



**Business
Services**

Guide for BTIP and Business Talk SIP services Microsoft Teams Direct Routing

13 february 2020

Teams Direct Routing AudioCodes Checklist 0.17
AudioCodes FAX checklist for Skype 1.1 (adapted to Teams)
Teams Direct Routing Ribbon Checklist 1.0
Teams Direct Routing Oracle Checklist 0.4

Contents

1	Main certified architectures	4
2	Parameters for connection to BTIP/BTalk	16
3	BTIP/BTalk/BTol certified versions	18
4	AudioCodes SBC Configuration Checklist for BTIP/BTalk/BTol	19
5	Ribbon SBC Configuration Checklist for BTIP/BTalk	39
6	Oracle SBC Configuration Checklist for BTIP/BTalk	47

1 Main certified architectures

Note that architectures with no Media Bypass nor Media Optimization are certified with AudioCodes, Ribbon and Oracle SBC.

Media Bypass has been certified so far with AudioCodes SBC. It is in progress also for Ribbon and Oracle. As a reminder, Media Bypass means bypassing Teams cloud (actually Teams Media Processors) for media flows.

Media Optimization would be keeping media flow within BVPN for internal users. Orange is being involved in the Microsoft Technology Adoption Program (TAP) for this feature. Formal certification is expected in Q2/2020.

Concerning the FAX support, Business talk and BTIP support the following usage:

- FAX servers connected to the IPBX* -and sharing same dial plan-,
- FAX servers as separate ecosystems -and separate dial plan-,
- Analog FAX machines, usually connected to specific gateways* (seen as IPBX ecosystem or not).

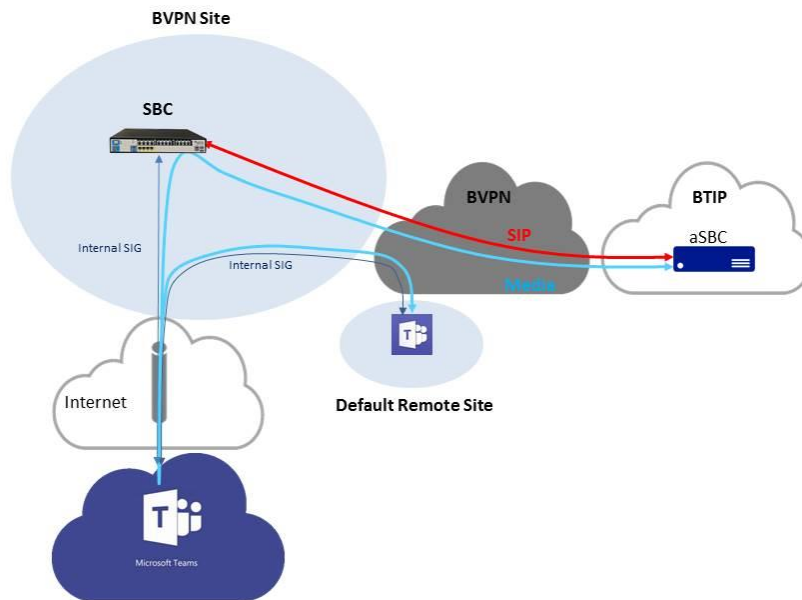
Microsoft Teams does not directly handle FAX, neither analog devices. Those devices can only be interconnected with Teams through the Direct Routing SBC or ATA boxes linked to the Direct Routing SBC and would be fully managed by the Direct Routing SBC. This has been certified with AudioCodes devices so far.

FAX flows are handled via T.38 transport only.

Note also that BTIP/BTalk/BToI redundancy mechanisms are not shown on the drawings. This is not the aim of this document.

1.1 Standalone mode

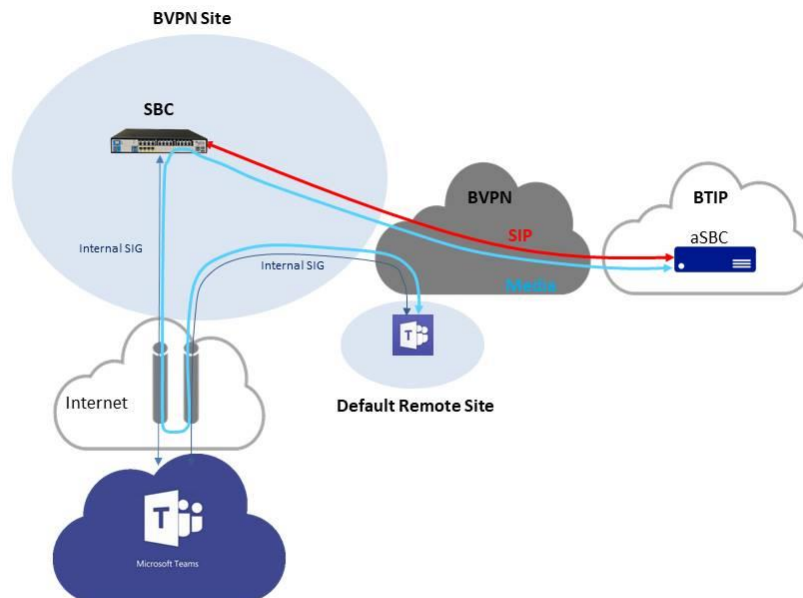
Example 1a – offnet call from a BVPN remote site without Media Bypass



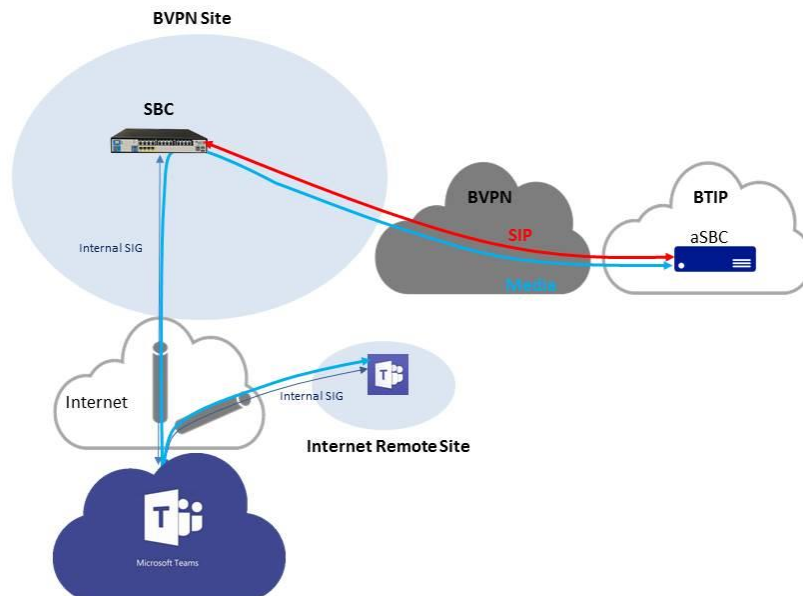
Here, the Teams user belongs to a BVPN site, as does the SBC. There is no Internet breakout within the local site, though that could be the recommended architecture.

Without Media Bypass, media flows cross Internet to reach Teams Media Processors and SBC.

Example 2 – offnet call from a BVPN remote site with Media Bypass

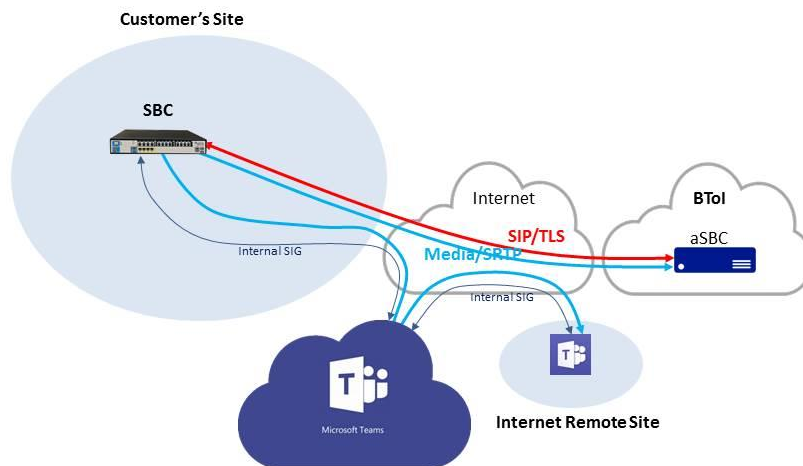


With Media Bypass, media flows cross Internet and join directly Teams user and SBC. They may cross a Microsoft Transport Relay for NAT traversal reasons, but Transport Relays are much more numerous than Media Processors and provide no time consuming treatment of the media.

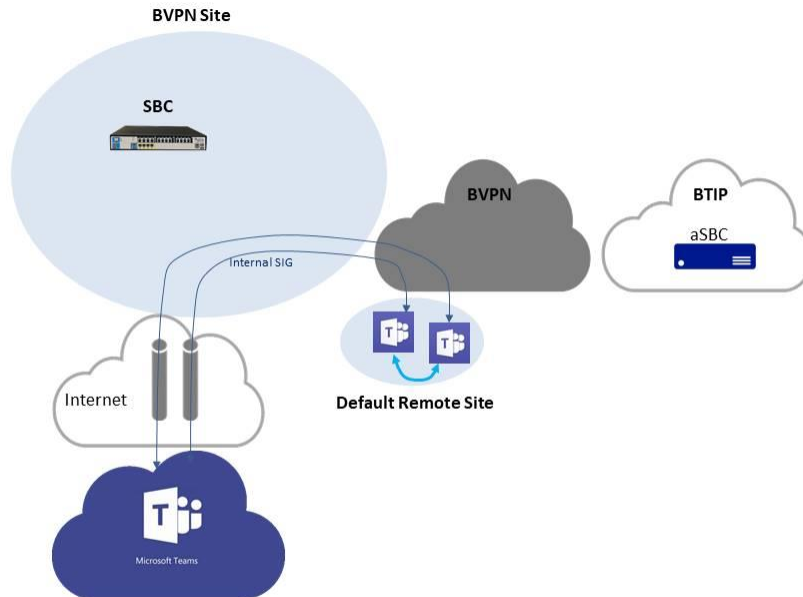
Example 3 – offnet call from an Internet remote site

Here, the Teams user does not belong to a BVPN site and is located on Internet.

Example 4 – offnet call from an Internet remote site with BTol (Business Talk over Internet)



BVPN is not mandatory in a Business Talk over Internet architecture. Here is a full Internet architecture. Note that the flows are encrypted from end to end.

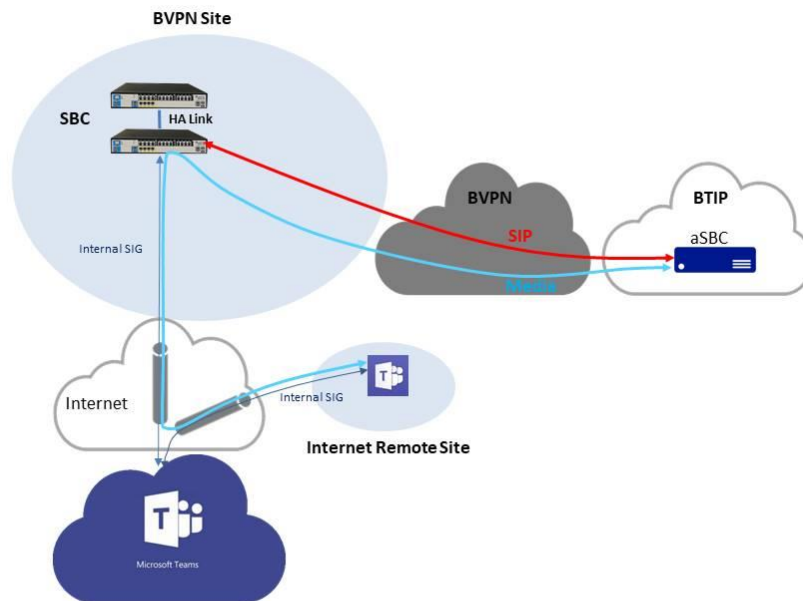
Example 5 – onnet BVPN call

In a BVPN architecture, media flows between Teams users belonging to a single BVPN are direct, whether they are on the same site or in distinct sites.

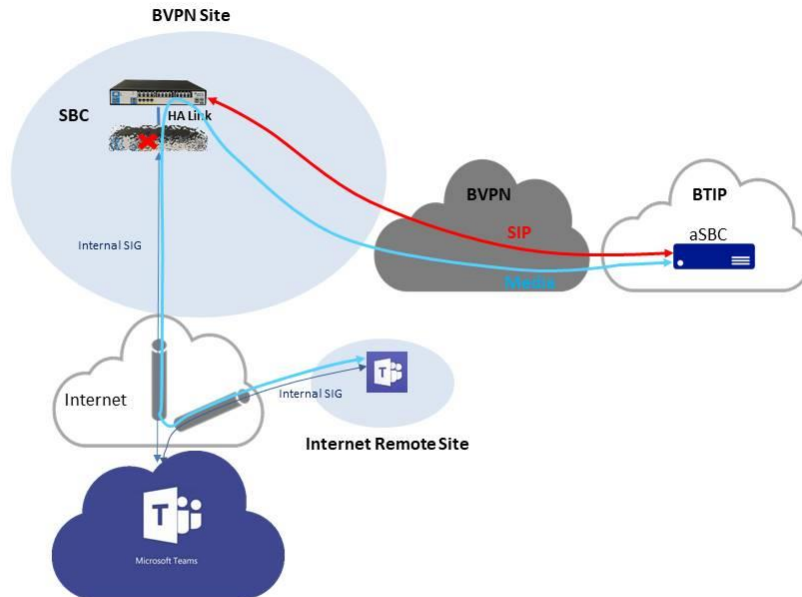
1.2 High Availability mode

High availability is provided by SBC vendor. This is active-passive mode with a single IP address. From BTIP/BTalk perspective, this is like a single SBC.

Example 1 – offnet call in nominal mode (and Media Bypass)



HA is fully managed by SBC themselves. From Teams and BTIP/BTalk points of view, the architecture behaves as if there was a single SBC.

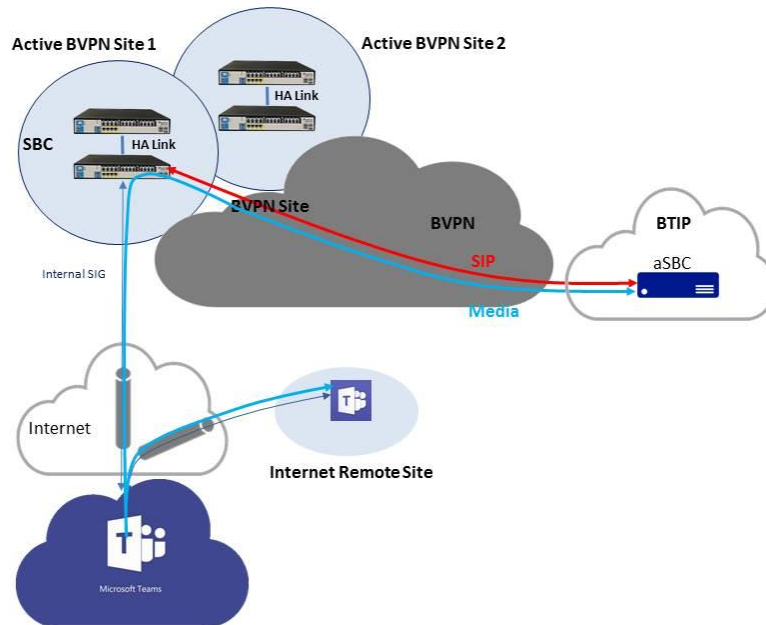
Example 2 – offnet call in backup mode (and Media Bypass)

When the nominal SBC fails, the backup SBC transparently handles the service. Current calls are not cut.

