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

18 october 2026

Teams Direct Routing AudioCodes Checklist
Teams Direct Routing Ribbon Checklist
Teams Direct Routing Oracle Checklist

Contents

1 Main certified architectures 4
1.1 Teams media capabilities 4
1.2 FAX 4
1.3 Redundancy 5
1.4 Standalone mode 5
1.5 High Availability mode 12
1.6 Active-active mode (resiliency) 15
1.7 BTIP in DROM (French Overseas Territories) 16
1.8 Analog devices 24
1.9 Reminder on emergency calls 28
1.10 Sizing considerations 28
2 Parameters for connection to BTIP/BTalk/BTol/BTIPol 31
2.1 Trunking integration 31
2.2 SBC IP addressing requirements 36
2.3 ACL for BTol/BTIPol 36
2.4 TLS integration for BTol/BTIPol 37
3 BTIP/BTalk/BTol/BTIPol certified versions 38
3.1 Teams 38
3.2 Certified SBC 38
3.3 Codecs on trunk 38
3.4 Restrictions in Local Media Optimization 39
3.5 Endpoints 39
4 AudioCodes SBC Configuration Checklist for BTIP/BTIPol/BTalk/BTol 40
4.1 Flow matrix with BTol 40
4.2 Flow matrix with BTIPol 40
4.3 Configuration checklist for Office365 Tenant 40
4.4 Configuration checklist for QoS in Teams client 45
4.5 Parameter not available via the web admin page 45
4.6 SBC IP addressing requirements 45
4.7 Configuration checklist for Mediant SBC – Standalone 46
4.8 Configuration checklist for Mediant SBC – HA 59
4.9 . Configuration checklist for Mediant SBC – LMO Asia 62
4.10 AudioCodes Analog Phones configuration checklist 71
4.11 AudioCodes FAX configuration checklist 78
5 Ribbon SBC Configuration Checklist for BTIP/BTalk/BTol/BTIPol 84
5.1 Flow matrix with BTol 84
5.2 Flow matrix with BTIPol 84
5.3 Configuration checklist for Office365 Tenant 84
5.4 Configuration checklist for QoS in Teams client 85
5.5 Step 1 – Teams Configuration 86
5.6 Step 2 – BT / BTIP / BTOI / BTIPOI Configuration 95
5.7 HA Configuration 99
5.8 Ribbon FAX configuration checklist 99
6 Oracle SBC Configuration Checklist for BTIP/BTalk 103

6.1 Warning 103
6.2 Configuration Requirements 103
6.3 ORACLE SBC - Standalone 108
6.4 ORACLE SBC - HA configuration 132

1 Main certified architectures

1.1 Teams media capabilities

1.1.1 Media Bypass

Teams 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.

1.1.2 Local Media Optimization "Europe" model

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).

1.1.3 Local Media Optimization "Asia" model

- **General overview**

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.

- **BTIP in DROM (French Overseas Territories)**

Despite its name, "Asia" model is applicable anywhere, especially in a "BTIP DROM" scope, where a central BTIP trunk is connected to a central Direct Routing SBC in European France, while users in French overseas territories take advantage of a local BTIP trunk connected to a local downstream SBC (see also 1.7 BTIP in DROM (French Overseas Territories).

1.2 FAX

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).
- With BTIP (France only), G.711 inband fax passthrough is available by default. T.38 is available upon request.
- With BT, both G.711 inband fax passthrough and T.38 are available by default.
- T.38 and G.711 inband fax are enabled on BTIP and BTalk networks without an end-to-end guarantee. Orange cannot certify the reliability of fax interoperability that may occur at interconnection points with terminating carriers.

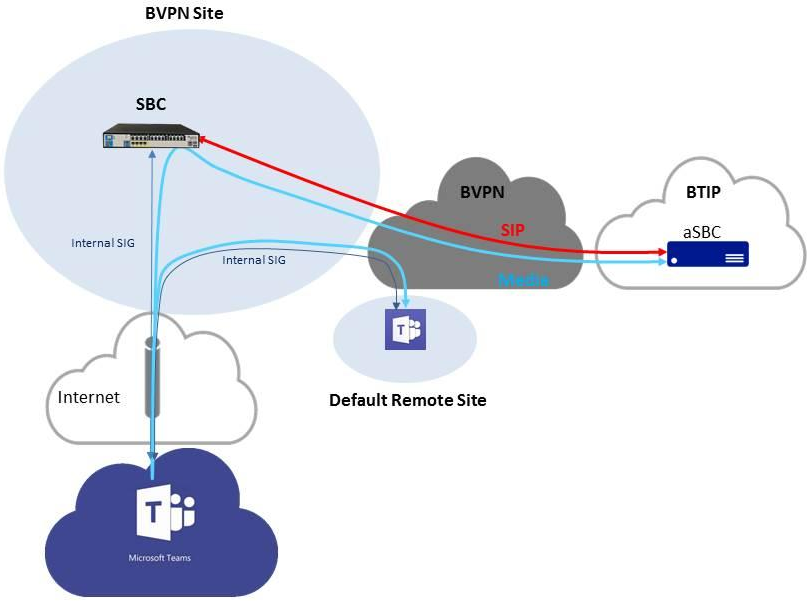
Microsoft Teams does not directly handle FAX, neither analog device. Those devices can only be interconnected with Teams through the Direct Routing SBC or ATA boxes linked to the Direct Routing SBC and would be fully managed by the Direct Routing SBC.

1.3 Redundancy

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

1.4 Standalone mode

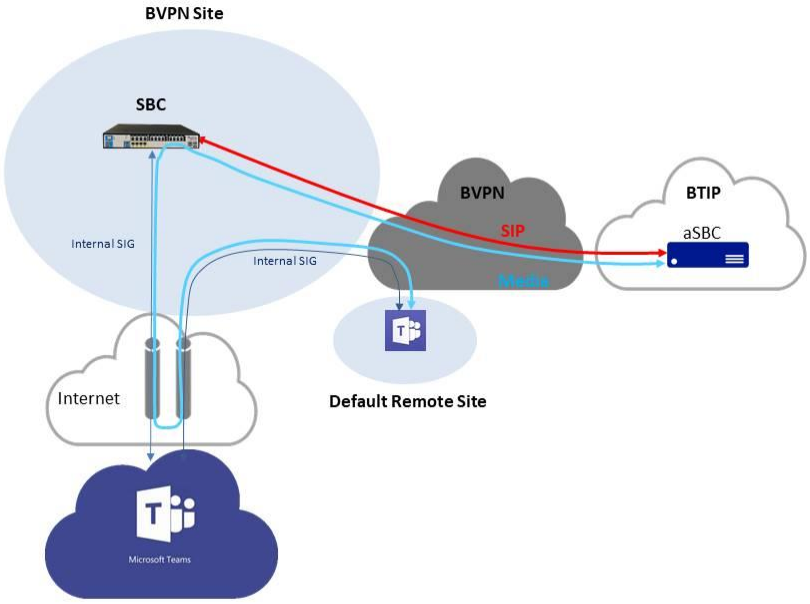
Example 1 – offnet call from a BVPN remote site without Media Bypass



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.

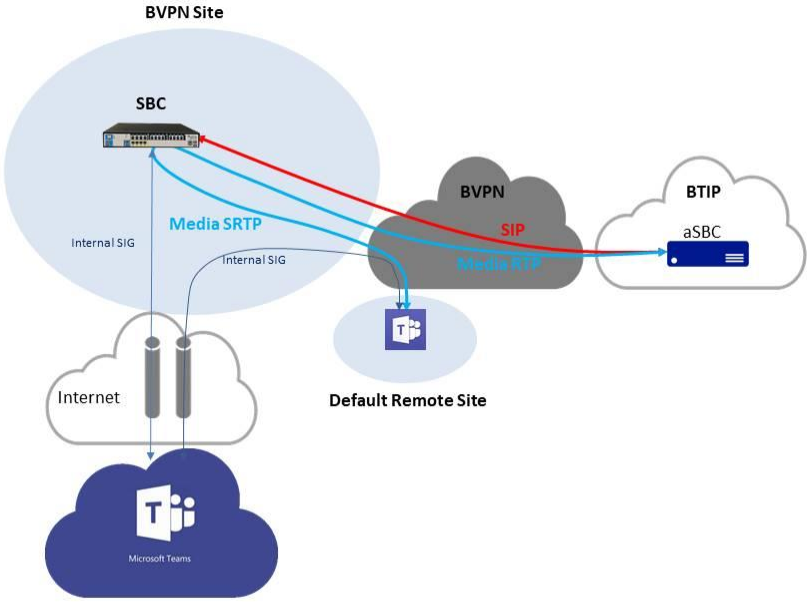
Without Media Bypass, media flows cross Internet to reach Teams Media Processors and SBC.

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



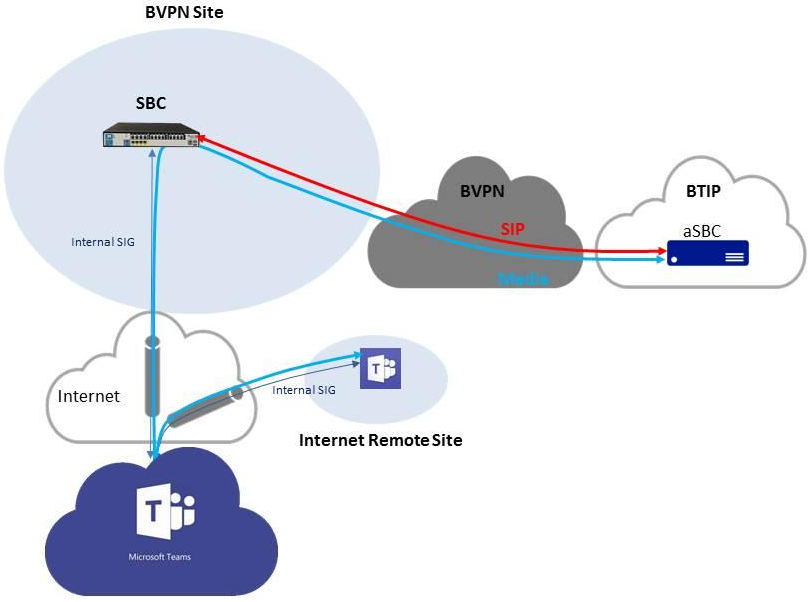
With Media Bypass, media flows cross Internet and join directly Teams user and SBC. They may cross a Microsoft Transport Relay for NAT traversal reasons, but Transport Relays are much more numerous that Media Processors and provide no time consuming treatment of the media.

