



**Business
Services**

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

13 october 2021

Teams Direct Routing AudioCodes Checklist 0.41
AudioCodes Analog Phones Checklist 1.1
AudioCodes FAX Checklist for Skype 1.1 (adapted to Teams)
Teams Direct Routing Ribbon Checklist 1.11
Ribbon FAX Checklist 1.0
Teams Direct Routing Oracle Checklist 0.15



Contents

1	Main certified architectures	4
1.1	Standalone mode	5
1.2	High Availability mode	12
1.3	Active-active mode (resiliency)	15
1.4	Analog devices	17
1.5	Sizing considerations	21
2	Parameters for connection to BTIP/BTalk/BToI/BTIPol	23
2.1	Trunking integration	23
2.2	SBC IP addressing requirements	28
2.3	TLS integration for BToI/BTIPol	28
3	BTIP/BTalk/BToI/BTIPol certified versions	29
3.1	Teams	29
3.2	Certified SBC	29
3.3	Codecs on trunk	29
3.4	Restrictions in Local Media Optimization	30
3.5	Endpoints	30
4	AudioCodes SBC Configuration Checklist for BTIP/BTIPol/BTalk/BToI	31
4.1	Flow matrix with BToI	31
4.2	Flow matrix with BTIPol	31
4.3	Configuration checklist for Office365 Tenant	31
4.4	Configuration checklist for QoS in Teams client	32
4.5	SBC IP addressing requirements	33
4.6	Configuration checklist for Mediant SBC – Standalone	33
4.7	Configuration checklist for Mediant SBC – HA	49
4.8	. Configuration checklist for Mediant SBC – LMO Asia	51
4.9	AudioCodes Analog Phones configuration checklist	62
4.10	AudioCodes FAX configuration checklist	69
5	Ribbon SBC Configuration Checklist for BTIP/BTalk/BToI/BTIPol	73
5.1	Flow matrix with BToI	73
5.2	Flow matrix with BTIPol	73
5.3	Configuration checklist for Office365 Tenant	73
5.4	Configuration checklist for QoS in Teams client	74
5.5	Step 1 – Teams Configuration	75
5.6	Step 2 – BT / BTIP / BTOI / BTIPol Configuration	81
5.7	Ribbon FAX configuration checklist	85
6	Oracle SBC Configuration Checklist for BTIP/BTalk	88
6.1	Warning	88
6.2	Configuration Requirements	88
6.3	ORACLE SBC - Standalone	91
6.4	ORACLE SBC - HA configuration	116

1 Main certified architectures

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

Local Media Optimization “Europe” model has been certified with AudioCodes and Ribbon so far. With this feature, offnet media flows to/from internal users remain within BVPN or LAN, but are anchored to private LAN interface of DR SBC (see “Example 3 – offnet call from a BVPN remote site with Local Media Optimization Europe Model” below).

Local Media Optimization “Asia” model has been certified with AudioCodes so far, involving Proxy and Downstream SBC. It may be useful to keep media flow geographically local for users that are on very remote BVPN sites that may take advantage of a local Business Talk aSBC (see “Example 5a – offnet call from a BVPN remote site with Local Media Optimization Asia model” and “Example 5b – offnet call from a BVPN central site with Local Media Optimization Asia model” below).

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).

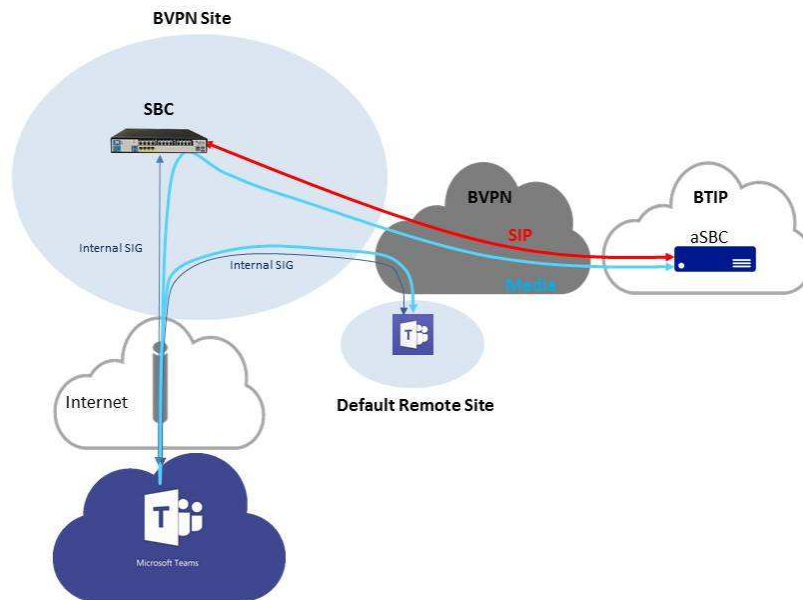
Microsoft Teams does not directly handle FAX, neither analog devices. Those devices can only be interconnected with Teams through the Direct Routing SBC or ATA boxes linked to the Direct Routing SBC and would be fully managed by the Direct Routing SBC.

FAX flows are handled via T.38 transport only.

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

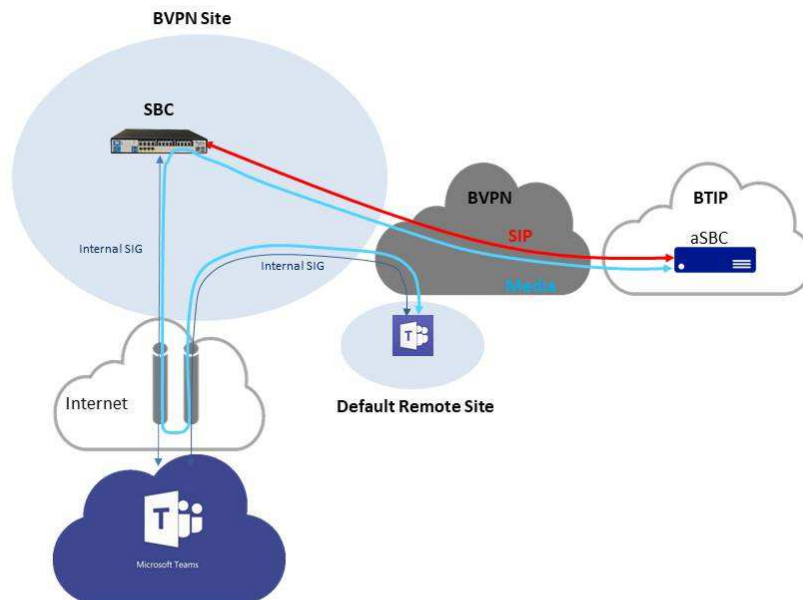
1.1 Standalone mode

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



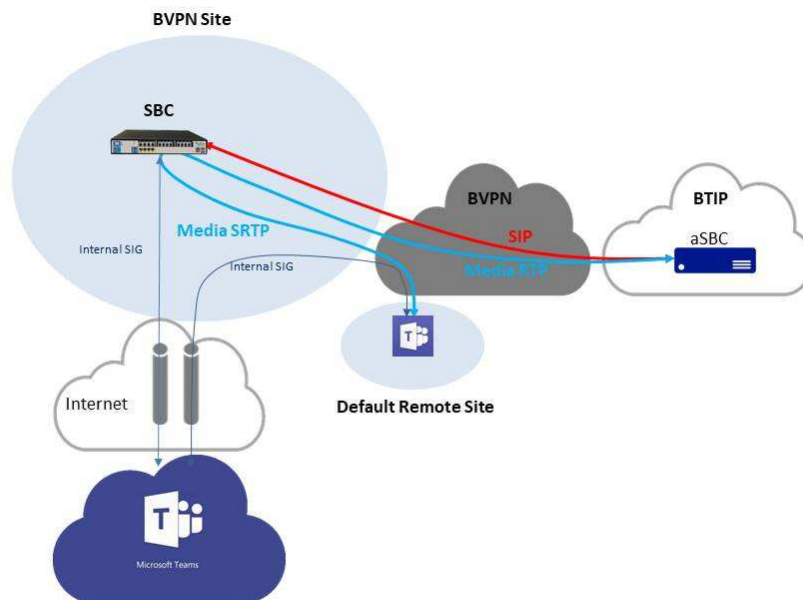
Here, the Teams user belongs to a BVPN site, as does the SBC. There is no Internet breakout within the local site, though that could be the recommended architecture.

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

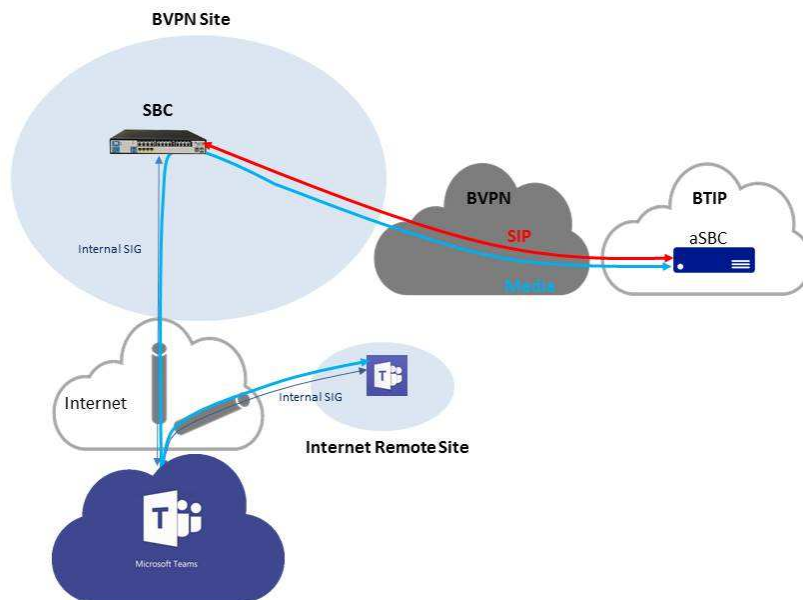
With Media Bypass, media flows cross Internet and join directly Teams user and SBC. They may cross a Microsoft Transport Relay for NAT traversal reasons, but Transport Relays are much more numerous than Media Processors and provide no time consuming treatment of the media.

Example 3 – offnet call from a BVPN remote site with Local Media Optimization Europe Model



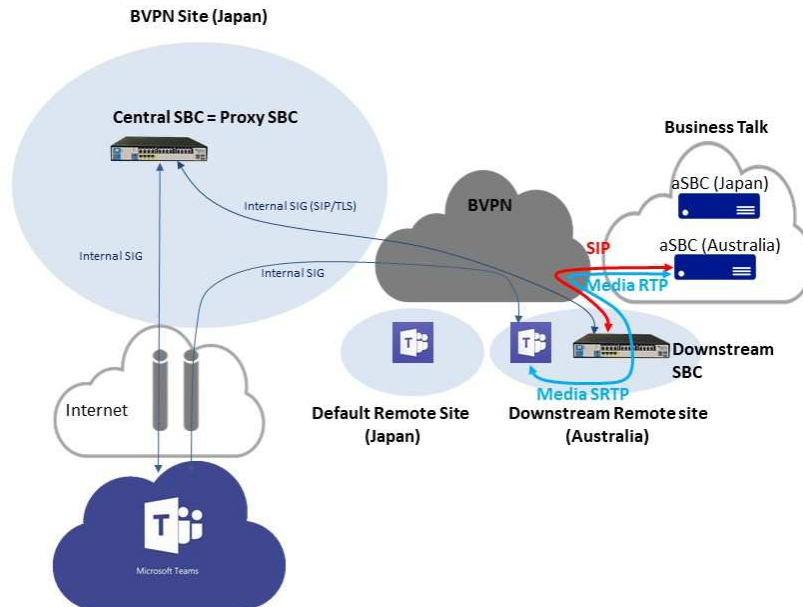
With Local Media Optimization configured, offnet media flow remains on BVPN or LAN for internal Teams users. It aims at using a shorter path to the BT/BTIP SIP trunk and better voice quality than Internet quality. It also saves Internet bandwidth. With “Europe” model, media flows are anchored to the private interface of the Direct Routing SBC. “Asia” model, with which direct media is expected, is not available yet with BT/BTIP.

Example 4 – offnet call from an Internet remote site without Media Bypass (and with or without Local Media Optimization)



Here, the Teams user does not belong to a BVPN site and is located on Internet. Media Bypass is not activated. Local Media Optimization has no effect on call flows involving Internet users.

Example 5a – offnet call from a BVPN remote site with Local Media Optimization Asia model

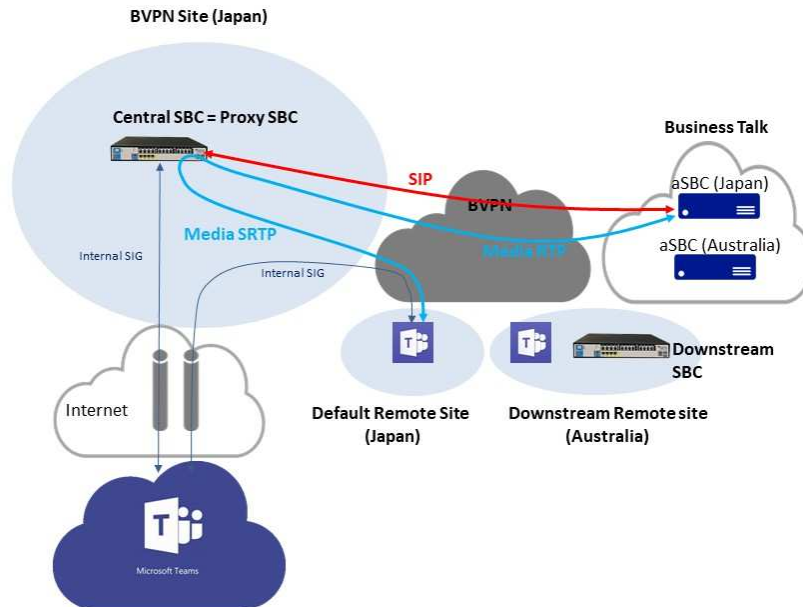


Orange Restricted

Local Media Optimization Asia Model may be useful to keep media flow geographically local for users that are on very remote BVPN sites that may take advantage of a local Business Talk aSBC. For instance, the central SBC may be in Japan, while there are some users in Australia (drawing above). Another instance would be in a BTIP “DROM” context, with a central SBC in France and users in West French Indies. A valid solution would be to use locally a separate Direct Routing SBC, but Local Media Optimization Asia model allows to use local **downstream** SBC that does not need to have a public @IP because they need a trunk to the central SBC only. That avoids deploying local DMZ as no Internet access is required.

In this architecture, central SBC may be named **proxy** SBC as well, meaning it is the front-end SBC from Teams point of view, screening the **downstream** SBC.

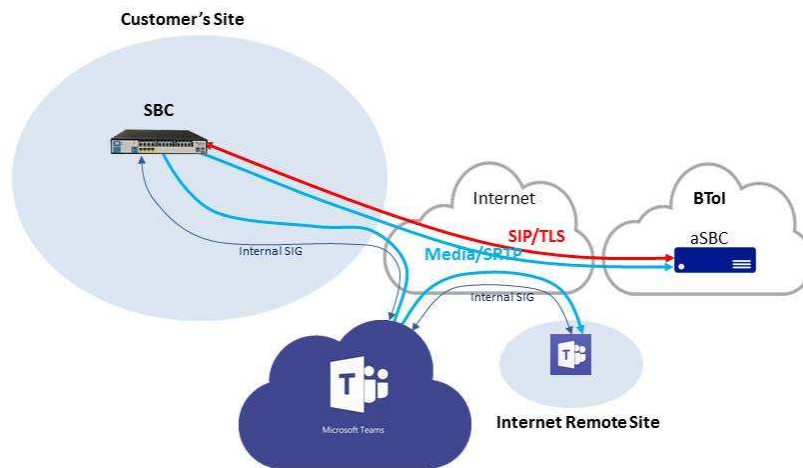
Example 5b – offnet call from a BVPN central site with Local Media Optimization Asia model



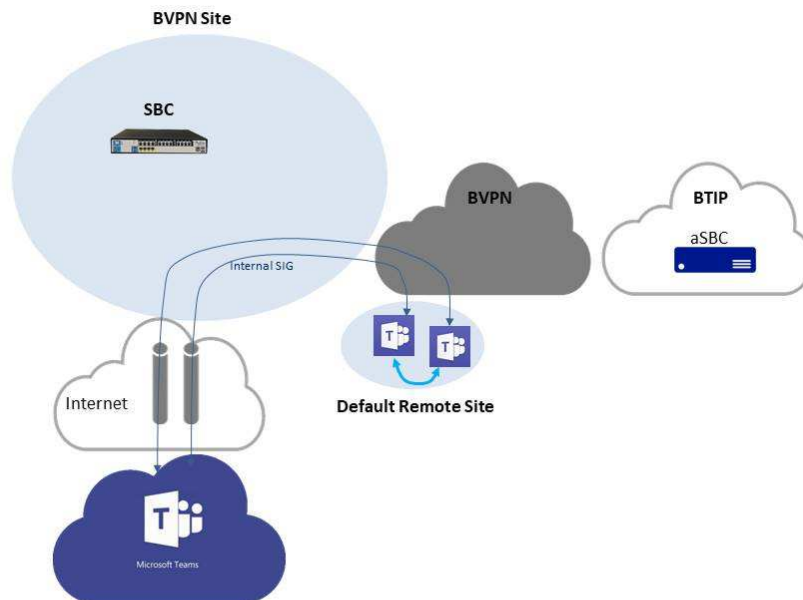
Orange Restricted

This example is linked to example 5a and shows that a user in Japan uses the central SBC that is trunked to the Japanese aSBC of Business Talk. This is like Local Media Optimization Europ model.

Example 6 – 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. Media Bypass is not activated, but it could be.