1.3 Active-active mode (resiliency)

From BTIP/BTalk perspective, meaning of active-active mode for incoming offnet calls is actually round-robin mode.

Example 1 – offnet call in an architecture combining two BVPN sites in active-active mode with two SBC in High Availability mode in each



Here is an example of a somewhat highly resilient architecture that mixes spatial redundancy with load balancing and high availability on each SBC site. The two geographic SBC sites are supposed to be both located in the same region as the a-SBC pair they are trunked to.

Teams use DNS load balancing between the two geographic SBC sites for routing outbound offnet calls. On the other and, BTIP/BTalk provides round-robin between the two sites. The two sites are active-active. In addition, there is here an active-passive resilience within each site.

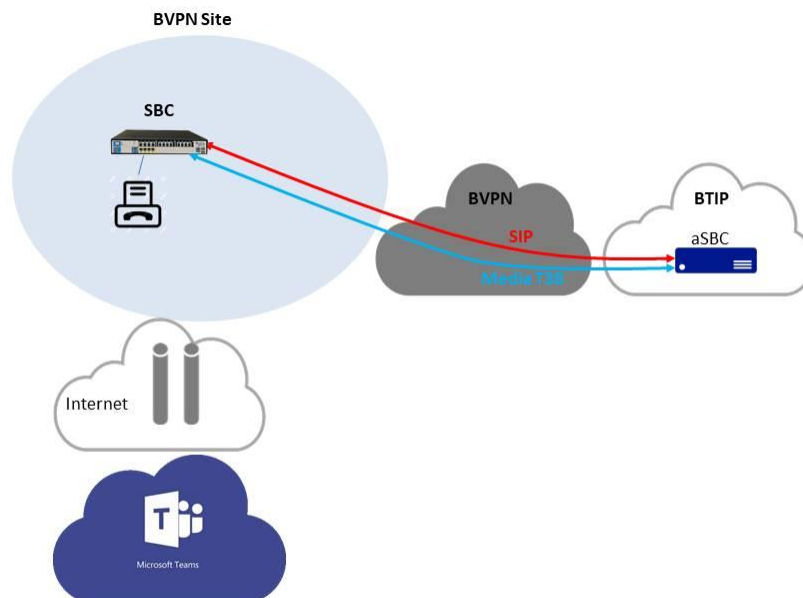
In the next chapter describing connections to BTIP/BTalk, this architecture would be “N SBC pairs - BTalk round robin mode over N pairs in vendor HA mode” with N=2. Of course, a simpler architecture without the High Availability part could be considered as well.

1.4 FAX

FAX on Direct Routing SBC (so far AudioCodes GW) with or without Gateway (so far Media Pack GW) is certified both on French (BTIP) and International (BTalk) scopes. FAX protocol is T.38.

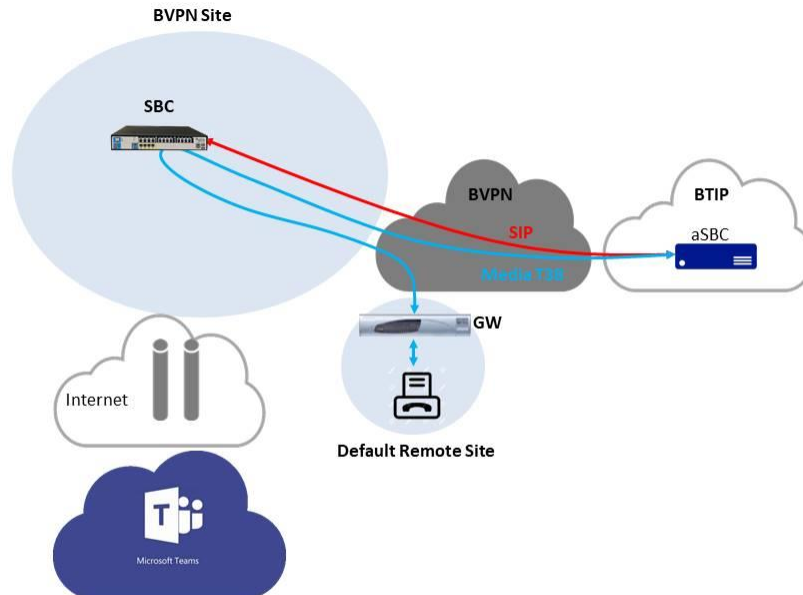
FAX calls to and from Business Talk consumes the same SIP Trunk that is used for interconnection with Teams. When a call is made from FAX or to FAX, the Direct Routing SBC bypasses Teams, which does not talk T.38.

Example 1 - FAX directly connected to SBC



The analog FAX device can be connected directly to DR SBC to FXS ports. Call is routed directly between Business Talk / Business Talk IP and FAX.

Example 2 - FAX connected to a cascaded GW behind SBC



In this architecture FAX device is connected to an analog telephony adapter. It is integrated with DR SBC which can be placed in other remote site or in datacenter. DR SBC with no directly connected endpoints can be virtualized.

Same as in previous architecture call is routed directly between Business Talk / Business Talk IP and FAX and bypasses Teams.

1.5 Sizing considerations

Without Media Optimization, flows between SBC and aSBC only are involved in RTVo.

Regarding codec usage in the standard architecture:

- RTP G711 is used between Direct Routing SBC and BTIP/BT,
- SRTP G711 is forced between Teams and The Direct Routing SBC so that transcoding is avoided,
- encrypted SILK or G722 is used between Teams Client and Teams Media Processors,

Therefore, a channel for an offnet call may be considered to consume 100 kbps throughout its path.

	Central site			Remote site with Internet breakout			Remote site without Internet breakout	
	CE Router		Internet router	CE Router		Internet router	CE Router	
	RTVo	D1		RTVo	D1		RTVo	D1
Offnet calls								
From/to central site	1		2					
From/to remote site with Internet breakout	1		1			1		
From/to remote site without Internet breakout	1	1	2					1
Onnet BVPN calls								
From/to a local client								
Between central site and a remote client		1						
Between remote site with Internet breakout and a remote client					1			
Between remote site without Internet breakout and a remote client								1
External calls (between BVPN & Internet clients)								
From/to central site			1					
From/to remote site with Internet breakout						1		
From/to remote site without Internet breakout		1	1					1

In this table, far end site is not considered. Note that when a call is put on hold, there is no Music on Hold played so far with Direct Routing.

2 Parameters for connection to BTIP/BTalk

Head Quarter (HQ) architecture	Level of Service	@IP used by the service
Single SBC	No redundancy	SBC IP@
SBC pair - Vendor HA mode	Local redundancy with nominal/backup behavior. No loss of calls in case of nominal's failure. Single site.	SBC pair floating IP@
	Extended local redundancy with nominal/backup behavior. No loss of calls in case of nominal's failure. Two sites linked at L2 level.	
N SBC - BTalk round robin mode - Mono region	Local redundancy and load sharing with round robin behavior. Loss of calls handled by a SBC that fails. DNS load balancing from Teams point of view. Single site.	SBC1 IP@ SBC2 IP@ ... SBCN IP@
	Geographical redundancy and load sharing with round robin behavior. Loss of calls handled by a SBC that fails. DNS load balancing from Teams point of view. M sites ($M \leq N$) in the same region (i.e. attached to the same aSBC pair with a single T1T7).	
N SBC pairs - BTalk round robin mode over N pairs in vendor HA mode - Mono region	Local + geographical redundancy and load sharing. If a SBC fails locally, active calls not lost and handled by new active SBC. If a full site fails, active calls are lost, but all users keep the offnet service. In addition, there is a load-balancing between sites : round-robin from BTIP/BT side and DNS load balancing from Teams side.	SBC pair1 floating IP@ SBC pair2 floating IP@ ... SBC pairN floating IP@

2 SBC pairs - BTalk round robin mode over 2 pairs in vendor HA mode - Multi region (Business Talk only). Limited to 2 pairs for easier understanding. May be extended to N pairs, at least one per involved region.	For users in region 1: offnet calls to/from users of the region 1 are routed through the Direct Routing SBC pair of region 1, located in site 1. For Business Talk, a T1T7 per region permits this routing. For Teams, a second route must be configured for users. If a single SBC in site 2 fails, the backup SBC handles the traffic. If a single SBC in site 1 fails, the backup SBC handles the traffic. If the full site fails, Direct Routing SBC pair of region 2 rescues the offnet service of users, assuming that RTD is acceptable for VoIP.	SBC pair1 floating IP@ SBC pair2 floating IP@
	For users in region 2: offnet calls to/from users of the region 2 are routed through the Direct Routing SBC pair of region 2, located in site 2. For Business Talk, a T1T7 per region permits this routing. For Teams, a second route must be configured for users. If a single SBC in site 2 fails, the backup SBC handles the traffic. If the full site fails, Direct Routing SBC pair of region 1 rescues the offnet service of users, assuming that RTD is acceptable for VoIP.	
2 SBC Nominal / Backup mode	- Local redundancy: both SBC are hosted on the same site, though HA is preferred here if supported by SBC vendor OR - Geographical redundancy both SBC are hosted on 2 different sites with WAN onnectivity	SBC1 @IP SBC2 @IP
2 SBC pairs Nominal / Backup mode	'- Local and geographical redundancy SBC pairs are hosted on 2 different sites with WAN onnectivity, each pair on one site	SBC pair1 floating @IP SBC pair2 floating @IP

Remote Site (RS) architecture**	Level of Service
Remote site without survivability	No survivability, no trunk redundancy

3 BTIP/BTalk/BTol certified versions

3.1 Teams

There is no release numbering of Microsoft Teams. This is continuous delivery. Therefore, the compatibility of the 3 main components, i.e. certified AudioCodes w Teams and BTIP/BTalk cannot be fully committed at any time.

3.2 Certified SBC

Certified with standard architectures are:

Vendor	Model	Release	BTIP	BTalk	BTol	Media Bypass	Media Optimization	FAX
AudioCodes	M500/800/1000/2600/4000/9000 & VE	v.7.20A, build 254.475+	✓	✓	✓	✓	Planned	✓
Ribbon	Edge 1000/2000 & SweLite	8.0.1v181+	✓	✓	In progress	In progress	Planned	In progress
Oracle	Acme Packet 1100/3900/4600/6300/6350 & VME	S-Cz8.3.0 p3	✓	✓	No	In progress	Planned	No

3.3 Endpoints

As far as Media Optimization is not certified for BTIP/BTalk, all Microsoft-certified endpoints are certified with Direct Routing and BTIP/BTalk.

4 AudioCodes SBC Configuration Checklist for BTIP/BTalk/BToI

The checklist below presents all steps of configuration required for VISIT SIP Teams deployment.

Configuration checklist regarding **Trunk configuration on the Tenant**

Parameters to configure:

Fqdn	<i><Customer SBC Public FQDN></i>
SipSignallingPort	<i>5061</i>
MaxConcurrentSessions	<i><Number of max sessions></i>
Enabled	<i>\$true</i>
ForwardPai	<i>\$true</i>
SendSipOptions	<i>\$true</i>

```
#New-CsOnlinePSTNGateway -Fqdn sbc.contoso.com -SipSignallingPort 5061 -
MaxConcurrentSessions 50 -Enabled $true -ForwardPai $true -MediaBypass $false -
ForwardCallHistory $true -SendSipOptions $true
```

To activate media bypass at Tenant level:

```
#Set-CsOnlinePSTNGateway -Identity sbc.contoso.com -MediaBypass $true
```

Notes:

- **media bypass is only compatible from Audiocodes version 7.20A.254.475.**

4.1 Configuration checklist for Mediant SBC – Standalone

- Step 1 – IP Network configuration
- Step 2 – Teams configuration
- Step 3 – Business Talk configuration
- Step 4 – Routing configuration

Step 1 - IP Network configuration

Ethernet Groups

On the Mediant WebUi Interface:
SETUP > IP Network > Core entities >
Ethernet Groups

- ✓ 1 Ethernet Group for Teams (**GROUP_1**)
- ✓ 1 Ethernet Group for BTIP or BToI (**GROUP_2**)
- ✓ [Optional] 1 Ethernet Group for HA (**GROUP_3**)

Ethernet Devices

SETUP > IP Network > Core entities > Ethernet Devices	✓ 1 Ethernet Device for Teams (EthD_Teams) ✓ [Optional] 1 Ethernet Device for HA (EthD_HA) ✓ <u>If BT/BTIP:</u> ✓ 1 Ethernet Device for BTIP (EthD_BTIP) ✓ <u>If BTol:</u> ✓ 1 Ethernet Device for BTIP (EthD_BTol) ✓ 1 Ethernet Device for BTIP (EthD_LAN)
IP Interfaces	
SETUP > IP Network > Core entities > IP Interface Devices	✓ 1 IP Interface for Teams (IPInt_Teams) ✓ [Optional] 1 IP Interface for HA (IPInt_HA) ✓ <u>If BT/BTIP:</u> ✓ 1 IP Interface for BTIP (IPInt_BTIP) ✓ <u>If BTol:</u> ✓ 1 IP Interface for BTol (IPInt_BTol) ✓ 1 IP Interface for LAN (IPInt_LAN)
NAT Translation	
SETUP > IP Network > Core entities > NAT Translation	✓ Create 1 rule for Teams signalization traffic - Source Interface : IPInt_Teams - Source Start Port : 5061 - Source End Port : 5061 - Target IP Address: <SBC Teams Public IP Address> - Target Start Port: - Target End Port: ✓ Create 1 rule for Teams media traffic - Source Interface : IPInt_Teams - Source Start Port : 49160 - Source End Port : 65529 - Target IP Address: <SBC Teams Public IP Address> - Target Start Port: - Target End Port: <u>If BTol:</u> ✓ Create 1 rule for BTol signalization traffic - Source Interface : IPInt_BTol - Source Start Port : 5061 - Source End Port : 5061 - Target IP Address: <SBC BTol Public IP Address> - Target Start Port: - Target End Port: ✓ Create 1 rule for Teams media traffic - Source Interface : IPInt_BTol - Source Start Port : 6000 - Source End Port : 40999 - Target IP Address: <SBC BTol Public IP Address> - Target Start Port:

	- Target End Port:
Security	
TLS Contexts	
On the Mediant WebUi Interface: SETUP > IP Network > Security > TLS Contexts	✓ Create new TLS Context for Teams traffic - Name: Teams-TLSContext - TLS Version: TLSv1.2 - DTLS Version: DTLSv1.2 - DH Key Size: 2048
SETUP > IP Network > Security > TLS Contexts > Teams-TLSContext > Change Certificate	Create a new CSR for Teams SBC FQDN and send it to the public certification authority for signing. Then upload it to the Mediant.
SETUP > IP Network > Security > TLS Contexts > Teams-TLSContext > Trusted Root Certificates	Import Root/ Intermediate Certificates
On the Mediant WebUi Interface: SETUP > IP Network > Security > TLS Contexts	<u>If BTol:</u> ✓ Create new TLS Context for BTol traffic - Name: BTol-TLSContext - TLS Version: TLSv1.2 - DTLS Version: DTLSv1.2 - DH Key Size: 2048
SETUP > IP Network > Security > TLS Contexts > BTol-TLSContext > Change Certificate	Create a new CSR for BTol SBC FQDN and send it to the public certification authority for signing. Then upload it to the Mediant.
SETUP > IP Network > Security > TLS Contexts > BTol-TLSContext > Trusted Root Certificates	Import Root/ Intermediate Certificates
Firewall [Warning: not fully tested]	
On the Mediant WebUi Interface: SETUP > IP Network > Security > Firewall	✓ Create new access lists for public DNS - Index: 0 - Description: <DNS public IP> (eg. 8.8.8.8) - Source IP: <DNS public IP> (eg. 8.8.8.8) - Prefix Length: 32 - Use specific interface: Enable - Interface Name: IPInt_Teams - Action Upon Match: Allow ✓ Create new access lists for each Teams proxy (6 in Total) - Index: 1 to 6 - Description: <Teams proxy IP> (eg. 52.114.76.76) - Source IP: < Teams proxy IP > (eg. 52.114.76.76) - Prefix Length: 32 - Use specific interface: Enable - Interface Name: IPInt_Teams - Action Upon Match: Allow ✓ Create new access list to block all other networks (6 in Total). This rule has to be the last of the list. - Index: 49 - Description: 0.0.0.0 - Source IP: 0.0.0.0