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



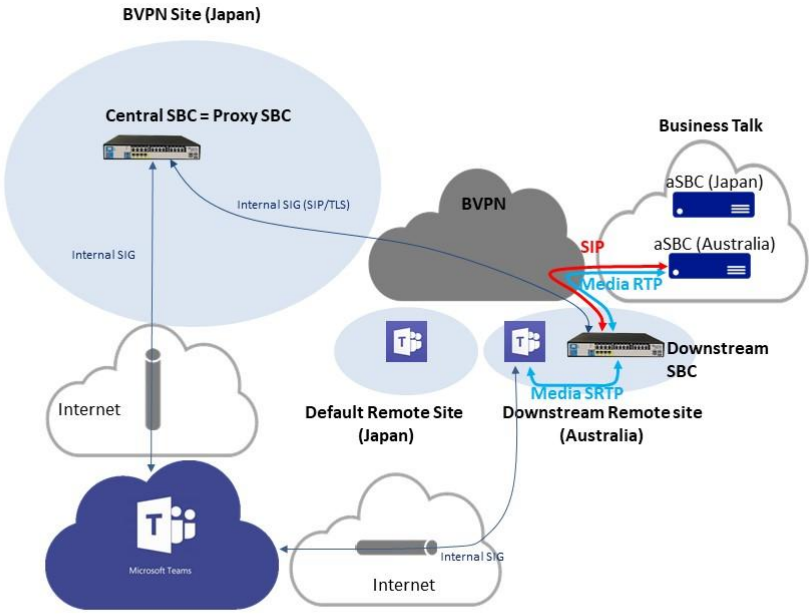
With Local Media Optimization configured, offnet media flow remains on BVPN or LAN for internal Teams users. It aims at using a shorter path to the BT/BTIP SIP trunk and better voice quality than Internet quality. It also saves Internet bandwidth. With “Europe” model, media flows are anchored to the 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

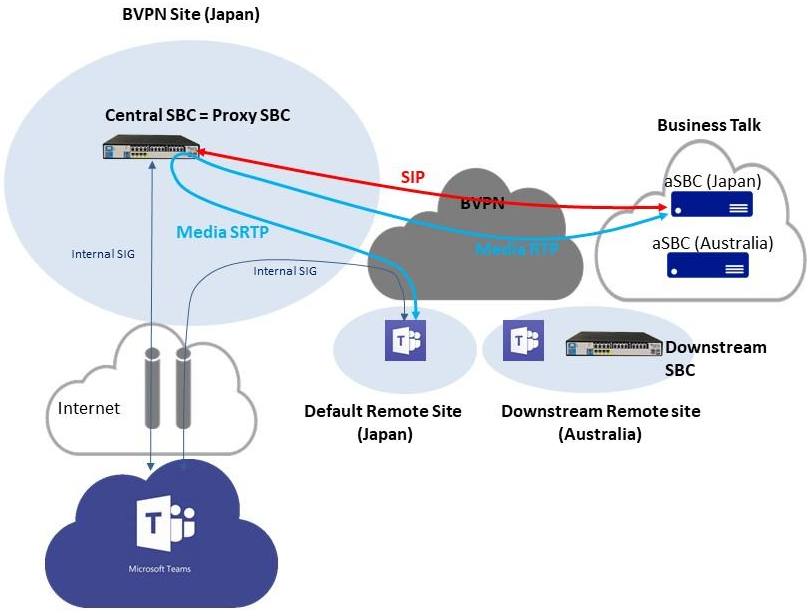


Orange Restricted

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.

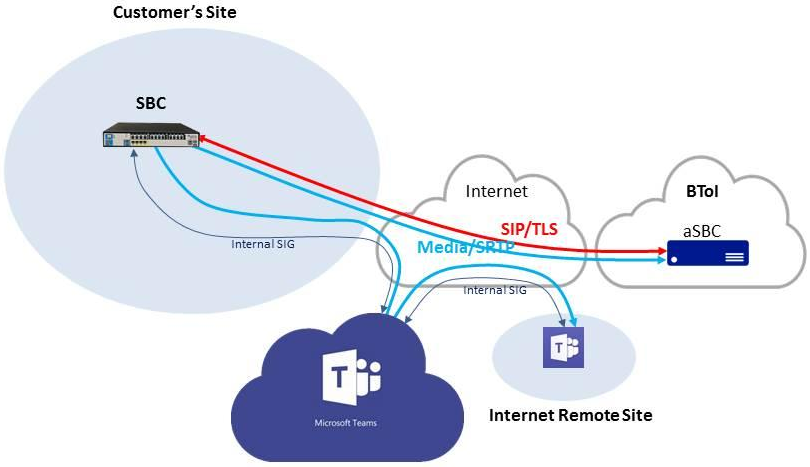
Example 5b – offnet call from a BVPN central site with Local Media Optimization Asia model



Orange Restricted

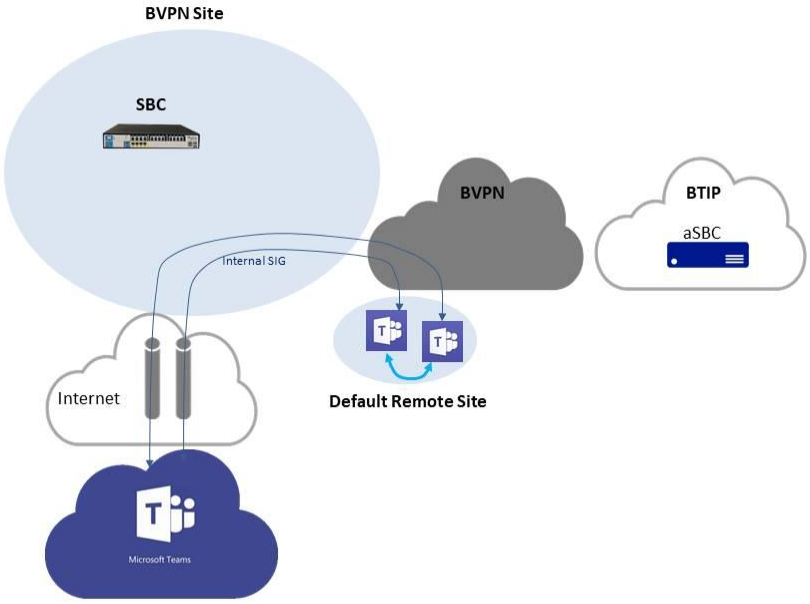
This example is linked to example 5a and shows that a user in Japan uses the central SBC that is trunked to the Japanese aSBC of Business Talk. This is like Local Media Optimization Europ model.

Example 6 – offnet call from an Internet remote site with BToI (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



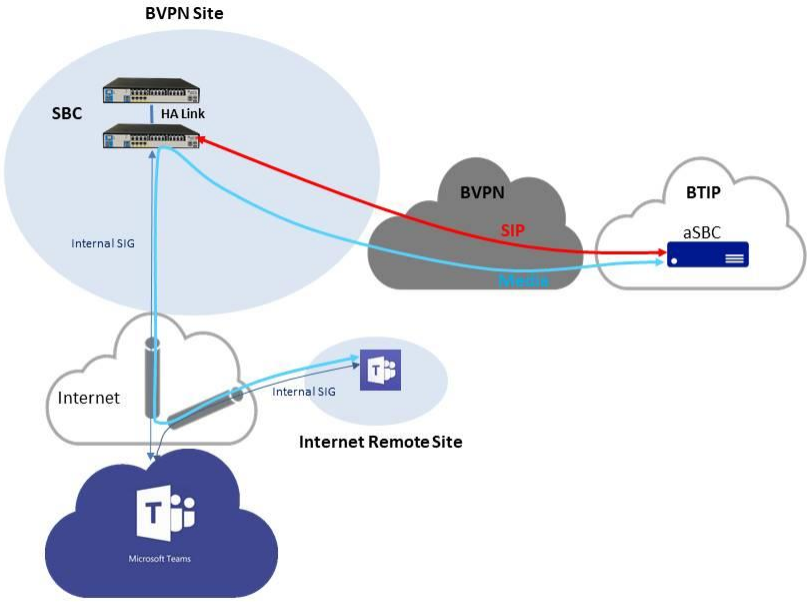
In a BVPN architecture, media flows between Teams users belonging to a single BVPN are direct, whether they are on the same site or in distinct sites.

1.5 High Availability mode

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

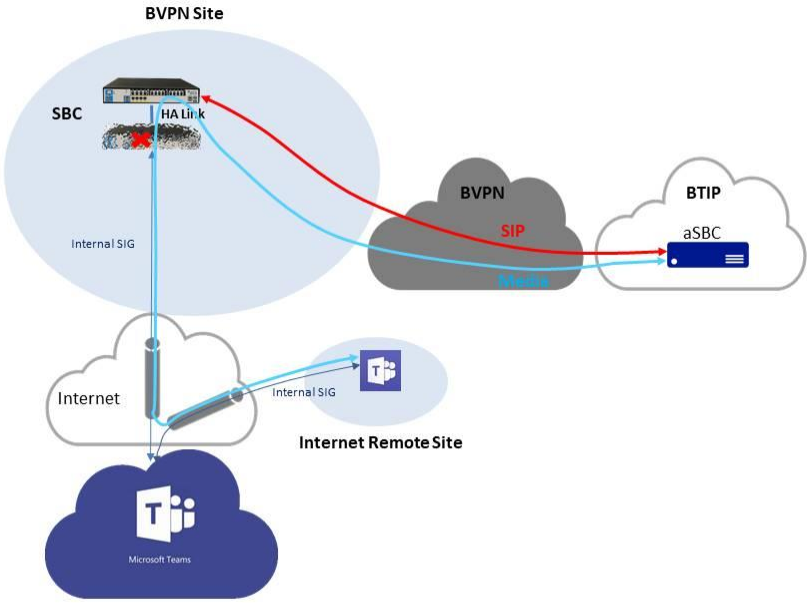
From BTIP/BTalk perspective, this is like a single SBC.

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



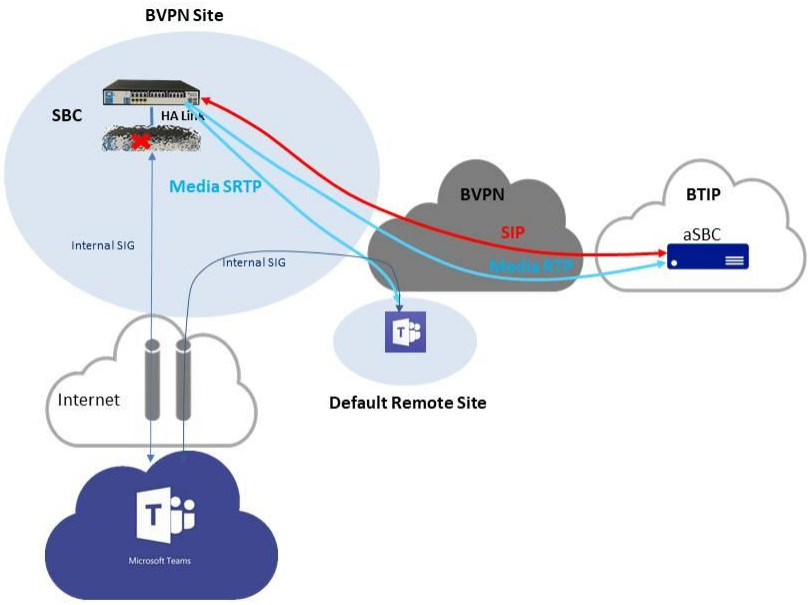
HA is fully managed by SBC themselves. From Teams and BTIP/BTalk points of view, the architecture behaves as if there was a single SBC.