Example 7 – onnet BVPN call

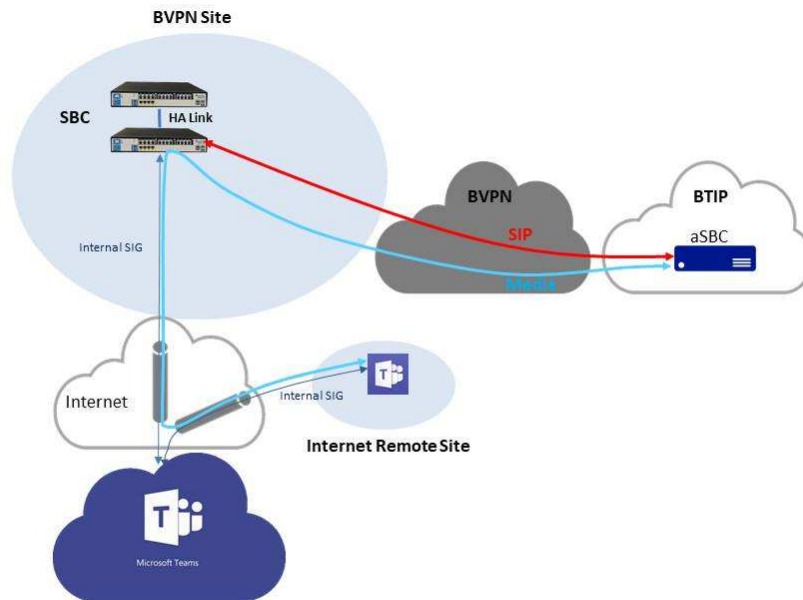
In a BVPN architecture, media flows between Teams users belonging to a single BVPN are direct, whether they are on the same site or in distinct sites.

1.2 High Availability mode

High availability is provided by SBC vendor. This is active-passive mode with a single IP address.

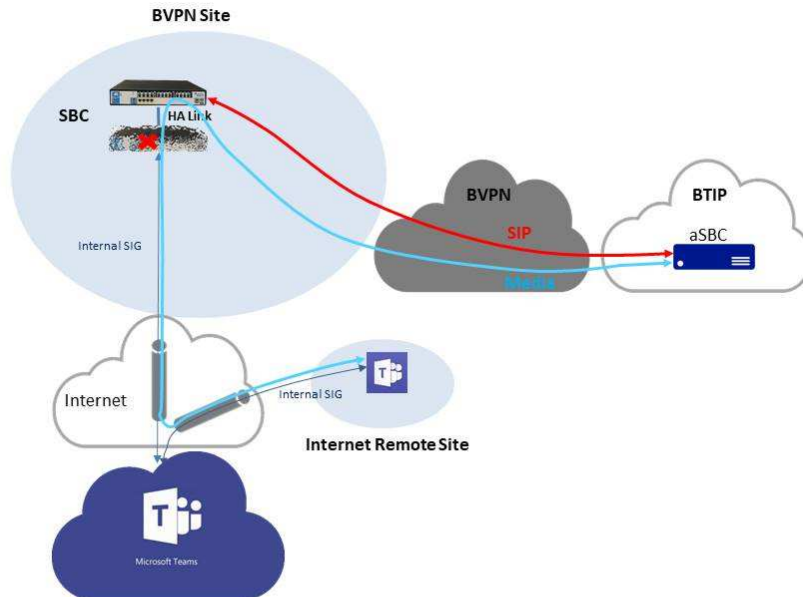
From BTIP/BTalk perspective, this is like a single SBC.

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



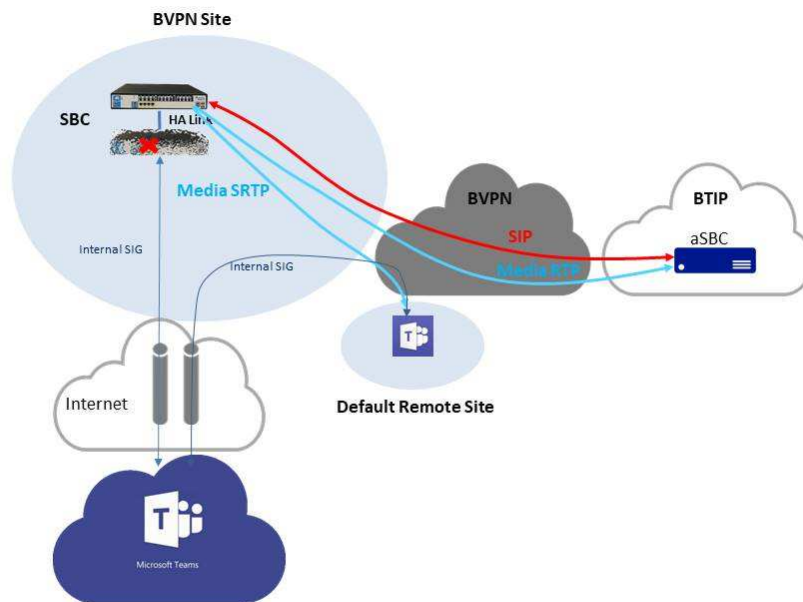
HA is fully managed by SBC themselves. From Teams and BTIP/BTalk points of view, the architecture behaves as if there was a single SBC.

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. Here, Media Bypass is activated, but could not be.

**Example 3 – same as example 2 with a BVPN Teams user and Local Media Optimization
“Europe” model**

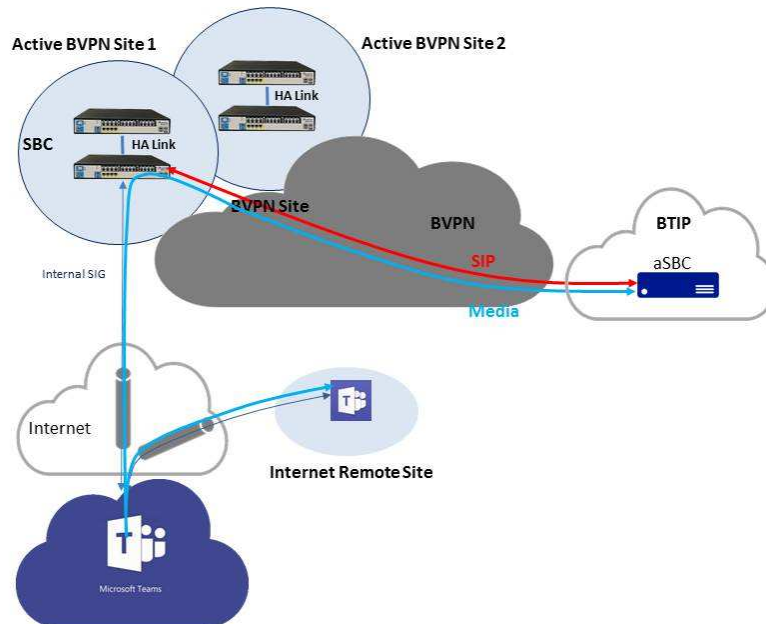


1.3 Active-active mode (resiliency)

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.

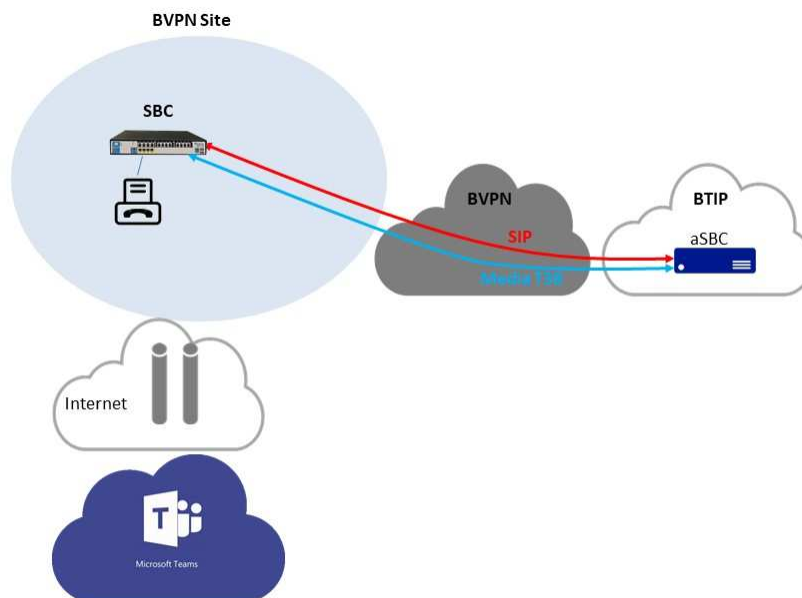
1.4 Analog devices

1.4.1 FAX

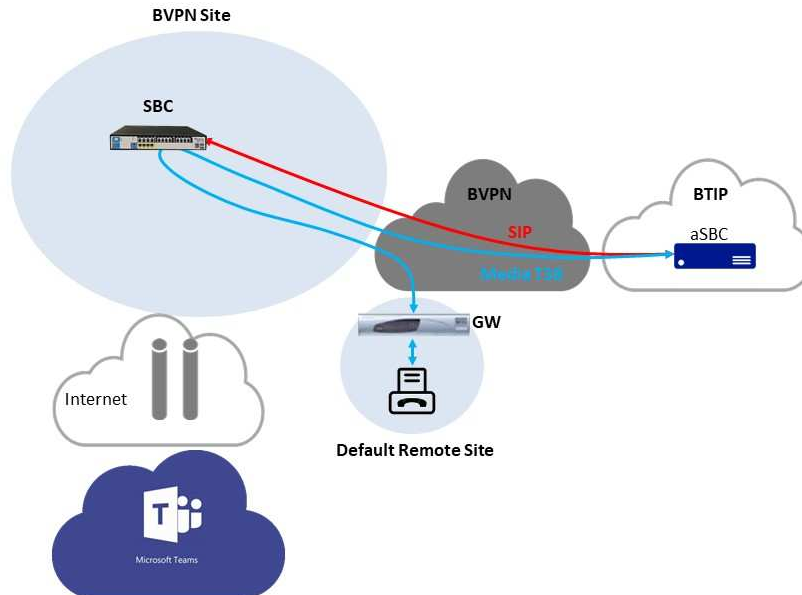
FAX on Direct Routing SBC with or without Gateway is certified both on French (BTIP) and International (BTalk) scopes. FAX protocol is T.38.

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, for signaling as well as for media

Example 1 - FAX directly connected to SBC



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

Example 2 - FAX connected to a cascaded GW behind SBC

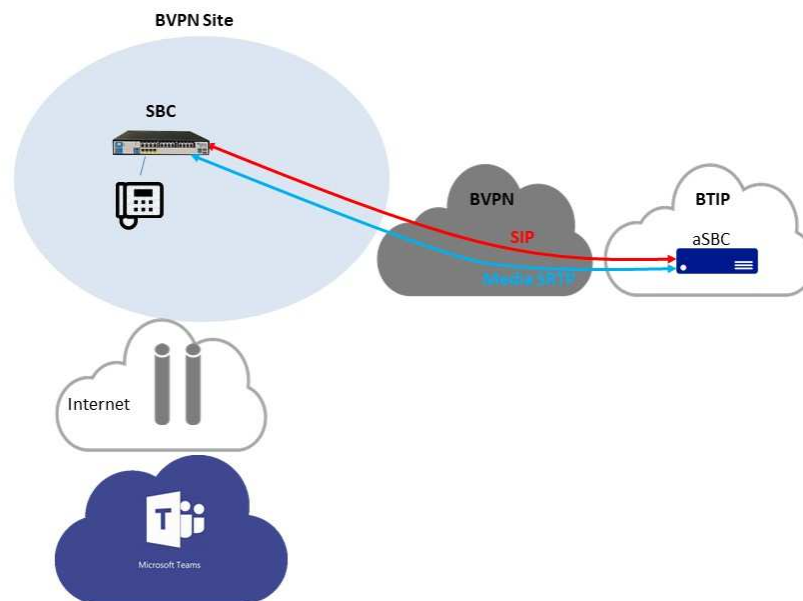
In this architecture FAX device is connected to an analog telephony adapter. It is integrated with DR SBC which can be placed in other remote site or in datacenter. DR SBC with no directly connected endpoints can be virtualized.

Same as in previous architecture call is routed directly between Business Talk / Business Talk IP and FAX and bypasses Teams. This has been certified so far with AudioCodes central SBC with AudioCodes GW (MPxxx or Mediant) and Ribbon Edge central SBC with Ribbon GW 1000/2000.

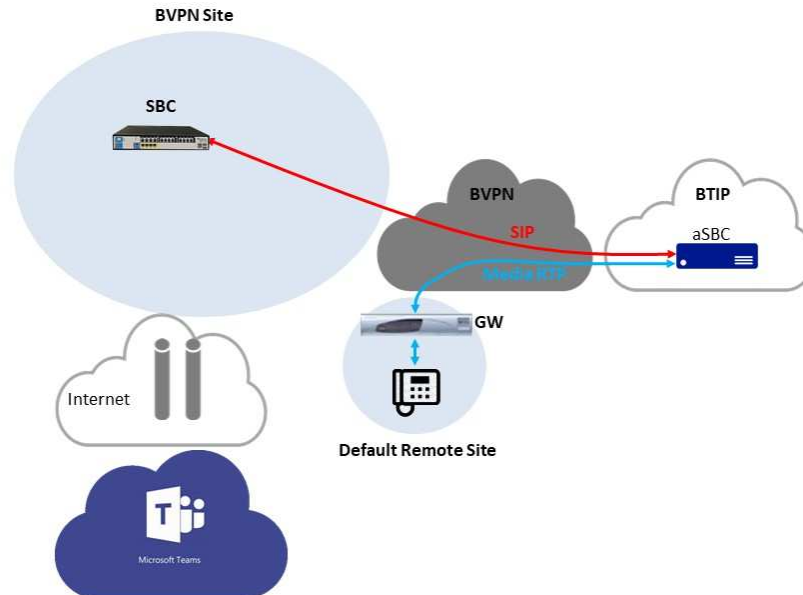
1.4.2 Analog phones

Analog phones on Direct Routing SBC with or without Gateway is certified both on French (BTIP) and International (BTalk) scopes, so far with AudioCodes only as central SBC and remote GW (MPxxx or Mediant).

Example 1 – Analog phone directly connected to central SBC



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

Example 2 – Analog phone connected to a cascaded GW behind SBC

In this architecture, 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. Note that direct media with BTIP/BTalk has been validated in this case.

1.5 Sizing considerations

1.5.1 Coders

Regarding codec usage in the standard architecture:

RTP G711, G729 or G722 is used between Direct Routing SBC and BTIP/BT (see 3.3 for more information on supported codecs on trunk),

Same codec is used in SRTP between Teams and The Direct Routing SBC so that transcoding is avoided, SRTP overhead compared to RTP is neglectable,

encrypted SILK or G722 is used between Teams Client and Teams Media Processors,

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

1.5.2 Real Time Voice (RTVo) classification

In Business VPN, voice flows are classified either by using "Access Control Lists" on CE routers or by trusting DSCP configuration of voice endpoints. "DSCP trust" is intended to become the main way of managing QoS. Therefore, take care to have the following DSCP values configured on your equipment (SBC, GW, Teams client, hardphones...):

- Voice media: **46** (= EF) *!! mandatory !!*
- Video media: **26** (=AF31) or **34** (= AF41)
- Signaling: : **24** (=CS3) or **26** (=AF31) or **40** (= CS5) or **46** (= EF)

Note that our configuration guidelines below include this configuration for SBC and Teams client.

Teams proposes no CAC mechanism to ensure that the RTVo bandwidth won't be overloaded and that may lead to packet loss in case of BVPN access saturation. It's up to you to take care of you consumption and properly size your access with the help of your sales contact.

1.5.3 Table of used channels

Following table recaps the use of channels for selected call flows. For onnet calls, channels consumed by possibly involved far end site are not considered.

	Central site		Remote site with Internet breakout		Remote site without Internet breakout	Remote site with downstream SBC (LMO Asia)
	CE Router RTVo	Internet router	CE Router RTVo	Internet router	CE Router RTVo	CE Router RTVo
Offnet calls without Local Media Optimization						
Client on central site	1	2				
Client on remote site w Internet breakout	1	1		1		
Client on remote site wo Internet breakout	2	2			1	
Offnet calls with Local Media Optimization Europe						
Client on central site	1					
Client on remote site w Internet breakout	2		1		1	
Client on remote site wo Internet breakout	2		1		1	
Offnet calls with Local Media Optimization Asia						
<i>Client served by central SBC</i>						
Client on central site	1					
Client on remote site w Internet breakout	2		1		1	
Client on remote site wo Internet breakout	2		1		1	
<i>Client served by downstream SBC</i>						
Client on remote site with downstream SBC						1
Client on remote site w Internet breakout			1		1	2
Client on remote site wo Internet breakout			1		1	2
Offnet calls from/to Analog devices						
<i>Without Local Media Optimization Asia (device served by central SBC)</i>						
FAX on central site	1					
FAX on remote site w Internet breakout	2		1			
FAX on remote site wo Internet breakout	2				1	
Analog Phone (AP) on central site	1					
AP on remote site w Internet breakout			1			
AP on remote site wo Internet breakout					1	
<i>With Local Media Optimization Asia (device served by downstream SBC)</i>						
FAX on remote site with downstream SBC						1
FAX on remote site w Internet breakout			1			2
FAX on remote site wo Internet breakout					1	2
Analog Phone (AP) on downstream SBC						1
AP on remote site w Internet breakout			1			
AP on remote site wo Internet breakout					1	
Onnet BVPN calls						
From/to a local client						
Between central site and a remote client	1					
Between remote site w Internet breakout and a remote client			1			
Between remote site wo Internet breakout and a remote client					1	
Between AP on central site and a remote client	1					
Between AP on remote site w Internet breakout and a remote client			1			
Between AP on remote site w Internet breakout and a remote client					1	
External calls (between BVPN & Internet clients)						
Client on central site		1				
Client on remote site w Internet breakout				1		
Client on remote site wo Internet breakout	1	1			1	