	- Prefix Length: 0 - Use specific interface: Enable - Interface Name: IPInt_Teams - Action Upon Match: Block <u>If BTol:</u> ✓ Create new access lists for public DNS - Index: 0 - Description: <DNS public IP> (eg. 8.8.8.8) - Source IP: <DNS public IP> (eg. 8.8.8.8) - Prefix Length: 32 - Use specific interface: Enable - Interface Name: IPInt_BTol - Action Upon Match: Allow ✓ Create new access lists for each Teams proxy (6 in Total) - Index: 1 - Description: <BTol public IP> - Source IP: <BTol public IP> - Prefix Length: 32 - Use specific interface: Enable - Interface Name: IPInt_BTol - Action Upon Match: Allow ✓ Create new access list to block all other networks (6 in Total). This rule has to be the last of the list. - Index: 49 - Description: 0.0.0.0 - Source IP: 0.0.0.0 - Prefix Length: 0 - Use specific interface: Enable - Interface Name: IPInt_BTol - Action Upon Match: Block
--	--

Step 2 - Teams Configuration

Coder Groups

On the Mediant WebUi Interface:
SETUP > Signaling&Media > Coders &
Profiles > Coder Groups

- ✓ Configure AudioCodersGroups_1
 - Coder Name: **G711A-law**
 - Packetization Time: **20**
 - Rate: **64**
 - Payload Type: **8**
 - Silence Suppression: **Disabled**

Allowed Audio Coder Groups

On the Mediant WebUi Interface:
SETUP > Signaling&Media > Coders &
Profiles > Allowed Audio Coders
Groups

- ✓ Create Teams_AudioCoders
- ✓ Select the created entry, then click on "Allowed Audio Coders 0 Items" and click on new:
 - Coder Name: **G711A-law**

IP Profile

SETUP > Signaling&Media > Coders &
Profiles > IP Profiles

- ✓ Create new IP Profile for Teams
 - Name: **Teams-IPProfile**
 - SBC Media Security Mode: **SRTP**
 - SBC Enforce MKI Size: **Enforce**
 - Reset SRTP Upon Re-key: **Enable**
 - Generate SRTP Keys Mode: **Always**
 - Remote Early Media RTP Detection Mode: **By Media**
 - Extension Coders Group: **AudioCodersGroup_1**
 - Allowed Audio Coder: **Teams_AudioCoders**
 - Allowed Coders mode: **Restriction and Preference**
 - RTCP Mode: **Generate Always**
 - ICE Mode: **Lite**
 - Remote Update Support: **Not Supported**
 - Remote re-INVITE: **Supported only with SDP**
 - Remote Delayed Offer Support: **Not Supported**
 - Remote REFER Mode: **Handle locally**
 - Remote 3xx Mode: **Handle locally**
 - Remote Hold Format: **Inactive**

Media Realm

SETUP > Signaling&Media > Core
Entities > Media Realms

- ✓ Create new Media Realm for Teams traffic
 - Name: **Teams-Media**
 - Topology location: **UP**
 - IPv4 Interface Name: **IPInt_Teams**
 - Port Range Start: **49160**
 - Number of Media Session Legs: **1637**
 - Default Media Realm: **Yes**

SIP Interface

SETUP > Signaling&Media > Core
Entities > SIP Interface

- ✓ Create new SIP Interface for Teams traffic
 - Name : **Teams-SIPInterface**
 - Topology Location: **UP**
 - Network Interface : **IPInt_Teams**
 - UDP Port : **0**
 - TCP Port: **0**
 - TLS Port: **5061**
 - Enable TCP Keep alive: **Enable**

	- Classification Failure response Type: 0 - Media Realm: Teams-Media - TLS Context Name: Teams-TLSContext - TLS Mutual Authentication: Disable
Proxy Set	
SETUP > Signaling&Media > Core Entities > Proxy Set	✓ Create new Proxy Set for Teams traffic - Name : Teams-Proxies - SBC IPv4 SIP Interface : Teams-SIPInterface - TLS Context Name: Teams-TLSContext - Proxy Keep-Alive : Using OPTIONS - Proxy Keep-Alive Time : 600 - Proxy Hot swap: Enable - Proxy Load Balancing method: Random Weights (Proxy Address Table) : Create 3 Entries for Teams Proxies - Index: 0 - Proxy Address: sip.pstnhub.microsoft.com:5061 - Transport Type: TLS - Priority Proxy: 1 - Proxy Random Weight: 1 - Index: 1 - Proxy Address: sip2.pstnhub.microsoft.com:5061 - Transport Type: TLS - Priority Proxy: 2 - Proxy Random Weight: 1 - Index: 2 - Proxy Address: sip3.pstnhub.microsoft.com:5061 - Transport Type: TLS - Priority Proxy: 3 - Proxy Random Weight: 1
Message Manipulation	
SETUP > Signaling&Media > Message Manipulations	✓ Create new message manipulation "Teams_Privacy_Removal" - Name : Teams_Privacy_Removal - Manipulation Set ID: 1 - Row Role: Use Current Condition - Match> Message Type: Invite.Request - Match> Condition: Header.From.URL.user != 'anonymous' - Action> Action Subject: Header.Privacy - Action> Action Type: Remove - Action> Action Value:
SETUP > Signaling&Media > Message Manipulations	✓ Create new message manipulation "Teams_Privacy_Modification" - Name : Teams_Privacy_Modification - Manipulation Set ID: 2 - Row Role: Use Current Condition - Match> Message Type: Any - Match> Condition: Header.Privacy contains ',' - Action> Action Subject: Header.Privacy - Action> Action Type: Modify

	✓ Action> Action Value: 'id'
IP Group	
SETUP > Signaling&Media > Core Entities > IP Group	✓ Create new IP Group for Teams traffic - Name : Teams-IPGroup - Topology Location: UP - Proxy Set: Teams-Proxies - IP Profile: Teams-IPProfile - Media Realm: Teams-Media - SIP Group Name: <Customer Teams Public FQDN> - Classify by Proxy Set: Disable - Local Host Name: <Customer Teams Public FQDN> - Always use src Address: Yes - DTLS Context: Teams-TLSContext - Proxy Keep-Alive using IP Group settings: Enable - Inbound Message Manipulation Set: 1 (Manipulation set id including manipulations:"Teams_Privacy_Removal") - Outbound Message Manipulation Set: 2 (Manipulation set id including manipulations:"Teams_Privacy_Modify")
Media Security	
SETUP > Signaling&Media > Media > IP Media Security	✓ Configure following parameters: - Media Security : Enable
RTP / RTCP settings	
SETUP > Signaling&Media > Media > IP RTP/RTCP Settings	✓ Configure following parameters: - RTP UDP Port Spacing : 10 - RFC2833 TX Payload Type: 101 - FC 2833 Rx Payload Type: 101
DSP Settings	
SETUP > Signaling&Media > Media > DSP Settings	✓ Configure following parameters: - Answer Detector Activity Delay: 512 - Answer Detector Silence Time: 96 - Answer Detector Sensitivity: 2 - Energy Detector Quality Factor: 0 - Energy Detector Threshold: 0
Proxy & Registration	
SETUP > Signaling&Media > Message Manipulation > Proxy & Registration	✓ Configure following parameters: - Gateway Name: <Customer SBC Teams Public FQDN> - Use Gateway Name for Options: Yes
Message Condition	
SETUP > Signaling&Media > SIP Definitions > Message Conditions	✓ Create new message condition for incoming SIP messages - Name : a teams contact - Condition: header.contact.url.host contains 'pstnhub.microsoft.com'
Classification	
SETUP > Signaling&Media > SBC > Classification	✓ Create new classification - Name : From Teams-IPGroup - Source SIP Interface: Teams-SIPInterface - Source IP Address: 52.114.*.* - Destination Host: <Customer SBC Teams Public FQDN> - Message Condition: a teams contact

	- Source IP Group: Teams-IPGroup
SBC General Settings	
SETUP > Signaling&Media > SBC > SBC General Settings	✓ Configure following parameters: - SBC Performance Profile: Optimized for transcoding

Step 3 - Business Talk Configuration

Coder Groups	
On the Mediant WebUi Interface: SETUP > Signaling&Media > Coders & Profiles > Coder Groups	✓ Configure AudioCodersGroups_2 - Coder Name: G711A-law - Packetization Time: 20 - Rate: 64 - Payload Type: 8 - Silence Suppression: Disabled
Allowed Audio Coder Groups	
On the Mediant WebUi Interface: SETUP > Signaling&Media > Coders & Profiles > Allowed Audio Coders Groups	✓ Create BTIP_AudioCoders ✓ Select the created entry, then click on "Allowed Audio Coders 0 Items" and click on new: - Coder Name: G711A-law
IP Profile	
SETUP > Signaling&Media > Coders & Profiles > IP Profiles	✓ Create new IP Profile for Business Talk <u>If BT/BTIP:</u> - Name: BTIP-IPProfile - SBC Media Security Mode: RTP - <u>If BTol:</u> - Name: BTol-IPProfile - SBC Media Security Mode: SRTP - <u>For Both BT/BTIP and BTol:</u> - Symmetric MKI: Disable - MKI Size: 0 - Extension Coders Group: AudioCodersGroup_2 - Allowed Audio Coders: AudioCoders_BTIP - Allowed Coders Mode: Restriction and Preference - RFC2833 DTMF Payload Type: 101 - P-Asserted-Identity header mode: Add - Remote REFER Mode: Handle locally - Remote Replaces Mode : Handle Locally - Remote 3xx Mode: Handle locally - Remote Hold Format: Send Only
Media Realm	
SETUP > Signaling&Media > Core Entities > Media Realms	✓ Create new Media Realm for Business Talk <u>If BT/BTIP:</u> - Name: BTIP-Media - Topology location: DOWN - IPv4 Interface Name: IPInt_BTIP - Port Range Start: 16400 - Number of Media Session Legs: 1000

	<u>If BTol:</u> - Name: BTol-Media - Topology location: DOWN - IPv4 Interface Name: IPInt_BTol - Port Range Start: 6000 - Number of Media Session Legs: 3500 <u>For Both BT/BTIP and BTol:</u> - Default Media Realm: No
SIP Interface	
SETUP > Signaling&Media > Core Entities > SIP Interface	✓ Create new SIP Interface for Business Talk <u>If BT/BTIP:</u> - Name : BTIP-SIPInterface - Topology location: DOWN - Network Interface : IPInt_BTIP - TCP Port: 5060 - TLS Port: 0 - Media Realm: BTIP-Media <u>If BTol:</u> - Name : BTol-SIPInterface - Network Interface : IPInt_BTol - TCP Port: 0 - TLS Port: 5061 - Media Realm: BTol-Media - TLS Context Name: BTol-TLSContext - TLS Mutual Authentication: Enable <u>For Both BT/BTIP and BTol:</u> - Topology Location: DOWN - UDP Port : 0
Proxy Set	

SETUP > Signaling&Media > Core Entities > Proxy Set	✓ Create new Proxy Set for Business Talk <u>If BT/BTIP:</u> - Name : BTIP-Proxies - SBC IPv4 SIP Interface : BTIP-SIPInterface - Proxy Keep-Alive: Using OPTIONS - Proxy Keep-Alive Time: 600 - Redundancy Mode: Homing - Proxy Hot swap: Enable <u>If BTol:</u> - Name : BTIP-Proxies - SBC IPv4 SIP Interface : BTIP-SIPInterface - Proxy Keep-Alive : Using OPTIONS - Proxy Keep-Alive Time : 600 (Proxy Address Table) : <u>If BT/BTIP:</u> Create 2 Entries for Business Talk Proxies - Proxy Address : <Nominal SBC ACME>:5060 - Transport Type : TCP - Proxy Address : <Backup SBC ACME>:5060 - Transport Type : TCP <u>If BTol:</u> Create the Entries for Business Talk Proxy - Proxy Address : < BTol Public @IP >:5061 - Transport Type: TLS
Message Manipulation	
SETUP > Signaling&Media > Message Manipulations	✓ Create new message manipulation "User-Agent_Modification » - Name : User-Agent_Modification - Manipulation Set ID: 31 - Row Role: Use Current Condition - Match> Message Type: any - Match> Condition: - Action> Action Subject: Header.User-Agent - Action> Action Type: Modify - Action> Action Value: Header.User-Agent.Content + 'Teams'
IP Group	
SETUP > Signaling&Media > Core Entities > IP Group	✓ Create new IP Group for Business Talk <u>If BT/BTIP:</u> - Name : BTIP-IPGroup - Proxy Set: BTIP-Proxies - IP Profile: BTIP-IPProfile - Media Realm: BTIP-Media - DTLS Context: <empty> <u>If BTol:</u> - Name : BTol-IPGroup - Proxy Set: BTol-Proxies - IP Profile: BTol-IPProfile

	- Media Realm: BTol-Media - DTLS Context: BTol-TLSContext <u>For Both BT/BTIP and BTol:</u> - Topology Location: DOWN - Outbound Message Manipulation Set: 3 (Manipulation set id including manipulations "User-Agent_Modification")
	-

Step 4 – Routing configuration

IP to IP Routing

On the Mediant WebUi Interface:
SETUP > Signaling&Media > SBC >
Routing > IP-to-IP Routing

✓ Create 4 IP to IP routing rules:

1st one regarding OPTIONS Messages:

- Name: **SIP-OPTIONS-Terminate**
- Match > Source IP Group: **Any**
- Match > Request Type: **OPTIONS**
- Match > ReRoute IP Group: **Any**
- Action > Destination Type: **Dest Address**
- Action > Destination Address: **internal**

2nd one regarding REFER Messages:

- Name: **REFER-Terminate**
- Match > Source IP Group: **Any**
- Match > Request Type: **REFER**
- Match > ReRoute IP Group: **Any**
- Action > Destination Type: **Request URI**
- Action > Destination Address: **Teams-IPGroup**

3rd one regarding Business Talk to Teams traffic:

- Name: **BTIP(or BTol) to Teams**
- Match > Source IP Group: **BTIP-IPGroup (or BTol-IPGroup)**
- Match > ReRoute IP Group: **Any**
- Action > Destination IP Group: **Teams-IPGroup**

4th one regarding Teams to Business Talk traffic:

- Name: **Teams to BTIP(or BTol)**
- Match > Source IP Group: **Teams-IPGroup**
- Match > ReRoute IP Group: **Any**
- Action > Destination IP Group: **BTIP-IPGroup (or BTol-IPGroup)**

4.2 Configuration checklist for Mediant SBC – HA

- Step 1 – Configuration of the first SBC Mediant for HA
- Step 2 – Configuration of the second SBC Mediant for HA
- Step 3 – Initialize HA on the devices

Step 1 – Configuration of the first Mediant for HA

Note: During this stage, make sure that the second device is powered off or disconnected from network.