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.

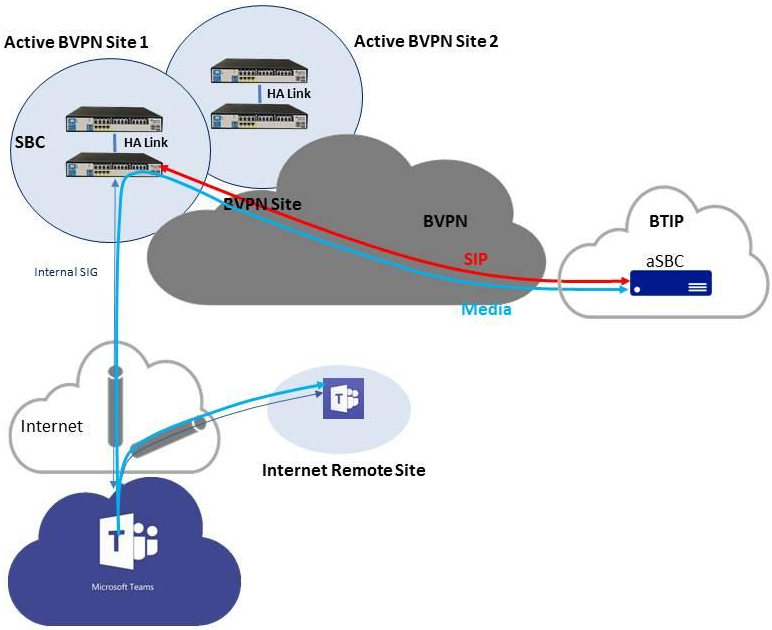
Example 3 – same as example 2 with a BVPN Teams user and Local Media Optimization "Europe" model



1.6 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.

1.7 BTIP in DROM (French Overseas Territories)

1.7.1 Definition

BTIP DROM is part of the french offer dedicated to multi-site companies with some locations in French Overseas departments (aka “DROM”).

- IPBX located in continental France or in DROM
- Users located in continental France and in DROM

BTIP in DROM offer aims at keeping the media flows locally, typically for French customers with a central site in Continental France et other sites in DROM such as Caribbean or Indian Ocean. As a cloud service, Teams has no real location, but Direct Routing SBC may have a location. Flows may become more complex than with a regular IPBX and the way to optimizing them may sound sometimes not natural. For instance, as shown below, it is better not to have multiple trunks in case of a single Direct Routing SBC.

1.7.2 Choice of outbound trunk

In BTIP DROM, outbound trunk must depend on the calling site. A call initiated in a Guadeloupean site must be routed to the Caribbean aSBC. Local aSBC have been installed in following regions:

- Caribbean area: for sites of Martinique (+596), Guadeloupe, Saint Barthelemy, Saint Martin (+590), Guyane (+594)
- Réunion: for sites of La Réunion or Mayotte (+262)

SIP trunks must not be used when users call each other with their DID. The call must be considered as local. This is Teams standard behavior.

With Teams, this outbound constraint, and thus the use of BTIP DROM, may not be relevant in some architectures. For instance, as shown below, it is better not to have multiple trunks in case of a single Direct Routing SBC.

1.7.3 « To » header: supported formats for outbound calls to PSTN

Domestic number

- E164 format is preferred: +Country code followed by phone number without “0” prefix
  Ex : +590 590 88 67 21, +262 262 25 79 02 ou +33 1 25 58 58 58
- Authorized: 0ZABPQMCDU ou 0262PQMCDU for DROM (ex: La Réunion)
  Ex: 0 590 88 67 21, 0 262 25 79 02 ou 02 56 48 58 58
- Tolerated : +33 262PQMCDU for (ex: La Réunion)
  Ex : +33 590 88 67 21 (La Guadeloupe) or +33 262 25 79 02

International number

- E164 : +CC NSN
  Ex : +48 504135755

Short number

- +33 followed by short number (preferred) or short number
  Ex : +33 3000 ou 3000

Emergency number

- +33 followed by emergency number (preferred) or emergency number
  Ex : +33112 ou 112

1.7.4 « From » header: supported formats supportés for outgoing calls to PSTN

- E164 format is preferred: +Country code followed by phpone number without “0” prefix
  Ex : +33 3 68 45 57 56, +262 262 69 97 03 or +590 590 68 22 41

- Authorized: 0ZABPQMCDU or 0262PQMCDU for DROM (ex: La Réunion)
  Ex: 03 68 45 57 56, 0 262 69 97 03 ou 0 590 68 22 41

- Tolerated: +33 262PQMCDU forDROM (ex: La Réunion)
  Ex : +33 262 69 97 03 or +33 590 68 22 41 (La Guadeloupe)

1.7.5 Comparison of architectures with or without BTIP DROM

This chapter describes some possible architectures with Teams Direct Routing and the impact on voice quality for companies with sites in continental France and in DROM.

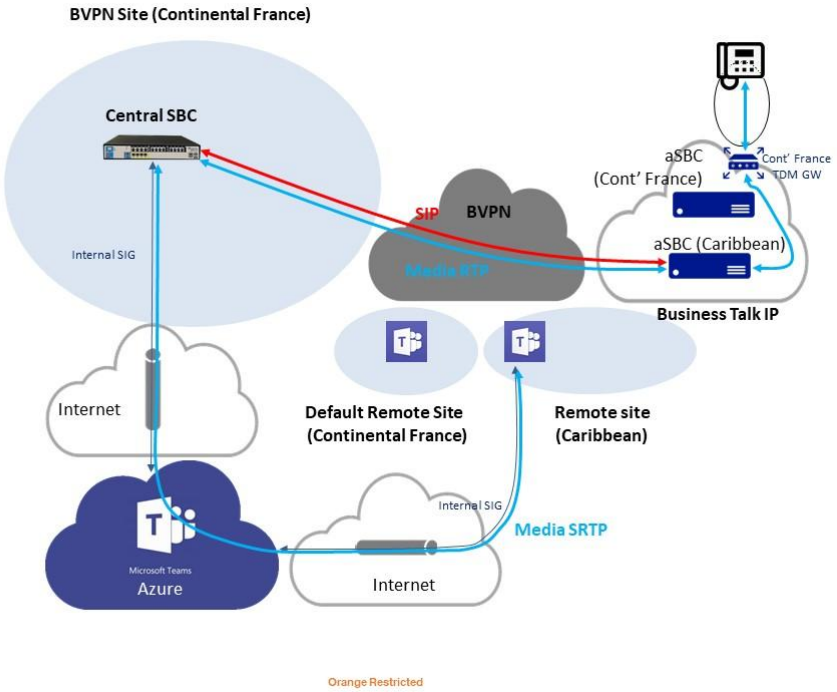
<table>
<tr><th></th><th>noMBP</th><th>MBP</th><th>LMOE</th><th>LMOA</th></tr>
<tr><td>Two trunks on central DR SBC, one with aSBC in Continental France and one with aSBC in DROM (1.7.6)</td><td colspan="3">Not recommended</td><td>N/A</td></tr>
<tr><td rowspan="2">Single trunk on central DR SBC with aSBC in Continental France (1.7.7)</td><td>OK for administrative telephony</td><td>Not recommended</td><td>OK for administrative telephony</td><td rowspan="2">N/A</td></tr>
<tr><td colspan="3">This is standard BTIP and not BTIP DROM architecture</td></tr>
<tr><td>One trunk per plate and one DR SBC per plate (1.7.8)</td><td colspan="3">OK</td><td>N/A</td></tr>
<tr><td>One trunk per plate and LMO “Asia” with one downstream SBC per plate (1.7.9)</td><td colspan="3">N/A</td><td>OK</td></tr>
</table>

1.7.6 Two trunks on central DR SBC, one with aSBC in Continental France and one with aSBC in DROM

The aim of this architecture would be to take advantage of the DROM aSBC for local users. However, it is **not recommended** as shown in the following example, an offnet call between a Caribbean user and an offnet customer located in Continental France. In this case, 3 long legs are involved, leading to a possible bad voice quality:

- leg between Caribbean user and DR SBC located in Continental France,
- leg between DR SBC and DROM aSBC located in the Caribbean,

- leg between DROM aSBC in the Caribbean and TDM Gateway located in Continental France.



Note that the issue would be the same if Local Media Optimization "Europe" model would be enabled. The only difference would be the path of the first leg, remaining in BVPN instead of Internet and Azure, but still crossing the Atlantic Ocean.

1.7.7 Single trunk on central DR SBC with aSBC in Continental France

➢ Without Media ByPass

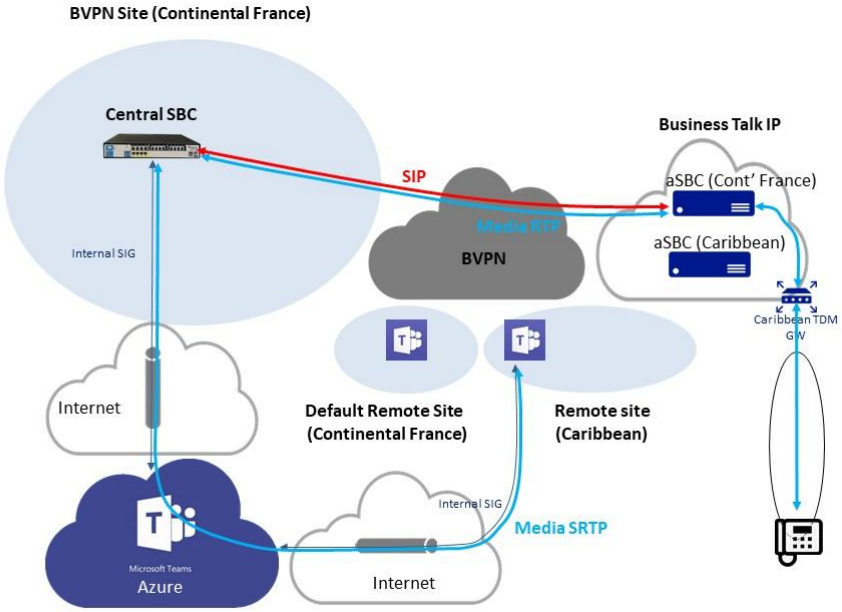
This architecture is valid for administrative telephony, though advantage is not taken of the DROM aSBC. No Local Media Optimization is enabled in Microsoft Teams Direct Routing. The worst case would be considering an offnet call between a Caribbean user and a local customer. 2 long legs are involved:

- between Caribbean user and DR SBC located in Continental France, through Internet and Azure (assuming Media Bypass is not enabled),
- between BTIP aSBC in Continental France and Caribbean TDM Gateway, through BVPN.

