, and docs (G+/)	>_	Ģ	Ļ	ŝ	?	\odot	g
«	Home > Virtual networks > Create virtual network							
	Create virtual network \Box \times							
🛧 Home	A							
🖪 Dashboard	* Name Virtual_NW_Teams							
∃ All services	* Address space 👔							
- 🛧 FAVORITES	10.4.0.0/16							
All resources	10.4.0.0 - 10.4.255.255 (65536 addresses)							
😭 Resource groups	Add an IPv6 address space 🚯							
🔇 App Services	* Subscription							
🦘 Function App	Microsoft Azure Enterprise - SBC 🗸							
👼 SQL databases	* Resource group							
🞾 Azure Cosmos DB	MSTeams V Create new							
💶 Virtual machines	* Location							
😵 Load balancers	(US) East US 🗸							
Storage accounts	*							

Microsoft Azure	\wp Search resources, services, and docs (G+/)	≥_	Ð	Ļ	?	\odot
«	Home > Virtual networks > Create virtual network					
Create a resource	Create virtual network \Box $ imes$					
🛧 Home	* Location					
🗔 Dashboard	(US) East US 🗸					
i≡ All services	Subnet					
★ FAVORITES	* Name					
All resources	default					
😭 Resource groups	* Address range 👔					
🔇 App Services	10.4.0.0 - 10.4.0.255 (256 addresses)					
🦘 Function App	DDoS protection 🕤					
👼 SQL databases	Service endpoints 👩					
🞾 Azure Cosmos DB	Disabled Enabled					
🔮 Virtual machines	Firewall 🚯					
💠 Load balancers	Disabled Enabled					
Storage accounts	v					
↔ Virtual networks	Create Automation options					
A <u>.</u> .						

Similarly, create a virtual network for the PSTN side.

Creating Public IP

Create Public IP in the resource groups to be associated with the network interfaces.

Provide the following information in the designated fields:

- Name of the Public IP address
- Subscription
- Resource Group (created above)
- Location (same as Resource Group location)
- SKU type as Standard

Microsoft Azure	\sim Search resources, services, and docs (
«	Home > Public IP addresses > Create public IP address
+ Create a resource	Create public IP address \Box $ imes$
🛧 Home	
🗔 Dashboard	 * IP Version ● IPv4 ○ IPv6 ○ Both
E All services	* SKU 🕦
- 🔶 FAVORITES	🔵 Basic 💿 Standard
All resources	IPv4 IP Address Configuration
😭 Resource groups	* Name
🔇 App Services	PublicIP_Teams
🦘 Function App	* IP address assignment
💀 SQL databases	O Dynamic O Static
🖉 Azure Cosmos DB	* Idle timeout (minutes) 1
👰 Virtual machines	DNS name label 🙃
💠 Load balancers	
Storage accounts	.eastus.cloudapp.azure.com 💌
↔ Virtual networks	Create Automation options

Microsoft Azure	
«	Home > Public IP addresses > Create public IP address
Create a resource	Create public IP address \Box $ imes$
🛧 Home	Dunamic Static
🗔 Dashboard	t lalle timesent (minuter)
E All services	4
— 🛧 FAVORITES —————	DNS name label n
All resources	
😭 Resource groups	.eastus.cloudapp.azure.com
🔇 App Services	* Subscription
🦘 Function App	Microsoft Azure Enterprise - SBC 🗸
🕺 SQL databases	* Resource group
💋 Azure Cosmos DB	Create new
👥 Virtual machines	* Location
💠 Load balancers	(US) East US 🗸
Storage accounts	
↔ Virtual networks	Create Automation options

Creating network interfaces

For MS Teams deployment, we have to create two network interfaces

- S0P0-Facing the PSTN trunk
- S0P1-Facing the MS Teams

Configure the applicable Create Network interface fields, including:

- Name: S0P0_PSTN
- Subnet: From the drop down, select the subnet created for S0P0 interface
- Private IP: Set to static
- Private IP Address: Set to an address within the subnet, in this case, we're using 10.4.0.5
- Network Security Group: Select the group configured for SBC media Interfaces