Ethernet Groups	
On the Mediant WebUi Interface: SETUP > IP Network > Core entities > Ethernet Groups	✓ Use a dedicated Ethernet Group for HA (GROUP_3)
Ethernet Devices	
SETUP > IP Network > Core entities > Ethernet Devices	✓ Create 1 Ethernet Device for HA - Name: EthD_HA - VLAN ID: 3 - Underlying interface: GROUP3 - Tagging: Untagged - MTU: 1500
IP Interfaces	
SETUP > IP Network > Core entities > IP Interface Devices	✓ Create 1 IP Interface for HA (IPInt_HA) - Name: IPInt_HA - Application Type: MAINTENANCE - Ethernet Device: EthD_HA - IP Address: 192.168.0.1 - Prefix length: 24 - Default Gateway: 0.0.0.0
HA Settings	
SETUP > IP Network > Core entities > HA Settings	✓ Configure following parameters: - HA Remote Address: 192.168.0.2 - Preempt Mode: Enable - HA Device Name: SBC1 - Redundant HA Device Name: SBC2

- Save the configuration to flash without RESET
- Power Down the first Mediant and move to next section (Step2)

Step 2 – Configuration of the second Mediant for HA

Note: During this stage, make sure that the first device is powered off or disconnected from network.

Ethernet Groups	
On the Mediant WebUi Interface: SETUP > IP Network > Core entities > Ethernet Groups	✓ Configuration must be identical comparing to the first Mediant.
Ethernet Devices	
SETUP > IP Network > Core entities > Ethernet Devices	✓ Configuration must be identical comparing to the first Mediant.
IP Interfaces	
SETUP > IP Network > Core entities > IP Interface Devices	✓ Create 1 IP Interface for HA (IPInt_HA) - Name: IPInt_HA - Application Type: MAINTENANCE - Ethernet Device: EthD_HA - IP Address: 192.168.0.2 - Prefix length: 24 - Default Gateway: 0.0.0.0
HA Settings	
SETUP > IP Network > Core entities > HA Settings	✓ Configure following parameters: - HA Remote Address: 192.168.0.1 - Preempt Mode: Enable - HA Device Name: SBC2 - Redundant HA Device Name: SBC1

- Save the configuration to flash without RESET
- Power Down the second Mediant and move to next section (Step3)

Step 3 – Initialize HA on the devices

Note: You must connect both ports (two) in the Ethernet Group of the Maintenance interface to the network (i.e., two network cables are used). This provides 1+1 Maintenance port redundancy.

1. Cable the devices to the network.
2. Power up the devices; the redundant device synchronizes with the active device and updates its configuration according to the active device. The synchronization status is indicated as follows:

4.3 AudioCodes FAX configuration checklist

4.3.1 FXS fax on Mediant configuration

4.3.1.1 Telephony profile

The FXS ports with fax devices connected requires dedicated configuration for fax. To create TelProfile go to **SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Tel Profiles**.

Create new profile by pressing  and set:

Parameter	Value	Description
Name	TelProfile_FXS FAX	Profile name
Fax Signaling Method	T.38 Relay	Select T.38 protocol for fax transmission

4.3.1.2 FXS port configuration update

Go to **SETUP > SIGNALING & MEDIA > GATEWAY > Trunks & Groups > Trunk Groups**

Update TEL PROFILE NAME on chosen trunk group to **TelProfile_FXS FAX**

4.3.1.3 Update IP Profile

Go to **SETUP > SIGNALING & MEDIA > CODERS & PROFILES > IP Profiles**.

Select profile defined for Business Talk IP Group and update parameters:

Parameter	Value	Description
MEDIA SECURITY		
SBC Media Security Mode	RTP	Disable secured RTP to avoid TLS in SDP
Gateway Media Security Mode	Disable	Disable secured RTP to avoid TLS in SDP
GATEWAY FAX AND MODEM		
Fax Signaling Method	T.38 Relay	Use T38 for fax transmission

4.3.1.4 General fax parameters

Go to **SETUP > SIGNALING & MEDIA > MEDIA > Fax/Modem/CID Settings** and update:

Parameter	Value	Description
Fax Transport Mode	T.38 Relay	Use T38 for fax transmission
Fax Relay Redundancy Depth	1	Set pages transmission redundancy
Fax Relay Enhanced Redundancy Depth	4	Set fax negotiation redundancy

4.3.1.5 Routing

The routing of fax calls must be reconfigured to bypass Teams. Go to **SETUP > SIGNALING & MEDIA > GATEWAY > Routing > Tel->IP Routing**. Select line assigned to chosen FXS or create new one:

Parameter	Value	Description
Source Trunk Group IP	<i><trunkID></i>	Trunk ID for selected FXS port
Destination IP Group	<i><BT IP Group></i>	IP Group for Business Talk aSBC
SIP Interface	<i><SIP Interface></i>	SIP Interface for Business Talk aSBC access

Go to **SETUP > SIGNALING & MEDIA > GATEWAY > Routing > IP->Tel Routing**. Create new entry:

Parameter	Value	Description
Source SIP Interface	<i><SIP Interface></i>	SIP Interface for Business Talk aSBC access
Destination Phone Pattern	<i><FAX DID></i>	Set FAX DID accessed by BT
Destination Type	Trunk Group	
Trunk Group ID	<i><Trunk Group IP></i>	Trunk ID for selected FXS port
Source IP Group	<i><BT IP Group></i>	IP Group for Business Talk aSBC

Go to **SETUP > SIGNALING & MEDIA > SBC > Routing > IP-to-IP Routing**. Create new entry:

Parameter	Value	Description
Source IP Group	<i><BT IP Group></i>	IP Group for Business Talk aSBC
Destination Username Pattern	<i><FAX DID></i>	Set FAX DID accessed by BT
Destination Type	Gateway	

When created please move new entry before default Business Talk route.

4.3.1.6 V34-fax-transport-type

The next, V34FaxTransportType parameter can be set only using CLI/configuration file and is not visible in web application. To set this parameter go to dedicated configuration page: <https://<MediantIP>/AdminPage> (note: subpage address is case sensitive).

Go to "ini Parameters" subsite using left sided menu.

Parameter name: **V34FAXTRANSPORTTYPE**

Enter value: **1**

Click "Apply New Value".

If parameter is set correctly you should see output:

Parameter Name: V34FAXTRANSPORTTYPE
Parameter New Value: 1
Parameter Description: Determines the V.34 fax transport method.

4.3.2 FXS fax on MediaPack cascaded behind Mediant

The fax integration on MediaPack with Business Talk through Mediant is based on assumption that fax calls are not sent to Teams. In such scenario Mediant gateway only mediates in communication.

4.3.2.1 MediaPack configuration

The MediaPack gateway must be first integrated directly with Mediant. The MediaPack endpoints are registered to Mediant using SIP REGISTER

Telephony Profile

The telephony profile assigned to FXS port must be updated to enable T.38 protocol. Go to **VoIP -> Coders and Profiles -> Tel Profile Settings**. Select appropriate profile (or create new one) and update **Fax Signaling Method** to **T.38 Relay**:

Note: Assigned Tel Profile can be checked under **VoIP -> GW and IP to IP -> Hunt Group -> Endpoint Phone Number**

Configure fax transmission parameters

Go to **VoIP -> Media -> Fax/Modem/CID Settings** and set following parameters:

Parameter	Value	Description
Fax Transport Mode	T.38 Relay	Enable T.38
V.34 Modem Transport Type	Disable	Disable V.34 signals (block SG3 fax)
Fax Relay Redundancy Depth	1	Redundancy of transmitting pages
Fax Relay Enhanced Redundancy Depth	4	Redundancy of fax signalization

4.3.2.2 Mediant configuration

Configuration starts from integration with MediaPack.

IP to IP Routing

Click **New** to create routing for outgoing fax calls from MediaPack to BT/BTIP

Parameter	Value	Description
General > Name	MediaPack_AD_to_BT	

Match > Source IP Group	IPG_MediaPack_AD	
Match > Request Type	All	
Action > Destination Type	IP Group	
Action > Destination IP Group	<BT IP Group>	IP Group for Business Talk aSBC
Action > Destination SIP Interface	<SIP Interface>	SIP Interface for Business Talk aSBC access

Click **New** to create routing for incoming fax calls from BT/BTIP to MediaPack

Parameter	Value	Description
General > Name	BT_to_MediaPack_AD	
Match > Source IP Group	<BT IP Group>	
Match > Request Type	All	
Match > Destination Username	<Fax phone number>	
Action > Destination Type	All Users	

Note: place these rules before default entry forwarding calls to Teams

Also, calls must be routed directly:

- From IP Group defined for calls from MediaPack towards Business Talk
- From IP Group defined for calls from Business Talk towards “All Users” destination (if MediaPack is configured to register FXSW ports on Mediant)

4.4 Configuration checklist for Mediant SBC – HA

- Step 1 – Configuration of the first SBC Mediant for HA
- Step 2 – Configuration of the second SBC Mediant for HA
- Step 3 – Initialize HA on the devices

Step 1 – Configuration of the first Mediant for HA

Note: During this stage, make sure that the second device is powered off or disconnected from network.

Ethernet Groups

On the Mediant WebUi Interface: SETUP > IP Network > Core entities > Ethernet Groups	✓ Use a dedicated Ethernet Group for HA (GROUP_3)
Ethernet Devices	
SETUP > IP Network > Core entities > Ethernet Devices	✓ Create 1 Ethernet Device for HA - Name: EthD_HA - VLAN ID: 3 - Underlying interface: GROUP3 - Tagging: Untagged - MTU: 1500
IP Interfaces	
SETUP > IP Network > Core entities > IP Interface Devices	✓ Create 1 IP Interface for HA (IPInt_HA) - Name: IPInt_HA - Application Type: MAINTENANCE - Ethernet Device: EthD_HA - IP Address: 192.168.0.1 - Prefix length: 24 - Default Gateway: 0.0.0.0
HA Settings	
SETUP > IP Network > Core entities > HA Settings	✓ Configure following parameters: - HA Remote Address: 192.168.0.2 - Preempt Mode: Enable - HA Device Name: SBC1 - Redundant HA Device Name: SBC2

- Save the configuration to flash without RESET
- Power Down the first Mediant and move to next section (Step2)

Step 2 – Configuration of the second Mediant for HA

Note: During this stage, make sure that the first device is powered off or disconnected from network.

Ethernet Groups	
On the Mediant WebUi Interface: SETUP > IP Network > Core entities > Ethernet Groups	✓ Configuration must be identical comparing to the first Mediant.
Ethernet Devices	
SETUP > IP Network > Core entities > Ethernet Devices	✓ Configuration must be identical comparing to the first Mediant.
IP Interfaces	
SETUP > IP Network > Core entities > IP Interface Devices	✓ Create 1 IP Interface for HA (IPInt_HA) - Name: IPInt_HA - Application Type: MAINTENANCE - Ethernet Device: EthD_HA - IP Address: 192.168.0.2

	- Prefix length: 24 - Default Gateway: 0.0.0.0
HA Settings	
SETUP > IP Network > Core entities > HA Settings	✓ Configure following parameters: - HA Remote Address: 192.168.0.1 - Preempt Mode: Enable - HA Device Name: SBC2 - Redundant HA Device Name: SBC1

- Save the configuration to flash without RESET
- Power Down the second Mediant and move to next section (Step3)

Step 3 – Initialize HA on the devices

Note: You must connect both ports (two) in the Ethernet Group of the Maintenance interface to the network (i.e., two network cables are used). This provides 1+1 Maintenance port redundancy.

3. Cable the devices to the network.
4. Power up the devices; the redundant device synchronizes with the active device and updates its configuration according to the active device. The synchronization status is indicated as follows:

5 Ribbon SBC Configuration Checklist for BTIP/BTalk

The checklist below presents all steps of configuration required for VISIT SIP Teams offer deployment. The configuration checklist order respects the configuration guideline chapters for more information about the order please refer to [2]

Configuration checklist regarding **Trunk configuration on the Tenant**

```
Set-CsOnlinePSTNGateway -Identity sbc.contoso.com -ForwardCallHistory $true -  
ForwardPai $true
```

Configuration checklist regarding **Ribbon SBC – Standalone**

- Step 1 – Teams configuration
- Step 2 – Business Talk configuration

Step 1 - Teams Configuration

Certificate for the SBC Direct Routing Interface

On the SBC WebUi Interface:
Settings > Security > SBC Certificates

- ✓ Generate SBC Edge CSR
 - Common name: **@hostname.domain.tld**
 - ISO Country code: **@Country**
 - Locality: **@Locality**
 - Organization: **@Organization**
 - Key Length: **2048**

TLS Profile

On the SBC WebUi Interface:
Security > TLS Profiles

- ✓ Create TLS Profile Teams
 - Description: **TLS Profile Teams**
 - TLS Protocol : **TLS 1.2 Only**
 - Validation Client FQDN : **Disabled**

Node Leve Settings

On the SBC WebUi Interface:
System > Node-Level Settings

- ✓ Configure DNS and NTP with your appropriate configuration
 - Hostname: **@hostname**
 - Domain Name: **@domain.tld**
 - Time Zone: **GMT+1**
 - Use NTP: **Yes**
 - NTP Server: **@NTP_IPAddress**
 - Use Primary DNS: **Yes**
 - Primary Server IP: **@DNS_IPAddress**
 - Use Secondary DNS: **Yes**
 - Secondary Server IP: **@DNS_IPAddress**

Node Interface

On the SBC WebUi Interface:
Networking Interfaces > Logical Interfaces

- ✓ Configure the parameters
 - Description: **Interface-Teams**
 - Primary Address: **@Private-IPAddress-BTIPTeams**
 - Primary Netmask: **@Netmask**
 - Media Next Hop IP: **@Gateway**

SIP Profile

On the SBC WebUi Interface:
SIP > SIP Profiles

- ✓ Create SIP Profile Teams
 - Description : **SIP Profile Teams**
 - FQDN in From Header Location: **SBC Edge FQDN**
 - FQDN in Contact Header: **SBC FQDN**

Media SDES-SRTP Profile

On the SBC WebUi Interface:
Media > SDES-SRTP Profiles

- ✓ Create new Media SDES-SRTP Profile
 - Description: **MCP Teams**
 - Operation Option: **Required**

Media Profile

On the SBC WebUi Interface:
Media > Media Profiles

- ✓ Create Media Profile > Voice Codec Profile
 - Description : **Default G11A**
 - Codec: **G.711 A-law**
- ✓ Create Media Profile > Voice Codec Profile
 - Description : **Default G11u**