The highest measured Round-Trip Delay (RTD) in BVPN between Continental France and DROM leads to a MOS > 4 (few users dissatisfied). It concerns the Indian Ocean and is lower for the Caribbean.

However, here, half on the flow only is on BVPN. The other part uses Internet and Azure. Microsoft networking ensures that most part of the leg stays in Azure network, which implements Quality of Service, and a little is over the Internet. That may be enough for administrative telephony.

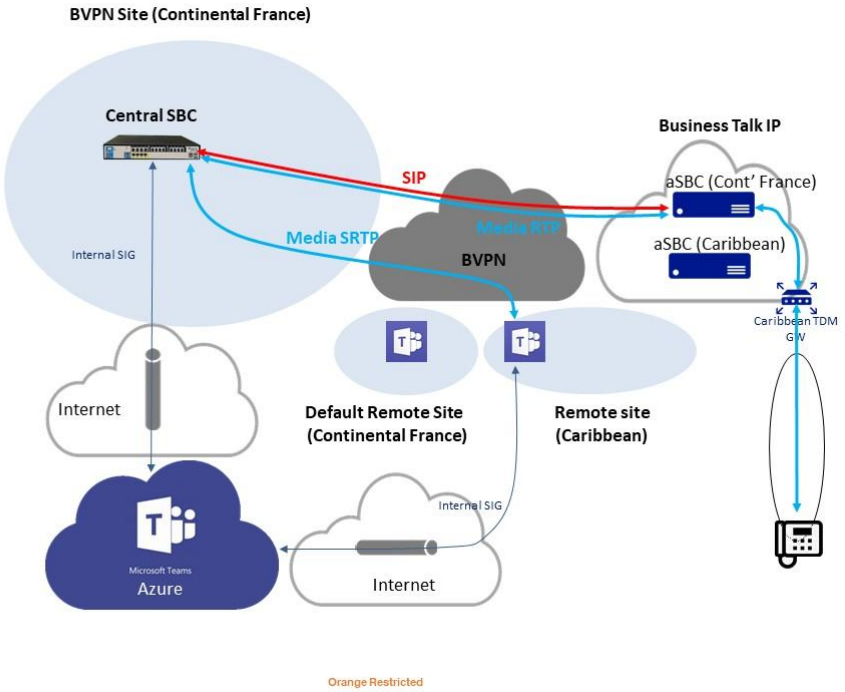
With Media Bypass, the part of the Internet may be higher. This is why it is less recommended.



Orange Restricted

➢ **with Local Media Optimization "Europe"**

With LMO "Europe", there is no leg on Internet + Azure and only the Round-Trip Delay on BVPN is relevant. That may be enough for administrative telephony as well.



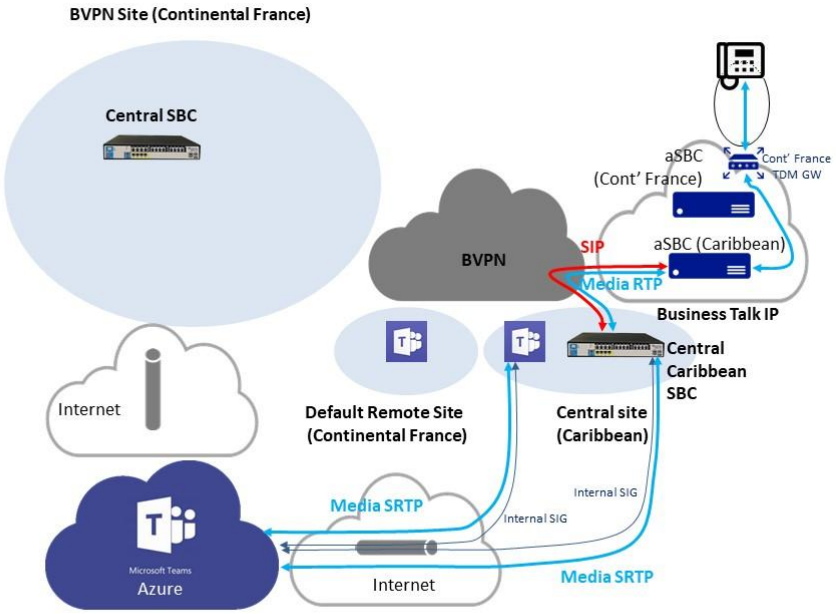
Orange Restricted

1.7.8 One trunk per plate and one DR SBC per plate

➢ **Without Media ByPass**

This architecture is basically deploying two Direct Routing SBC on the same tenant, each one owning its BTIP trunk, here without Media Bypass. Offnet calls are routed locally.

Worst case would be calls between a Caribbean user and a Continental French customer (or reversely), that cross the Atlantic Ocean only once through BVPN between Caribbean aSBC and Continental French TDM Gateway. This architecture is recommended for good voice quality.

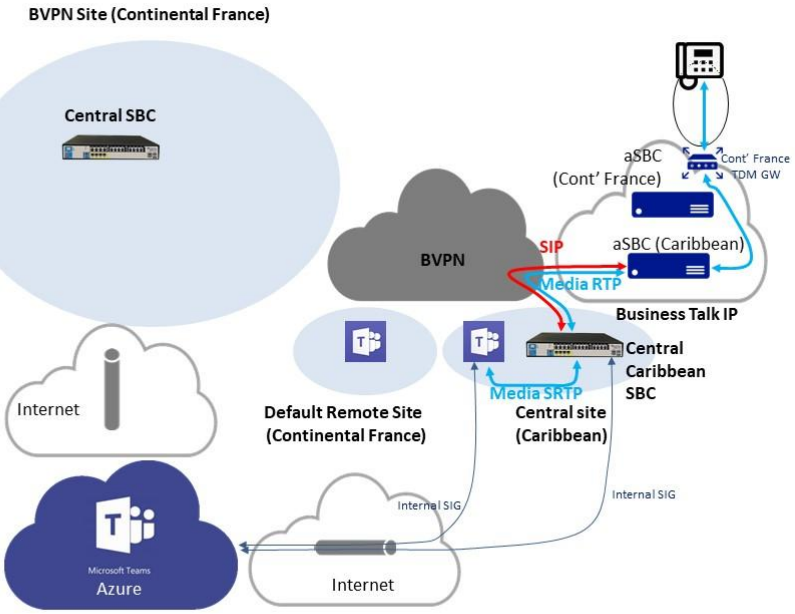


Orange Restricted

➢ With Local Media Optimization "Europe"

This architecture is a variant of above. It is basically deploying two Direct Routing SBC on the same tenant, each one owning its BTIP trunk, with Local Media Optimization "Europe" model enabled. Offnet calls are fully routed locally.

Worst case would be calls between a Caribbean user and a Continental French customer (or reversely), that cross the Atlantic Ocean only once through BVPN between Caribbean aSBC and Continental French TDM Gateway. This architecture is fully recommended for good voice quality.

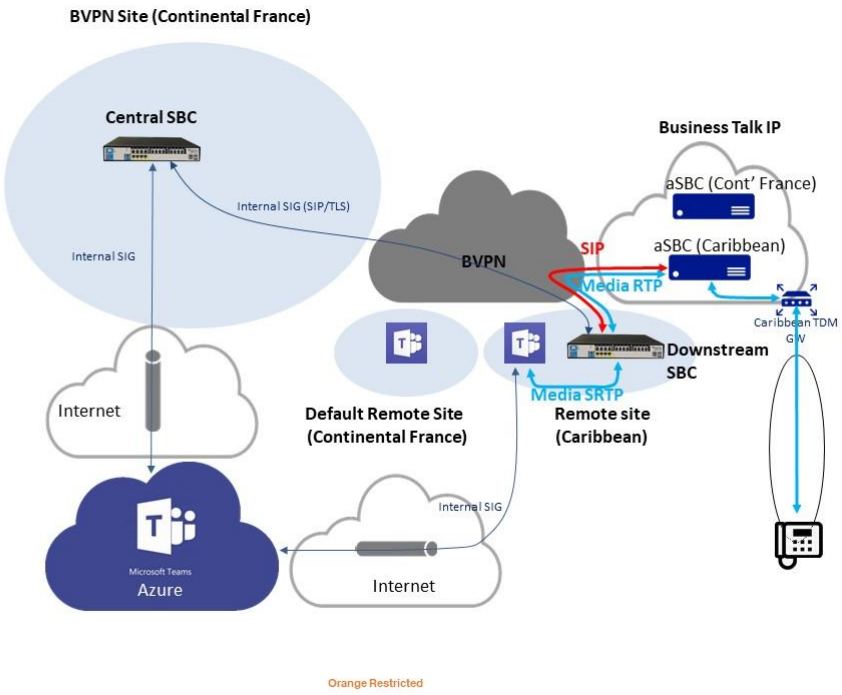


Orange Restricted

1.7.9 One trunk per plate and LMO “Asia” with one downstream SBC per plate

The architecture depicted here uses Local Media Optimization “Asia” model already described at 1.4. The main difference with above is that the Downstream SBC has no trunk with Teams, but only with the Central SBC and therefore does not need to be open on the Internet.

This is also a recommended architecture for BTIP DROM.



1.7.10 Operator Connect

TBD

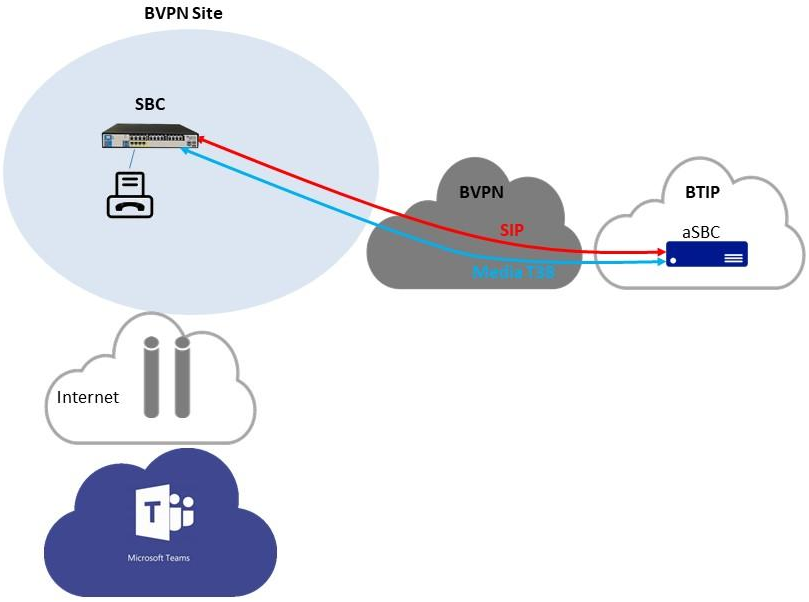
1.8 Analog devices

1.8.1 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.