2 Parameters for connection to BTIP/BTalk/BTol/BTIPol

2.1 Trunking integration

Head Quarter (HQ) architecture	Level of Service	@IP / FQDN used by the service
Single SBC	No redundancy	BTIP/BTalk : SBC IP@ BTol: SBC public IP@ or FQDN DNS Type A BTIPol: SBC public FQDN type A
SBC pair - Vendor HA mode	Local redundancy with nominal/backup behavior. No loss of calls in case of nominal's failure. Single site.	BTIP/BTalk: SBC pair floating IP@ BTol: SBC public floating IP@ or FQDN DNS Type A BTIPol: SBC public floating FQDN DNS Type A
	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.	BTIP/BTalk: SBC1 IP@ SBC2 IP@ ... SBCN IP@ BTol: SBC1 public IP@ or FQDN DNS Type A SBC2 public IP@ or FQDN DNS Type A ... SBCN public IP@ or FQDN DNS Type A BTIPol: SBC1 public FQDN DNS Type A SBC2 public FQDN DNS Type A ... SBCN public FQDN DNS Type A
	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.	<u>BTIP/BTalk:</u> SBC pair1 floating IP@ SBC pair2 floating IP@ ... SBC pairN floating IP@ BTol: SBC pair1 public floating IP@ or FQDN DNS Type A SBC pair2 public floating IP@ or FQDN DNS Type A ... SBC pairN public floating IP@ or FQDN DNS Type A BTIPol: SBC pair1 public floating FQDN DNS Type A SBC pair2 public floating FQDN DNS Type A ... SBC pairN public floating FQDN DNS Type A
N SBC – DNS Resiliency - Mono region	Local redundancy and load sharing with DNS resiliency behavior. Loss of calls handled by a SBC that fails. DNS load balancing from Teams point of view. Geographical redundancy and load sharing with DNS resiliency 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).	BTIP/Talk: Not applicable BTol or BTIPol: SBC public FQDN DNS Type SRV
N SBC pairs – DNS Resiliency 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 : DNS resiliency BTIPol/BTol side and DNS load balancing from Teams side	BTIP/BTalk: Not applicable BTol or BTIPol: SBC pairs public FQDN DNS Type SRV

2 SBC pairs - BTalk T1T7 rescue 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. 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.	<u>BTIP/BTalk:</u> SBC pair1 floating IP@ SBC pair2 floating IP@ <u>BTol:</u> SBC pair1 public floating IP@ or FQDN DNS Type A SBC pair2 public floating IP@ or FQDN DNS Type A <u>BTIPol:</u> SBC pair1 public floating FQDN DNS Type A SBC pair2 public floating FQDN DNS Type A
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 connectivity	<u>BTIP/BTalk:</u> SBC1 IP@ SBC2 IP@ <u>BTol:</u> SBC1 public IP@ or FQDN DNS Type A SBC2 public IP@ or FQDN DNS Type A <u>BTIPol:</u> SBC pair1 public FQDN DNS Type A SBC pair2 public FQDN DNS Type A
2 SBC pairs Nominal / Backup mode	'- Local and geographical redundancy SBC pairs are hosted on 2 different sites with WAN connectivity, each pair on one site	<u>BTIP/BTalk:</u> SBC pair1 IP@ SBC pair2 IP@ <u>BTol:</u> SBC pair1 public IP@ or FQDN DNS Type A SBC pair2 public IP@ or FQDN DNS Type A

		BTIPol: SBC pair1 public FQDN DNS Type A SBC pair2 public FQDN DNS Type A
Remote Site (RS) architecture**	Level of Service	
Remote site without SBC	No survivability, no trunk redundancy	
Remote site with single downstream SBC for Local Media Optimization "Asia model"	Allows offnet media for local users not to transit through central SBC, but stay local. No redundancy of the downstream SBC	BTIP DROM/BTalk : Downstream SBC IP@ BTol: Downstream SBC public IP@ or FQDN DNS Type A BTIPol DROM: Downstream SBC public FQDN type A
Remote site with downstream SBC pair for Local Media Optimization "Asia model" - Vendor HA mode	Local redundancy of the downstream SBC with nominal/backup behavior. No loss of calls in case of nominal's failure. Single site.	BTIP/BTalk: Downstream SBC pair floating IP@ BTol: Downstream SBC public floating IP@ or FQDN DNS Type A BTIPol: Downstream SBC public floating FQDN DNS Type A
	Extended local redundancy of the downstream SBC with nominal/backup behavior. No loss of calls in case of nominal's failure. Two sites linked at L2 level.	
Remote site with N downstream SBC for Local Media Optimization "Asia model" - BTalk round robin mode - Mono region (Premium architecture)	Local redundancy and load sharing of the downstream SBC with round robin behavior. Loss of calls handled by a SBC that fails. Single site.	<u>BTIP/BTalk:</u> Downstream SBC1 IP@ Downstream SBC2 IP@ ... Downstream SBCN IP@ BTol: Downstream SBC1 public IP@ or FQDN DNS Type A Downstream SBC2 public IP@ or FQDN DNS Type A ... Downstream SBCN public IP@ or FQDN DNS Type A BTIPol: Downstream SBC1 public FQDN DNS Type A Downstream SBC2 public FQDN DNS Type A ... Downstream SBCN public FQDN DNS Type A
	Geographical redundancy and load sharing of the downstream with round robin behavior. Loss of calls handled by a SBC that fails. M sites ($M \leq N$) in the same region (i.e. attached to the same aSBC pair with a single T1T7).	

Remote site with N downstream SBC pairs for Local Media Optimization "Asia model" - BTalk round robin mode over N pairs in vendor HA mode - Mono region (Premium+ architecture)	Local + geographical redundancy and load sharing of the downstream SBC. 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.	<u>BTIP/BTalk:</u> Downstream SBC pair1 floating IP@ Downstream SBC pair2 floating IP@ ... Downstream SBC pairN floating IP@ <u>BTol:</u> Downstream SBC pair1 public floating IP@ or FQDN DNS Type A Downstream SBC pair2 public floating IP@ or FQDN DNS Type A ... Downstream SBC pairN public floating IP@ or FQDN DNS Type A <u>BTIPol:</u> Downstream SBC pair1 public floating FQDN DNS Type A Downstream SBC pair2 public floating FQDN DNS Type A ... Downstream SBC pairN public floating FQDN DNS Type A
Remote site with 2 downstream SBC for Local Media Optimization "Asia model" Nominal / Backup mode	- Local redundancy: both downstream 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 connectivity	<u>BTIP/BTalk:</u> Downstream SBC1 IP@ Downstream SBC2 IP@ <u>BTol:</u> Downstream SBC1 public IP@ or FQDN DNS Type A Downstream SBC2 public IP@ or FQDN DNS Type A <u>BTIPol:</u> Downstream SBC pair1 public FQDN DNS Type A Downstream SBC pair2 public FQDN DNS Type A
Remote site with 2 downstream SBC pairs for Local Media Optimization "Asia model" Nominal / Backup mode	- Local and geographical redundancy Downstream SBC pairs are hosted on 2 different sites with WAN onnectivity, each pair on one site	<u>BTIP/BTalk:</u> Downstream SBC pair1 IP@ Downstream SBC pair2 IP@ <u>BTol:</u> Downstream SBC pair1 public IP@ or FQDN DNS

		Type A Downstream SBC pair2 public IP@ or FQDN DNS Type A BTIPol: Downstream SBC pair1 public FQDN DNS Type A Downstream SBC pair2 public FQDN DNS Type A
--	--	---

2.2 SBC IP addressing requirements

For BT/BTIP:

- **Internet facing Interface:** 1 Public IP address + 1 Private IP address NATed to the Public IP
 - Note: cf. NAT translation rule.
- **BT/BTIP SIP trunk Interface:** 1 IP address
- **Management Interface:** 1 IP address
 - Note: For BT/BTIP customers, this interface is generally shared with the BT/BTIP SIP trunk interface. This assumption has been taken in this document.
- **[Optional] HA interface:** 1 IP address (non-routed)

For Business Talk over Internet (BTol), or BTIPol :

- **Internet facing Interface:** 1 Public IP

Notes:

 - For BTol/BTIPol customers, this interface is shared between TEAMS and BTol/BTIPol SIP Trunk.
 - BTol/BTIPol recommends not to use NAT (cf. NAT translation rule).
- **Management Interface:** 1 IP address
- **[Optional] HA interface:** 1 IP address (non-routed)

2.3 TLS integration for BTol/BTIPol

Root and intermediate Certificate (PEM format) must be transmitted to Orange BTIP/BTalk team

3 BTIP/BTalk/BToI/BTIPol 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 DR SBC 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	BToI	BTIPol ⁽¹⁾	Codec	MBP ⁽²⁾	LMO ⁽³⁾	AP ⁽⁴⁾	FAX
Audio-Codes	M500/800/1000/2600/4000/9000 & VE	v.7.20A, build 258.475+	✓	✓	✓	✓	G.722 G.711 G.729	✓	✓ Europe Asia	✓	✓
Ribbon	Edge 1000/2000 & SweLite	9.0.4+ (but not 9.0.5)	✓	✓	✓	✓	G.711 Other planned	✓	✓ Europe	Plan-ned	✓
Oracle	Acme Packet 1100/3900/4600 /6300/6350 & VME	S-Cz8.3.0 p3+	✓	✓	Cust. request	Cust. request	G.722 G711 G729	✓	Ongoing	No	No

(1) BTIPol (BTIP Internet) service is not yet open at the time this document is produced. Please check with your sales contact

(2) MBP = Media Bypass

(3) LMO = Local Media Optimization "Europe" model and/or "Asia" model

(4) AP = Analog Phones

3.3 Codecs on trunk

3.3.1 Monocodec

Only G711 (A or μ laws) and G.729 are allowed

3.3.2 Multicodec (provided that Multicodec has been validated in table above)

On BTIP/BTIPI, only following configurations are allowed:

- G711A, G729
- G722, G711A
- G722, G711A, G729

On Btalk/BTol, only following configurations are allowed:

- G711 (A/μ), G729
- G722, G711 (A/μ)
- G722, G711 (A/μ), G729

3.4 Restrictions in Local Media Optimization

Some features may be unavailable due to Teams restrictions. Please check following link before applying LMO to your configuration:

<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-media-optimization#known-issues>

3.5 Endpoints

As far as Local Media Optimization “Asia” model, that would allow direct RTP between Teams endpoint and BTIP/BTalk aSBC, is not certified, all Microsoft-certified endpoints are certified with Direct Routing and BTIP/BTalk. Indeed, RTP is at least screened by DR SBC.

4 AudioCodes SBC Configuration Checklist for BTIP/BTIPoI/BTtalk/BToI

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

4.1 Flow matrix with BToI

Source	Source IP	Source port	Destination	Destination IP	Destination port	Comment
SBC	SBC public @IP	TLS 5061	BToI	BToI public @IP	TLS 5061	SIP Outgoing
BToI	BToI public @IP	Any	SBC	SBC public @IP	TLS 5061	SIP Incoming
SBC	SBC public @IP	Range defined in Media Realm	BToI	BToI public @IP	UDP 6000-46000	Media outgoing
BToI	BToI public @IP	UDP 6000-46000	SBC	SBC public @IP	Range defined in Media Realm	Media incoming

4.2 Flow matrix with BTIPoI

Source	Source IP	Source port	Destination	Destination IP	Destination port	Comment
SBC	SBC public @IP	TLS 5061	BTIPoI	BTIPoI SIP public @IP	TLS 5061	SIP Outgoing
BTIPoI	BTIPoI SIP public @IP	Any	SBC	SBC public @IP	TLS 5061	SIP Incoming
SBC	SBC public @IP	Range defined in Media Realm	BTIPoI	BTIPoI media public @IP	UDP 6000-38000	Media outgoing
BTIPoI	BTIPoI media public @IP	UDP 6000-38000	SBC	SBC public @IP	Range defined in Media Realm	Media incoming

4.3 Configuration checklist for Office365 Tenant

Parameters to configure the SIP Trunk between Tenant and SBC:

Fqdn	<Customer SBC Public FQDN>
SipSignallingPort	5062
MaxConcurrentSessions	<Number of max sessions>
Enabled	\$true
ForwardPai	\$true
SendSipOptions	\$true

Powershell cmdlet:

```
#New-CsOnlinePSTNGateway -Fqdn sbc.contoso.com -SipSignallingPort 5062 -
MaxConcurrentSessions 50 -Enabled $true -ForwardPai $true -MediaBypass
$false -ForwardCallHistory $true -SendSipOptions $true
```

To activate media bypass:

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

Note: media bypass is only compatible from Audiocodes version 7.20A.254.475.

To activate local media optimization (Europe Scenario) at Tenant level:

```
#Set-CSOnlinePSTNGateway -Identity sbc.contoso.com -GatewaySiteID "MySite"
-ProxySBC $null -BypassMode Always
```

```
#New-CsTenantNetworkRegion -identity "MyRegion" -description "DR Media
Optimization SBCs for MyRegion"
```

```
#New-CsTenantNetworkSite -identity "MySite" -NetworkRegionID "MyRegion" -
description "DR M0 Remote Site in MyRegion"
```

```
#New-CsTenantNetworkSubnet -identity <Network IP address> -MaskBits
<network range: example 24 or 25> -NetworksiteID "MySite" -description
"MySite Voice Subnet"
```

```
#New-CsTenantTrustedIPAddress -identity <Public NAT for MySite> -MaskBits
<network range: ex 24 or 25> -description "Public NAT for MySite"
```

Note: Local Media Optimization is only compatible from Audiocodes version 7.20A.258.475

4.4 Configuration checklist for QoS in Teams client

QoS management is done by configuring the Teams.exe at Windows level.

This configuration is done either locally or by GPO:

- Locally: Use policy-based Quality of Service (QoS) within Group Policy, and create a policy for Teams Audio with following parameters:

Parameter	Value	Description
Policy Name	Teams Audio	
Application Name	Teams.exe	
Protocol	Both	TCP and UDP
Source Port Start	50000	Source ports used by Teams desktop clients are managed in the Teams Admin center. Microsoft recommends to keep this initial port range.
Source Port End	50019	
DSCP value	46	DSCP=46 Expedited Forwarding (EF)

- By GPO: #new-NetQosPolicy -Name "Teams Audio" -AppPathNameMatchCondition "Teams.exe" -IPProtocolMatchCondition Both -IPSrcPortStartMatchCondition 50000 -IPSrcPortEndMatchCondition 50019 -DSCPAction 46 -NetworkProfile All

4.5 SBC IP addressing requirements

For BT/BTIP:

- **Internet facing Interface:** 1 Public IP address + 1 Private IP address NATed to the Public IP
 - Note: cf. NAT translation rule.
- **BT/BTIP SIP trunk Interface:** 1 IP address
- **Management Interface:** 1 IP address
 - Note: For BT/BTIP customers, this interface is generally shared with the BT/BTIP SIP trunk interface. This assumption has been taken in this document.
- **[Optional] HA interface:** 1 IP address (non-routed)

For Business Talk over Internet (BTol), or BTIPol :

- **Internet facing Interface:** 1 Public IP
 - Notes:
 - For BTol/BTIPol customers, this interface is shared between TEAMS and BTol/BTIPol SIP Trunk.
 - BTol/BTIPol recommends not to use NAT (cf. NAT translation rule).
- **Management Interface:** 1 IP address
- **[Optional] HA interface:** 1 IP address (non-routed)

4.6 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 5 – Pre-Recorded Tones files

4.6.1 Step 1 - IP Network configuration

Ethernet Groups

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

- 1 Ethernet Group for Teams and BTol/BTIPol (**GROUP_1**)
- 1 Ethernet Group for BTIP or LAN (**GROUP_2**)
- [Optional] 1 Ethernet Group for HA (**GROUP_3**)

If BT/BTIP :

- ✓ GROUP_1 is dedicated to Teams Only
- ✓ GROUP_2 is shared between BT/BTIP and Management

If BTol/BTIPol :

- ✓ GROUP_1 is shared between Teams and BTol/BTIPol
- ✓ GROUP_2 is dedicated Management Only

Ethernet Devices

SETUP > IP Network > Core entities >
Ethernet Devices

- 1 Ethernet Device for Teams and BTol/BTIPol (**EthD_Teams**)
- 1 Ethernet Device for BTIP or LAN (**EthD_LAN or EthD_BTIP**)
- [Optional] 1 Ethernet Device for HA (**EthD_HA**)

If BTIP :

- ✓ EthD_BTIP associated to GROUP2

If BTol/BTIPol :

- ✓ EthD_Teams (shared with BTol): associated to GROUP1
- ✓ EthD_LAN: associated to GROUP2

IP Interfaces

SETUP > IP Network > Core entities >
IP Interface Devices

- ✓ 1 IP Interface for Teams (IPInt_Teams) (shared with BTol/BTIPol)
- ✓ 1 IP Interface for LAN (IPInt_LAN or IPInt_BTIP)
- ✓ [Optional] 1 IP Interface for HA (IPInt_HA)
- ✓ IPInt_Teams: associated to "EthD_Teams", Media and SIG

If BT/BTIP:

- ✓ IPInt_BTIP: associated to "EthD_BTIP", Media, SIG, OAM

If BTol / BTIPol:

- ✓ IPInt_Teams: associated to "EthD_Teams", Media, SIG
- ✓ IPInt_LAN: associated to "EthD_LAN", OAM

If HA mode :

- ✓ IPInt_HA: associated to "EthD_HA", used for HA mode

NAT Translation

SETUP > IP Network > Core entities >
NAT Translation

If BT/ BTIP:

Create 1 rule for signalization and media traffic

- Source Interface : **IPInt_Teams**
- Source Start Port : **1024**
- Source End Port : **65535**
- Target IP Address: **<SBC Public IP Address>**

	- Target Start Port: - Target End Port: If BTol / BTIPol: General recommendation is not to use NAT translation for BTol/BTIPol. The SBC IP interface dedicated to Teams and BTol/BTIPol will be assigned the SBC Public IP address.
Security	
TLS Contexts	
On the Mediant WebUi Interface: SETUP > IP Network > Security > TLS Contexts	Create new TLS Context for Teams traffic (shared with BTol/BTIPol) - 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/BTol/BTIPol 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
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 If BTol / BTIPol: Create new access lists for each BTol/BTIPol aSBC (2 in total if nominal/backup) - Index: 1 - Description: <BTOI / BTIPol public IP> - Source IP: <BTOI / BTIPol public IP> - 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
--	--

4.6.2 Step 2 - Teams configuration

Allowed Audio Coder Groups

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: **G722**
- Coder Name: **G711A-law**
- Coder Name: **G711U-law**
- Coder Name: **G729**