	- Codec: G.711 u-law
Media List	
On the SBC WebUi Interface: Media >Media List	✓ Create new Media List: - Description : ML Teams - Media Profil List: Default G711A Default G711u - SDES-SRTP Profile : MCP Teams
SIP Server Table	
On the SBC WebUi Interface: SIP > SIP Server Tables	✓ Create new SIP Server Table: - Description: SIP Server Teams ✓ Create SIP Server IP/FQDN Server Host - HOST FQDN/IP: sip.pstnhub.microsoft.com - Port: 5061 - Protocol: TLS - TLS Profile: TLS Profile Teams Transport - Monitor: SIP Options ✓ Create SIP Server IP/FQDN Server Host - HOST FQDN/IP: sip2.pstnhub.microsoft.com - Port: 5061 - Protocol: TLS - TLS Profile: TLS Profile Teams Transport - Monitor: SIP Options ✓ Create SIP Server IP/FQDN Server Host - HOST FQDN/IP: sip3.pstnhub.microsoft.com - Port: 5061 - Protocol: TLS - TLS Profile: TLS Profile Teams Transport - Monitor: SIP Options
Voice Routing	
On the SBC WebUi Interface: SIP > Transformation Tables	✓ Create new Transformation Table: - Description: Teams to BTIP
Call Routing > Call Routing Table	✓ Create new Call Routing Table: - Description: CR Teams to BTIP ✓ Update CR Teams to BTIP - Description: Teams to BTIP - Number/Name transformation Table: Teams to BTIP - Destination Signaling Group: SG to BTIP <i>* refer to BTIP Configuration</i>
Message Manipulation	

SIP > Message Manipulation > Condition Rules Table	✓ Create new Condition Rule: - Description: Anonymous Call Checking - Match Type: from - Operation: Regex - Match Regex: ^((?!anonymous).)*\$
SIP > Message Manipulation > Message Rules Table	✓ Create new SIP Message Rule Table: - Description: Privacy-Removal - Application message: Selected Message - Message Selection: INVITE ✓ Create new Header Rule: - Description: Privacy Removal - Condition expression: Match All Condition > Anonymous Call Checking - Header Action: Remove - Header Name: Privacy
Signaling Group	
On the SBC WebUi Interface: Signaling Groups	✓ Create new Signaling Group: - Description: SG to Teams SIP Channels and Routing - Call Routing Table: CR Teams to BTIP - SIP Profile: SIP Profile Teams - SIP Server Table: SIP Server Teams - Loadbalancing: Priority: Register All Media Information - Media List ID: ML Teams SIP IP Details - Signaling/Media Private IP: @Private-IPAddress-TeamsInterface * if use NAT Outbound - Outbound NAT Traversal: Static NAT - NAT Public IP: @Public-IPAddress-TeamsInterface Listen Port - Port: 5061 - Protocol: TLS - TLS Profile ID: TLS Profile Teams Federated IP/FQDN - IP/FQDN: sip.pstnhub.microsoft.com - Netmask/prefix: 255.255.255.255 - IP/FQDN: sip2.pstnhub.microsoft.com - Netmask/prefix: 255.255.255.255 - IP/FQDN: sip3.pstnhub.microsoft.com - Netmask/prefix: 255.255.255.255

	Message Manipulation: Enabled Inbound Message Manipulation Message Table List: Privacy-Removal
--	--

Step 2 - BTIP Configuration	
Node Interface	
On the SBC WebUi Interface: Networking Interfaces > Logical Interfaces	✓ Configure the parameters - Description: Interface-BTIP - Primary Address: @Private-IPAddress-BTIPInterface - Primary Netmask: @Netmask - Media Next Hop IP: @Gateway
SIP Profile	
On the SBC WebUi Interface: SIP > SIP Profiles	✓ Create SIP Profile Teams - Description : SIP Profile BTIP - SBC Edge Diagnostic Header: Disable - UA Header : empty
Media Profile	
On the SBC WebUi Interface: Media > Media Profiles	✓ Create Media Profile > Voice Codec Profile - Description : Default G11A - Codec: G.711 A-law ✓ Create Media Profile > Voice Codec Profile - Description : Default G11u - Codec: G.711 u-law
Media List	
On the SBC WebUi Interface: Media >Media List	✓ Create new Media List: - Description : ML BTIP - Media Profil List: Default G711A Default G711u - SDES-SRTP Profile : None
SIP Server Table	
On the SBC WebUi Interface: SIP > SIP Server Tables	✓ Create new SIP Server Table: - Description: SIP Server BTIP ✓ Create SIP Server IP/FQDN Server Host - HOST FQDN/IP: @SBC-BTIP-IPAddress - Port: 5060 - Protocol: TCP Transport - Monitor: SIP Options ✓ Create SIP Server IP/FQDN Server Host - HOST FQDN/IP: @SBC-BTIP-IPAddress - Port: 5060 - Protocol: TCP Transport - Monitor: SIP Options
Voice Routing	
On the SBC WebUi Interface: SIP > Transformation Tables	✓ Create new Transformation Table: - Description: BTIP to Teams

Call Routing > Call Routing Table	✓ Create new Call Routing Table: - Description: CR BTIP to Teams ✓ Update CR Teams to BTIP - Description: BTIP to Teams - Number/Name transformation Table: BTIP to Teams - Destination Signaling Group: SG to Teams* <i>* refer to Teams Configuration</i>
Message Manipulation	
On the SBC WebUi Interface: SIP > Message Manipulation > Message Rules Table	✓ Create new SIP Message Rule Table: - Description: User-Agent ✓ Create new Header Rule: - Description: User-Agent - Header Action: Modify - Header Name: User-Agent - Header Value: Modify - Add/Edit: ○ Type of value: Token ○ Value: user-agent ○ Suffix: \ Teams
Signaling Group	
On the SBC WebUi Interface: Signaling Groups	✓ Create new Signaling Group: - Description: SG to BTIP SIP Channels and Routing - Call Routing Table: CR BTIP to Teams - SIP Profile: SIP Profile BTIP - SIP Server Table: SIP Server BTIP Media Information - Media List ID: ML BTIP SIP IP Details - Signaling/Media Private IP: @Private-IPAddress-BTIPInterface Listen Port - Port: 5060 - Protocol: TCP Federated IP/FQDN - IP/FQDN: @SBC-BTIP-IPAddress - Netmask/prefix: 255.255.255.255 - IP/FQDN: @SBC-BTIP-IPAddress - Netmask/prefix: 255.255.255.255 Message Manipulation: Enabled Outbound Message Manipulation - Message Table List: User-Agent

6 Oracle SBC Configuration Checklist for BTIP/BTalk

6.1 Configuration Requirements

6.1.1 Tenant configuration

- Pair the SBC to the tenant:

Command:

```
New-CsOnlinePSTNGateway
```

```
-Fqdn <SBC FQDN>
-SipSignallingPort 5061
-MaxConcurrentSessions <Number>
-Enabled $true
-ForwardPai $true
-MediaBypass $false
-ForwardCallHistory $true
-SendSipOptions $true
```

6.1.2 Firewall and used ports

Source	IP	Destination	IP	Protocol	Port	Comment
SBC	Public @IP	Any	Any	UDP	53	Public DNS
SBC	Public @IP	Teams SIP Proxy	52.114.0.0/16	TCP	5061	SIP/TLS
SBC	Public @IP	Teams Media Processor	52.112.0.0/14	UDP	49152-53247	Media traffic
Teams SIP Proxy	52.114.0.0/16	SBC	Public @IP	TCP	5061	SIP/TLS
Teams Media Processor	52.112.0.0/14	SBC	Public @IP	UDP	49152-65535	Media traffic

6.1.3 SBC network configuration (wired or virtually wired)

There are five interfaces that will need IP addresses:

- For the Internet facing LAN: 1 private IP NATed to the public IP (if NAT)
- Customer trunk LAN: 1 IP address
- [Optional] HA LAN: 1 or 2 IP address depending if HA is redounded
- Admin configuration: 1 IP address for CLI configuration

6.1.4 Certificates

Following requirements regarding Certificate configuration:

- Certificate of the certification authority, signing the Microsoft Phone System Direct Routing service (Baltimore, format X.509 Base64)
- 1 cyphered file containing both the private key and the public certificate per domain used on the SBC, signed by a trusted Certificate Authority to be known by Microsoft Phone System Direct Routing service, aka such as Digicert CA which Orange has chosen as CA provider
Note: for the multi-tenant SBC solution, this should be a wildcard certificate, aka *.teams.orange.com
- Certificate of the trusted certificate authority, and of each sub-authority having signed the above certificate (format X.509 Base64)

1.1.1. License

- No license is required on Virtual Machine Edition
- *****

6.1.5 User Agent

Within VISIT SIP Teams context, User agent header must have following format:

User-Agent: ORACLE <SBC Model>/v.8.1.0 \ Teams

6.2 ORACLE SBC - Standalone

6.2.1 First step

6.2.1.1 Setup Entitlements

Configure SBC features:

Element	Configuration
Setup entitlements	OracleSBC1# setup entitlements

Example:

```
OracleSBC1# setup entitlements
-----
Entitlements for Session Border Controller
Last Modified: 2019-04-23 09:58:38
-----
 1 : Session Capacity           : 12000
 2 : Accounting                 : enabled
 3 : IPv4 - IPv6 Interworking   :
 4 : IWF (SIP-H323)            : enabled
 5 : Load Balancing           : enabled
 6 : Policy Server              : enabled
 7 : Quality of Service        : enabled
 8 : Routing                   : enabled
 9 : SIPREC Session Recording   : enabled
10: Admin Security             :
11: ANSSI R226 Compliance      :
12: IMS-AKA Endpoints          : 0
13: IPSec Trunking Sessions    : 0
14: MSRP B2BUA Sessions       : 0
15: SRTP Sessions              : 2000
16: Transcode Codec AMR Capacity : 0
17: Transcode Codec AMRWB Capacity : 0
```

To “unlock” SRTP feature like “media-sec-policy” you must give a number for “SRTP Sessions”.

6.2.2 IP Network configuration

6.2.2.1 Physical interface configuration

3 interfaces need to be configured:

- wancom0: admin interface (CLI)
- s0p0: media interface to Teams (media)
- s0p1: media interface to BTIP (media)

Interface	Configuration
Wancom0	Configured at first initial boot
S0p0	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# system OracleSBC1 (system)# phy-interface OracleSBC1 (phy-interface)# name s0p0 OracleSBC1 (phy-interface)# operation-type Media OracleSBC1 (phy-interface)# port 0 OracleSBC1 (phy-interface)# slot 0 OracleSBC1 (phy-interface)# done </pre>
S0p1	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# system OracleSBC1 (system)# phy-interface OracleSBC1 (phy-interface)# name s0p1 OracleSBC1 (phy-interface)# operation-type Media OracleSBC1 (phy-interface)# port 0 OracleSBC1 (phy-interface)# slot 1 OracleSBC1 (phy-interface)# done </pre>

6.2.2.2 Network interface configuration

Interface	Configuration
Wancom0	Configured at first initial boot
S0p0 To Teams	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# system OracleSBC1 (system)# network-interface OracleSBC1 (network-interface)# name s0p0 OracleSBC1 (network-interface)# hostname <SBC FQDN> OracleSBC1 (network-interface)# ip-address <SBC Public IP> OracleSBC1 (network-interface)# netmask <Netmask> OracleSBC1 (network-interface)# gateway <GW IP> OracleSBC1 (network-interface)# dns-ip-primary <Primary Public DNS> OracleSBC1 (network-interface)# dns-ip-backup1 <Backup Public DNS> OracleSBC1 (network-interface)# dns-domain <DNS Domain> OracleSBC1 (network-interface)# add-hip-ip <SBC Public IP> OracleSBC1 (network-interface)# add-icmp-ip <SBC Public IP> OracleSBC1 (network-interface)# add-ssh-ip <SBC Public IP> OracleSBC1 (network-interface)# gw-heartbeat OracleSBC1 (gateway-heartbeat)# select OracleSBC1 (gateway-heartbeat)# state enabled OracleSBC1 (gateway-heartbeat)# heartbeat 1 OracleSBC1 (gateway-heartbeat)# retry-count 2 OracleSBC1 (gateway-heartbeat)# retry-timeout 1 OracleSBC1 (gateway-heartbeat)# health-score 30 OracleSBC1 (gateway-heartbeat)# done OracleSBC1 (gateway-heartbeat)# exit OracleSBC1 (network-interface)# done </pre>

S0p1 To BTIP	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# system OracleSBC1 (system)# network-interface OracleSBC1 (network-interface)# name s0p1 OracleSBC1 (network-interface)# ip-address <SBC Private IP> OracleSBC1 (network-interface)# netmask <Netmask> OracleSBC1 (network-interface)# gateway <GW IP> OracleSBC1 (network-interface)# add-hip-ip <SBC Private IP> OracleSBC1 (network-interface)# add-icmp-ip <SBC Private IP> OracleSBC1 (network-interface)# gw-heartbeat OracleSBC1 (gateway-heartbeat)# select OracleSBC1 (gateway-heartbeat)# state enabled OracleSBC1 (gateway-heartbeat)# heartbeat 1 OracleSBC1 (gateway-heartbeat)# retry-count 2 OracleSBC1 (gateway-heartbeat)# retry-timeout 1 OracleSBC1 (gateway-heartbeat)# health-score 31 OracleSBC1 (gateway-heartbeat)# done OracleSBC1 (gateway-heartbeat)# exit OracleSBC1 (network-interface)# done </pre>
--	--

6.2.3 Teams configuration

6.2.3.1 Certificate

Microsoft Teams Direct Routing Interface only allows TLS connections from SBCs for SIP traffic with a certificate signed by one of the trusted certification authorities.

The step below describes how to request a certificate for SBC External interface and configure it based on the example of Symantec | DigiCert.

The process includes the following steps:

1. Create a certificate-record "Certificate-record" is configuration element on Oracle SBC which captures information for a TLS certificate – such as common-name, key-size, key-usage etc. Following certificate-records are required on the Oracle ESBC in order for the SBC to connect with Microsoft Teams:

- SBC 1 certificate-record assigned to SBC
- IntermediateCA 1 certificate-record for intermediateCA
- Root 1 certificate-record for root cert (Baltimore for Teams SIP proxy)

2. Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority

3. Deploy the SBC and Root/Intermediary certificates on the SBC

Step 1 – Creating the certificate

Navigate to certificate-record config element under security and then configure a certificate record for SBC as shown below

Element	Configuration
---------	---------------

Certificate-record SBCCertificate	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# security OracleSBC1 (security)# certificate-record OracleSBC1 (certificate-record)# name SBCCertificate OracleSBC1 (certificate-record)# country <Country> e.g. FR OracleSBC1 (certificate-record)# state <State> e.g. Paris OracleSBC1 (certificate-record)# locality <Locality> e.g. Paris OracleSBC1 (certificate-record)# organization <Organization> e.g. Orange OracleSBC1 (certificate-record)# unit <unit> e.g. "Orange Business Services" OracleSBC1 (certificate-record)# common-name <SBC FQDN> OracleSBC1 (certificate-record)# key-size 2048 OracleSBC1 (certificate-record)# trusted enabled OracleSBC1 (certificate-record)# key-usage-list (digitalSignature keyEncipherment) OracleSBC1 (certificate-record)# extended-key-usage-list (serverAuth ClientAuth) OracleSBC1 (certificate-record)# key-algor rsa OracleSBC1 (certificate-record)# digest-algor sha256 OracleSBC1 (certificate-record)# ecdsa-key-size p256 OracleSBC1 (certificate-record)# done </pre>
Certificate-record IntermediateCA	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# security OracleSBC1 (security)# certification-record OracleSBC1 (certificate-record)# name SBCInter OracleSBC1 (certificate-record)# country <Country> e.g. FR OracleSBC1 (certificate-record)# state <State> e.g. Paris OracleSBC1 (certificate-record)# locality <Locality> e.g. Paris OracleSBC1 (certificate-record)# organization <Organization> e.g. Orange OracleSBC1 (certificate-record)# unit <unit> e.g. "Orange Business Services" OracleSBC1 (certificate-record)# common-name SBCInter OracleSBC1 (certificate-record)# key-size 2048 OracleSBC1 (certificate-record)# trusted enabled OracleSBC1 (certificate-record)# key-usage-list (digitalSignature keyEncipherment) OracleSBC1 (certificate-record)# extended-key-usage-list (serverAuth ClientAuth) OracleSBC1 (certificate-record)# key-algor rsa OracleSBC1 (certificate-record)# digest-algor sha256 OracleSBC1 (certificate-record)# ecdsa-key-size p256 OracleSBC1 (certificate-record)# done </pre>
Certificate-record Baltimore	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# security OracleSBC1 (security)# certification-record OracleSBC1 (certificate-record)# name BaltimoreRoot OracleSBC1 (certificate-record)# country <Country> e.g. FR OracleSBC1 (certificate-record)# state <State> e.g. Paris OracleSBC1 (certificate-record)# locality <Locality> e.g. Paris OracleSBC1 (certificate-record)# organization <Organization> e.g. Orange OracleSBC1 (certificate-record)# unit <unit> e.g. "Orange Business Services" OracleSBC1 (certificate-record)# common-name "Baltimore CyberTrust Root" OracleSBC1 (certificate-record)# key-size 2048 OracleSBC1 (certificate-record)# trusted enabled OracleSBC1 (certificate-record)# key-usage-list (digitalSignature keyEncipherment) </pre>