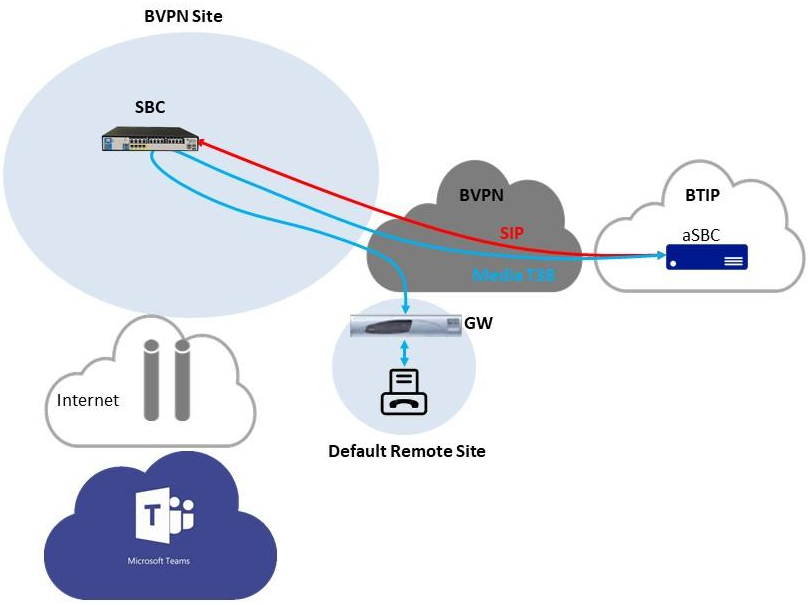
FAX calls to and from Business Talk consumes the same SIP Trunk that is used for interconnection with Teams. When a call is made from FAX or to FAX, the Direct Routing SBC bypasses Teams, which does not talk T.38, for signaling as well as for media

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



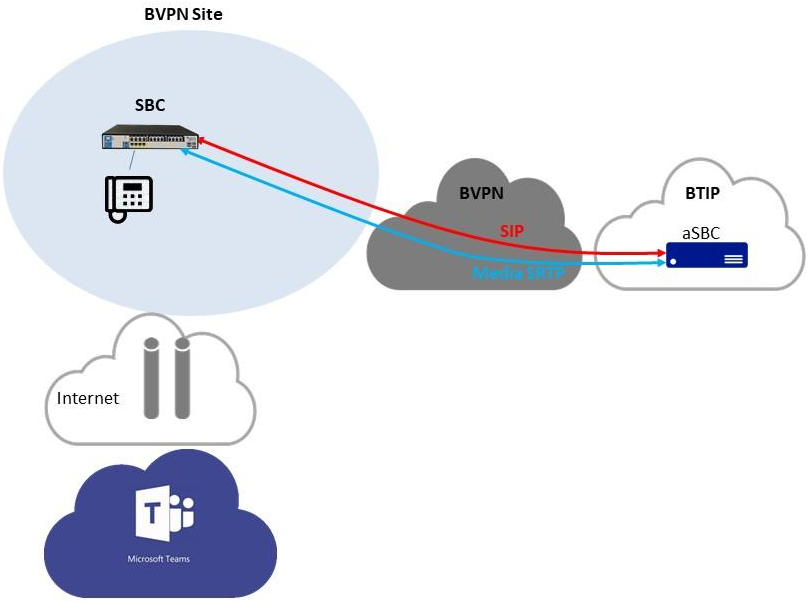
In this architecture FAX device is connected to an analog telephony adapter. It is integrated with DR SBC which can be placed in other remote site or in datacenter. DR SBC with no directly connected endpoints can be virtualized.

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.

1.8.2 Analog phones

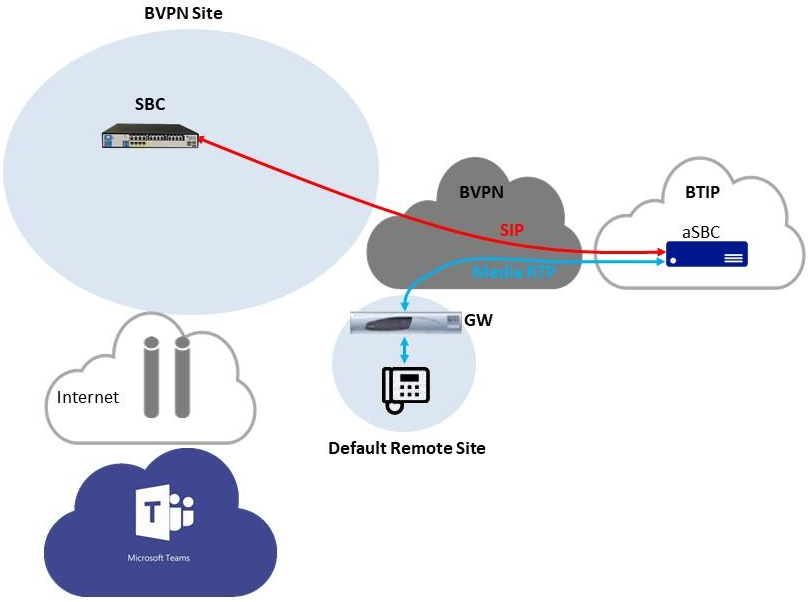
Analog phones on Direct Routing SBC with or without Gateway is certified both on French (BTIP) and International (BTalk) scopes, so far with AudioCodes only as central SBC and remote GW (MPxxx or Mediant).

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.

1.9 Reminder on emergency calls

(Extract of Access SIP profile for connecting PBX to BTIP/BT SIP or FIAs2 services V3.5)

PBX may send a PIDF-LO body for providing geographical information BUT this information must be fulfilled with great care because, if provided, this will be used in case of Emergency call for locating caller. OBS is not responsible for the relevance of the provided information or its format.

Generally, PIDF-LO must not be used on BTIP (French trunk offer). In any case, please contact OBS before using this PIDF-LO body.

1.10 Sizing considerations

1.10.1 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 offnet call may be considered to consume at most 100 kbps throughout its path.

1.10.2 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.

1.10.3 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						
Client served by central SBC						
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	
Client served by downstream SBC						
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						
Without Local Media Optimization Asia						
(device served by central SBC)						
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	
With Local Media Optimization Asia						
(device served by downstream SBC)						
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.	<u>BTIP/BTalk:</u> 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 <= 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.	BTIP/BTalk: 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 <= 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@ BTol: SBC pair1 public floating IP@ or FQDN DNS Type A SBC pair2 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
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@ BTol: SBC1 public IP@ or FQDN DNS Type A SBC2 public IP@ or FQDN DNS Type A BTIPol: 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@ BTol: 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 downstrealm 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 <= 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@ BTol: 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 BTIPol: 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@ BTol: Downstream SBC1 public IP@ or FQDN DNS Type A Downstream SBC2 public IP@ or FQDN DNS Type A BTIPol: 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@ BTol: Downstream SBC pair1 public IP@ or FQDN DNS Type A

		Downstream SBC pair2 public IP@ or FQDN DNS Type A BTIPoI: 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 be taken in this document.
- **[Optional] HA interface:** 1 IP address (non-routed)

For Business Talk over Internet (BToI), or BTIPoI :

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

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

2.3 ACL for BToI/BTIPoI

The WAN or public IP interface is usually exposed to the public Internet through a DMZ, so it is strongly recommended to use an Access Control List for protecting access.

For instance, as a prerequisite, Ribbon recommends reading the SBC Edge Security Hardening Checklist to understand how to secure the SBC into your network infrastructure.

2.4 TLS integration for BTol/BTIPol

In case of encrypted SIP trunk architecture, TLS configuration is mandatory to exchange a certificate with Orange BT/BTIP A-SBC. Orange's TLS implementation operates in "Mutual Authentication" mode (also known as "two-way" authentication).

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

The encrypted architecture requires the usage of an encryption Key and Ciphers present in a TLS Context in order. A specific Orange BTALK TLS Context have to created.

This SIP signaling will be configured to be compliant with Orange BTalk specification:

- ✓ For **encrypted BTALK SIP Trunk** architecture we need to configure **TLS V1.3** or most possibly supported **TLS V1.2**
- ✓ **Key size 2048 (Minimum)**
- ✓ **Cipher list per below is recommended as Cipher Client/Server through TLS V1.3:**
  - **TLS_AES_256_GCM_SHA384 (Recommended)**
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
- ✓ **Cipher list per below is compatible as Cipher Client/Server through TLS V1.2:**
  - **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Compatible)**
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- ✓ **TLS Mutual authentication activated.**

Orange BTIP/BTalk over Internet Public certificate- Extended Key Usages (EKU) within only "Server Authentication" role must be accepted regarding overall public CA's removal of "Client Authentication Role" explained in **Chapter TLS Mutual Authentication Mechanism support regarding public certificate Extended Key Usage (EKU) change**

3 BTIP/BTalk/BTol/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	BTol	BTIPol(1)	Codec	MBP(2)	LMO(3)	AP(4)	FAX
Audio-Codes	M500/800/1000/ 2600/4000/9000 & VE	v.7.40A, build 502.278+ v.7.40A, build 605.092+	√	√	√	√	G.722 G.711 G.729	√	√ Europe Asia	√	√
Ribbon	Edge 1000/2000 & SweLite	12.3 build 40 +	√	√	√	√	G.711 Other plan-ned	√	√ Europe	Plan -ned	√
Oracle	Acme Packet 1100/3900/4600 /6300/6350 & VME	S-Cz9.3.0 p8	√	√	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/BToI, 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/BTalk/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 6000-20000	Media outgoing
BToI	BToI public @IP	UDP 6000-20000	**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 TLS Mutual Authentication Mechanism support regarding public certificate Extended Key Usage (EKU) change

Since mid-2026 public Certificate Authorities (CA's) have progressively issued TLS certificates with the **Server Authentication Extended Key Usage only (EKU),** removing Client Authentication EKU by default, in all end-entity public certificate.

This change follows the **Google Chrome Root Program requirement** (decision made in last October 2024) that publicly **trusted TLS x.509 certificates must no longer support both Server Authentication and Client Authentication purposes, leaving only Server Authentication EKU in.**

Some CAs, such as DigiCert, offer a **grace period** during which End- Entity certificates with both Server Authentication and Client Authentication EKUs can still be requested.

By default, DigiCert issues certificates with Server Authentication EKU only. This dual-EKU option is available on request until 1 March 2027. After that date, only Server Authentication EKU will be included.

Source: https://knowledge.digicert.com/alerts/sunsetting-client-authentication-eku-from-digicert-public-tls-certificates

Please check your CA provider current policy:

1. Grace period available: dual-EKU certificates remain supported for a limited period of time
2. No grace period: both the Orange aSBC and the customer eSBC/IPBX are oblige using Server Authentication EKU–only in their respective End- Entity certificates.