Microsoft Azure	\gg Search resources, services, and docs (G+/)
«	Home > Network interfaces > Create network interface
+ Create a resource	Create network interface \Box \times
🛧 Home	
🗔 Dashboard	* Name SOPO_PSTN
E All services	* Virtual network
- 🛨 FAVORITES	Virtual_NW_Teams ~
All resources	* Subnet 🚯
(🕥 Resource groups	default (10.4.0.0/24) 🗸
🔇 App Services	Private IP address assignment
🤣 Function App	Dynamic Static
👼 SQL databases	* Private IP address
🖉 Azure Cosmos DB	10.4.0.5
👰 Virtual machines	Network security group 🕜
💠 Load balancers	TowardsPSTN

Microsoft Azure	₽ Search	resource	es, ser
*	Home > Network interfaces > Creat	e netwo	ork in
Create a resource	Create network interface		\times
🕈 Home			
Dashboard	* Private IP address		
All services	10.4.0.5	~	
	Network security group ① TowardsPSTN	>	
All resources			
🕥 Resource groups	Private IP address (IPv6)		
🔇 App Services	* Subscription		
🦘 Function App	Microsoft Azure Enterprise - SBC	\sim	
💀 SQL databases	* Resource group 🚯		
Z Azure Cosmos DB	MSTeams Create new	~	
👥 Virtual machines	* Location		
Load balancers	(US) East US	\checkmark	
Storage accounts			Ŧ
↔ Virtual networks	Create Automation options		
🚸 Azure Active Directory 🗸 🗸			

After the network interfaces are created ,go to the network interface and click on IP configurations.

Microsoft Azure		rces, services, an	d docs (G+/)			2	Ð	Ļ	٤ <u>ن</u> ې	?	\odot
«	Home > S0P0_PSTN - IP configurations	lome > S0P0_PSTN - IP configurations									
+ Create a resource	SOPO_PSTN - IP configura	tions									
🛧 Home	A contraction of the contra	Add F		Discard							
료 Dashboard	Search (Ctrl+/)	Add	Joave 💦 L	Jiscara							
All services	Overview	IP forwardir	ng settings								
+ FAVORITES	Activity log	IP forwarding	9		Disable	d Enal	oled				
All resources	Access control (IAM)	Virtual netwo	ork		Virtual_N	IW_Team	IS				
🕅 Resource groups	🥔 Tags	IP configura	itions								
🔇 App Services	Settings	* Subnet			default	(10.4.0.0/	24)				
🦘 Function App	IP configurations										
👼 SQL databases	DNS servers		configurations								
🞾 Azure Cosmos DB	Network security group	NAME	IP VERSION	ТҮРЕ		PRIV	ATE IP AD	DRESS			PUBLIC IF
👤 Virtual machines	Properties	ipconfig1	IPv4	Primary		10.4	.0.5 (Sta	atic)			-
Load balancers	Locks										
Storage accounts	Export template										
<> Virtual networks	Support + troubleshooting										
🚸 Azure Active Directory 🚽	 Effective econsitient value 										

Enable the Public IP address and associate the Public IP created previously. Save the config after that.

Microsoft Azure	ρ Search resources, services, and docs (G+/)		▶_	Ŗ
«	Home > S0P0_PSTN - IP configurations > ipconfig1			
- Create a resource	ipconfig1	$\square \times$		
🛧 Home	Save X Discard			
🖪 Dashboard				
∃ All services	Public IP address settings			
- 🛨 FAVORITES	Disabled Enabled			
All resources				
🕅 Resource groups	PublicIP_Teams (52.168.34.96)	>		
🔇 App Services				
interview Section App	Private IP address settings			
👼 SQL databases	Virtual network/subnet Virtual_NW_Teams/default			
🞾 Azure Cosmos DB	Assignment			
👤 Virtual machines	Dynamic Static			
Load balancers	* IP address			
Storage accounts	104.0.5			
↔ Virtual networks				

Follow the above procedure and create SOP1 interface facing the Teams side.

Attaching network interfaces to the Oracle SBC

Once the network interfaces are created ,they have to be attached to the Oracle VM running on Azure.

Azure requires that we stop the SBC instance before we can create or attach additional networking interfaces for Media.

From Azure's navigation list, on the left side of the portal, Select "Virtual machines"

Select the instance we created previously . Once you select it, you will see displayed an instance-specific navigation pane on the left side of the dialog

- At the top, click on "Stop"
- Once the VM is stopped and deallocated, click on Networking under Settings in the instance specific navigation menu.



Next, "Attach Network Interface" and attach the two previously created network interfaces S0P0-PSTN and S0P1-MSTeams

Start your instance after creating and attaching all interfaces.