	OracleSBC1 (certificate-record)# extended-key-usage-list serverAuth
	OracleSBC1 (certificate-record)# key-algor rsa
	OracleSBC1 (certificate-record)# digest-algor sha256
	OracleSBC1 (certificate-record)# ecdsa-key-size p256
	OracleSBC1 (certificate-record)# done

Step 2 – Generating a certificate signing request

Generate a certificate signing request only for SBCCertificate to create a certificate request and upload it to Digicert for signage:

Element	Configuration
Certificate signing request	OracleSBC1# generate-certification-request SBCCertificate Should return something like this : <pre> -----BEGIN CERTIFICATE REQUEST----- MIIEC7zCCAAdCAQAwYsxCzAJBgNVBAYTAKZSMQ4wDAYDVQQIEWVQYXJpczEOMAwG A1UEBjMFUGFyaXMxODZANBgNVBAoTBk9yYW5nZTEhMB8GA1UECxMYT3JhbmdlIEIj c2luZXNzIFN1cnZpY2VzMScwJgYDVQQDEeXocTYWnmD3Lm1zdmlzaXQ2Lm9uZS51 cXVhbnQubmV0MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv/NxxJUw 2JEhNE3NBvYfKYC0kniJkaB3r4Y+QCPOlgkL5qK9bsVTpow7mhmpoan4NlgZQwfKqA UigABDIVwiS0avpLpo98FM5fCFg0J1GZXe/E9URek9g4NV8D1yyDgZoeDWbtuq6h S/nlob96NjuHO+wSaxWviOeQk0icB+7+o9YZ1tCSPRIFTC8jh3UGgym7Way7UKyJ 7b6FQ7DYJifsd6hAfASx9xfnDRW9RaWr1Qn1kjXeFXwJRSLALawVn6vaFznAkXGL 5thaEi3MirbinRJQxdtmBqd5hF4wZxIQpZS4qvVS00+EjQ7+mxvXYBQo08mzmSy vSmWu3Yw3jZREwIDAQABoB4wHAYJKoZIhvcNAQkOMQ8wDTALBgNVHQ8EBAMCBAAw DQYJKoZIhvcNAQELBQADggEBALZl1CeQjm0ovxpvrVjfF2NPnVEBYucs2t8vJnCzr 1a6NxdBT5sF/100fss67X/X8TAIgOWX1It81xC7ydoItophuiTiI4R1zL6njC5Op brCHNHFRJBQxdnCFpwYDV3RFf8HsmiczHNv3cYbGYtlwbySuOpia+RCTPST1Rg vr1hdSVuCzRCrt51nEE5X+vmb0RK2nJ+4CGgNGy6MLyRQ0aIFxnRF/wCWdr+zjQ rDjrRknTct0tB/QaQklVgpcvZG3XJ90Q3toqXpo6F2Fq8q99/75aUg1680G8J3CMu mZ5K+yldScQuS6Dq1EJt0RZ8IUrNYcn8sB/uhGWxm4Qy79c= -----END CERTIFICATE REQUEST-----</pre>

Step 3 – Deploy SBC & root/intermediate certificates

SBCInter



SBCCertificate



 IntermediateCA	03/05/2019 12:06	Certificat de sécur...	2 Ko
 ssl_certificate	03/05/2019 12:06	Certificat de sécur...	3 Ko

Element	Configuration
Import-certificate	OracleSBC1# import-certificate try-all SBCCertificate At this point – paste the signed SBC certificate and then issue command “;”

6.2.3.2 TLS Profile

Create a TLS context for Teams with following parameters:

TLS configuration needs as parameters the name* of certificate records.

Element	Configuration
TLSv1.2	OracleSBC1# configure terminal OracleSBC1 (configure)# security OracleSBC1 (security)# tls-profile OracleSBC1 (tls-profile)# name TeamsTLS OracleSBC1 (tls-profile)# end-entity-certificate <SBCCertificate>* OracleSBC1 (tls-profile)# trusted-ca-certificates (<BaltimoreRoot>* <SBCInter>*) OracleSBC1 (tls-profile)# cipher-list ALL OracleSBC1 (tls-profile)# verify-depth 10 OracleSBC1 (tls-profile)# mutual-authenticate enabled OracleSBC1 (tls-profile)# tls-version tlsv12 OracleSBC1 (tls-profile)# cert-status-check disabled OracleSBC1 (tls-profile)# ignore-dead-responder disabled OracleSBC1 (tls-profile)# allow-self-signed-cert disabled OracleSBC1 (tls-profile)# done

6.2.3.3 Enable media manager

Element	Configuration
Media-manager	OracleSBC1# configure terminal OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# media-manager OracleSBC1 (media-manager-config)# state enabled OracleSBC1 (media-manager-config)# options +audio-allow-asymmetric-pt OracleSBC1 (media-manager-config)# options +xcode-gratuitous-rtcp- report-generation OracleSBC1 (media-manager-config)# done

6.2.3.4 Steering pool

Element	Configuration
Steering pool	OracleSBC1# configure terminal

Teams	OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# steering pool OracleSBC1 (steering-pool)# ip-address <SBC Public IP> OracleSBC1 (steering-pool)# start-port 49152 OracleSBC1 (steering-pool)# end-port 65535 OracleSBC1 (steering-pool)# realm-id ToTeams OracleSBC1 (steering-pool)# done
Steering pool BTIP	OracleSBC1# configure terminal OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# steering pool OracleSBC1 (steering-pool)# ip-address <SBC Private IP> OracleSBC1 (steering-pool)# start-port 6000 OracleSBC1 (steering-pool)# end-port 65535 OracleSBC1 (steering-pool)# realm-id ToBTIP OracleSBC1 (steering-pool)# done

6.2.3.5 Session agent

Microsoft Teams use different SIP Proxy who can send/receive traffic from the SBC.

Element	Configuration
Session agent sip.pstnhub.microsoft.com	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# session-agent OracleSBC1 (session-agent)# hostname sip.pstnhub.microsoft .com OracleSBC1 (session-agent)# port 5061 OracleSBC1 (session-agent)# transport-method StaticTLS OracleSBC1 (session-agent)# realm-id ToTeams OracleSBC1 (session-agent)# ping-method OPTIONS OracleSBC1 (session-agent)# ping-interval 30 OracleSBC1 (session-agent)# refer-call-transfer enabled OracleSBC1 (session-agent)# done
Session agent sip2.pstnhub.microsoft.com	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# session-agent OracleSBC1 (session-agent)# hostname sip2.pstnhub.microsoft .com OracleSBC1 (session-agent)# port 5061 OracleSBC1 (session-agent)# transport-method StaticTLS OracleSBC1 (session-agent)# realm-id ToTeams OracleSBC1 (session-agent)# ping-method OPTIONS OracleSBC1 (session-agent)# ping-interval 30 OracleSBC1 (session-agent)# refer-call-transfer enabled OracleSBC1 (session-agent)# done
Session agent sip3.pstnhub.microsoft.com	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# session-agent OracleSBC1 (session-agent)# hostname sip3.pstnhub.microsoft .com OracleSBC1 (session-agent)# port 5061

	OracleSBC1 (session-agent)# transport-method StaticTLS OracleSBC1 (session-agent)# realm-id ToTeams OracleSBC1 (session-agent)# ping-method OPTIONS OracleSBC1 (session-agent)# ping-interval 30 OracleSBC1 (session-agent)# refer-call-transfer enabled OracleSBC1 (session-agent)# done
Session agent Sip-all.pstnhub.microsoft.com	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# session-agent OracleSBC1 (session-agent)# hostname sip-all.pstnhub.microsoft.com OracleSBC1 (session-agent)# port 5061 OracleSBC1 (session-agent)# transport-method StaticTLS OracleSBC1 (session-agent)# realm-id ToTeams OracleSBC1 (session-agent)# refer-call-transfer enabled OracleSBC1 (session-agent)# done

6.2.3.6 Session group

Defined session group with all session agents configured earlier to prevent connectivity issue when the active session agent became unreachable:

Element	Configuration
Session group	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# session-group OracleSBC1 (session-group)# group-name TeamsGrp OracleSBC1 (session-group)# dest (sip.pstnhub.microsoft.com sip2.pstnhub.microsoft.com sip3.pstnhub.microsoft.com) OracleSBC1 (session-group)# sag-recursion enabled OracleSBC1 (session-group)# stop-sag-recurse 300-407,409-599 OracleSBC1 (session-group)# done

6.2.3.7 Local policy

Create local policy to manage the traffic between different realm (BTIP to Teams / Teams to BTIP):

Element	Configuration
Local policy From Teams to BTIP	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# local-policy OracleSBC1 (local-policy)# from-address * OracleSBC1 (local-policy)# to-address * OracleSBC1 (local-policy)# source-realm ToTeams OracleSBC1 (local-policy)# policy-attribute OracleSBC1 (local-policy-attribute)# next-hop sag:BTIPGrp OracleSBC1 (local-policy-attribute)# realm ToBTIP OracleSBC1 (local-policy-attribute)# done

	OracleSBC1 (local-policy)# done
Local policy From BTIP to Teams	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# local-policy OracleSBC1 (local-policy)# from-address * OracleSBC1 (local-policy)# to-address * OracleSBC1 (local-policy)# source-realm ToBTIP OracleSBC1 (local-policy)# policy-attribute OracleSBC1 (policy-attribute)# next-hop sag:TeamsGrp OracleSBC1 (policy-attribute)# realm ToTeams OracleSBC1 (local-policy-attribute)# done OracleSBC1 (local-policy)# done
Local policy From ANY to Teams (REFER Method)	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# local-policy OracleSBC1 (local-policy)# from-address * OracleSBC1 (local-policy)# to-address * OracleSBC1 (local-policy)# source-realm * OracleSBC1 (local-policy)# policy-attribute OracleSBC1 (policy-attribute)# methods REFER OracleSBC1 (policy-attribute)# next-hop sag:TeamsGrp OracleSBC1 (policy-attribute)# realm ToTeams OracleSBC1 (local-policy-attribute)# done OracleSBC1 (local-policy)# done

6.2.3.8 Codec policy

Element	Configuration
Codec policy	OracleSBC1# configure terminal OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# codec-policy OracleSBC1 (codec-policy)# name CodecToTeams OracleSBC1 (codec-policy)# allow-codecs (PCMA telephone-event) OracleSBC1 (codec-policy)# done

6.2.3.9 Sip manipulation

SIP Manipulation FixCLineNAT:

The following manipulation is configured to change SDP "c" line to change private IP address to public IP address when the SBC is placed behind NAT device.

Element	Configuration
SIP Manipulation FixCLineNAT	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name FixCLineNAT
SIP Mime SDP rule	OracleSBC1 (sip-manipulation)# mine-sdp-rules

MSR_FixCLine	OracleSBC1 (sip-mime-sdp-rules)# name MSR_FixCLine OracleSBC1 (sip-mime-sdp-rules)# msg-type any OracleSBC1 (sip-mime-sdp-rules)# comparison-type manipulate OracleSBC1 (sip-mime-sdp-rules)# sdp-session-rule OracleSBC1 (sip-sdp-session-rules)# name SR_FixCLine OracleSBC1 (sip-sdp-session-rules)# comparison-type manipulate OracleSBC1 (sip-sdp-session-rules)# sdp-line-rules OracleSBC1 (sip-sdp-line-rules)# name LR_FixCLine OracleSBC1 (sip-sdp-line-rules)# type c OracleSBC1 (sip-sdp-line-rules)# action replace OracleSBC1 (sip-sdp-line-rules)# new-value "IN IP4 <Public @IP>" OracleSBC1 (sip-sdp-line-rules)# done OracleSBC1 (sip-sdp-line-rules)# exit OracleSBC1 (sip-sdp-session-rules)# done OracleSBC1 (sip-sdp-session-rules)# exit OracleSBC1 (sip-mime-sdp-rules)# exit OracleSBC1 (sip-mime-sdp-rules)# done
SIP Header rule HR_FixCLine	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name HR_FixCLine OracleSBC1 (sip-header-rules)# header-name Content-Type OracleSBC1 (sip-header-rules)# action manipulation OracleSBC1 (sip-header-rules)# element-rule OracleSBC1 (sip-element-rules)# name ER_FixCLine OracleSBC1 (sip-element-rules)# parameter application/sdp OracleSBC1 (sip-element-rules)# type mime OracleSBC1 (sip-element-rules)# action find-replace-all OracleSBC1 (sip-element-rules)# match-value "c=IN IP4 <Private @IP>" OracleSBC1 (sip-element-rules)# new-value "c=IN IP4 <Public @IP>" OracleSBC1 (sip-element-rules)# done OracleSBC1 (sip-element-rules)# exit OracleSBC1 (sip-header-rules)# done OracleSBC1 (sip-header-rules)# exit OracleSBC1 (sip-manipulation)# done

SIP Manipulation: PSTNHub

Element	Configuration
Sip Manipulation PSTNHub	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name PSTNHub
SIP Header rule HR_AlterFrom	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name HR_AlterFrom OracleSBC1 (sip-header-rules)# header-name From OracleSBC1 (sip-header-rules)# action manipulate OracleSBC1 (sip-header-rules)# element-rules OracleSBC1 (sip-element-rules)# name ER_AlterFrom OracleSBC1 (sip-element-rules)# type uri-host OracleSBC1 (sip-element-rules)# action find-replace-all OracleSBC1 (sip-element-rules)# new-value <SBC FQDN> OracleSBC1 (sip-element-rules)# done