In the 2nd scenario, where both endpoints use public certificates with the Server Authentication EKU only, Orange validates mutual TLS interoperability through testing.

The impact on mutual authentication may depend on:

- which endpoint acts as the TLS client or TLS server.
- and the vendor capabilities for handling certificates without the Client Authentication EKU

➢ Case 1: Audiocodes eSBC initiates the TLS handshake :

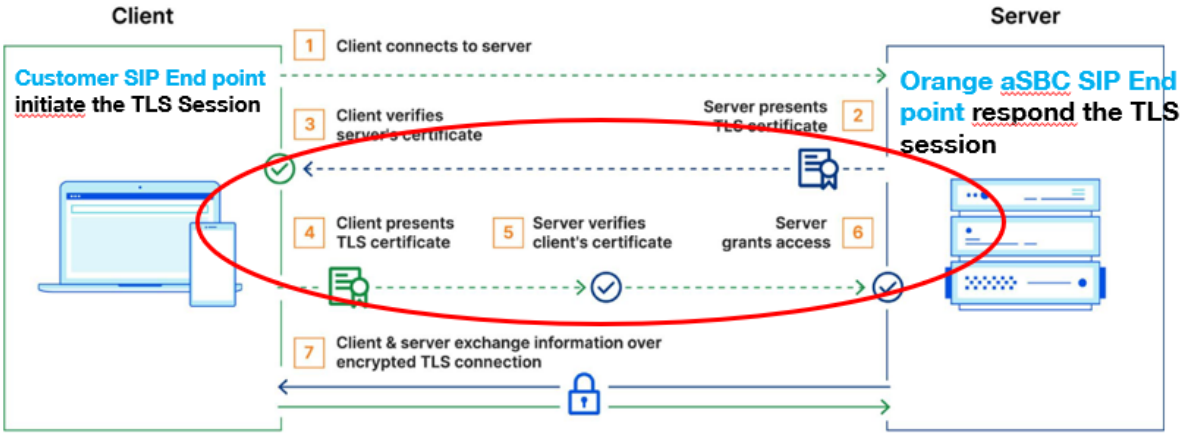
In this scenario:

- The Audiocodes eSBC acts as the TLS client.
- The Orange aSBC acts as the TLS server.
- The Audiocodes eSBC initiates the TLS handshake.

The Orange aSBC requests a certificate from the Audiocodes eSBC in order to perform mutual TLS authentication.

TLS handshake sequence

1. The Orange aSBC requests the customer certificate (TLS message “Certificate request”)
2. The Audiocodes eSBC presents its certificate with Server Authentication (serverAuth) EKU only [4].
3. The Orange aSBC verifies the certificate [5] and grants access [6].



Result: Mutual TLS continues to work when the Audiocodes eSBC initiates the connection, even if the customer public certificate contains the serverAuth EKU only.
No specific Audiocodes configuration change is required for this scenario.

➢ Case 2: mTLS supported by Audiocodes eSBC without considering missing Client Auth EKU in Orange SBC public certificate.

In this scenario:

- The Orange aSBC acts as the TLS client.
- The Audiocodes eSBC acts as the TLS server.
- The Orange aSBC initiates the TLS handshake.

The Audiocodes eSBC requests a certificate from Orange in order to perform mutual TLS authentication. Orange presents its public certificate containing the serverAuth EKU only.

Default behavior — TLS handshake failure

By default, the Audiocodes eSBC requires a certificate presented by a TLS client to include the clientAuth EKU. It therefore rejects the Orange certificate.

As a result, mutual TLS authentication fails, and the TLS handshake cannot be completed.

Configuration required to restore mutual TLS

Starting from **Audiocodes eSBC version 7.40A.600.627 LTS**, Audiocodes provides the parameter:

"Allow Client Auth Key Usage"

To allow Orange certificates containing serverAuth EKU only, the customer must set this parameter to:

"Always"

With this setting, the Audiocodes eSBC accepts the Orange certificate even when the clientAuth EKU is not present. More details from Audiocodes official release notes (extract per below)

2.2.3.1.15Configurable TLS Client Certificate clientAuth EKU Validation

In X.509 TLS certificates, the clientAuth value is specified in the Extended Key Usage (EKU) field and indicates that the certificate can be used by a client to authenticate itself to a server:

```
Extended Key Usage:
  - TLS Web Client Authentication (clientAuth)
```

However, Public Certificate Authorities (CAs) like DigiCert and GlobalSign are phasing out support for issuing TLS certificates with the clientAuth EKU. CAs will issue TLS certificates with only the serverAuth EKU.

Up until now, the device rejected TLS certificates received from clients for client authentication that included the EKU extension but without the clientAuth value (serverAuth etc.).

To address this industry change and improve interoperability, the device now supports configurable behavior for validating the EKU field of client certificates during TLS handshake. A new parameter has been added to the TLS Contexts table:

- **Web Interface:** 'Allow Client Auth Key Usage'
- **Ini:** [AllowClientAuthKeyUsage]
- **CLI:** `client-auth-key-usage-mode`

The parameter can be configured to:

- **Always** – The device accepts client certificates regardless of the clientAuth EKU.
- **According to EKU extension rules** (default) – The device accepts client certificates only if they include the clientAuth EKU.

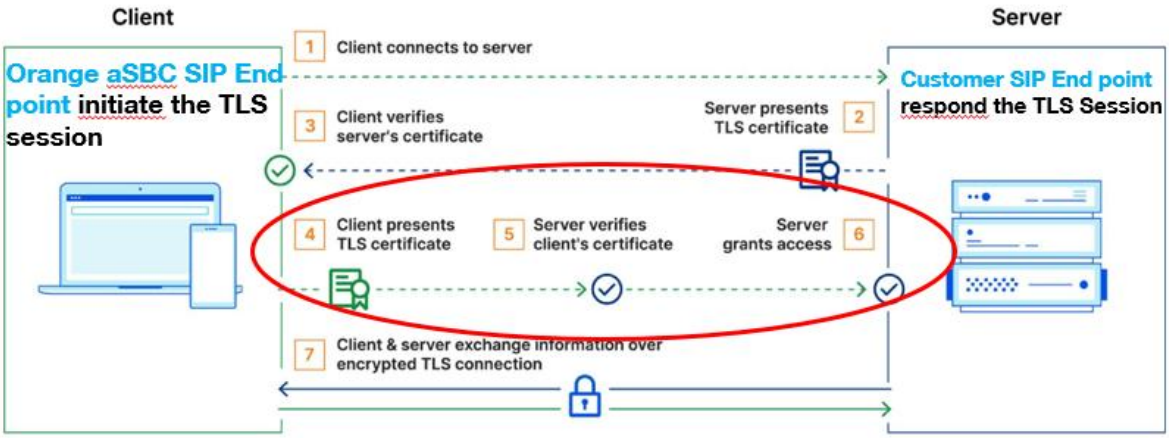
Applicable Application: All

Applicable Products: All

'Allow Client Auth Key Usage' `client-auth-key-usage-mode` [AllowClientAuthKeyUsage]	Defines whether the device accepts or rejects client TLS certificates based on the presence of the 'clientAuth' value in the Extended Key Usage (EKU) field. ■ [0] **Always** = The device accepts client certificates regardless of whether the clientAuth EKU is present or not. ■ [1] **According to EKU extension rules** = (Default) The device accepts client certificates only if they include the clientAuth EKU (and rejects certificates that lack the value). **Note:** Certificate Authorities (CAs) such as DigiCert and GlobalSign are gradually discontinuing the issuance of TLS certificates that include the clientAuth EKU.

TLS handshake sequence after the configuration change

1. The Audiocodes eSBC requests the Orange aSBC certificate.
2. The Orange aSBC presents its certificate with Server Authentication (serverAuth) EKU only **[4]**.
3. **The Audiocodes eSBC verifies the certificate, accept it regardless of whether the Client Authentication (clientAuth) EKU is not present [5]** and grants access **[6]**.



Security consideration: Please note this specific Audiocodes eSBC configuration option reduce customer security concern with Orange: End customer Audiocodes eSBC security heavily change by accepting Orange aSBC certificate without taking into considerations Orange public certificates EKU's in and must accept by End Customer.

Please go to section 4.8 TLS Context for Orange TLS context configuration details.

4.4 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	***$true***
ForwardCallHistory	***$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 MO 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

4.5 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*

4.6 Parameter not available via the web admin page

Some parameters cannot be set via the Web Admin and must be configured via CLI or directly edited in the .INI file:

Parameter: sbc-100trying-upon-reinvite

Enables the device to send a SIP 100 Trying response upon receipt of a reINVITE request. BusinessTalk infrastructure must receive a response within the next 200ms following any INVITE/reINVITE. By default, the Audiocodes SBC does not generates 100 TRYING when receiving a reINVITE, enabling the parameter will force the SBC to generate it.

Via CLI: configure voip > sbc settings > sbc-100trying-upon-reinvite on

Via .ini file: inside the [SIP Params] section add the following line:

SBC100TRYINGUPONREINVITE = 1

4.7 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 be 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)

4.8 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

4.8.1 *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 BToI/BTIPoI (**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 BToI/BTIPoI : ✓ EthD_Teams (shared with BToI): 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 BToI/BTIPoI) ✓ 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 BToI / BTIPoI: ✓ 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 BToI / BTIPoI: General recommendation is not to use NAT translation for BToI/BTIPoI. The SBC IP interface dedicated to Teams and BToI/BTIPoI 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 - Name: **Teams-TLSContext** - TLS Version: **TLSv1.2** - DTLS Version: **DTLSv1.2** - DH Key Size: **2048**
For BToI/BTIPoI)	Create new TLS context for BTOI traffic: - Name: BTOI-TLSContext

	- TLS Version: TLSv1.2 and TLSv1.3 - DTLS Version: DTLSv1.2 - Cipher Server: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - Cipher Client: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - Cipher Server TLS1.3: TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256 - Cipher Client TLS1.3: TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256 - 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: **<BTOl / BTIPol public IP>** - Source IP: **<BTOl / 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**

4.8.2 *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: **Only If Required** - Remote Early Media RTP Detection Mode: **By Media** - Allowed Audio Coder: **Teams_AudioCoders** - Allowed Coders mode: **Restriction and Preference** - RTCP Mode: **Generate Always** - RFC 2833 Mode: **Extend** - 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 Replaces Mode : **Handle Localy** - 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** - UDP 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_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})(.*)(101\r\n.*)** - 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)(.*)(18)(.*)(a=maxptime:200)(.*)** - 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** - Media TLS 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") If LMO (Europe Scenario): - Internal Media Realm: BTIP-Media - Teams Media Optimization handling: Teams Decides - Teams Media Optimization Initial 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**