About Microsoft Teams Direct Routing

Microsoft Teams Direct Routing allows a customer provided SBC to connect to Microsoft Phone System. The customer provided SBC can be connected to almost any telephony trunk or interconnect 3rd party PSTN equipment. The scenario allows:

- Use virtually any PSTN trunk with Microsoft Phone System;
- Oracle Enterprise Session Border Controllers are Microsoft certified to work for Direct Routing. Additional information can be found at

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers

Planning Direct Routing

If you are planning to configure direct routing with Oracle SBC $\,$, you must ensure that the following prerequisites are completed before proceeding further

- Licensing and DNS requirements
- SBC domain names
- Public trusted certificate for the SBC
- SIP Signaling: FQDNs

Licensing Requirements

Make sure that the following license requirements are met by the Direct routing users.(ie the users must be assigned the following licenses in Office 365)

- Microsoft Phone System
- Microsoft Teams + Skype for Business Plan 2 if included in Licensing Sku

DNS Requirements

Create DNS records for domains in your network that resolve to your SBC.

Before you begin, make sure that you have the following per every SBC you want to pair:

- Public IP address (Assigned to the MS Teams interface on Azure cloud)
- FQDN name resolving to the above mentioned Public IP address

SBC Domain Names

The SBC domain name must be from one of the names registered in "Domains" of the tenant. You cannot use the

*.onmicrosoft.com tenant for the domain name.

For example, on the picture below, the administrator registered the following DNS names for the tenant:

DNS Name	Can be used for SBC FQDN	Examples of FQDN names
woodgrovebank.us	Yes	 Valid names: <u>sbc1.woodgrovebank.us</u> <u>ussbcs15.woodgrovebank.us</u> <u>europe.woodgrovebank.us</u> Non-Valid name: <u>sbc1.europe.woodgrovebank.us</u> (requires registering domain name europe.atatum.biz in "Domains" first)
woodgrovebankus.onmicrosoft.com	No	Using *.onmicrosoft.com domains is not supported for SBC names
hybrdvoice.org	Yes	 Valid names: <u>sbc1. hybridvoice.org</u> <u>ussbcs15. hybridvoice.org</u> <u>europe. hybridvoice.org</u> Non-Valid name: <u>sbc1.europe.hybridvoice.org</u> (requires registering domain name europe. <u>hybridvoice.org</u> in "Domains" first)

Please activate and register the domain of tenant.



In this document the following FQDN and IP is used as an example:

Here 52.168.x.x is the public IP of the Azure cloud configured for interface facing MS Teams side

Public IP	FQDN
52.168.x.x	oracleesbc2.woodgrovebank.us

Public trusted certificate for the SBC

It is necessary to setup a public trusted certificate for direct routing. This certificate is used to establish TLS connection between Oracle SBC and MS Teams. The certificate needs to have the SBC FQDN in the subject, common name, or subject alternate name fields. For root certificate authorities used to generate SBC certificate ,refer to Microsoft documentation. <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc</u>

Please refer to the Oracle SBC with Microsoft Teams documentation suitable for your environment (media bypass/non-media bypass) and model (enterprise and carrier) for the steps to configure the following,

- Configure Direct Routing –For pairing the SBC with direct routing
- Microsoft Teams Direct Routing Interface characteristics
- Requirements to SIP messages "Invite" and "Options" For SIP syntax changes according to MS Teams requirements

The links for the documentation are provided <u>here</u>

SBC configuration

This document explains specific changes on the SBC in the Azure cloud environment.

For detailed configuration of Oracle SBC with Microsoft Teams Media Bypass refer to

Oracle ESBC with Microsoft Teams Media Bypass - Enterprise Mode https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/SBC-MSFTTeams-MB-Enabled.pdf

For detailed configuration of Oracle SBC with Microsoft Teams Non-Media Bypass – Enterprise mode refer to https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/SBC-MSFTTeams-NON-MB.pdf

For detailed configuration of Oracle SBC with Microsoft Teams Non- Media Bypass – Carrier Model refer to https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/ESBC%20with%20MS%20Teams%20CarrierModel.pdf

Interface Mapping

The final step in deploying the Oracle SBC in Azure Public cloud is to verify the network interfaces have MAC addresses assigned to them.