	OracleSBC1 (sip-element-rules)# exit OracleSBC1 (sip-header-rules)# done
SIP Header rule HR_AlterContact	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name HR_AlterContact OracleSBC1 (sip-header-rules)# header-name Contact OracleSBC1 (sip-header-rules)# action manipulate OracleSBC1 (sip-header-rules)# element-rules OracleSBC1 (sip-element-rules)# name ER_AlterContact OracleSBC1 (sip-element-rules)# type uri-host OracleSBC1 (sip-element-rules)# action find-replace-all OracleSBC1 (sip-element-rules)# match-value <SBC Private @IP> OracleSBC1 (sip-element-rules)# new-value <SBC FQDN> OracleSBC1 (sip-element-rules)# done OracleSBC1 (sip-element-rules)# exit OracleSBC1 (sip-header-rules)# done
SIP Header rule HR_AddContactOptions	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name HR_AddContactOptions OracleSBC1 (sip-header-rules)# header-name Contact OracleSBC1 (sip-header-rules)# action add OracleSBC1 (sip-header-rules)# msg-type request OracleSBC1 (sip-header-rules)# methods OPTIONS OracleSBC1 (sip-header-rules)# new-value "sip:ping@<SBC FQDN>:5061;transport=tls" OracleSBC1 (sip-element-rules)# done OracleSBC1 (sip-header-rules)# exit
SIP Header rule HR_AddRROptions	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name HR_AddRROptions OracleSBC1 (sip-header-rules)# header-name Record-Route OracleSBC1 (sip-header-rules)# action add OracleSBC1 (sip-header-rules)# msg-type request OracleSBC1 (sip-header-rules)# methods OPTIONS OracleSBC1 (sip-header-rules)# new-value "sip:<SBC FQDN>" OracleSBC1 (sip-header-rules)# done OracleSBC1 (sip-header-rules)# exit
SIP Header rule HR_CheckUserAgent	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name HR_CheckUserAgent OracleSBC1 (sip-header-rules)# header-name User-Agent OracleSBC1 (sip-header-rules)# action manipulate OracleSBC1 (sip-header-rules)# msg-type request OracleSBC1 (sip-header-rules)# methods INVITE OracleSBC1 (sip-header-rules)# new-value "ORACLE SBC/v.8.1.0. \\ Teams" OracleSBC1 (sip-header-rules)# done OracleSBC1 (sip-header-rules)# exit

SIP Manipulation RemovePrivacy:

Element	Configuration
SIP Manipulation	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router

RemovePrivacy	OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name RemovePrivacy
SIP Header rule HR_RemovePrivacy	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rule)# name HR_RemovePrivacy OracleSBC1 (sip-header-rule)# header-name Privacy OracleSBC1 (sip-header-rule)# action delete OracleSBC1 (sip-header-rule)# comparison-type boolean OracleSBC1 (sip-header-rule)# msg-type out-of-dialog OracleSBC1 (sip-header-rule)# methods INVITE OracleSBC1 (sip-header-rule)# match-value \$FROM_USER.\$0!=an onymous OracleSBC1 (sip-header-rule)# done OracleSBC1 (sip-header-rule)# exit OracleSBC1 (sip-manipulation)# done

SIP Manipulation RespondOPTIONS:

Element	Configuration
SIP Manipulation RespondOPTIONS	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name RespondOPTIONS
SIP Header rule HR_Respond2OPTIONS	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rule)# name HR_RespondOPTIONS OracleSBC1 (sip-header-rule)# header-name From OracleSBC1 (sip-header-rule)# action reject OracleSBC1 (sip-header-rule)# methods OPTIONS OracleSBC1 (sip-header-rule)# new-value "200 OK" OracleSBC1 (sip-header-rule)# done

SIP Manipulation ChangeSDPForHold:

Element	Configuration
SIP Manipulation ChangeSDPForHold	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name ChangeSDPForHold
SIP Header rule HR_ChangeSDPForHold	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rule)# name HR_ChangeSDPForHold OracleSBC1 (sip-header-rule)# header-name Content-Type OracleSBC1 (sip-header-rule)# action manipulate OracleSBC1 (sip-header-rule)# msg-type reply OracleSBC1 (sip-header-rule)# methods INVITE OracleSBC1 (sip-header-rule)# element-rules OracleSBC1 (sip-element-rules)# name ER_InactToRecvonly OracleSBC1 (sip-element-rules)# parameter-name application/sdp OracleSBC1 (sip-element-rules)# type mime

	OracleSBC1 (sip-element-rules)# action find-and-replace OracleSBC1 (sip-element-rules)# comparison-type pattern-rule OracleSBC1 (sip-element-rules)# match-value a=inactive OracleSBC1 (sip-element-rules)# new-value a=recvonly OracleSBC1 (sip-header-rule)# done
--	--

SIP Manipulation ChangeUserAgent:

Element	Configuration
SIP Manipulation ChangeUserAgent	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name ChangeUserAgent
Header rule HR_ChangeUserAgent	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name HR_ChangeUserAgent OracleSBC1 (sip-header-rules)# header-name User-Agent OracleSBC1 (sip-header-rules)# action manipulate OracleSBC1 (sip-header-rules)# msg-type request OracleSBC1 (sip-header-rules)# methods INVITE OracleSBC1 (sip-header-rules)# new-value "ORACLE SBC/v.8.1.0. \ Teams" OracleSBC1 (sip-header-rules)# done OracleSBC1 (sip-header-rules)# exit OracleSBC1 (sip-manipulation)# done

SIP Manipulation ChangeServer:

Element	Configuration
SIP manipulation ChangeServer	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name ChangeServer
Header rule ChangeServer	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name HR_ChangeServer OracleSBC1 (sip-header-rules)# header-name Server OracleSBC1 (sip-header-rules)# action manipulate OracleSBC1 (sip-header-rules)# msg-type reply OracleSBC1 (sip-header-rules)# new-value "ORACLE SBC/v.8.1.0. \ Teams" OracleSBC1 (sip-header-rules)# done OracleSBC1 (sip-header-rules)# exit OracleSBC1 (sip-manipulation)# done

SIP Manipulation ChangePrivacy:

The following manipulation is configured to change Privacy header when PSTN send header parameters spaced by ";" e.g. "PRIVACY: id;user;header". Microsoft Teams doesn't support ";" inside Privacy header. ChangePrivacy change ";" to "," e.g. "PRIVACY: id,user,header".

Element	Configuration
SIP Manipulation ChangePrivacy	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name ChangePrivacy
SIP Header-rule HR_ChangePrivacy	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rule)# name HR_ChangePrivacy OracleSBC1 (sip-header-rule)# action manipulate OracleSBC1 (sip-header-rule)# methods INVITE OracleSBC1 (sip-header-rule)# header-name Privacy OracleSBC1 (sip-header-rule)# element-rule OracleSBC1 (sip-element-rules)# name ER_ChangePrivacy OracleSBC1 (sip-element-rules)# type header-value OracleSBC1 (sip-element-rules)# action find-replace-all OracleSBC1 (sip-element-rules)# match-value ; OracleSBC1 (sip-element-rules)# new-value , OracleSBC1 (sip-element-rules)# done OracleSBC1 (sip-element-rules)# exit OracleSBC1 (sip-header-rule)# done OracleSBC1 (sip-header-rule)# exit OracleSBC1 (sip-manipulation)# done

SIP Manipulation out-teams:

Element	Configuration
SIP manipulation out-teams	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name out-teams
SIP Header rule HR_CallFixCLineNAT	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name CallFixCLineNAT OracleSBC1 (sip-header-rules)# header-name From OracleSBC1 (sip-header-rules)# action sip-manip OracleSBC1 (sip-header-rules)# new-value FixCLineNAT OracleSBC1 (sip-header-rules)# done OracleSBC1 (sip-header-rules)# exit
SIP Header rule HR_CallPSTNHub	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name CallPSTNHub OracleSBC1 (sip-header-rules)# header-name From OracleSBC1 (sip-header-rules)# action sip-manip OracleSBC1 (sip-header-rules)# new-value PSTNHub OracleSBC1 (sip-header-rules)# done OracleSBC1 (sip-header-rules)# exit

SIP Manipulation in-teams:

Element	Configuration
SIP manipulation	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router

in-teams	OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name in-teams
SIP Header rule CallRespondOPTIONS	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name CallRespondOPTIONS OracleSBC1 (sip-header-rules)# header-name From OracleSBC1 (sip-header-rules)# action sip-manip OracleSBC1 (sip-header-rules)# new-value RespondOPTIONS OracleSBC1 (sip-header-rules)# done
SIP Header rule CallChangePrivacy	OracleSBC1 (sip-header-rules)# name CallChangePrivacy OracleSBC1 (sip-header-rules)# header-name Privacy OracleSBC1 (sip-header-rules)# action sip-manip OracleSBC1 (sip-header-rules)# new-value ChangePrivacy OracleSBC1 (sip-header-rules)# done OracleSBC1 (sip-header-rules)# exit OracleSBC1 (sip-manipulation)# done
SIP Header rule CallChangeSDPForHold	OracleSBC1 (sip-header-rules)# name CallChangeSDPForHold OracleSBC1 (sip-header-rules)# header-name From OracleSBC1 (sip-header-rules)# action sip-manip OracleSBC1 (sip-header-rules)# new-value ChangeSDPForHold OracleSBC1 (sip-header-rules)# done OracleSBC1 (sip-header-rules)# exit OracleSBC1 (sip-manipulation)# done

SIP Manipulation out-btip:

Element	Configuration
SIP manipulation out-btip	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name out-btip
SIP Header rule CallChangeUserAgent	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name CallChangeUserAgent OracleSBC1 (sip-header-rules)# header-name User-Agent OracleSBC1 (sip-header-rules)# action sip-manip OracleSBC1 (sip-header-rules)# new-value ChangeUserAgent OracleSBC1 (sip-header-rules)# done
SIP Header rule CallChangeServer	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name CallChangeServer OracleSBC1 (sip-header-rules)# header-name From OracleSBC1 (sip-header-rules)# action sip-manip OracleSBC1 (sip-header-rules)# new-value ChangeServer OracleSBC1 (sip-header-rules)# done

SIP Manipulation in-btip:

Element	Configuration
SIP manipulation	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router

in-btip	OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name in-btip
SIP Header rule CallChangePrivacy	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name CallChangePrivacy OracleSBC1 (sip-header-rules)# header-name Privacy OracleSBC1 (sip-header-rules)# action sip-manip OracleSBC1 (sip-header-rules)# new-value ChangePrivacy OracleSBC1 (sip-header-rules)# done

6.2.3.10 Consultative transfer

Element	Configuration
Consultative transfer	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-feature OracleSBC1 (sip-feature)# name replaces OracleSBC1 (sip-feature)# realm ToTeams OracleSBC1 (sip-feature)# support-mode-inbound Pass OracleSBC1 (sip-feature)# require-mode-inbound Pass OracleSBC1 (sip-feature)# proxy-require-mode-inbound Pass OracleSBC1 (sip-feature)# support-mode-outbound Pass OracleSBC1 (sip-feature)# require-mode-outbound Pass OracleSBC1 (sip-feature)# proxy-require-mode-outbound Pass OracleSBC1 (sip-feature)# done

6.2.3.11 SIP Profile

Element	Configuration
SIP profile	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-profile OracleSBC1 (sip-profile)# name foreplace OracleSBC1 (sip-profile)# redirection inherit OracleSBC1 (sip-profile)# ingress-conditional-cac-admit inherit OracleSBC1 (sip-profile)# egress-conditional-cac-admit inherit OracleSBC1 (sip-profile)# forked-cac-bw inherit OracleSBC1 (sip-profile)# cnam-lookup-dir egress OracleSBC1 (sip-profile)# replace-dialogs enabled OracleSBC1 (sip-profile)# done

6.2.3.12 SDES profile

Element	Configuration
SDES profile	OracleSBC1# configure terminal OracleSBC1 (configure)# security OracleSBC1 (security)# media-security OracleSBC1 (media-security)# sdes-profile

	<pre> OracleSBC1 (sdes-profile)# name SDES OracleSBC1 (sdes-profile)# crypto-list AES_CM_128_HMAC_SHA1_80 OracleSBC1 (sdes-profile)# srtp-auth enabled OracleSBC1 (sdes-profile)# srtp-encrypt enabled OracleSBC1 (sdes-profile)# srtcp-encrypt enabled OracleSBC1 (sdes-profile)# mki disabled OracleSBC1 (sdes-profile)# egress-offer-format same-as-ingress OracleSBC1 (sdes-profile)# srtp-rekey-on-re-invite disabled OracleSBC1 (sdes-profile)# done </pre>
--	---

6.2.3.13 RTCP policy

Element	Configuration
RTCP policy	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# rtcp-policy OracleSBC1 (rtcp-policy)# name rtcpGen OracleSBC1 (rtcp-policy)# rtcp-generate all-calls OracleSBC1 (rtcp-policy)# hide-cname disabled OracleSBC1 (rtcp-policy)# done </pre>

6.2.3.14 Net Management Control

Element	Configuration
Net-Management-Control	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# net-management-control OracleSBC1 (net-management-control)# name Emergency OracleSBC1 (net-management-control)# type priority OracleSBC1 (net-management-control)# treatment apply-local-policy OracleSBC1 (net-management-control)# protocol-next-hop SIP OracleSBC1 (net-management-control)# destination-identifier (+33112 +3318 +3317 +3315 +33114) OracleSBC1 (net-management-control)# done </pre>

6.2.3.15 Session constraint

Element	Configuration
Session-constraint	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# session-constraints OracleSBC1 (session-constraints)# name SessionConstraintEmergency </pre>

	OracleSBC1 (session-constraints)# max-sessions <X> e.g. 50 OracleSBC1 (session-constraints)# done
--	--

6.2.3.16 Media sec policy

Element	Configuration
Media sec policy	OracleSBC1# configure terminal OracleSBC1 (configure)# security OracleSBC1 (security)# media-security OracleSBC1 (media-security)# media-sec-policy OracleSBC1 (media-sec-policy)# name RTP OracleSBC1 (media-sec-policy)# pass-through disabled OracleSBC1 (media-sec-policy)# inbound OracleSBC1 (inbound)# mode rtp OracleSBC1 (inbound)# protocol none OracleSBC1 (inbound)# exit OracleSBC1 (media-sec-policy)# outbound OracleSBC1 (outbound)# mode rtp OracleSBC1 (outbound)# protocol none OracleSBC1 (outbound)# exit OracleSBC1 (media-sec-policy)# name SRTP OracleSBC1 (media-sec-policy)# pass-through disabled OracleSBC1 (media-sec-policy)# inbound OracleSBC1 (inbound)# profile SDES OracleSBC1 (inbound)# mode srtp OracleSBC1 (inbound)# protocol sdes OracleSBC1 (inbound)# exit OracleSBC1 (media-sec-policy)# outbound OracleSBC1 (outbound)# profile SDES OracleSBC1 (outbound)# mode srtp OracleSBC1 (outbound)# protocol sdes OracleSBC1 (outbound)# done

6.2.3.17 Realm

Element	Configuration
Realm ToTeams	OracleSBC1# configure terminal OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# realm-config OracleSBC1 (realm-config)# identifier ToTeams OracleSBC1 (realm-config)# network-interfaces s0p0:0 OracleSBC1 (realm-config)# mm-in-realm enabled OracleSBC1 (realm-config)# qos-enable enabled OracleSBC1 (realm-config)# net-management-control enabled OracleSBC1 (realm-config)# refer-call-transfer enabled OracleSBC1 (realm-config)# media-sec-policy SRTP OracleSBC1 (realm-config)# rtcp-policy rtcpGen OracleSBC1 (realm-config)# codec-policy CodecToTeams OracleSBC1 (realm-config)# done

6.2.3.18 SIP interface

Element	Configuration
SIP interface ToTeams	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-interface OracleSBC1 (sip-interface)# state enabled OracleSBC1 (sip-interface)# realm-id ToTeams OracleSBC1 (sip-interface)# in-manipulationid in-teams OracleSBC1 (sip-interface)# out-manipulationid out-teams OracleSBC1 (sip-interface)# sip-profile foreplace OracleSBC1 (sip-interface)# add-sdp-invite reinvite OracleSBC1 (sip-interface)# sip-port OracleSBC1 (sip-port)# address <SBC Public IP> OracleSBC1 (sip-port)# port 5061 OracleSBC1 (sip-port)# transport-protocol TLS OracleSBC1 (sip-port)# tls-profile TeamsTLS OracleSBC1 (sip-port)# allow-anonymous agents-only OracleSBC1 (sip-port)# done </pre>