4.8.3 *Step 3 – Business Talk configuration*

Allowed Audio Coder Groups	
SETUP > Signaling&Media > Coders & Profiles > Allowed Audio Coders Groups	If BT: 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** If BTIP: 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** If BTol/BTIPol: 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 If BT: - Name: **BTIP-IPProfile** - SBC Media Security Mode: **RTP** - Allowed Audio Coders: **AudioCoders_BT** If BTIP: - Name: **BTIP-IPProfile** - SBC Media Security Mode: **RTP** - Allowed Audio Coders: **AudioCoders_BTIP** If BTol: - Name: **BTol-IPProfile** - SBC Media Security Mode: **SRTP** - Allowed Audio Coders: **AudioCoders_BTol** For Both BT/BTIP and BTol: - Symmetric MKI: **Disable** - MKI Size**: 0**

	- Allowed Coders Mode: **Restriction** - RFC2833 DTMF Payload Type: **101** - RTP IP DiffServ: **46** - RTCP mode : **Generate Always** - 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 If BT/BTIP : - Name: **BTIP-Media** - Topology location: **DOWN** - IPv4 Interface Name: **IPInt_BTIP** - UDP Port Range Start**: 16400** - Number of Media Session Legs**: 1000** - Default Media Realm**: No** If BTol /BTIPol (edit Teams): - Name: **Teams-Media** - Topology location: **UP** - IPv4 Interface Name: **IPInt_Teams** - UDP 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 If BT/BTIP: - Name : **BTIP-SIPInterface** - Topology location: **DOWN** - Network Interface : **IPInt_BTIP** - TCP Port: **5060** - TLS Port: **0** - Media Realm**: BTIP-Media** If BTol / BTIPol: - 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** For Both BT/BTIP and BTol / BTIPol: - Topology Location: **DOWN** - UDP Port : **0**
Proxy Set	

SETUP > Signaling&Media > Core Entities > Proxy Set	Create new Proxy Set for Business Talk If BT/BTIP: - 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** If BTol: - 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** If BTIPol: - 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) : If BT/BTIP: 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** If BTol: 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** If BTIPol: 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	Create new message manipulation "**Add 101 to ACK SDP"** - Name: **Add 101 to ACK SDP** - Manipulation Set ID**: 4** - Row Role**: Use Current Condition** - Match> Message Type**: Ack** - Match> Condition**: Body.sdp !contains 'a=rtpmap:101 telephone-event/8000'** - Action> Action Subject**: Body.sdp** - Action> Action Type**: Add** - Action> Action Value**: 'a=rtpmap:101 telephone-event/8000\\a=fmtp:101 0-15'**
SETUP > Signaling&Media > Message Manipulations	For BTol/BTIPol only (not applicable to BTIP): 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	For BTol/BTIPol only (not applicable to BTIP): 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	For BTol/BTIPol only (not applicable to BTIP): 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	For BTol/BTIPol only (not applicable to BTIP): 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	For BTol/BTIPol only (not applicable to BTIP): 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.User** - Action> Action Type**: Modify** - Action> Action Value**: Header.Referred-By.URL.User**
SETUP > Signaling&Media > Message Manipulations	For BTol/BTIPol only (not applicable to BTIP): 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 If BT/BTIP: - Name : **BTIP-IPGroup** - Proxy Set**: BTIP-Proxies** - IP Profile**: BTIP-IPProfile** - Media Realm**: BTIP-Media** - Media TLS Context**: <empty>** If BTol / BTIPol: - Name : **BTol-IPGroup** - Proxy Set**: BTol-Proxies** - IP Profile**: BTol-IPProfile** - Media Realm**: Teams-Media** - Media TLS Context**: Teams-TLSContext** For Both BT/BTIP and BTol: - Topology Location**: DOWN** - Outbound Message Manipulation Set: **3** (Manipulation set id including manipulations "User-Agent_Modification") - Inbound Message Manipulation Set: 4

4.8.4 *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 BToI/BTIPoI) **to Teams** - Match > Source IP Group: **BTIP-IPGroup** (or BToI-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 BToI/BTIPoI) - Match > Source IP Group: **Teams-IPGroup** - Match > ReRoute IP Group: **Any** - Action > Destination IP Group: **BTIP-IPGroup** (or BToI-IPGroup)

4.8.5 *Step 5 – Pre-Recorded-Tones*

Auxiliary Files	
On the Mediant WebUi Interface: SETUP>ADMINISTRATION>MAINTENANCE>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)

4.9 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

4.9.1 *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)

4.9.2 *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)

4.9.3 *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

4.10 . Configuration checklist for Mediant SBC – LMO Asia

4.10.1 Configuration for Proxy SBC

- Office365 Tenant

Tenant configuration for Proxy SBC remain the same as the one described 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 - 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** - Media TLS 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: **Only If Required** - 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: **Only If Required** - 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** - UDP 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**

4.10.2 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

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**

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/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
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**

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** - UDP 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** - Media TLS 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**

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'**

Step 4 - Routing configuration	
IP to IP Routing	
On the Mediant WebUi Interface:	Create 3 IP to IP routing rules:

SETUP > Signaling&Media > SBC > Routing > IP-to-IP Routing	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**

4.11 AudioCodes Analog Phones configuration checklist

4.11.1 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 - 1st Coder Name: **G.711A-law** - Packetization Time: **20** - Rate: **64** - Payload Type: **8** - Silence Suppression: **Disabled** - 2nd 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 - 1st coder name: **G.711A-law** - Packetization Time: **20** - Rate: **64** - Payload Type: **8** - Silence Suppression: **Disabled** - 2nd 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: **TelP_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**

4.11.2 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: **<xxxxxxxxx>** - Trunk Group ID: **<ID>** - Tel Profile Name: **AD-TelProfile**

4.11.3 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.

4.11.4 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.**

4.12 AudioCodes FAX configuration checklist

✓ *FAX support:*

- **G.711 Inband Fax**
  - For G.711 inband fax transmission, customers may implement any inband fax configuration, including, but not limited to, autonomous mode, passthrough mode, and voice mode. V.152 is explicitly excluded and is not supported.
  - Customers are solely responsible for configuring their own fax equipment. Orange does not recommend any specific G.711 inband fax configuration, as fax transmission performance may depend on the behavior of fax gateways and on any transcoding operations performed within the core network.
  - Consequently, Orange does not provide technical support for issues related to G.711 inband fax transmission.
- **T.38 fax transport mode**
  - SIP endpoint SHALL support "image t38" as SDP media description information.
  - If the call is established with a codec different from T38, when the FAX is detected, a media session modification MUST be operated as described below.

Main T.38 configuration in following chapters

4.12.1 FXS fax on Mediant configuration

➢ Telephony profile

The FXS ports with fax devices connected require 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_FXSFAX	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_FXSFAX

➢ Update IP Profile

Note
Please note that there are differences for BT and BTIP configuration for this point.

Configuration for BT architecture

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
SBC FAX		
Remote Renegotiate on fax detection	**No**	Describes if the **remote rene**gotiate on fax detection
GATEWAY FAX AND MODEM		
Fax Signaling Method	**T.38 Relay**	Use T38 for fax transmission

Configuration for BTIP architecture

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**

Note
Please note that there are differences for BT and BTIP configuration for this point.

Configuration for BT architecture

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
CNG Detector Mode	**Event only**	Determines the fax CNG tone detector mode.
Fax Relay Redundancy Depth	**1**	Set pages transmission redundancy
Fax Relay Enhanced Redundancy Depth	**4**	Set fax negotiation redundancy
Fax/Modem Bypass Coder Type	**8**	Sets the **Fax/Modem** bypass coder

Go to **SETUP** > **SIGNALING & MEDIA** > **MEDIA** > **RTP/RTCP Settings** and update:

Parameter	Value	Description
Modem Bypass Payload Type	8	**Modem Bypass** (VBD) Payload type.

The next, EnableFaxModemInbandNetworkDetection 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: **EnableFaxModemInbandNetworkDetection**
Enter value: **1**

Click "Apply New Value".

If parameter is set correctly you should see output:

```
Parameter Name: ENABLEFAXMODEMINBANDNETWORKDETECTION
Parameter New Value: 1
Parameter Description: Enables or disables inband network detection related
to fax/modem.
```