- Access the serial console through the Azure portal under support + troubleshooting
- Log into enable mode
- Run the command

>show interface mapping			
Interface Mapping Info			
Eth-IF	MAC-Addr	Label	
wancom0	00:0D:3A:10:5D:FB	#generic	
wancoml	00:0D:3A:17:F0:38	#generic	
s0p0	00:0D:3A:17:FB:EF	#generic	
wancom2	FF:FF:FF:FF:FF	#dummy	
spare	FF:FF:FF:FF:FF	#dummy	
s1p0	FF:FF:FF:FF:FF	#dummy	
s0p1	FF:FF:FF:FF:FF	#dummy	
s1p1	FF:FF:FF:FF:FF	#dummy	
s0p2	FF:FF:FF:FF:FF	#dummy	
s1p2	FF:FF:FF:FF:FF	#dummy	
s0p3	FF:FF:FF:FF:FF	#dummy	
s1p3	FF:FF:FF:FF:FF	#dummy	

- As you can see above, since we have not configured all eight network interfaces possible on the SBC, we'll need to correct the interface to MAC address mappings.
- The interface mapping branch on the SBC includes a swap command, which allows us to make those adjustments. A reboot is required for the changes to take effect.
- While in enable mode in the SBC CLI, type:

```
> # interface-mapping (enter)
> (interface-mapping) # swap wancom1 s1p0
Interface Mapping Info after swapping
_____
Eth-IF MAC-Addr
                               Label
wancom0 00:0D:3A:10:5D:FB
                               #generic
wancom1 FF:FF:FF:FF:FF
                               #dummy
s0p0
       00:0D:3A:17:FB:EF
                               #generic
wancom2 FF:FF:FF:FF:FF
                               #dummy
spare
      FF:FF:FF:FF:FF
                               #dummy
       00:0D:3A:17:F0:38
                               #generic
s1p0
s0p1
       FF:FF:FF:FF:FF
                               #dummy
s1p1
       FF:FF:FF:FF:FF:FF
                               #dummy
s0p2
       FF:FF:FF:FF:FF
                               #dummy
                               #dummy
s1p2
       FF:FF:FF:FF:FF
s0p3
       FF:FF:FF:FF:FF
                               #dummy
s1p3
       FF:FF:FF:FF:FF
                               #dummy
Changes could affect service, and Requires Reboot to become effective.
Continue [y/n]?: y (enter)
```

When the SBC comes back up from reboot, it is now ready for full configuration.

Note: This setting is available only through the CLI now. GUI will be enhanced in the near future to support this feature.

Also note that the usage of "swap" command is based on customer environment. Depending on the setup ,the mapping may vary.

System-Config in SBC

The CLI users can access the configuration by accessing configure terminal->system->system-config .

```
NN3900-101(system-config) # hostname SBC1
NN3900-101(system-config) # location Cloud
NN3900-101(system-config) # done
```

NN3900-101(system-config)# done		
system-config		
hostname	SBC1	
description		
location	Cloud	
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-12-miss-report	enabled	
snmp-syslog-his-table-length	1	
snmp-syslog-level	WARNING	
system-log-level	NOTICE	
process-log-level	NOTICE	
process-log-ip-address	0.0.0.0	

restart	епартео
exceptions	
telnet-timeout	0
console-timeout	0
remote-control	enabled
cli-audit-trail	enabled
source-routing	disabled
cli-more	disabled
terminal-height	24
debug-timeout	0
trap-event-lifetime	0
ids-syslog-facility	-1
pko-rake-pkt	0
pko-rake-burst	0
options	
default-v6-gateway	::
ipv6-signaling-mtu	1500
ipv4-signaling-mtu	1500
cleanup-time-of-day	00:00
snmp-engine-id-suffix	
snmp-agent-mode	v1v2
forwarding-cores	1
dos-cores	1
transcoding-cores	2
last-modified-by	admin@172.18.0.105
last-modified-date	2019-09-25 07:37:52

For WebGUI users, Go to system->system-config

Note: Please follow the link below for steps to activate the WebGUI. https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/SBC-MSFTTeams-MB-Enabled.pdf.