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: **Disable**
- Generate SRTP Keys Mode: **Always**
- Remote Early Media RTP Detection Mode: **By Media**
- Allowed Audio Coder: **Teams_AudioCoders**
- Allowed Coders mode: **Restriction and Preference**
- RTCP Mode: **Generate Always**
- ICE Mode: **Disable/Lite**
(Lite only required when MediaBypass activated at Tenant level)
- RTP IP DiffServ: **46**
- Signalling DiffServ: **24**
- 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**

If BTol/BTIPol, the following parameters must be changed:

- **Diversion Header Mode:** Remove
- **History-Info Header Mode:** Add

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: 5062 - 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 : 180 - 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 "M=x-data_Removal" - Name : M=x-data_Removal - Manipulation Set ID: 1 - Row Role: Use Current Condition - Match> Message Type: Reinvite

	- Match> Condition: Body.sdp regex (.*)(m=audio)(.)(m=x-data)(.)(.*) - Action> Action Subject: Body.sdp - Action> Action Type: Modify - Action> Action Value: \$1+\$2+\$3
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'
SETUP > Signaling&Media > Message Manipulations	Create new message manipulation "Teams_Busy_Here_Cause34_Removal" - Name: Teams_Busy_Here_Cause34_Removal - Manipulation Set ID: 1 - Row Role: Use Current Condition - Match> Message Type: Any - Match> Condition: Header.Request-URI.MethodType=='486' AND Header.Reason.Reason.Cause == '34' - Action> Action Subject: Header.Reason - Action> Action Type: Remove
SETUP > Signaling&Media > Message Manipulations	Create new message manipulation "Keep_First_Codec" - Name: Keep_First_Codec - Manipulation Set ID: 2 - Row Role: Use Current Condition - Match> Message Type: Any - Match> Condition: Body.sdp regex (.RTP/SAVP)([0-9]{1,3})(.)(.*) - Action> Action Subject: Body.sdp - Action> Action Type: Modify - Action> Action Value: \$1+\$2+\$4
SETUP > Signaling&Media > Message Manipulations	Create new message manipulation "Add_Annexb_No_1" - Name: Add_Annexb_No_1 - Manipulation Set ID: 1 - Row Role: Use Current Condition - Match> Message Type: Invite.Request - Match> Condition: Body.sdp regex (.)(m=audio)(.)(.*) - Action> Action Subject: Body.sdp - Action> Action Type: Modify Action> Action Value: \$0+'a=fmtp:18 annexb=no'+\$7
SETUP > Signaling&Media > Message Manipulations	Create new message manipulation "Add_Annexb_No_2" - Name: Add_Annexb_No_2 - Manipulation Set ID: 1 - Row Role: Use Current Condition - Match> Message Type: Invite.Request - Match> Condition: Body.sdp regex (.)(a=fmtp:18 annexb=yes)(.)(.*) - Action> Action Subject: Body.sdp

	- Action> Action Type: Modify - Action> Action Value: \$1+'a=fmtp:18 annexb=no'+\$3
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") <u>If LMO (Europe Scenario):</u> - Internal Media Realm: BTIP-Media - Teams Media Optimization handling: Teams Decides - Teams Media Optimization Behavior: Internal
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 > SIP Definitions > 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 : 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: * - Destination Host: <Customer SBC Teams Public FQDN> - Message Condition: 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 SRTP

4.6.3 Step 3 – Business Talk configuration

Allowed Audio Coder Groups	
SETUP > Signaling&Media > Coders & Profiles > Allowed Audio Coders Groups	<u>If BT:</u> Create BT_AudioCoders Select the created entry, then click on "Allowed Audio Coders 0 Items" and click on new: - Coder Name: G722 - Coder Name: G711A-law - Coder Name: G711U-law - Coder Name: G729 <u>If BTIP:</u> Create BTIP_AudioCoders Select the created entry, then click on "Allowed Audio Coders 0 Items" and click on new: - Coder Name: G722 - Coder Name: G711A-law - Coder Name: G729 <u>If BTol/BTIPol:</u> Create BTol_AudioCoders (or BTIPol) 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:</u> - Name: BTIP-IPProfile - SBC Media Security Mode: RTP - Allowed Audio Coders: AudioCoders_BT <u>If BTIP:</u> - Name: BTIP-IPProfile - SBC Media Security Mode: RTP - Allowed Audio Coders: AudioCoders_BTIP <u>If BTol:</u> - Name: BTol-IPProfile - SBC Media Security Mode: SRTP - Allowed Audio Coders: AudioCoders_BTol <u>For Both BT/BTIP and BTol:</u> - Symmetric MKI: Disable - MKI Size: 0 - Allowed Coders Mode: Restriction - RFC2833 DTMF Payload Type: 101 - RTP IP DiffServ: 46 - Signaling DiffServ: 24

	- P-Asserted-Identity header mode: Add - Remote REFER Mode: Handle locally - Remote Replaces Mode : Handle Locally - Play RBT to Transferee : yes - Remote 3xx Mode: Handle locally - Remote Hold Format: Send Only
Media Realm	
SETUP > Signaling&Media > Core Entities > Media Realms	Create new or edit Teams 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 - Default Media Realm: No <u>If BTol /BTIPol (edit Teams):</u> - Name: Teams-Media - Topology location: UP - IPv4 Interface Name: IPInt_Teams - Port Range Start: 6000 - Number of Media Session Legs: 5953
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 / BTIPol:</u> - Name : BTol-SIPInterface - Network Interface : IPInt_Teams - TCP Port: 0 - TLS Port: 5061 - Media Realm: Teams-Media - TLS Context Name: Teams-TLSContext - TLS Mutual Authentication: Enable <u>For Both BT/BTIP and BTol / BTIPol:</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: 300 - Redundancy Mode: Homing - Proxy Hot swap: Enable <u>If BTol:</u> - Name : BTol-Proxies - SBC IPv4 SIP Interface : BTol-SIPInterface - TLS Context Name : Teams-TLSContext - Proxy Keep-Alive : Using OPTIONS - Proxy Keep-Alive Time : 300 - Redundancy Mode : Homing - Proxy Hot swap : Enable <u>If BTIPol:</u> - Name : BTIPol-Proxies - SBC IPv4 SIP Interface : BTIPol-SIPInterface - TLS Context Name : Teams-TLSContext - Proxy Keep-Alive : Using OPTIONS - Proxy Keep-Alive Time : 300 - DNS Resolve Method : SRV (Proxy Address Table) : <u>If BT/BTIP:</u> Create 2 Entries for Business Talk Proxies First, the Nominal entry (mandatory to get the higher priority) - Proxy Address : <Nominal SBC ACME>:5060 - Transport Type : TCP Then, the Backup entry (lower priority) - Proxy Address : <Backup SBC ACME>:5060 - Transport Type : TCP <u>If BTol:</u> Create the Entries for Business Talk Proxy - Proxy Address : < Nominal BTol SBC FQDN >:5061 Transport Type: TLS - Proxy Address : < Backup BTol SBC FQDN >:5061 Transport Type: TLS <u>If BTIPol:</u> Create the Entries for Business Talk Proxy - Proxy Address : < BTIPol SBC FQDN SRV > - Transport Type: TLS
Message Manipulation	
SETUP > Signaling&Media > Message Manipulations	Create new message manipulation "User-Agent_Modification » - Name : User-Agent_Modification - Manipulation Set ID: 3

	- 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'
SETUP > Signaling&Media > Message Manipulations	<u>For BTol/BTIPol only (not applicable to BTIP):</u> Create new message manipulation "Add Diversion1 twds BTol" - Name : Add Diversion1 twds BTol - Manipulation Set ID: 3 - Row Role: Use Current Condition - Match> Message Type: INVITE - Match> Condition: Header.History-Info exists - Action> Action Subject: Header.Diversion - Action> Action Type: Add Action> Action Value: '<sip:temp@[SBC_Public_fqdn];user=phone>'
SETUP > Signaling&Media > Message Manipulations	<u>For BTol/BTIPol only (not applicable to BTIP):</u> Create new message manipulation "Modify Diversion1 twds BTol" - Name : Modify Diversion1 twds BTol - Manipulation Set ID: 3 - Row Role: Use Current Condition - Match> Message Type: INVITE - Match> Condition: Header.History-Info.0 regex (<sip:)(.)(@)(.)(*) - Action> Action Subject: Header.Diversion.URL.User - Action> Action Type: Modify - Action> Action Value: \$2
SETUP > Signaling&Media > Message Manipulations	<u>For BTol/BTIPol only (not applicable to BTIP):</u> Create new message manipulation "Remove History-Info twds BTol" - Name : Remove History-Info twds BTol - Manipulation Set ID: 3 - Row Role: Use Current Condition - Match> Message Type: INVITE - Action> Action Subject: Header.History-Info - Action> Action Type: Remove
SETUP > Signaling&Media > Message Manipulations	<u>For BTol/BTIPol only (not applicable to BTIP):</u> Create new message manipulation "Add Diversion2 twds BTol" - Name : Add Diversion2 twds BTol - Manipulation Set ID: 3 - Row Role: Use Current Condition - Match> Message Type: INVITE - Match> Condition: Header.Referred-By exists - Action> Action Subject: Header.Diversion - Action> Action Type: Add Action> Action Value: '<sip:temp@[SBC_Public_fqdn];user=phone>'
SETUP > Signaling&Media > Message Manipulations	<u>For BTol/BTIPol only (not applicable to BTIP):</u> Create new message manipulation "Modify Diversion2 twds BTol"

	- Name : Modify Diversion2 twds BTol - Manipulation Set ID: 3 - Row Role: Use Current Condition - Match> Message Type: INVITE - Match> Condition: Header.Referred-By exists - Action> Action Subject: Header.Diversion.URL - Action> Action Type: Modify - Action> Action Value: Header.Referred-By.URL
SETUP > Signaling&Media > Message Manipulations	<u>For BTol/BTIPol only (not applicable to BTIP):</u> Create new message manipulation “Remove Referred-By twds BTol» - Name : Remove Referred-By twds BTol - Manipulation Set ID: 3 - Row Role: Use Current Condition - Match> Message Type: INVITE - Action> Action Subject: Header.Referred-By - Action> Action Type: Remove
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 / BTIPol:</u> - Name : BTol-IPGroup - Proxy Set: BTol-Proxies - IP Profile: BTol-IPProfile - Media Realm: Teams-Media - DTLS Context: Teams-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”)

4.6.4 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: **All**
- Match > Call Trigger: **REFER**
- Match > ReRoute IP Group: **Teams-IPGroup**
- Action > Destination Type: **Request URI**
- Action > **Destination IP Group:** **Teams-IPGroup**

3rd one regarding Business Talk to Teams traffic:

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

4.6.5 Step 5 – Pre-Recorded-Tones

Auxiliary Files

On the Mediant WebUi Interface:
SETUP>ADMINISTRATION>MAINT
ENANCE>Auxiliary Files

Load a **Prerecorded Tones file** in auxiliary files for ring back tone to be played on transfer scenarios (can be created with AudioCodes DConvert tool based on an audio file with the right codec, ex: G711)

4.7 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

4.7.1 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 (example) - 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 (example) - Preempt Mode: Disable / Enable (depends on customer's choice) - Preempt Priority: 5 (only if Preempt Mode is Enable) - HA Device Name: SBC1 - HA Remote Preempt Priority: 4 (only if Preempt Mode is Enable) - Redundant HA Device Name: SBC2

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

4.7.2 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 (example) - 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 (example) - Preempt Mode: Disable / Enable (depends on customer's choice) - Preempt Priority: 4 (only if Preempt Mode is Enable) - HA Device Name: SBC2 - HA Remote Preempt Priority: 5 (only if Preempt Mode is Enable) - Redundant HA Device Name: SBC1

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

4.7.3 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.
3. Access the active device with its' OAMP IP address and configure the device as required

4.8 . Configuration checklist for Mediant SBC – LMO Asia

4.8.1 Configuration for Proxy SBC

➤ Office365 Tenant

Tenant configuration for Proxy SBC remain the same as the one describe in section [2.3](#)

Parameters to configure the SIP Trunk between Tenant and Downstream gateway:

Fqdn	<Downstream GW FQDN>
SipSignallingPort	5062
MaxConcurrentSessions	<Number of max sessions>
Enabled	\$true
ForwardPai	\$true
SendSipOptions	\$false
ForwardCallHistory	\$true
MediaBypass	\$true
GatewaySiteId	<SiteId>
ProxySBC	<Customer proxy SBC Public FQDN>
BypassMode	Always

Powershell cmdlet:

```
#New-CsOnlinePSTNGateway -Identity <Downstream SBC FQDN> -SipSignalingPort 5062 -
ForwardCallHistory $true -ForwardPai $true -Enabled $true -MediaBypass $true -GatewaySiteId <SiteId>
-ProxySbc <Proxy SBC FQDN> -BypassMode Always -SendSipOptions $false
```

➤ Proxy SBC Teams side

Step 1 – Reuse the configuration checklist for Mediant SBC – Standalone section [2.6](#) except for IP Group and IP Profile entities

Step 2 – Configure the Teams IP Group and IP Profile for LMO Asia

4.8.2 Step 2 - Modify the Teams IP Group and IP Profile for LMO Asia

IP Group	
SETUP > Signaling&Media > Core Entities > IP Group	Create new IP Group for Teams traffic - Name : Teams-LMOAsia-IPGroup - Topology Location: UP - Proxy Set: Teams-Proxies - IP Profile: Teams-IPProfile - Media Realm: Teams-Media - Internal Media Realm: BTIP-Media - Classify by Proxy Set: Disable

	- Local Host Name: <Customer Teams Public FQDN> - Always use src Address: Yes - DTLS Context: Teams-TLSContext - Teams Local Media Optimization handling: Teams Decides - Teams Local Media Optimization Behavior: DirectMedia - 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")
IP Profile	
SETUP > Signaling&Media > Coders & Profiles > IP Profiles	Create new IP Profile for Teams - Name: Teams-LMOAsia-IPProfile - SBC Media Security Mode: SRTP - SBC Enforce MKI Size: Enforce - Reset SRTP Upon Re-key: Disable - Generate SRTP Keys Mode: Always - Remote Early Media RTP Detection Mode: By Media - Allowed Audio Coder: Teams_AudioCoders - Allowed Coders mode: Restriction and Preference - RTCP Mode: Generate Always - ICE Mode: Lite - RTP IP DiffServ: 46 - Signalling DiffServ: 24 - P-Asserted-Identity header mode: As is - SIP Update Support: Not Supported - Remote re-INVITE: Supported only with SDP - Remote Delayed Offer Support: Not Supported - Remote REFER Mode: Regular - Remote 3xx Mode: Transparent - Remote Hold Format: Inactive

➤ Proxy SBC Downstream GW side

DNS	
SETUP > IP Network > DNS > Internal DNS	Create new internal DNS row - Domain Name: <Downstream SBC FQDN> - First IP Address: <Downstream SBC IP> - Second IP Address: 0.0.0.0 - Third IP Address: 0.0.0.0
Allowed Audio Coder Groups	
SETUP > Signaling&Media > Coders & Profiles > Allowed Audio Coders Groups	Create BT_AudioCoders or BTIP_AudioCoders Select the created entry, then click on "Allowed Audio Coders 0 Items" and click on new: If BTIP: - Coder Name: G722 - Coder Name: G711A-law - Coder Name: G711U-law - Coder Name: G729

	If BT: - Coder Name: G722 - Coder Name: G711A-law - Coder Name: G729
IP Profile	
SETUP > Signaling&Media > Coders & Profiles > IP Profiles	Create new IP Profile for GW LMO Asia - Name: GW-LMOAsia-IPProfile - SBC Media Security Mode: SRTP - SBC Enforce MKI Size: Don't Enforce - Generate SRTP Keys Mode: Always - Allowed Audio Coder: BT_AudioCoders or BTIP_AudioCoders - Allowed Coders mode: Restriction and Preference - RFC2833 DTMF Payload Type: 101 - RTP IP DiffServ: 46 - Signalling DiffServ: 24 - P-Asserted-Identity header mode: Add - Play RBT to Transferee: yes - Remote REFER Mode: Regular - Remote 3xx Mode: Transparent - Remote Hold Format: Send Only
Media Realm	
SETUP > Signaling&Media > Core Entities > Media Realms	Create new Media Realm for GW - Name: GW-Media - Topology location: DOWN - IPv4 Interface Name: IPInt_GW - Port Range Start: 16400 - Number of Media Session Legs: 1000
SIP Interface	
SETUP > Signaling&Media > Core Entities > SIP Interface	Create new SIP Interface for downstream GW traffic - Name : GW-LMOAsia-SIPInterface - Topology Location: DOWN - Network Interface : IPInt_GW - UDP Port : 0 - TCP Port: 0 - TLS Port: 5061 - Enable TCP Keep alive: Enable - Classification Failure response Type: 500 - Media Realm: GW-Media - TLS Context Name: Teams-TLSContext - TLS Mutual Authentication: Disable
Proxy Set	
SETUP > Signaling&Media > Core Entities > Proxy Set	Create new Proxy Set for GW traffic - Name : GW-LMOAsia-Proxy - SBC IPv4 SIP Interface: GW-LMOAsia-SIPInterface - TLS Context Name: Teams-TLSContext - Proxy Keep-Alive: Using OPTIONS - Proxy Keep-Alive Time: 300 (Proxy Address Table) : Create 1 Entry for GW Proxy - Index: 0

	- Proxy Address: <Gateway FQDN>:5061 - Transport Type: TLS - Priority Proxy: 1 - Proxy Random Weight: 1
IP Group	
SETUP > Signaling&Media > Core Entities > IP Group	Create new IP Group for GW traffic - Name : GW-LMOAsia-IPGroup - Topology Location: DOWN - Proxy Set: GW-LMOAsia-Proxy - IP Profile: GW-LMOAsia-IPProfile - Media Realm: GW-Media - Outbound Message Manipulation Set: 3 - Internal Media Realm: GW-Media - Classify by Proxy Set: Enable - Media TLS Context: Teams-TLSContext
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: * - Destination Host: <Customer Downstream private FQDN> - Message Condition: a teams contact Source IP Group: Teams-IPGroup