6.2.4 BTIP configuration

6.2.4.1 Enable SIP config

Element	Configuration
SIP config	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1# (session-router)# sip-config OracleSBC1 (sip-config)# home-realm-id ToBTIP OracleSBC1 (sip-config)# registrar-domain * OracleSBC1 (sip-config)# registrar-host * OracleSBC1 (sip-config)# registrar-port 5060 </pre>

	OracleSBC1 (sip-config)# dialog-transparency disabled OracleSBC1 (sip-config)# options +inmanip-before-validate OracleSBC1 (sip-config)# options +max-udp-length=0 OracleSBC1 (sip-config)# options +reinvite-trying=yes
--	---

6.2.4.2 Media profile

Element	Configuration
Media profile	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# media-profile OracleSBC1 (media-profile)# name PCMA OracleSBC1 (media-profile)# payload-type 8 OracleSBC1 (media-profile)# clock-rate 8000 OracleSBC1 (media-profile)# parameters silenceSupp:off OracleSBC1 (media-profile)# done

6.2.4.3 Codec policy

Element	Configuration
Codec policy	OracleSBC1# configure terminal OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# codec-policy OracleSBC1 (codec-policy)# name CodecBTIP OracleSBC1 (codec-policy)# allow-codecs (PCMA telephone-event) OracleSBC1 (codec-policy)# order-codecs PCMA OracleSBC1 (codec-policy)# done

6.2.4.4 Session agent

Element	Configuration
Session router active	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# session-agent OracleSBC1 (session-agent)# hostname <@IP aSBC 1> OracleSBC1 (session-agent)# port 5060 OracleSBC1 (session-agent)# transport-method StaticTCP OracleSBC1 (session-agent)# realm-id ToBTIP OracleSBC1 (session-agent)# refer-call-transfer enabled OracleSBC1 (session-agent)# done
Session router backup	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# session-agent OracleSBC1 (session-agent)# hostname <@IP aSBC 2> OracleSBC1 (session-agent)# port 5060 OracleSBC1 (session-agent)# transport-method StaticTCP OracleSBC1 (session-agent)# realm-id ToBTIP

	OracleSBC1 (session-agent)# refer-call-transfer enabled OracleSBC1 (session-agent)# done
--	---

6.2.4.5 Session group

Element	Configuration
Session group	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# session-group OracleSBC1 (session-group)# group-name BTIPGrp OracleSBC1 (session-group)# dest (<@IP aSBC 1> <@IP aSBC 2>) OracleSBC1 (session-group)# sag-recursion OracleSBC1 (session-group)# stop-sag-recurse 300-407,409-599 OracleSBC1 (session-group)# done

6.2.4.6 Realm

Element	Configuration
Realm ToBTIP	OracleSBC1# configure terminal OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# realm-config OracleSBC1 (realm-config)# identifier ToBTIP OracleSBC1 (realm-config)# network-interfaces s0p1:0 OracleSBC1 (realm-config)# mm-in-realm enabled OracleSBC1 (realm-config)# qos-enabled enabled OracleSBC1 (realm-config)# refer-call-transfer enabled OracleSBC1 (realm-config)# media-sec-policy RTP OracleSBC1 (realm-config)# rtcp-policy rtcpGen OracleSBC1 (realm-config)# codec-policy CodecBTIP OracleSBC1 (realm-config)# done

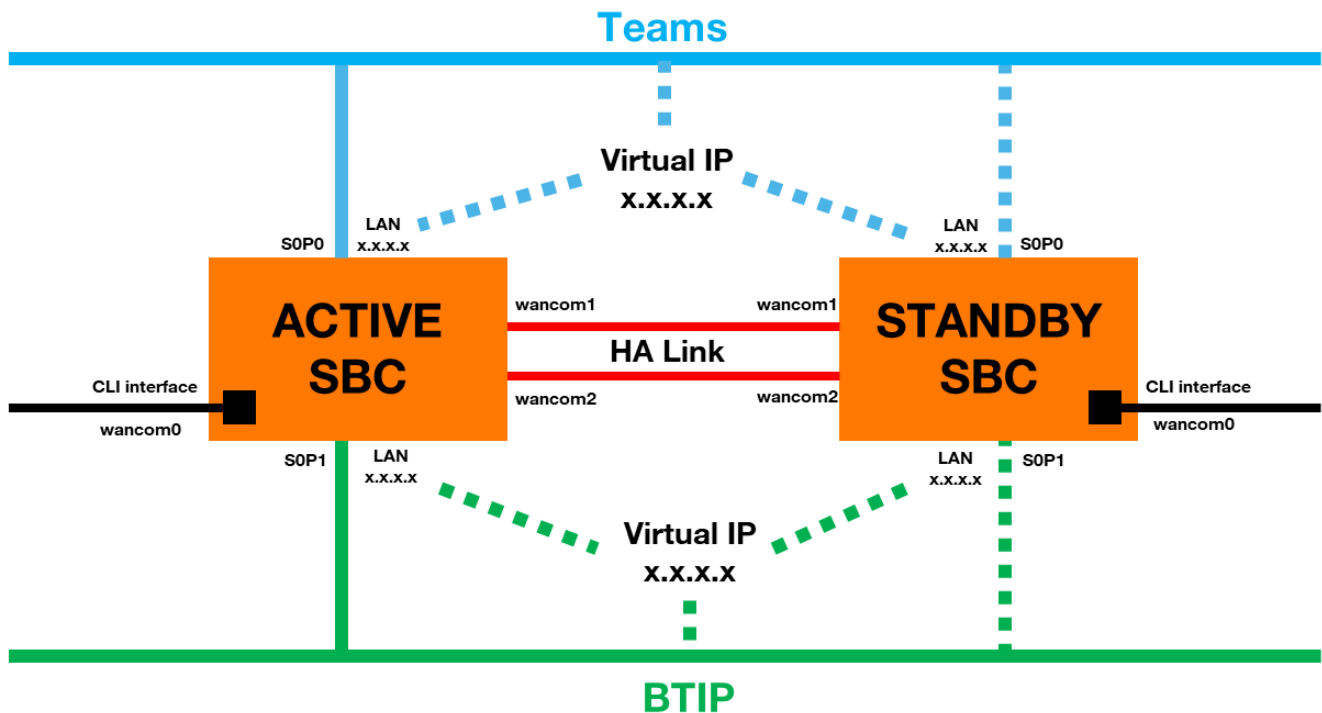
6.2.4.7 SIP interface

Element	Configuration
---------	---------------

SIP interface	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-interface OracleSBC1 (sip-interface)# state enabled OracleSBC1 (sip-interface)# realm-id ToBTIP OracleSBC1 (sip-interface)# options +update-interworking OracleSBC1 (sip-interface)# initial-inv-trans-expire 6 OracleSBC1 (sip-interface)# out-manipulationid out-btip OracleSBC1 (sip-interface)# in-manipulationid in-btip OracleSBC1 (sip-interface)# sip-port OracleSBC1 (sip-port)# address <Private @IP> OracleSBC1 (sip-port)# port 5060 OracleSBC1 (sip-port)# transport-protocol TCP OracleSBC1 (sip-port)# allow-anonymous agents-only OracleSBC1 (sip-port)# done </pre>
-----------------------------	--

6.3 ORACLE SBC - HA configuration

This section describes the Oracle SBC configuration in HA mode (Two SBC in a high availability mode). The HA topology validated within VISIT Teams offer is displayed in the figure below:



Only the Active SBC is used, while the second SBC is considered as a backup device (standby).

Following steps have to be performed to ensure correct integration within VISIT Teams offer:

- First SBC configuration
 - NTP synchronization
 - Virtual MAC address
 - Primary & Secondary utility address
 - Wancom1 & Wancom2 physical configuration
 - Wancom1 & Wancom2 network configuration
 - Redundancy
- Secondary SBC configuration

6.3.1 First SBC configuration

6.3.1.1 NTP synchronization

Element	Configuration
NTP sync	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# ntp-sync OracleSBC1 (ntp-config)# add-server <NTP @IP> OracleSBC1 (ntp-config)# done </pre>

6.3.1.2 Virtual MAC address

Element	Configuration
Virtual MAC address	<pre> OracleSBC1# show interfaces </pre>

Identify "Ethernet address is 00:08:25:XX:YY:ZN", 00:08:25 refers to Acme Packet, XX:YY:Z refers to the specific SBC. N is a 0-f hexadecimal value available for Oracle SBC. To create a virtual MAC address replace the "N" value with unused hexadecimal values for Oracle SBC: 8,9,e or f. Example:

Ethernet address s0p0: 00:08:25:A2:45:BF

→ Virtual MAC 1: 00:08:25:A2:45:B8

→ Virtual MAC 2: 00:08:25:A2:45:B9

Element	Configuration
Virtual MAC address	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# system OracleSBC1 (system)# phy-interface OracleSBC1 (phy-interface)# select <name>: 1: s0p0 2: s0p1 Selection: 1 OracleSBC1 (phy-interface)# virtual-mac <Virtual MAC 1> OracleSBC1 (phy-interface)# done OracleSBC1 (phy-interface)# select <name>: 1: s0p0 2: s0p1 Selection: 2 OracleSBC1 (phy-interface)# virtual-mac <Virtual MAC 2> OracleSBC1 (phy-interface)# done </pre>

6.3.1.3 Primary & Secondary utility address

Primary and Secondary utility addresses have to be in the same subnet than Public @IP (to teams) and Private @IP (to BTIP):

Element	Configuration
Primary & Secondary utility address	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# system OracleSBC1 (system)# network-interface OracleSBC1 (network-interface)# select <name>:<sub-port-id>: 1: s0p0:0 ip=Public @IP gw= GW @IP 2: s0p1:0 ip=Private @IP gw= GW @IP Selection: 1 OracleSBC1 (network-interface)# pri-utility-addr <@IP> OracleSBC1 (network-interface)# sec-utility-addr <@IP> OracleSBC1 (network-interface)# done OracleSBC1 (network-interface)# select <name>:<sub-port-id>: 1: s0p0:0 ip=Public @IP gw= GW @IP 2: s0p1:0 ip=Private @IP gw= GW @IP Selection: 2 OracleSBC1 (network-interface)# pri-utility-addr <@IP> OracleSBC1 (network-interface)# sec-utility-addr <@IP> OracleSBC1 (network-interface)# done </pre>

6.3.1.4 Wancom1 & Wancom2 physical configuration

Element	Configuration
Wancom1 physical configuration	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# system OracleSBC1 (system)# phy-interface OracleSBC1 (phy-interface)# name wancom1 OracleSBC1 (phy-interface)# operation-type Control OracleSBC1 (phy-interface)# port 1 OracleSBC1 (phy-interface)# slot 0 OracleSBC1 (phy-interface)# wancom-health-score 7 </pre>
Wancom2 physical configuration	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# system OracleSBC1 (system)# phy-interface OracleSBC1 (phy-interface)# name wancom2 OracleSBC1 (phy-interface)# operation-type Control OracleSBC1 (phy-interface)# port 2 OracleSBC1 (phy-interface)# slot 0 OracleSBC1 (phy-interface)# wancom-health-score 8 </pre>

6.3.1.5 Wancom1 & Wancom2 network configuration

Element	Configuration
Wancom1 network configuration	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# system OracleSBC1 (system)# network-interface OracleSBC1 (network-interface)# name wancom1 OracleSBC1 (network-interface)# pri-utility-addr 169.254.1.1 OracleSBC1 (network-interface)# sec-utility-addr 169.254.1.2 OracleSBC1 (network-interface)# netmask 255.255.255.252 OracleSBC1 (network-interface)# done </pre>
Wancom2 network configuration	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# system OracleSBC1 (system)# network-interface OracleSBC1 (network-interface)# name wancom2 OracleSBC1 (network-interface)# pri-utility-addr 169.254.2.1 OracleSBC1 (network-interface)# sec-utility-addr 169.254.2.2 OracleSBC1 (network-interface)# netmask 255.255.255.252 OracleSBC1 (network-interface)# done </pre>

6.3.1.6 Redundancy

Element	Configuration
Redundancy	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# system OracleSBC1 (system)# redundancy OracleSBC1 (redundancy)# peers OracleSBC1 (rdncy-peer)# name OracleSBC1 OracleSBC1 (rdncy-peer)# type Primary OracleSBC1 (rdncy-peer)# destinations OracleSBC1 (rdncy-peer-dest)# address 169.254.1.1:9090 OracleSBC1 (rdncy-peer-dest)# network-interface wancom1:0 OracleSBC1 (rdncy-peer-dest)# done OracleSBC1 (rdncy-peer-dest)# address 169.254.2.1:9090 OracleSBC1 (rdncy-peer-dest)# network-interface wancom2:0 OracleSBC1 (rdncy-peer-dest)# done OracleSBC1 (rdncy-peer-dest)# exit OracleSBC1 (rdncy-peer)# done OracleSBC1 (rdncy-peer)# name <Target name SBC2> e.g. OracleSBC2 OracleSBC1 (rdncy-peer)# type Secondary OracleSBC1 (rdncy-peer)# destinations OracleSBC1 (rdncy-peer-dest)# address 169.254.1.2:9090 OracleSBC1 (rdncy-peer-dest)# network-interface wancom1:0 OracleSBC1 (rdncy-peer-dest)# done OracleSBC1 (rdncy-peer-dest)# address 169.254.2.2:9090 OracleSBC1 (rdncy-peer-dest)# network-interface wancom2:0 OracleSBC1 (rdncy-peer-dest)# done OracleSBC1 (rdncy-peer-dest)# exit </pre>

	OracleSBC1 (rdncy-peer)# done OracleSBC1 (rdncy-peer)# exit OracleSBC1 (rdncy)# done
--	---

Reboot primary SBC, redundancy configuration require reboot to take effect:

Element	Configuration
Reboot	OracleSBC1 # save-config OracleSBC1 # activate-config OracleSBC1 # reboot

6.3.2 Secondary SBC configuration

Get the wancom0 IP address for the SBC1, try to ping this address on the secondary SBC and acquire its configuration:

Element	Configuration
Acquire config	OracleSBC2# ping <Wancom0 SBC1 @IP> OracleSBC2# acquire-config <Wancom0 SBC1 @IP> OracleSBC2# reboot force activate

Issuing “show health” and “display-current-cfg-version” commands to display the state of redundancy. The same numbers of current configuration version indicate that both SBCs are synchronized.

Element	Configuration
SBC state	OracleSBC1# show health OracleSBC1# display-current-cfg-version OracleSBC2# show health OracleSBC2# display-current-cfg-version

```

Redundancy Protocol Process (v3):
  State      Active
  Health     100
  Lowest Local Address 169.254.1.1:9090
  1 peer(s) on 2 socket(s):
  OracleSBC2: v3, Standby, health=100, max silence=1050
                  last received from 169.254.1.2 on wancom1:0

Switchover log:
  
```

```

Redundancy Protocol Process (v3):
  State      Standby
  Health     100
  Lowest Local Address 169.254.1.2:9090
  1 peer(s) on 2 socket(s):
  OracleSBC1: v3, Active, health=100, max silence=1050
                  last received from 169.254.2.1 on wancom2:0

Switchover log:
  
```

```

OracleSBC1# display-current-cfg-version
Current configuration version is 57
  
```

```

OracleSBC2# display-current-cfg-version
Current configuration version is 57
  
```