ORACLE	Home Configuration Monitor and Trace	Widgets System
📑 Save 💠 Wizards - 🍄	Commands -	
Objects media-manager 	Modify System config	
security	Hostname:	oracleesbc2.woodgrovebank.us
 session-router system capture-receiver 	Description:	ESBC to Microsoft Teams Direct Routing
fraud-protection	Location:	Bedford, MA
host-route network-interface	Mib system contact:	
network-parameters	Mib system name:	
ntp-config	Mib system location:	
phy-interface redundancy-config	Acp TLS profile:	×
snmp-address-entry	SNMP enabled:	 Image: A start of the start of
snmp-community	Enable SNMP auth traps:	
snmp-group-entry	Enable SNMP syslog notify:	
snmp-view-entry	Enable SNMP monitor traps:	
spl-config	Enable env monitor traps:	
system-access-list	Enable mblk_tracking:	
system-config	Enable I2 miss report:	✓
tdm-config		

For SBC, if transcoding is required, transcoding cores have to be set in system-config. Please refer to documentation here for more information and set cores according to your environment.

https://docs.oracle.com/cd/E85213_01/doc/sbc_scz739_essentials.pdf

Deploying SBC behind Azure NATing

The SPL-configuration is a must for SBC deployed in Cloud Environments.

Here, the SBC is placed behind the Azure NAT. The SBC behind SPL NAT plugin is essential for proper signaling and voice path between the SBC deployed on Azure cloud and PSTN

The plug-in changes information in SIP messages to hide the end point located inside the private network of Azure SBC. Configure the Support for SBC Behind NAT SPL plug-in for each SIP interface on the SBC. Here there are two interfaces, one on the side facing Teams and the other on the PSTN side. 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 configured in Azure Cloud for particular network interface.

Here is an example configuration with SBC Behind NAT SPL config. The SPL is applied to the Teams side SIP interface.

To configure SBC Behind NAT SPL Plug in using the GUI, Go to session-router->sip-interface->spl-options and input the following value, save and activate.

HeaderNatPublicSipIfIp=<Public IP of the Interface facing Teams>,HeaderNatPrivateSipIfIp=<Private IP of the interface facing Teams>

Here HeaderNatPublicSipIfIp is the public interface ip and HeaderNatPrivateSipIfIp is the private ip.

ORACLE	Configuration Monitor and Trace	Widgets System		
E Save Q Wizards - Q Come	nands •			
d Objects	Modify SIP interface			
media-manager				
security	State	8		
session-router	Realm ID:	Access		
access-control	Description			
account-config	CERCIPACITY OF CONTRACT OF CONTRACT.			
account-group				
allowed-elements-profile	T.P. sada			
class-profile	ar pra			
diameter-manipulation	Add Edit C	opy Delete		
enforcement-profile	Address Port	Transport protoco	d TLS profile	Allow anonymou
enum-config	10.0.4.4 5080	UDP		agents-only
filter-config				
▶ h323				
home-subscriber-server				
http-alg	7			
huf-config				
Idap-config	Initial inv trans expire:	0	Range	0.9999999999
local-policy	Session max life limit	0		
local-response-map	Proxy mode:	7	1	
local-routing-contig				
media-profile	Redrect action:		~	
net-management-control	Nat traversal:	none	*	
gos-constraints	Nat interval:	30	Range	0.4294967295)
response-map	TCP out interval			
session anent		W.	parqu	0.4294957200
session anent id sula	Registration caching.	0		
session-constraints	Min reg expire:	300	Range	0.9999999999
session-group	Registration interval:	3600	(Range	0.4294967295)
session-recording-group	Route to registrar:	0		
session-recording-server	free and and and a			
session-timer-profile	Secured network.			
session-translation	Uri figlin domain:			
sip-advanced-logging	Options:	Add L Edit L 1	Contentia	
sip-config				
sip-feature				
sip-feature-caps				
sip-interface				
sip-manipulation				
sip-monitoring				
sip-recursion-policy				
surrogate-agent	spr options.	HeaderNatPublicSipifip+172	2.18.0.5.Heak	

Similarly configure the PSTN side as well.

To configure SBC Behind NAT SPL Plug in using the CLI, Go to configure terminal-> session-router->sip-interface-> Select the sip-interface

```
spl-options + HeaderNatPublicSipIfIp=<Public IP of the Interface facing
Teams>,HeaderNatPrivateSipIfIp=<Private IP of the interface facing Teams>
```

Click on done. Save and activate the config.



AzureSBC1# sh con sip-interface sh	
sip-interface	
realm-id	Access
sip-port	
address	10.0.4.4
port	5065
sip-port	
address	10.0.4.4
port	5065
transport-protocol	TCP
allow-anonymous	agents-only
options	strip-route-headers
spl-options	HeaderNatPublicSipIfIp=172.18.0.5,Header
NatPrivateSipIfIp=10.0.4.4	



CONNECTWITHUS



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

Worldwide Inquiries Phone: +1.650.506.7000 Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2019, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0616