4.8.3 Configuration for Downstream Gateway

Step 1 – General Settings

Step 2 – IP Network Configuration

Step 3a & b – Trunks Configuration: Proxy SBC side and BT/BTIP side

Step 4 – Routing configuration

4.8.4 Step 1 – General Settings

NTP Configuration	
On the Mediant WebUi Interface: SETUP > Administration > Time & Date	- Enable NTP: Enabled - Primary NTP Server Address: <IP Address> - Secondary NTP Server Address: <IP Address> - UTC Offset Time: Hours:0 Minutes:0 - Daylight Saving Time: Disable
Media Security	
SETUP > Signaling&Media > Media > Media Security	- Media Security: Enable
RTP/RTCP	
SETUP > Signaling&Media > Media > RTP/RTCP Settings	- RTP UDP Port Spacing: 10
Proxy & Registration	
SETUP > Signaling&Media > SIP Definitions > Proxy&Registration	- Gateway Name: Gateway FQDN - Use Gateway Name for OPTIONS: Yes

4.8.5 Step 2 – IP Network Configuration

Ethernet Groups	
On the Mediant WebUi Interface: SETUP > IP Network > Core entities > Ethernet Groups	✓ 1 Ethernet Group shared between the Teams Proxy SBC and BT/BTIP (GROUP_1)
Ethernet Devices	
SETUP > IP Network > Core entities > Ethernet Devices	✓ 1 Ethernet Device shared between the Teams Proxy SBC and BT/BTIP (EthD) - Name: EthD - Underlying Interface: GROUP_1 - Tagging: Untagged - MTU: 1500
IP Interfaces	
SETUP > IP Network > Core entities > IP Interface Devices	✓ 1 IP Interface shared between the Teams Proxy SBC and BT/BTIP () - Name: IPInt

	- Application Type: OAMP, Media, Control - Interface Mode: IPv4 manual - IP Address: <GW IP Address> - Prefix length: <Subnet Size> - Default Gateway: <GW default gateway> - Ethernet Device: EthD
TLS Contexts	
On the Mediant WebUi Interface: SETUP > IP Network > Security > TLS Contexts	Create new TLS Context - Name: Self-Signed-TLS - 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/BToI/BTIPol 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
Internal DNS	
On the Mediant WebUi Interface: SETUP > IP Network > DNS > Internal DNS	- Domain Name: <Proxy SBC FQDN> - First IP address: <Proxy SBC private IP> - Second IP Address: 0.0.0.0 - Third IP Address: 0.0.0.0

4.8.6 Step 3a - Trunks configuration – Proxy SBC side

SIP Interface	
SETUP > Signaling&Media > Core entities > SIP Interface	Create new SIP Interface for the Teams Proxy SBC traffic - Name: ProxyTeams-SIPInterface - Topology Location: UP - Network Interface: IPInt - UDP Port: 0 - TCP Port: 0 - TLS Port: 5061 - Enable TCP Keep alive: Enable - Classification Failure Response Type: 0 - Media Realm: GW-Media - TLS Context Name: Self-Signed-TLS - TLS Mutual Authentication: Disable
Proxy Set	
SETUP > Signaling&Media > Core Entities > Proxy Set	Create new Proxy Set for the Teams proxy traffic - Name: ProxyTeams-Proxy - SBC IPv4 SIP Interface: ProxyTeams-SIPInterface - TLS Context Name: Self-Signed-TLS - Proxy Keep-Alive: Using OPTIONS - Proxy Keep-Alive Time: 300 - Proxy Hot swap: Enable (Proxy Address Table): Create 1 Entry for the Teams Proxy SBC - Index: 0 - Proxy Address: <Proxy SBC FQDN @IP>5061 - Transport Type: TLS - Priority Proxy: 1 - Proxy Random Weight: 1
Media Realms	
SETUP > Signaling&Media > Core Entities > Media Realms	Create new Media Realm for the Teams proxy traffic - Name: GW-Media - Topology location: UP - IPv4 Interface Name: IPInt - Port Range Start: 16400 - Number of Media Session Legs: 1000
IP Group	
SETUP > Signaling&Media > Core Entities > IP Group	Create new IP Group for the Teams proxy traffic - Name : ProxyTeams-IPG - Topology Location: UP - Proxy Set: ProxyTeams-Proxy - IP Profile: ProxyTeams-IPProfile - Media Realm: GW-Media - Internal Media Realm: GW-Media - SIP Group Name: <Downstream SBC FQDN> - Classify by Proxy Set: Enable - Local Host Name: <Downstream SBC FQDN> - Always use src Address: Yes

	- DTLS Context: Self-Signed-TLS - Teams Local Media Optimization Initial Behavior: DirectMedia - Proxy Keep-Alive using IP Group settings: Enable
IP Profile	
SETUP > Signaling&Media > Coders & Profiles > IP Profiles	Create new IP Profile for the Teams proxy traffic - Name: ProxyTeams-IPProfile - SBC Media Security Mode: Secured - Remote Early Media RTP Detection Mode: By Media - Allowed Audio Coder: Teams_AudioCoders - Allowed Coders mode: Restriction and Preference - RTCP Mode: Generate Always - ICE Mode: Lite - SIP Update Support: Not Supported - Remote re-INVITE: Supported only with SDP - Remote Delayed Offer Support: Not Supported - Remote Representation Mode: Replace contact - Remote Replaces Mode: Handle locally - Remote REFER Mode: Handle locally - Remote 3xx Mode: Handle locally - Play RBT To Transferee: No - Remote Hold Format: Inactive
Coders	
SETUP > Signaling&Media > Coders & Profiles > Allowed Audio Coders Groups	Create new allowed coders for the Teams proxy traffic - Name: Teams-Audiocodes - Allowed Audio Coder Item: G722, G711A-Law, G711U-Law, G729

4.8.7 Step 3b - Trunks configuration – BT/BTIP side

SIP Interface	
SETUP > Signaling&Media > Core entities > SIP Interface	Create new SIP Interface for BT/BTIP - Name: BTIP-SIPInterface - Topology Location: UP - Network Interface: IPInt - UDP Port: 0 - TCP Port: 5060 - TLS Port: 0 - Enable TCP Keep alive: Enable - Classification Failure Response Type: 0 - Media Realm: GW-Media
Proxy Set	
SETUP > Signaling&Media > Core Entities > Proxy Set	Create new Proxy Set for BT/BTIP - Name: BTIP-Proxy - SBC IPv4 SIP Interface: ProxyTeams-SIPInterface - TLS Context Name: Self-Signed-TLS - Proxy Keep-Alive: Using OPTIONS - Proxy Keep-Alive Time: 300 - Redundancy Mode: Homing - Proxy Hot swap: Enable (Proxy Address Table): Create 2 Entries for nominal/backup BT/BTIP infra - Index: 0 - Proxy Address: <Nominal SBC ACME>:5060 - Transport Type: TCP - Priority Proxy: 1 - Proxy Random Weight: 1 - Index: 1 - Proxy Address: <Backup SBC ACME>:5060 - Transport Type: TCP - Priority Proxy: 2 - Proxy Random Weight: 1
IP Group	
SETUP > Signaling&Media > Core Entities > IP Group	Create new IP Group for BT/BTIP - Name: BTIP-IPG - Topology Location: UP - Proxy Set: BTIP-Proxy - IP Profile: BTIP-IPProfile - Media Realm: GW-Media - Outbound Message Manipulation Set: 1 - Internal Media Realm: GW-Media - Classify by Proxy Set: Enable
IP Profile	
SETUP > Signaling&Media > Coders & Profiles > IP Profiles	Create new IP Profile for BT/BTIP - Name: ProxyTeams-IPProfile - SBC Media Security Mode: Secured

	- Remote Early Media RTP Detection Mode: By Media - Allowed Audio Coder: Teams_AudioCoders - Allowed Coders mode: Restriction and Preference - RTCP Mode: Generate Always - ICE Mode: Lite - SIP Update Support: Not Supported - Remote re-INVITE: Supported only with SDP - Remote Delayed Offer Support: Not Supported - Remote Representation Mode: Replace contact - Remote Replaces Mode: Handle locally - Remote REFER Mode: Handle locally - Remote 3xx Mode: Handle locally - Play RBT To Transferee: No - Remote Hold Format: Inactive
Coders	
SETUP > Signaling&Media > Coders & Profiles > Allowed Audio Coders Groups	Create new allowed coders for BTIP - Name: BTIP-Audiocodes - Allowed Audio Coder Item: G722, G711A-Law, G729 Or Create new allowed coders for BT - Name: BT-Audiocodes Allowed Audio Coder Item: G722, G711A-Law, G711U-Law, G729
Message Manipulation	
SETUP > Signaling&Media > Message Manipulation > Message Manipulations	Create new message manipulation - Name: User-Agent_Modification - Manipulation Set ID: 1 - Message Type: Any - Action Subject: Header.User-Agent - Action Type: Modify - Action Value: Header.User-Agent.Content + ' Downstream'

4.8.8 Step 4 - Routing configuration

IP to IP Routing

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

Create 3 IP to IP routing rules:

First one regarding REFER Messages:

- Name: **REFER-Terminate**
- Match > Source IP Group: **Any**
- Match > Request Type: **All**
- Match > Call Trigger: **REFER**
- Match > ReRoute IP Group: **ProxyTeams-IPG**
- Action > Destination Type: **IPGroup**
- Action > Destination IP Group: **ProxyTeams-IPG**

2nd one regarding BT/BTIP to Proxy Teams traffic:

- Name: **From BTIP to Proxy Teams**
- Match > Source IP Group: **BTIP-IPG**
- Match > ReRoute IP Group: **Any**
- Action > Destination IP Group: **ProxyTeams-IPG**

3rd one regarding Proxy Teams to BT/BTIP traffic:

- Name: **From Proxy Teams to BTIP**
- Match > Source IP Group: **ProxyTeams-IPG**
- Match > ReRoute IP Group: **Any**
- Action > Destination IP Group: **BTIP-IPG**

4.9 AudioCodes Analog Phones configuration checklist

4.9.1 Architecture “Type 1” - Analog Phones connected to DR SBC through remote MediaPack (ATA)

Checklist:

Step 1 – Setup DR SBC trunk configuration towards ATA

Step 2 – Configure ATA to connect with DR SBC gateway

SIP-trunk configuration From DR SBC to MediaPack gateway

Step 1 - Setup DR SBC trunk configuration towards ATA

IP Interface	
On the vSBC DR WebUi Interface: SETUP > IP NETWORK > CORE ENTITIES > IP interface	1 IP Interface for ATA (MPxxx-IP_Inter) - Name: MPxxx-IP_Inter - Application Type: Media + Control - Ethernet Device: <Eth_dev to MPxxx> - Interface Mode: IPv4 Manual - IP Address: DR_SBC @IP - Prefix Length: <Mask> - Default Gateway: <Net. GW>
Media Realm	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Media Realms	Create new Media Realm for ATA (BT media profile can be re-use) - Name: BT Media - IPv4 Interface Name: MPxxx-IP_Inter - UDP Port Range Start: 6000 - Number of Media Session Legs: 1000 - UDP Port Range End: 6999 - TCP Port Range Start: 0 - TCP Port Range End: 0
SIP Interfaces	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > SIP Interface	Create SIP Interface for ATA traffic - Name : MPxxx-SIP_Inter - Network Interface : MPxxx-IP_Inter - Application Type: SBC - UDP Port : 5060 - TCP Port: 5060 - Media Realm: BT Media - Direct Media: Enable
Proxy Set & Proxy IP	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Proxy Sets	Create Proxy Set for ATA traffic - Name : MPxxx-ProxySet - SBC IPv4 SIP Interface : MPxxx-SIP_Inter - Proxy Address/Port: <MP@IP>:5060

	- Transport Type: TCP
IP Group	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > IP Groups	Create IP Group for ATA - Name: MPxxx-IPG - Type: Server: Server - Proxy Set: MPxxx-ProxySet - IP Profile: <GW IP Profile> - Media Realm: BT Media
IP to IP Routing	
	Create IP to IP Routing from Teams to ATA - Name: Teams-to-MPxxx - Source IP Group: Any - Destination Username Pattern: <Pattern> - Destination Type: IP Group - Destination IP Group: MPxxx-IPG

SIP-trunk configuration From MediaPack to DR SBC gateway

Step 2 - Configure ATA to connect with DR SBC gateway

General Parameters	
On the MediaPack WebUi Interface: CONFIGURATION > SIP DEFINITIONS > General Parameters	Configure General Parameters on MediaPack - Enable Early Media: Enable - SIP TCP Local Port: 5060 - SIP TCP Destination Port: 5060
Coders Profile	
CONFIGURATION > CODERS and PROFILES > Coders	Configure Coders for MediaPack - 1 st Coder Name: G.711A-law - Packetization Time: 20 - Rate: 64 - Payload Type: 8 - Silence Suppression: Disabled - 2 nd Coder Name: G.729 - Packetization Time: 20 - Rate: 8 - Payload Type: 18 - Silence Suppression: Disabled
Coders Group Setting	
CONFIGURATION > CODERS and PROFILES > Coders Group Settings	✓ Configure Coders Group for MediaPack - Coder Group ID: 1 - 1 st coder name: G.711A-law - Packetization Time: 20 - Rate: 64 - Payload Type: 8 - Silence Suppression: Disabled - 2 nd coder: G.729 - Packetization Time: 20 - Rate: 8 - Payload Type: 18

	- Silence Suppression: Disabled
Tel Profile	
CONFIGURATION > CODERS and PROFILES > Tel Profile Settings	✓ Create Tel Profile on MediaPack - Profile ID: <1,2,3...> - Profile Name: TelIP_AD - Enable Early Media: Enable - Coder Group: <1,2,3...>
IP Profile	
CONFIGURATION > CODERS and PROFILES > IP Profile Settings	✓ Create IP Profile on MediaPack - Profile ID: <1,2,3...> - Profile Name: IPP_AD - Early Name: Enable - Coder Group: <1,2,3...>
Hunt Group Routing	
CONFIGURATION > GW and IP to IP > Routing > IP to Hunt Group Routing	✓ Create Hunt Group on MediaPack - Dest. Phone Prefix: <phone prefix> - Src. Phone Prefix: * - Src. IP Address: * - Hunt Group: <1,2,3...>
Endpoint Phone Number	
CONFIGURATION > GW and IP to IP > HUNT GROUP > Endpoint Phone Number	✓ Configure Analog Phone Number on MediaPack - Channel(s) : <1,2,3...> - Phone Number: <number> - Hunt Group: <1,2,3...> - Tel Profile ID: <1,2,3...>
Number Manipulation for IP->Tel	
CONFIGURATION > GW and IP to IP > Manipulations > Dest Number IP->Tel	✓ Create number manipulation from IP to Tel - Index : <1,2,3...> - Dest Prefix: <1,2,3...> - Stripped Digits from Left: <...> - Prefix to add: <...>
CONFIGURATION > GW and IP to IP > Manipulations > Dest Number Tel->IP	✓ Create number manipulation from Tel to IP - Index : <1,2,3...> - Dest Prefix: <1,2,3...> - Stripped Digits from Left: <...> - Prefix to add: <...>
Routing	
CONFIGURATION > GW and IP to IP > Routing > Tel to IP Routing	✓ Create call routing between MediaPack and DR SBC - Src. Hunt Group: <1,2,3...> - Dest. Phone Prefix: <Prefix> - Src. Phone Prefix: * - Dest. IP Address: <IP DR SBC> - Port: 5060 - Transport Type: UDP - IP Profile ID: <1,2,3...> - Media Realm: Teams-Media
DTMF	

CONFIGURATION > GW and IP to IP > DTMF and Supplementary > DTMF & Dialing

- ✓ Configure DTMF on Media Pack
 - 1st Tx DTMF Option: **RFC 2833**
 - RFC 2833 Payload Type: **101**

4.9.2 Architecture “Type 2” - Analog Phones connected to DR SBC through remote Local gateway (e.g. AudioCodes Mediant)

Checklist:

- Step 1 – Setup DR SBC trunk configuration towards Local gateway
- Step 2 – Configure AudioCodes Local Gateway to connect with DR SBC gateway
- Step 3 – Configure FXS Interface on Local gateway

SIP-trunk configuration From DR SBC to Local gateway

Step 1 - Setup DR SBC trunk configuration towards AudioCodes Local Gateway

IP Interface	
On the vSBC DR WebUi Interface: SETUP > IP NETWORK > CORE ENTITIES > IP interface	1 IP Interface for Local GW (LocalGW-IP_Inter) - Name: LocalGW-IP_Inter - Application Type: Media + Control - Ethernet Device: <Eth_dev to Local GW> - Interface Mode: IPv4 Manual - IP Address: DR_SBC @IP - Prefix Length: <Mask> - Default Gateway: <Net. GW>
Media Realm	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Media Realms	Create new Media Realm for Local GW (BT media profile can be re-use) - Name: GWAC-Media - IPv4 Interface Name: LocalGW-IP_Inter - UDP Port Range Start: 6000 - Number of Media Session Legs: 1000 - UDP Port Range End: 6999 - TCP Port Range Start: 6000 - TCP Port Range End: 6999
SIP Interfaces	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > SIP Interface	Create SIP Interface for Local GW traffic - Name : LocalGW-SIP_Inter - Network Interface : LocalGW-IP_Inter - Application Type: SBC - UDP Port : 5060 - TCP Port: 5060 - Media Realm: BT Media

	- Direct Media: Enable
Proxy Set & Proxy IP	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Proxy Sets	Create Proxy Set for Local GW traffic - Name : LocalGW-ProxySet - SBC IPv4 SIP Interface : LocalGW-IP_Inter - Proxy Address/Port: <MP@IP>:5060 - Transport Type: TCP
IP Group	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > IP Groups	Create IP Group for Local GW - Name: LocalGW-IPG - Type: Server: Server - Proxy Set: LocalGW-ProxySet - IP Profile: <GW IP Profile> - Media Realm: GWAC-Media
IP to IP Routing	
	Create IP to IP Routing from Teams to Local GW - Name: Teams-to-LocalGW - Source IP Group: Any - Destination Username Pattern: <Pattern> - Destination Type: IP Group - Destination IP Group: LocalGW-IPG

SIP-trunk configuration From Local gateway to DR SBC gateway

Step 2 - Configure AudioCodes Local Gateway to connect with DR SBC gateway

IP Interface	
On the Local gateway WebUi Interface: SETUP > IP NETWORK > CORE ENTITIES > IP interface	1 IP Interface on Local GW (GW-IP_Inter) - Name: GW-IP_Inter - Application Type: Media + Control - Ethernet Device: <Eth_dev to Local GW> - Interface Mode: IPv4 Manual - IP Address: LocalGW_SBC @IP - Prefix Length: <Mask> - Default Gateway: <Net. GW>
Media Realm	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Media Realms	Create new Media Realm on Local GW (BT media profile can be re-use) - Name: DRSBC-Media - IPv4 Interface Name: GW-IP_Inter - Port Range Start: 6000 - Number of Media Session Legs: 1000
SIP Interfaces	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > SIP Interface	Create SIP Interface on Local GW traffic - Name : DRSBC-SIP_Inter - Network Interface : GW-IP_Inter - Application Type: GW - UDP Port : 5060 - TCP Port: 5060 - Media Realm: DRSBC-Media

	- Direct Media: Disable
Proxy Set & Proxy IP	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Proxy Sets	Create Proxy Set on Local GW traffic - Name : DR_SBC-ProxySet - SBC IPv4 SIP Interface : DRSBC-SIP_Inter - Proxy Address/Port: <DR_SBC@IP>:5060 - Transport Type: TCP
IP Group	
SETUP > SIGNALING&MEDIA > CORE ENTITIES > IP Groups	Create IP Group on Local GW - Name: DR_SBC-IPG - Type: Server: Server - Proxy Set: DR_SBC-ProxySet - IP Profile: <GW IP Profile> - Media Realm: DRSBC-Media

FXS interfaces on Local gateway

Step 3 - FXS ports on Local gateway	
Tel Profiles	
On the Local gateway WebUi Interface: SETUP > SIGNALING&MEDIA > CODERS&PROFILES > Tel Profiles	Configure Tel Profile on Local GW - Name: AD-TelProfile - CodersGroup: <GW_coders_group> - Enable Early Media: Enable
Trunk Groups Settings	
SETUP > SIGNALING&MEDIA > GATEWAY > Trunk Groups Settings	Create new Trunk Group on Local gateway - Name: AD - Trunk Group ID: <1,2,3...> - Channel Select Mode: By Dest Phone Number - Registration Mode: Don't Register
Trunk Groups	
SETUP > SIGNALING&MEDIA > GATEWAY > Trunk Groups	Create SIP Interface on Local GW traffic - Module : Module FXS - Channels: <1,2,3...> - Phone Number: <xxxxxxxx> - Trunk Group ID: <ID> - Tel Profile Name: AD-TelProfile

4.9.3 Architecture “Type 3” Analog Phone connected to DR SBC - AudioCodes hardware (SBC+MGW)

 **This architecture inferred from previous one, but actually not tested in lab.**

Checklist:

Step 1 – Setup DR SBC hardware (SBC+MGW) as “Mediant SBC – Standalone” – follow the checklist showing in 2.2 chapter from [VISIT SIP Teams – Configuration Checklist](#) [4] document:

Step 1.1 – IP Network configuration

Step 1.2 – Teams configuration

Step 1.3 – Business Talk configuration

Step 1.4 – Routing configuration

Step 1.5 – Pre-Recorded Tones files

Step 2 – Configure FXS Interface on DR SBC hardware – follow the checklist from [2.2.3](#) chapter of this document.

4.9.4 Configure Flash Hook

Configure Flash Hook on the AudioCodes local Gateway

Step 1 - FXS ports on Local gateway

Tel Profiles

On the Local gateway WebUi Interface:
SETUP >

Configure FlasHook on Local GW

- Enable Call Transfer Using Reinvites: **1**
- Flash Keys Sequence Style: **1**
- Flash Keys SequenceTimeout: **2000**

Configure Flash Hook on the MediaPack (ATA)

 **The Flash Hook features does not work for Analog Phones connected to MediaPack gateway.**

4.10 AudioCodes FAX configuration checklist

4.10.1 FXS fax on Mediant configuration

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 **+ New** and set:

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

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**

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

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

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.

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.

4.10.2 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.

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

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)

5 Ribbon SBC Configuration Checklist for BTIP/BTalk/BToI/BTIPoI

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

5.1 Flow matrix with BToI

Source	Source IP	Source port	Destination	Destination IP	Destination port	Comment
SBC	SBC public @IP	TLS 5061	BToI	BToI public @IP	TLS 5061	SIP Outgoing
BToI	BToI public @IP	Any	SBC	SBC public @IP	TLS 5061	SIP Incoming
SBC	SBC public @IP	Range defined in Media System Configuration	BToI	BToI public @IP	UDP 6000-46000	Media outgoing
BToI	BToI public @IP	UDP 6000-46000	SBC	SBC public @IP	Range defined in Media System Configuration	Media incoming

5.2 Flow matrix with BTIPoI

Source	Source IP	Source port	Destination	Destination IP	Destination port	Comment
SBC	SBC public @IP	TLS 5061	BTIPoI	BTIPoI SIP public @IP	TLS 5061	SIP Outgoing
BTIPoI	BTIPoI SIP public @IP	Any	SBC	SBC public @IP	TLS 5061	SIP Incoming
SBC	SBC public @IP	Range defined in Media System Configuration	BTIPoI	BTIPoI media public @IP	UDP 6000-38000	Media outgoing
BTIPoI	BTIPoI media public @IP	UDP 6000-38000	SBC	SBC public @IP	Range defined in Media System Configuration	Media incoming

5.3 Configuration checklist for Office365 Tenant

Parameters to configure the SIP Trunk between Tenant and SBC:

Fqdn	<Customer SBC Public FQDN>
SipSignallingPort	5062
MaxConcurrentSessions	<Number of max sessions>
Enabled	\$true
ForwardPai	\$true
SendSipOptions	\$true

Powershell cmdlet to add a new SBC :

```
#New-CsOnlinePSTNGateway -Fqdn sbc.contoso.com -SipSignallingPort 5062 -
MaxConcurrentSessions 50 -Enabled $true -ForwardPai $true -MediaBypass $false -
ForwardCallHistory $true -SendSipOptions $true
```

Powershell cmdlet to update an SBC on Tenant (without MBP)

```
Set-CsOnlinePSTNGateway -Identity sbc.contoso.com -SipSignallingPort 5062 -
MaxConcurrentSessions 50 -Enabled $true -ForwardPai $true -MediaBypass $false -
ForwardCallHistory $true -SendSipOptions $true
```

To activate media bypass:

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

To activate Local Media Optimization Europe:

```
Set-CsOnlinePSTNGateway -Identity sbc.contoso.com -GatewaySiteID $null -
MediaBypass $true -ProxySBC $null -BypassMode Always
```

5.4 Configuration checklist for QoS in Teams client

QoS management is done by configuring the Teams.exe at Windows level.

This configuration is done either locally or by GPO:

- Locally: Use policy-based Quality of Service (QoS) within Group Policy, and create a policy for Teams Audio with following parameters:

Parameter	Value	Description
Policy Name	Teams Audio	
Application Name	Teams.exe	
Protocol	Both	TCP and UDP
Source Port Start	50000	Source ports used by Teams desktop clients are managed in the Teams Admin center. Microsoft recommends to keep this initial port range.
Source Port End	50019	
DSCP value	46	DSCP=46 Expedited Forwarding (EF)

- By GPO: *#new-NetQosPolicy -Name "Teams Audio" -AppPathNameMatchCondition "Teams.exe" -IPProtocolMatchCondition Both -IPSrcPortStartMatchCondition 50000 -IPSrcPortEndMatchCondition 50019 -DSCPAction 46 -NetworkProfile All*

Configuration checklist regarding **Ribbon SBC – Standalone**

5.5 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 Teams Side

On the SBC WebUi Interface: Security > TLS Profiles	Create TLS Profile Teams - Description: TLS Profile Teams - TLS Protocol : TLS 1.2 Only - Mutual Authentication : Disabled - Validation Client FQDN : Enabled
--	---

Node Level 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 (1000/2000) / Networking Interfaces (SWe-Lite)

On the SBC WebUi Interface: For SWe-Lite Networking Interfaces > Logical Interfaces For 1000/2000 Node Interfaces > Logical Interfaces	Configure the parameters - Ethernet 1 IP - Description: Interface-Teams and BTol/BTIPol - Primary Address: @Private-IPAddress-BT(all) - Teams - Primary Netmask: @Netmask - Media Next Hop IP: @Gateway (Swe-Lite only) IF BT / BTIP : This interface is dedicated to Teams Only Node Interface Ethernet 2 IP is for BT/BTIP IF BTol / BTIPol : This interface is shared between Teams and BTol/BTIPol Node Interface Ethernet 2 IP should be disabled
---	---

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 - Calling info source: "From" Header Only
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 G711A - Codec: G.711 A-law Create Media Profile > Voice Codec Profile - Description : Default G711u - 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 - Media DSCP: 46
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 - Keep Alive Frequency: 180s 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 - Keep Alive Frequency: 180s 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 - Keep Alive Frequency: 180s
Voice Routing	
On the SBC WebUi Interface: SIP > Transformation Tables Call Routing > Transformation Call Routing > Call Routing Table	Create new Transformation Table: - Description: Teams to BTIP (or BTOI/BTIPol) Create new Call Routing Table: - Description: CR Teams to BTIP (or BTOI/BTIPol) Update CR Teams to BTIP (or BTOI/BTIPol) - Description: Teams to BTIP (or BTOI/BTIPol) - Number/Name transformation Table: Teams to BTIP (or BTOI/BTIPol) - Destination Signaling Group: SG to BT / BTIP (or BTOI/BTIPol) <i>* refer to BTIP Configuration</i>
Message Manipulation	
SIP > Message Manipulation > Condition Rules Table SIP > Message Manipulation > Message Rules Table	Create new Condition Rule: - Description: Anonymous Call Checking - Match Type: from - Operation: Regex - Match Regex: ^((?!anonymous).)*\$ Create new Condition Rule: - Description: URL User - Match Type: SG User Value 1 - Operation: Regex - Match Regex: (< sip:)(.*)@(.*) 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 Create new SIP Message Rule Table: - Description: Privacy-Modification - Application message: Selected Message - Message Selection: INVITE Create new Header Rule: - Description: Privacy Modification - Header Action: Modify

SIP > Message Manipulation > Message Rules Table	- Header Name: Privacy - Header Value – Modify: id (Literal) <u>For BTIPol only:</u> Create new SIP Message Rule Table: - Description: Diversion to Hsitory-Info twds Teams - (Note that Hsitory is miswritten intentionally) - Application message: All Messages - Message Selection: INVITE Create new Header Rule: - Description: Collect Diversion - Header Action: Modify - Header Name: Diversion - Header value: SG User Value 1 - Create new Header Rule: - Description: Send Diversion to History-Info - Condition Expression: URL User - Header Action: Add - Header Name: History-Info - Header value: SG User Value 1 Create new Header Rule: - Description: Remove Diversion - Header Action: Remove - Header Name: Diversion Create new Condition Rule: - Description: Check Reason cause=34 - Match Type: SG User Value 2 - Operation: Regex - Match Regex: ^.*cause=34.*\$ Create new SIP Message Rule Table: - Description: Remove Reason header if cause=34 - Application message: Selected Message - Message Selection: 486 Busy Here Create new Header Rule: - Description: Detect Reason header cause=34 - Header Action: Modify - Header Name: Reason - Header Ordinal Number: All - Header Value: Copy Value to SG UserValue 2 Create new Header Rule: - Description: Remove Reason header if cause=34 - Condition Expression: Check Reason cause=34 - Header Action: Remove - Header Name: Reason - Header Ordinal Number: All - Header Value: Copy Value to SG UserValue 2
---	--

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 (or BTOI/BTIPol) - SIP Profile: SIP Profile Teams - SIP Server Table: SIP Server Teams - Loadbalancing: Priority: Register All Media Information - Media List ID: ML Teams * if Media Bypass or Local Media Optimisation - RTCP Multiplexing: Enable SIP IP Details - Signaling/Media Private IP: @Private-IPAddress-TeamsInterface - Signaling DSCP: 40 * if Local Media Optimization - Teams Local Media Optimization = Enable - Private Media Source IP: @Private-IPAddress-Local Interface. * if Media Bypass or Local Media Optimization - ICE Support: Enable - ICE Mode = Lite * if use NAT Outbound - Outbound NAT Traversal: Static NAT - NAT Public IP: @Public-IPAddress - TeamsInterface Listen Port - Port: 5062 - 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



	Remove Reason header if cause=34 Outbound Message Manipulation Message Table List: Privacy-Modification Diversion to Hsitory-Info twds Teams
--	--

5.6 Step 2 – BT / BTIP / BTOI / BTIPOI Configuration

Node Interface BT/BTIP only	
On the SBC WebUi Interface: Networking Interfaces > Logical Interfaces	Configure the parameters - Ethernet 2 IP - Description: Interface-BT/BTIP - Primary Address: @Private-IPAddress-BT/BTIP - Primary Netmask: @Netmask - Media Next Hop IP: @Gateway (Swe-Lite only)
SIP Profile	
On the SBC WebUi Interface: SIP > SIP Profiles	Create SIP Profile Teams - Description : SIP Profile BT/BTIP/BTOI - SBC Edge Diagnostic Header: Disable - UA Header : empty
TLS Profile BTol/BTIPol only	
On the SBC WebUi Interface: Security > TLS Profiles	Create TLS Profile Teams - Description: BTol/BTIPol TLS Profile - TLS Protocol : TLS 1.2 Only - Mutual Authentication : Enabled - Client Cipher List : ▪ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ▪ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - Validation Client FQDN : Disabled
Media Profile	
On the SBC WebUi Interface: Media > Media Profiles	Create Media Profile > Voice Codec Profile - Description : Default G711A - Codec: G.711 A-law Create Media Profile > Voice Codec Profile - Description : Default G711μ - Codec: G.711 μ-law
SDS-SRTP Profiles BTol/BTIPol only	
On the SBC WebUi Interface: Media > SDS-SRTP Profiles	Edit the Teams SDS-SRTP profile: - Description : MCP Teams & BTOI
Media List for BTIP/BTIPOI	
On the SBC WebUi Interface: Media >Media List	Create new Media List: - Description : ML BT/BTIP, or ML BTOI/BTIPOI - Media Profil List: Default G711A - SDS-SRTP Profile : None (BTIP), or MCP Teams & BTOI (BTIPOI) - Media DSCP: 46
Media List for BT/BTOI	
On the SBC WebUi Interface: Media >Media List	Create new Media List: - Description : ML BT/BTIP, or ML BTOI/BTIPOI - Media Profil List: Default G711A Default G711μ - SDS-SRTP Profile : None (BT), or MCP Teams & BTOI (BTOI) - Media DSCP: 46

SIP Server Table BTol	
On the SBC WebUi Interface: SIP > SIP Server Tables	Create new SIP Server Table: - Description: SIP Server BTol Create SIP Server IP/FQDN Server Host - Priority: 1 - HOST FQDN/IP: Nominal-SBC-BTol-FQDN - Port: 5061 - Protocol: TLS - TLS Profile: TLS Profile Teams & BTol / BTIPol - Monitor: SIP Options - Keep Alive Frequency: 300s Create SIP Server IP/FQDN Server Host - Priority: 2 - HOST FQDN/IP: Backup-SBC-BTol-FQDN - Port: 5061 - Protocol: TLS - TLS Profile: TLS Profile Teams & BTol / BTIPol - Monitor: SIP Options - Keep Alive Frequency: 300s
SIP Server Table BTIPol	
On the SBC WebUi Interface: SIP > SIP Server Tables	Create new SIP Server Table: - Description: SIP Server BTIPol Create SIP Server SRV Server Host - HOST SRV : SRV SBC-BTIPol - Port: 5061 - Protocol: TLS - TLS Profile: TLS Profile Teams & BTol / BTIPol - Monitor: SIP Options - Keep Alive Frequency: 300s
SIP Server Table BT/BTIP	
On the SBC WebUi Interface: SIP > SIP Server Tables	Create new SIP Server Table: - Description: SIP Server BT/BTIP Create SIP Server IP/FQDN Server Host - Priority: 1 - HOST FQDN/IP: @SBC-BT/BTIP-IPAddress - Port: 5060 - Protocol: TCP Transport - Monitor: SIP Options - Keep Alive Frequency: 300s Create SIP Server IP/FQDN Server Host

	- Priority: 2 - HOST FQDN/IP: @SBC-BT/BTIP-IPAddress - Port: 5060 - Protocol: TCP Transport - Monitor: SIP Options - Keep Alive Frequency: 300s
Voice Routing	
On the SBC WebUi Interface: SIP > Transformation Tables Call Routing > Call Routing Table	Create new Transformation Table: - Description: BT/BTIP (or BTOI/BTIPol) to Teams Create new Call Routing Table: - Description: CR BT/BTIP (or BTOI/BTIPol) to Teams Update CR BT/BTIP (or BTOI/BTIPol) to Teams - Description: BT/BTIP (or BTOI/BTIPol) to Teams - Number/Name transformation Table: BT/BTIP (or BTOI/BTIPol) 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: - o Type of value: Token - o Value: user-agent - o Suffix: \ Teams
Signaling Group BT/BTIP	
On the SBC WebUi Interface: Signaling Groups	Create new Signaling Group: - Description: SG to BT / BTIP SIP Channels and Routing - Call Routing Table: CR BT - All to Teams - SIP Profile: SIP Profile BT - SIP Server Table: SIP Server BT – All - Load balancing: Priority: Register All Media Information - Media List ID: ML BT/BTIP SIP IP Details - Signaling/Media Private IP: Ethernet 2 IP - Signaling DSCP: 40 Listen Port

	- Port: 5060 - Protocol: TCP Federated IP/FQDN - IP/FQDN: @SBC-BT/BTIP-IPAddress - Netmask/prefix: 255.255.255.255 - IP/FQDN: @SBC-BT/BTIPI-IPAddress - Netmask/prefix: 255.255.255.255 Message Manipulation: Enabled Outbound Message Manipulation - Message Table List: User-Agent
Signaling Group BTol / BTIPol	
On the SBC WebUi Interface: Signaling Groups	Create new Signaling Group: - Description: SG to BTol / BTIPol SIP Channels and Routing - Call Routing Table: CR BTol / BTIPol to Teams - SIP Profile: SIP Profile BTol / BTIPol - SIP Server Table: SIP Server BTol / BTIPol - All - For BTol, Load balancing: Priority: Register All Media Information - Media List ID: ML BTol/BTIPol SIP IP Details - Signaling/Media Private IP: Ethernet 1 IP - Signaling DSCP: 40 - Outbound NAT Traversal : None (General recommendation is not to use NAT translation for BTol/BTIPol. The SBC IP interface dedicated to Teams and BTol/BTIPol will be assigned the SBC Public IP address). Listen Port - Port: 5061 - Protocol: TLS - TLS Profile: BTol/BTIPol TLS profile Federated IP/FQDN - IP/FQDN: FQDN SBC-BTOI / BTIPOI (IP acceptable for BTol) - Netmask/prefix: 255.255.255.255 - IP/FQDN: FQDN SBC-BTOI / BTIPOI (IP acceptable for BTol) - Netmask/prefix: 255.255.255.255 Message Manipulation: Enabled Outbound Message Manipulation - Message Table List: User-Agent

5.7 Ribbon FAX configuration checklist

5.7.1 FXS fax with Ribbon configuration

The following guide describes steps which should be followed to enable the use of analogue fax devices on Ribbon Gateway. It is assumed that initial configuration of the Ribbon gateway is already done.

5.7.2 Media Profile

It is necessary to enable T.38 support by setting T.38 Fax as a codec in Media Profile tab. In order to do that go to **SETTINGS > MEDIA > MEDIA PROFILE**

Create a new profile by pressing **Create Media Profile** and then **Fax Codec Profile**

Parameter	Value	Description
Description	T38 Profile	Profile name
Codec	T.38 Fax	Select T.38 protocol for fax transmission
Signalling Packet Redundancy	4	Signalization redundancy
Payload Packet Redundancy	1	Page transmission redundancy
Fallback to Passthrough	Disabled	FAX transmission cannot fallback to G711 passthrough. BT does not support G711 passthrough mode
Super G3 to G3 Fallback	Enabled	Force SG3 Fax calls switch to G3 mode. Speed is reduced to 14400bps. ECM is not disabled administratively.

5.7.3 Fax Media List

Go to **SETTINGS > MEDIA > MEDIA LIST** and press  to add a new Media List.

Parameter	Value	Description
Description	FAX Media List	Media List name
Media Profiles List	Default G711A T.38 Profile	Add here the voice codec (here: G.711A) and the fax media codec (here: T.38 Profile)
Digit (DTMF) Relay Type	RFC 2833	Specifies how DTMF digits are passed through data network.
Modem Passthrough	Disabled	Specifies whether modem passthrough is enabled when using the G.711 codec.
Fax Passthrough	Disabled	Specifies whether fax passthrough is enabled when using the G.711 codec.
CNG Tone Detection	Disabled	Specifies whether the SONUS-SBC system will detect Fax tones produced by the origination side fax machine.

5.7.4 FXS port configuration

To configure an FXS port go to **SETTINGS > NODE INTERFACES** and select the port to which a Fax machine will be connected.

Parameter	Value	Description
Analog Line Profile	<Country>	A country dependent parameter

5.7.5 CAS Signalling Profile

CAS Signalling Profiles control various aspects of loop start, DTMF, tone detection and other features associated with the variants of CAS calls. In order to create a CAS Signaling Profile go to **SETTINGS > CAS > CAS SIGNALING PROFILES**

Create a new profile by selecting **Create CAS Profile** and then **FXS Profile**.

Parameter	Value	Description
Description	<Profile Name>	CAS Signalling Profile name
Loop Start Type	Basic	Specifies the Loop Start method

5.7.6 Transformation Table

FXS FAX Towards BT

Outgoing FXS Fax makes use of the same Transformation Table as standard outgoing BT calls

BT Towards FXS FAX

Create a new Transformation Table for faxes incoming from BT. Go to **SETTINGS > CALL ROUTING > TRANSFORMATION** then press  and fill the description field to name the table. Select the newly created table and press  to add a new entry.

Parameter	Value	Description
Match Type	Mandatory / Optional	This option states whether the number matching should be mandatory or optional
Input Field - Value	<FXS Fax number>	Number matching rule. The backslash is used to treat plus "+" as character and not regex special symbol.
Output Field - Value	< FXS Fax number>	Set the same number in transformation output.

5.7.7 CAS Signalling Group

New CAS signalling group for fax devices must be created on Ribbon gateway. Calls from CAS dedicated for faxes will be routed differently so existing CAS for analogue phones cannot be used.

Parameter	Value	Description
Description	<CAS Signaling Group Name>	CAS Signalling Group Name

Channel Hunting	Own Number	Parameter must be set to Own Number to send incoming calls to a proper fax machine
Call Routing Table	<Call Routing Table Towards BT>	Select existing Call Routing Table Towards BT
CAS Signaling Profile	<CAS Signaling Profile>	Select existing CAS Signalling Profile

In **Assigned Channels** table create a new entry with dedicated phone number for each fax port.

5.7.8 Call Routing Table

FXS FAX Towards BT

Outgoing FXS Fax makes use of the same Call Routing Table as standard outgoing BT calls

BT Towards FXS FAX

Go to **SETTINGS > CALL ROUTING > CALL ROUTING TABLE** and select a proper call routing table for outgoing calls towards BT. Afterwards press  to add an entry to the table.

Parameter	Value	Description
Number/Name Transformation Table	<Transformation Table BT Towards FXS fax>	Select proper Transformation Table for incoming FXS fax
Destination Signaling Groups	<CAS Signaling Group>	Select existing CAS FXS Signalling Group
Media Mode	DSP	Enable Ribbon DSP resources for FAX transcoding purpose
Media List	FAX Media List	Select media list containing T.38 codec.

5.7.9 Update Codecs

Please make sure that FAX Media List is configured on the following:

Call Routing Table entry from CAS (FXS FAX) to BT

Call Routing Table entry from BT to CAS (FXS FAX)

Business Talk SIP Signaling Group(s)

6 Oracle SBC Configuration Checklist for BTIP/BTalk

6.1 Warning

This configuration checklist is for S-Cz8.4.0 and upper releases. If checklist for S-Cz8.3.0 is required, please ask your sale contact.

6.2 Configuration Requirements

6.2.1 Tenant configuration

Pair the SBC to the tenant:

Command:

```
New-CsOnlinePSTNGateway
-Fqdn <SBC FQDN>
-SipSignallingPort 5061
-MaxConcurrentSessions <Number>
-Enabled $true
-ForwardPai $true
-ForwardCallHistory $true
-SendSipOptions $true
-MediaBypass $true
-ProxySBC $null
-BypassMode Always
```

6.2.2 Firewall and used ports

With media-bypass mode activated, media flow do not more go through Microsoft Media-Processor equipment.

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
Teams SIP Proxy	52.114.0.0/16	SBC	Public @IP	TCP	5061	SIP/TLS
Internet	Any	SBC	Public @IP	UDP	49152-65535	Media traffic

SBC	Public @IP	Internet	Any	UDP	49152-53247	Media traffic
-----	------------	----------	-----	-----	-------------	---------------

6.2.3 SBC network configuration (wired or virtually wired)

Five interfaces 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

6.2.4 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)

6.2.5 License

- No license is required

6.2.6 User Agent

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

User-Agent: ORACLE <SBC Model>/v.8.3.0 \ Teams

6.2.7 QoS in Teams Client

QoS management is done by configuring the Teams.exe at Windows level.

This configuration is done either locally or by GPO:

- Locally: Use policy-based Quality of Service (QoS) within Group Policy, and create a policy for Teams Audio with following parameters:

Parameter	Value	Description
Policy Name	Teams Audio	
Application Name	Teams.exe	
Protocol	Both	TCP and UDP
Source Port Start	50000	Source ports used by Teams desktop clients are managed in the Teams Admin center. Microsoft recommends to keep this initial port range.
Source Port End	50019	
DSCP value	46	DSCP=46 Expedited Forwarding (EF)

- By GPO: `#new-NetQosPolicy -Name "Teams Audio" -AppPathNameMatchCondition "Teams.exe" -IPProtocolMatchCondition Both -IPSrcPortStartMatchCondition 50000 -IPSrcPortEndMatchCondition 50019 -DSCPAction 46 -NetworkProfile All`

6.3 ORACLE SBC - Standalone

6.3.1 First step

➤ 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”.

6.3.2 IP Network configuration

➤ Physical interface configuration

Three network interfaces:

- 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>

➤ 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> </pre>

	<pre> 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 (getway-heartbeat)# select OracleSBC1 (getway-heartbeat)# state enabled OracleSBC1 (getway-heartbeat)# heartbeat 1 OracleSBC1 (getway-heartbeat)# retry-count 2 OracleSBC1 (getway-heartbeat)# retry-timeout 1 OracleSBC1 (getway-heartbeat)# health-score 30 OracleSBC1 (getway-heartbeat)# done OracleSBC1 (getway-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 (getway-heartbeat)# select OracleSBC1 (getway-heartbeat)# state enabled OracleSBC1 (getway-heartbeat)# heartbeat 1 OracleSBC1 (getway-heartbeat)# retry-count 2 OracleSBC1 (getway-heartbeat)# retry-timeout 1 OracleSBC1 (getway-heartbeat)# health-score 31 OracleSBC1 (getway-heartbeat)# done OracleSBC1 (getway-heartbeat)# exit OracleSBC1 (network-interface)# done </pre>

6.3.3 Teams configuration

➤ 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	<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>
SBCCertificate	

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) 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 </pre>

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	<pre> OracleSBC1# generate-certification-request SBCCertificate </pre> Should return something like this :

	<pre> -----BEGIN CERTIFICATE REQUEST----- MIIC7zCCAdCAQAwYsxCzAJBgNVBAYTAkZSMQ4wDAYDVQQIEwVQYXJpczEOMAwG A1UEBxMFUGFyaXMxZDZANBgNVBAoTBk9yYW5nZTEhMB8GA1UECxMYT3Jhbmd1IEJ1 c2luZXNzIFN1cnZpY2VzMScwJgYDVQQDEx9ocTYwNmd3Lm1zdmlzaXQ2Lm9uZS51 cXVhbnQubmV0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv/NxxJUw 2JeNE3NBvYFkYC0kniJkaB3r4Y+QCPo1gkL5qK9bsVTwop7mHmpon4N1gZQwFKqA UigABDIWwiSOavpLpo98FM5fCFg0J1GZXe/E9URkK9g4NV8D1yyDgZoeDWBtuq6h S/n1ob96NjuH0+wSaxWvi0eQk0icB+7+o9YZ1tCS 7b6FQ7DYJifsd6hAfASx9xfnDRW9RaWr1Qn1kjXeFXwJRSLLaWVn6vaFznAkXGL 5thaEi3MirbinRJQXdtmBqd5hF4wZxIQpZS4qVtVS00+EjQ7+mxvXyBQo08mzmSy vSmWu3Yw3jZREwIDAQABO4wHAYJKoZIhvcNAQkOMQ8wDTALBgNVHQ8EBAMCBaAw DQYJKoZIhvcNAQELBQADggEBALZ1iCeQjm0ovxprVjFf2NPnVEbYUcs2t8vJnCZr 1a6NxdBT5sF/100fss67X/X8TAIgOWX1IIt81xC7ydoIt0hpUtiII4R1zL6nJC5oP brCHHnqFRJbQxdnCFpWYDV3Rff8HsmicizHNv3cYbGyTWbySuOpia+RCTPST1Rg vr1hdSVuCrzRCrt51nEE5X+Vmb0RK2nJ+4CGgNGy6MLyRQ0aIFxnRF/wCwdr+zjQ rDjrRknTc0tB/QaQk1VgpcvZG3XJ90Q3toqXpo6F2Fq8q99/75aUg1680G8J3CMu mZ5K+yldScQuS6Dq1EJt0RZ8IUrNYcn8sB/uhGwXm4Qy79c= -----END CERTIFICATE REQUEST----- </pre>
--	---

Step 3 – Deploy SBC & root/intermediate certificates

SBCInter	→	IntermediateCA	03/05/2019 12:06	Certificat de sécur...	2 Ko
SBCCertificate	→	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 “;

➤ 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
--	---

➤ **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)# options +dont-terminate-assoc-legs OracleSBC1 (media-manager-config)# done

➤ **Steering pool**

Element	Configuration
Steering pool Teams	OracleSBC1# configure terminal 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

➤ 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 180 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 180 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 180 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

➤ 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

➤ 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
--	---

➤ **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 (G722 PCMA PCMU G729 telephone-event) OracleSBC1 (codec-policy)# order-codecs (G722 PCMA PCMU G729) OracleSBC1 (codec-policy)# done

➤ **Media policy**

Signaling DSCP marking 24 (CS3)

Element	Configuration
Codec policy	OracleSBC1# configure terminal OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# media-policy OracleSBC1 (media-policy)# name DSCP OracleSBC1 (media-policy)# tos-settings OracleSBC1 (tos-settings)# media-type message OracleSBC1 (tos-settings)# media-sub-type sip OracleSBC1 (tos-settings)# tos-value 0x60 OracleSBC1 (tos-settings)# done

Audio DSCP marking 46 (EF)

Element	Configuration
Codec policy	OracleSBC1# configure terminal OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# media-policy OracleSBC1 (media-policy)# tos-settings OracleSBC1 (tos-settings)# media-type audio OracleSBC1 (tos-settings)# tos-value 0xb8 OracleSBC1 (tos-settings)# done

➤ Sip manipulation

SIP Manipulation FixCLineNAT:

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

Element	Configuration
SIP Manipulation FixCLineNAT	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name FixCLineNATOutbound
SIP Mime SDP rule MSR_FixCLine	OracleSBC1 (sip-manipulation)# mime-sdp-rules OracleSBC1 (sip-mime-sdp-rules)# name MSR_FixCLine OracleSBC1 (sip-mime-sdp-rules)# msg-type any OracleSBC1 (sip-mime-sdp-rules)# comparison-type case-sensitive OracleSBC1 (sip-mime-sdp-rules)# action manipulate OracleSBC1 (sip-mime-sdp-rules)# sdp-session-rule OracleSBC1 (sip-sdp-session-rules)# name SR_FixCLine OracleSBC1 (sip-sdp-session-rules)# action manipulate OracleSBC1 (sip-mime-sdp-rules)# comparison-type case-sensitive 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 find-replace-all OracleSBC1 (sip-sdp-line-rules)# match-value IN IP4 <Private @IP> OracleSBC1 (sip-sdp-line-rules)# new-value "IN IP4 <SBC 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-name application/sdp OracleSBC1 (sip-element-rules)# type mime OracleSBC1 (sip-element-rules)# action find-replace-all OracleSBC1 (sip-element-rules)# match-value <Private @IP> OracleSBC1 (sip-element-rules)# new-value <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 KeepFirstCodec

Element	Configuration
SIP Manipulation KeepFirstCodec	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name KeepFirstCodec </pre>
SIP Mime SDP rule MSR_KeepFirstCodec	<pre> OracleSBC1 (sip-manipulation)# mime-sdp-rules OracleSBC1 (sip-mime-sdp-rules)# name MSR_KeepFirstCodec OracleSBC1 (sip-mime-sdp-rules)# msg-type any OracleSBC1 (sip-mime-sdp-rules)# action manipulate OracleSBC1 (sip-mime-sdp-rules)# sdp-media-rule OracleSBC1 (sip-sdp-media-rules)# name MR_keepFirstCodec OracleSBC1 (sip-sdp-media-rules)# media-type audio[0] OracleSBC1 (sip-sdp-media-rules)# action manipulate OracleSBC1 (sip-sdp-media-rules)# comparison-type case-sensitive OracleSBC1 (sip-sdp-media-rules)# sdp-line-rules OracleSBC1 (sip-sdp-line-rules)# name LR_firstCodec OracleSBC1 (sip-sdp-line-rules)# type m OracleSBC1 (sip-sdp-line-rules)# action store OracleSBC1 (sip-sdp-line-rules)# comparison-type pattern-rule OracleSBC1 (sip-sdp-line-rules)# match-value ^(.RTP/SAVP)([0-9]{1,3})(.*)\$ OracleSBC1 (sip-sdp-line-rules)# done OracleSBC1 (sip-sdp-line-rules)# exit OracleSBC1 (sip-sdp-media-rules)# sdp-line-rule OracleSBC1 (sip-sdp-line-rules)# name LR_mLineFirstCodecOnly OracleSBC1 (sip-sdp-line-rules)# type m OracleSBC1 (sip-sdp-line-rules)# action replace OracleSBC1 (sip-sdp-line-rules)# comparison-type boolean OracleSBC1 (sip-sdp-line-rules)# match-value \$MSR_keepFirstCodec.\$MR_keepFirstCodec.\$LR_firstCodec OracleSBC1 (sip-sdp-line-rules)# new-value \$MSR_keepFirstCodec.\$MR_keepFirstCodec.\$LR_firstCodec.\$1+\$MSR_ keepFirstCodec.\$MR_keepFirstCodec.\$LR_firstCodec.\$2+" 101" OracleSBC1 (sip-sdp-line-rules)# done OracleSBC1 (sip-sdp-line-rules)# exit OracleSBC1 (sip-sdp-media-rules)# sdp-line-rule OracleSBC1 (sip-sdp-line-rules)# name LR_aLineFirstCodecOnly OracleSBC1 (sip-sdp-line-rules)# type a OracleSBC1 (sip-sdp-line-rules)# action delete OracleSBC1 (sip-sdp-line-rules)# comparison-type pattern-rule OracleSBC1 (sip-sdp-line-rules)# match-value (rtpmap fmt):(?!({\$MSR_keepFirstCodec.\$MR_keepFirstCodec.\$LR_ firstCodec.\$2})101)) OracleSBC1 (sip-sdp-line-rules)# done OracleSBC1 (sip-sdp-line-rules)# exit OracleSBC1 (sip-mime-sdp-rules)# done OracleSBC1 (sip-mime-sdp-rules)# exit </pre>

SIP Manipulation AddAnnexBNo

Element	Configuration
SIP Manipulation AddAnnexBNo	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name AddAnnexBNo
SIP Mime SDP rule MSR_AddAnnexBNo	OracleSBC1 (sip-manipulation)# mine-sdp-rules OracleSBC1 (sip-mime-sdp-rules)# name MSR_AddAnnexBNo OracleSBC1 (sip-mime-sdp-rules)# msg-type any OracleSBC1 (sip-mime-sdp-rules)# methods INVITE OracleSBC1 (sip-mime-sdp-rules)# action manipulate OracleSBC1 (sip-mime-sdp-rules)# sdp-media-rule OracleSBC1 (sip-sdp-media-rules)# name MR_TestG729 OracleSBC1 (sip-sdp-media-rules)# media-type audio OracleSBC1 (sip-sdp-media-rules)# action manipulate OracleSBC1 (sip-sdp-media-rules)# comparison-type case-sensitive OracleSBC1 (sip-sdp-media-rules)# sdp-line-rules OracleSBC1 (sip-sdp-line-rules)# name LR_MatchG729 OracleSBC1 (sip-sdp-line-rules)# type m OracleSBC1 (sip-sdp-line-rules)# action store OracleSBC1 (sip-sdp-line-rules)# comparison-type pattern-rule OracleSBC1 (sip-sdp-line-rules)# match-value \s18\b OracleSBC1 (sip-sdp-line-rules)# done OracleSBC1 (sip-sdp-line-rules)# exit OracleSBC1 (sip-sdp-media-rules)# sdp-line-rule OracleSBC1 (sip-sdp-line-rules)# name LR_Delete OracleSBC1 (sip-sdp-line-rules)# type a OracleSBC1 (sip-sdp-line-rules)# action delete OracleSBC1 (sip-sdp-line-rules)# comparison-type pattern-rule OracleSBC1 (sip-sdp-line-rules)# match-value ^.*annexb.*\$ OracleSBC1 (sip-sdp-line-rules)# done OracleSBC1 (sip-sdp-line-rules)# exit OracleSBC1 (sip-sdp-media-rules)# name MR_AddAnnexBno0 OracleSBC1 (sip-sdp-media-rules)# media-type audio[0] OracleSBC1 (sip-sdp-media-rules)# action manipulate OracleSBC1 (sip-sdp-media-rules)# comparison-type boolean OracleSBC1 (sip-sdp-media-rules)# match-value \$MSR_AddAnnexBNo.\$ MR_TestG729.\$LR_MatchG729[0] OracleSBC1 (sip-sdp-media-rules)# sdp-line-rule OracleSBC1 (sip-sdp-line-rules)# name LR_AddAnnexbNo OracleSBC1 (sip-sdp-line-rules)# type a OracleSBC1 (sip-sdp-line-rules)# action add OracleSBC1 (sip-sdp-line-rules)# new-value "fmtp:18 annexb=no" OracleSBC1 (sip-sdp-line-rules)# done OracleSBC1 (sip-sdp-line-rules)# exit OracleSBC1 (sip-mime-sdp-rules)# done OracleSBC1 (sip-mime-sdp-rules)# exit

SIP Manipulation DelReasonCause34:

Element	Configuration
SIP Manipulation DelReasonCause34	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name DelReasonHeaderCause34
SIP Header rule HR_DelReasonHeader	OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rule)# name HR_is486 OracleSBC1 (sip-header-rule)# header-name @status-line OracleSBC1 (sip-header-rule)# action store OracleSBC1 (sip-header-rule)# comparison-type pattern-rule OracleSBC1 (sip-header-rule)# msg-type reply OracleSBC1 (sip-header-rule)# element-type OracleSBC1 (sip-element-rule)# name is486Code OracleSBC1 (sip-element-rule)# type status-code OracleSBC1 (sip-element-rule)# action store OracleSBC1 (sip-element-rule)# match-val-type any OracleSBC1 (sip-element-rule)# comparison-type pattern-rule OracleSBC1 (sip-element-rule)# match-value 486 OracleSBC1 (sip-element-rule)# done OracleSBC1 (sip-element-rule)# exit OracleSBC1 (sip-header-rule)# done OracleSBC1 (sip-header-rule)# name HR_isCause34 OracleSBC1 (sip-header-rule)# header-name Reason OracleSBC1 (sip-header-rule)# action store OracleSBC1 (sip-header-rule)# comparison-type pattern-rule OracleSBC1 (sip-header-rule)# msg-type reply OracleSBC1 (sip-header-rule)# match-value ^.*cause=34.*\$ OracleSBC1 (sip-header-rule)# done OracleSBC1 (sip-header-rule)# name HR_DelReasonHeader OracleSBC1 (sip-header-rule)# header-name Reason OracleSBC1 (sip-header-rule)# action delete OracleSBC1 (sip-header-rule)# comparison-type pattern-rule OracleSBC1 (sip-header-rule)# msg-type reply OracleSBC1 (sip-header-rule)# match-value "\$HR_is486.\$is486Code & \$HR_isCause34" OracleSBC1 (sip-header-rule)# done OracleSBC1 (sip-header-rule)# exit OracleSBC1 (sip-manipulation)# done

SIP Manipulation RemovePrivacy:

Element	Configuration
SIP Manipulation RemovePrivacy	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router 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!=anonymous OracleSBC1 (sip-header-rule)# done OracleSBC1 (sip-header-rule)# exit OracleSBC1 (sip-manipulation)# done
--	---

SIP Manipulation FixALineNATInbound:

Element	Configuration
SIP Manipulation FixALineNATInbound	OracleSBC# configure terminal OracleSBC (configure)# session-router OracleSBC (session-router)# sip-manipulation OracleSBC (sip-manipulation)# name FixALineNATInbound
Header rule HR_FixALineNATInbound	OracleSBC (sip-manipulation)# header-rules OracleSBC (sip-header-rules)# name HR_FixALineNATInbound OracleSBC (sip-header-rules)# header-name Content-Type OracleSBC (sip-header-rules)# action manipulate OracleSBC (sip-header-rules)# msg-type any OracleSBC (sip-header-rules)# element-rule OracleSBC (sip-element-rules)# name ER_FixALineNATInbound OracleSBC (sip-element-rules)# parameter-name application/sdp OracleSBC (sip-element-rules)# type mime OracleSBC (sip-element-rules)# action find-replace-all OracleSBC (sip-element-rules)# match-value <SBC Public @IP> OracleSBC (sip-element-rules)# new-value <SBC Private @IP> OracleSBC (sip-element-rules)# done OracleSBC (sip-element-rules)# exit OracleSBC (sip-header-rules)# done OracleSBC (sip-header-rules)# exit OracleSBC (sip-manipulation)# 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.8.4.0 \l 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.8.4.0 \ 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	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name out-teams </pre>
SIP Header rule HR_CallFixCLineNAT	<pre> OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name CallFixCLineNATOutbound OracleSBC1 (sip-header-rules)# header-name From OracleSBC1 (sip-header-rules)# action sip-manip OracleSBC1 (sip-header-rules)# new-value FixCLineNATOutbound OracleSBC1 (sip-header-rules)# done OracleSBC1 (sip-header-rules)# exit OracleSBC1 (sip-manipulation)# done </pre>
SIP Header rule KeepFirstCodec	<pre> OracleSBC1 (sip-manipulation)# header-rules OracleSBC1 (sip-header-rules)# name CallKeepFirstCodec OracleSBC1 (sip-header-rules)# header-name From OracleSBC1 (sip-header-rules)# action sip-manip OracleSBC1 (sip-header-rules)# new-value KeepFirstCodec OracleSBC1 (sip-header-rules)# done OracleSBC1 (sip-header-rules)# exit OracleSBC1 (sip-manipulation)# done </pre>

SIP Manipulation in-teams:

Element	Configuration
SIP manipulation in-teams	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# sip-manipulation OracleSBC1 (sip-manipulation)# name in-teams </pre>
SIP Header rule CallChangePrivacy	<pre> 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 </pre>
SIP Header rule CallFixALineNATInbound	<pre> OracleSBC (sip-header-rules)# name CallFixALineNATInbound OracleSBC (sip-header-rules)# header-name From OracleSBC (sip-header-rules)# action sip-manip OracleSBC (sip-header-rules)# new-value FixALineNATInbound OracleSBC (sip-header-rules)# done </pre>
SIP Header rule CallAddAnnexBNo	<pre> OracleSBC (sip-header-rules)# name CallAddAnnexBNo OracleSBC (sip-header-rules)# header-name From OracleSBC (sip-header-rules)# action sip-manip OracleSBC (sip-header-rules)# new-value AddAnnexBNo OracleSBC (sip-header-rules)# done OracleSBC (sip-header-rules)# exit OracleSBC (sip-manipulation)# done </pre>

SIP Header rule CallDelReasonHeaderCause34	OracleSBC (sip-header-rules)# name CallDelReasonHeaderCause34 OracleSBC (sip-header-rules)# header-name From OracleSBC (sip-header-rules)# action sip-manip OracleSBC (sip-header-rules)# new-value DelReasonHeaderCause34 OracleSBC (sip-header-rules)# done OracleSBC (sip-header-rules)# exit OracleSBC (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-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 in-btip	OracleSBC1# configure terminal OracleSBC1 (configure)# session-router 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

➤ 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

➤ 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

➤ SDES profile

Element	Configuration
SDES profile	OracleSBC1# configure terminal OracleSBC1 (configure)# security OracleSBC1 (security)# media-security OracleSBC1 (media-security)# sdes-profile OracleSBC1 (sdes-profile)# name SDES OracleSBC1 (sdes-profile)# crypto-list AES_CM_128_HMAC_SHA1_80 OracleSBC1 (sdes-profile)# srtplib-auth enabled OracleSBC1 (sdes-profile)# srtplib-encrypt enabled OracleSBC1 (sdes-profile)# srtplib-encrypt enabled OracleSBC1 (sdes-profile)# mki disabled OracleSBC1 (sdes-profile)# egress-offer-format same-as-ingress OracleSBC1 (sdes-profile)# srtplib-rekey-on-re-invite disabled OracleSBC1 (sdes-profile)# done

➤ 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>

➤ 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>

➤ Session constraint

Element	Configuration
Session-constraint	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# session-constraints OracleSBC1 (session-constraints)# name SessionConstraintEmergency OracleSBC1 (session-constraints)# max-sessions <X> e.g. 50 OracleSBC1 (session-constraints)# done </pre>

➤ Media sec policy

Element	Configuration
Media sec policy	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# security OracleSBC1 (security)# media-security </pre>

	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)# done OracleSBC1 (inbound)# exit OracleSBC1 (media-sec-policy)# outbound OracleSBC1 (outbound)# mode rtp OracleSBC1 (outbound)# protocol none OracleSBC1 (outbound)# done 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)# done OracleSBC1 (inbound)# exit OracleSBC1 (media-sec-policy)# outbound OracleSBC1 (outbound)# profile SDES OracleSBC1 (outbound)# mode srtp OracleSBC1 (outbound)# protocol sdes OracleSBC1 (outbound)# done
--	---

➤ ICE-Profile

Element	Configuration
ICE-Profile	OracleSBC# configure terminal OracleSBC (configure)# media-manager OracleSBC (media-manager)# ice-profile OracleSBC (ice-profile)# name ice-profile OracleSBC (ice-profile)# stun-conn-timeout 0 OracleSBC (ice-profile)# stun-keep-alive-interval 0 OracleSBC (ice-profile)# stun-rate-limit 100 OracleSBC (ice-profile)# done

➤ Teams 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

	<pre> OracleSBC1 (realm-config)# refer-call-transfer enabled OracleSBC1 (realm-config)# media-sec-policy SRTP OracleSBC1 (realm-config)# rtcp-policy rtcpGen OracleSBC1 (realm-config)# rtcp-mux enabled OracleSBC1 (realm-config)# codec-policy CodecToTeams OracleSBC1 (realm-config)# ice-profile ice-profile OracleSBC1 (realm-config)# media-realm-list ToTeams OracleSBC1 (realm-config)# teams-fqdn <SBC FQDN> OracleSBC1 (realm-config)# teams-fqdn-in-uri enabled OracleSBC1 (realm-config)# sdp-inactive-only enabled OracleSBC1 (realm-config)# done </pre>
--	--

➤ 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>

6.3.4 BTIP configuration

➤ 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 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 </pre>

➤ Codec policy

Element	Configuration
Codec policy : CodecBTIP	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# codec-policy OracleSBC1 (codec-policy)# name CodecBTIP OracleSBC1 (codec-policy)# allow-codecs (G722 PCMA G729 telephone-event) OracleSBC1 (codec-policy)# done </pre>

Element	Configuration
Codec policy : CodecBT	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# media-manager OracleSBC1 (media-manager)# codec-policy OracleSBC1 (codec-policy)# name CodecBT OracleSBC1 (codec-policy)# allow-codecs (G722 PCMA PCMU G729 telephone-event) OracleSBC1 (codec-policy)# done </pre>

➤ Session agent

Element	Configuration
Session agent active	<pre> OracleSBC1# configure terminal OracleSBC1 (configure)# session-router OracleSBC1 (session-router)# session-agent OracleSBC1 (session-agent)# hostname <@IP aSBC 1> </pre>

	OracleSBC1 (session-agent)# port 5060 OracleSBC1 (session-agent)# transport-method StaticTCP OracleSBC1 (session-agent)# realm-id ToBTIP OracleSBC1 (session-agent)# ping-response enabled OracleSBC1 (session-agent)# ping-method OPTIONS OracleSBC1 (session-agent)# ping-interval 300 OracleSBC1 (session-agent)# refer-call-transfer enabled If session agent = BTIP (France). Then : OracleSBC1 (session-agent)# codec-policy CodecBTIP Else If session agent = BT(Int). Then : OracleSBC1 (session-agent)# codec-policy CodecBT OracleSBC1 (session-agent)# done
Session agent 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)# ping-response enabled OracleSBC1 (session-agent)# ping-method OPTIONS OracleSBC1 (session-agent)# ping-interval 300 OracleSBC1 (session-agent)# refer-call-transfer enabled If session agent = BTIP (France). Then : OracleSBC1 (session-agent)# codec-policy CodecBTIP Else If session agent = BT(Int). Then : OracleSBC1 (session-agent)# codec-policy CodecBT OracleSBC1 (session-agent)# done

➤ 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 enable OracleSBC1 (session-group)# stop-sag-recurse 300-407,409-599 OracleSBC1 (session-group)# done

➤ 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)# codec-policy CodecBTIP OracleSBC1 (realm-config)# rtcp-policy rtcpGen OracleSBC1 (realm-config)# constraint-name SessionConstraintEmergency OracleSBC1 (realm-config)# ringback-trigger refer OracleSBC1 (realm-config)# ringback-file <ringback file .raw>* OracleSBC1 (realm-config)# done
--	--

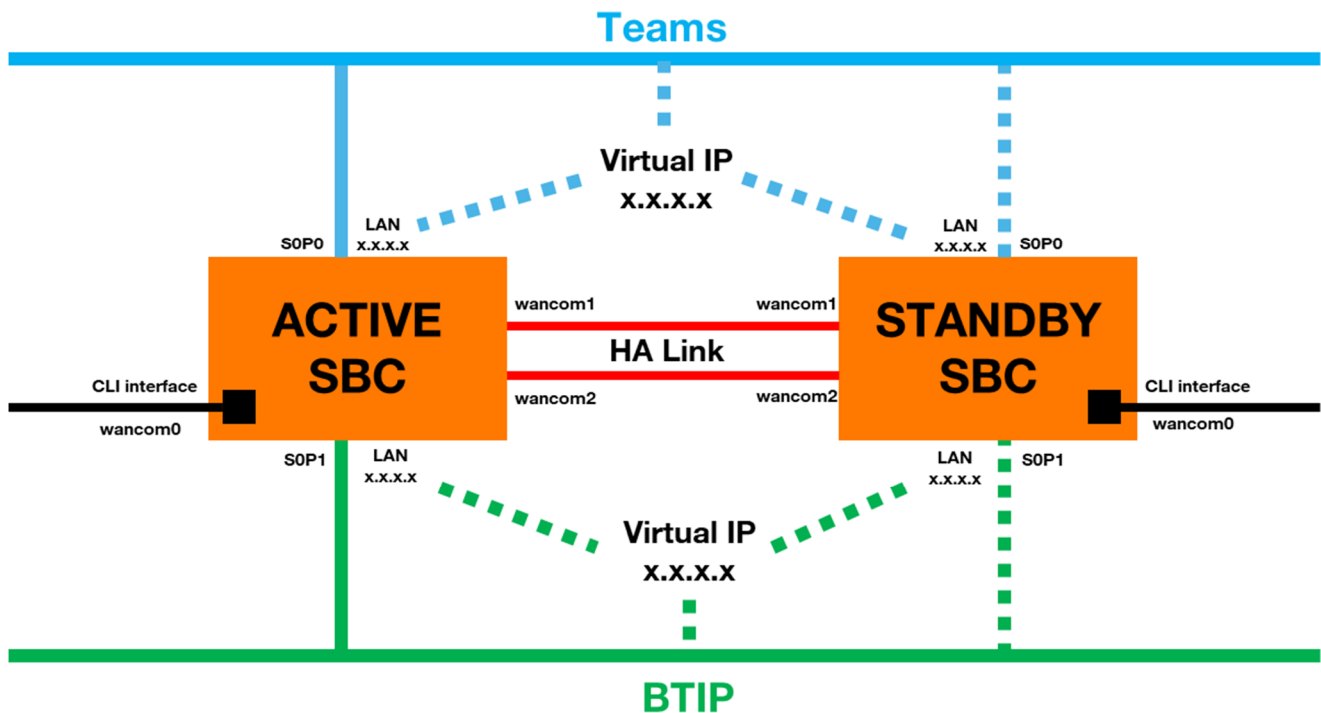
* Ringback file can be found [here](#)

➤ SIP interface

Element	Configuration
SIP interface	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)# 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

6.4 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
 - o NTP synchronization
 - o Virtual MAC address
 - o Primary & Secondary utility address
 - o Wancom1 & Wancom2 physical configuration
 - o Wancom1 & Wancom2 network configuration
 - o Redundancy
- Secondary SBC configuration

6.4.1 First SBC configuration

➤ 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>

➤ 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>

➤ 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>

➤ 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>

➤ 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>

➤ 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 OracleSBC1 (rdncy-peer)# done OracleSBC1 (rdncy-peer)# exit </pre>

	OracleSBC1 (rdncy)# done
--	---------------------------------

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

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

6.4.2 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
```