Configuration for BTIP architecture

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 Mediation Server. 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	*<trunkID>*	Trunk ID for selected FXS port
Destination IP Group	*<BT IP Group>*	IP Group for Business Talk aSBC
SIP Interface	*<SIP Interface>*	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	*<SIP Interface>*	SIP Interface for Business Talk aSBC access
Destination Phone Pattern	*<FAX DID>*	Set FAX DID accessed by BT
Destination Type	Trunk Group	
Trunk Group ID	*<Trunk Group IP>*	Trunk ID for selected FXS port
Source IP Group	*<BT IP Group>*	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	*<BT IP Group>*	IP Group for Business Talk aSBC
Destination Username Pattern	*<FAX DID>*	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.
```

4.12.2 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 Mediation Server. 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 Microsoft

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/BTol/BTIPol

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

5.1 Flow matrix with BTOl

5.1.1 Flow matrix with BTol

Source	Source IP	Source port	Destination	Destination IP	Destination port	Comment
SBC	SBC public @IP	TLS 5061	**BTol**	BTol public @IP	TLS 5061	SIP Outgoing
BTol	BTol public @IP	Any	**SBC**	SBC public @IP	TLS 5061	SIP Incoming
SBC	SBC public @IP	Range defined in Media System Configuration	**BTol**	BTol public @IP	UDP 6000-20000	Media outgoing
BTol	BTol public @IP	UDP 6000-20000	**SBC**	SBC public @IP	Range defined in Media System Configuration	Media incoming

5.2 Flow matrix with BTIPol

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

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** - Verify Peer Server Certificate: **Disabled**
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/BTIPoI)** Create new Call Routing Table: - Description: **CR Teams to BTIP (or BTOI/BTIPoI)** Update CR Teams to BTIP (or BTOI/BTIPoI) - Description: **Teams to BTIP (or BTOI/BTIPoI)** - Number/Name transformation Table: **Teams to BTIP (or BTOI/BTIPoI)** - Destination Signaling Group: **SG to BT / BTIP (or BTOI/BTIPoI)** ** refer to BTIP Configuration*
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:

SIP > Message Manipulation > Message Rules Table	- Description: **Privacy Modification** - Header Action: **Modify** - Header Name: **Privacy** - Header Value – Modify: **id** (Literal) For BTIPoI only: 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** Create new Header Rule: - Description: **PAI removal** - Header Action: **Remove** - Header Name: **P-Asserted-identiry** - Header value: **SG User Value 1**
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/BTIPoI)** - SIP Profile: **SIP Profile Teams** - SIP Server Table: **SIP Server Teams** - Loadbalacing: **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: **52.112.0.0** - Netmask/prefix: **255.252.0.0** - IP/FQDN: **52.120.0.0** - Netmask/prefix: **255.252.0.0** 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 TLS Mutual Authentication Mechanism support regarding public certificate Extended Key Usage (EKU) change

Since mid-2026 public Certificate Authorities (CA's) have progressively issued TLS certificates with the **Server Authentication Extended Key Usage only (EKU),** removing Client Authentication EKU by default, in all end-entity public certificate.

This change follows the **Google Chrome Root Program requirement** (decision made in last October 2024) that publicly **trusted TLS x.509 certificates must no longer support both Server Authentication and Client Authentication purposes, leaving only Server Authentication EKU in.**

Some CAs, such as DigiCert, offer a **grace period** during which End- Entity certificates with both Server Authentication and Client Authentication EKUs can still be requested.

By default, DigiCert issues certificates with Server Authentication EKU only. This dual-EKU option is available on request until 1 March 2027. After that date, only Server Authentication EKU will be included. Source: https://knowledge.digicert.com/alerts/sunsetting-client-authentication-eku-from-digicert-public-tls-certificates

Please check your CA provider current policy:

3. Grace period available: dual-EKU certificates remain supported for a limited period of time
4. No grace period: both the Orange aSBC and the customer eSBC/IPBX are oblige using Server Authentication EKU–only in their respective End- Entity certificates.

In the 2nd scenario, where both endpoints use public certificates with the Server Authentication EKU only, Orange validates mutual TLS interoperability through testing.

The impact on mutual authentication may depend on:

- which endpoint acts as the TLS client or TLS server.
- and the vendor capabilities for handling certificates without the Client Authentication EKU

➢ Case 1: Ribbon eSBC initiates the TLS handshake:

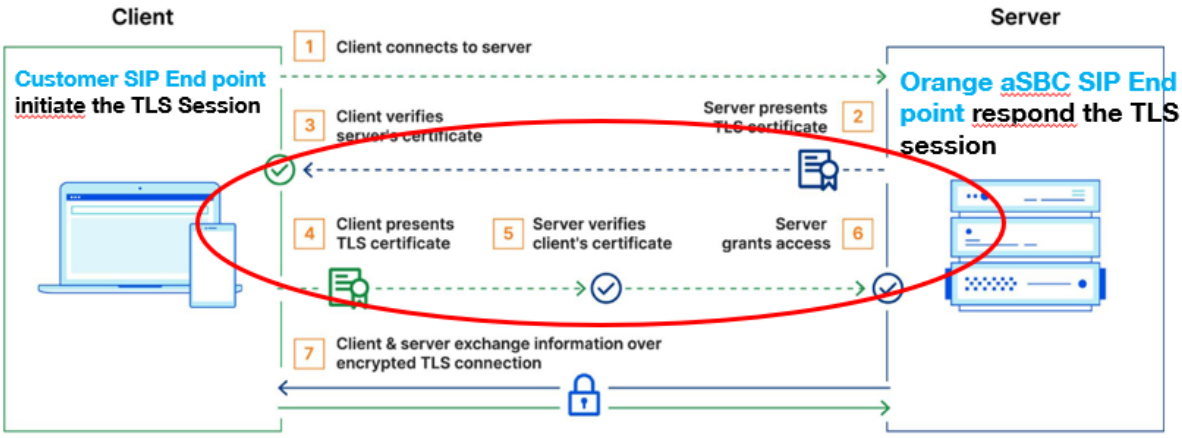
In this scenario:

- The Ribbon eSBC acts as the TLS client.
- The Orange aSBC acts as the TLS server.
- The Ribbon eSBC initiates the TLS handshake.

The Orange aSBC requests a certificate from the Ribbon eSBC to perform mutual TLS authentication.

TLS handshake sequence

4. The Orange aSBC requests the customer certificate (TLS message “Certificate request”)
5. The Ribbon eSBC presents its certificate with Server Authentication (serverAuth) EKU only [4].
6. The Orange aSBC verifies the certificate [5] and grants access [6].



Result: Mutual TLS continues to work when the Ribbon eSBC initiates the connection, even if the customer public certificate contains the serverAuth EKU only.
No specific Ribbon configuration change is required for this scenario.

➢ Case 2: mTLS supported by Ribbon eSBC without considering missing Client Auth EKU in Orange SBC public certificate.

In this scenario:

- The Orange aSBC acts as the TLS client.
- The Ribbon eSBC acts as the TLS server.
- The Orange aSBC initiates the TLS handshake.

The Ribbon eSBC requests a certificate from Orange in order to perform mutual TLS authentication. Orange presents its public certificate containing the serverAuth EKU only.

Default behavior — TLS handshake failure

By default, the Ribbon eSBC requires a certificate presented by a TLS client to include the clientAuth EKU. It therefore rejects the Orange certificate.
As a result, mutual TLS authentication fails, and the TLS handshake cannot be completed.

Configuration required to restore mutual TLS

Ribbon eSBC provides the parameter:

"Validate Client FQDN"

To allow Orange certificates containing serverAuth EKU only, the customer must set this parameter to:

"Disabled"

With this setting, the Ribbon eSBC accepts the Orange certificate even when the clientAuth EKU is not present. More details from Ribbon Edge 12.2.X MTLS official documentations(extract per below)

Validate Client FQDN

Specifies the reverse DNS lookup of a peer's FQDN. Used to verify the identity of the SIP peer client certificate.

This action takes place when both, **Mutual Authentication** and **Validate Client FQDN** are enabled. **Validate Client FQDN** is an enhanced security feature of SBC Edge Portfolio, which could be disabled if the common name in the certificate is an IP address (some ITSP's do that). When the **Validate Client FQDN** is enabled, this option allows SBC Edge Portfolio to perform an FQDN match of an incoming peer certificate common name (CN) or Subject Alternate Name (SAN) against a reverse DNS lookup of the IP address to an FQDN.

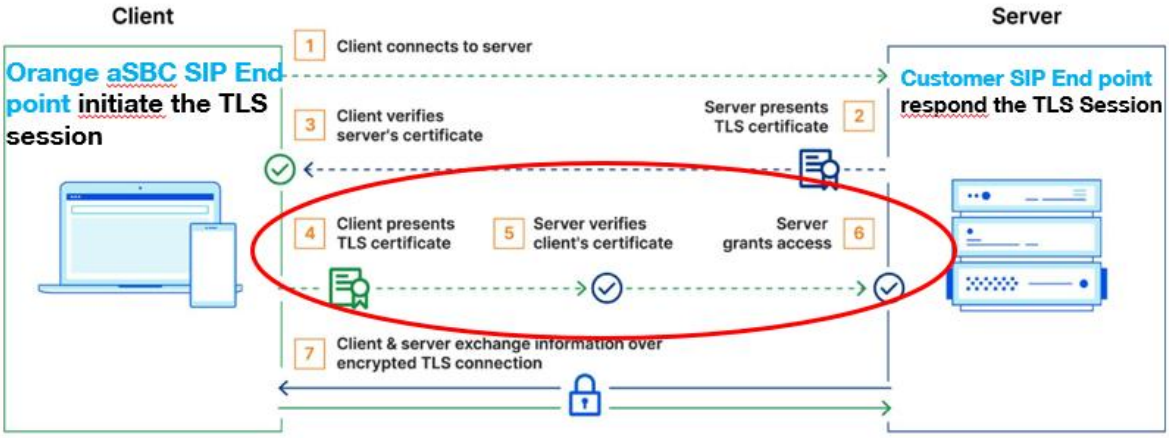
SBC Edge Portfolio does not validate IP addresses to identify a peer server, but only Fully Qualified Domain Names (FQDN).

MTLS Illustration Notes

Step 3 - Always takes place when Mutual Authentication is enabled. If MTLS is disabled, then **Verify Peer Server Certificate** can be disabled.
Step 4 - This action takes place when MTLS is enabled and **Validate Server FQDN** is enabled. If **Verify Peer Server Certificate** is disabled, the **Validate Server FQDN** is also disabled. **Validate Server FQDN** is an enhanced security feature of SBC Edge Portfolio, which can be disabled if the common name in the certificate is an IP address (some ITSP's do that). The **Validate Server FQDN Enabled** option allows SBC Edge Portfolio to perform an FQDN match of an incoming peer certificate CN or SAN against the host configured in the SIP Server table of SBC Edge Portfolio (protocol must be TLS and the Host FQDN).
Steps 5, 6, 7 and 8 - If MTLS is enabled, steps 5, 6, and 7 are mandatory and point 8 could be made optional but the steps 5 through 8 are performed by default. If MTLS is disabled, steps 5 through 8 will not be performed.
Step 8 - This action takes place when MTLS is enabled and **Validate Client FQDN** is enabled. If MTLS is disabled, the **Validate Client FQDN** is also disabled. **Validate Client FQDN** is an enhanced security feature of SBC Edge Portfolio, which can be disabled if the common name in the certificate is an IP address (some ITSP's do that). The **Validate Client FQDN Enabled** option allows SBC Edge Portfolio to perform an FQDN match of an incoming peer certificate CN or SAN against a reverse DNS lookup of the IP address to an FQDN.

TLS handshake sequence after the configuration change

4. The Ribbon eSBC requests the Orange aSBC certificate.
5. The Orange aSBC presents its certificate with Server Authentication (serverAuth) EKU only [4].
6. The Ribbon eSBC verifies the certificate, accept it regardless of whether the Client Authentication (clientAuth) EKU is not present [5] and grants access [6].



Security consideration: Please note this specific Ribbon eSBC configuration option reduce customer security concern with Orange: End customer Ribbon eSBC security heavily change by accepting Orange aSBC certificate without taking into considerations Orange public certificates EKU's in and must accept by End Customer.

Please go to 5.7 TLS profile configuration for Orange TLS context configuration details.

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

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 for BTol/BTIPol - Description: **BTol/BTIPol TLS Profile** - TLS Protocol **: TLS 1.3 Only** - Mutual Authentication : **Enabled** - Client Cipher List : ▪ TLS_AES_256_GCM_SHA384 ▪ TLS_AES_128_GCM_SHA256 ▪ TLS_CHACHA20_POLY1305_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**
SDES-SRTP Profiles BTol/BTIPol only	
On the SBC WebUi Interface: Media > SDES-SRTP Profiles	Edit the Teams SDES-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** - SDES-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** - SDES-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/BTIPoI) **to Teams** Create new Call Routing Table: - Description: **CR BT/BTIP** (or BTOI/BTIPoI) **to Teams** Update CR BT/BTIP (or BTOI/BTIPoI) to Teams - Description: **BT/BTIP** (or BTOI/BTIPoI) **to Teams** - Number/Name transformation Table: **BT/BTIP** (or BTOI/BTIPoI) **to Teams** - Destination Signaling Group: **SG to Teams*** * *refer to Teams Configuration*
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**

5.8 HA Configuration

Enable HA	
On the SBC WebUi Interface: System > Node-Level Settings	Enable HA: - Local IP Address: <@local IP address for HA> - Local IP Netmask: <@Netmask X.X.X.X> - Remote IP Address: <@remote HA IP address> Do the same steps on both HA SBCs, swap local and remote IP address to your need.

5.9 Ribbon FAX configuration checklist

✓ *FAX support:*

- **G.711 Inband Fax**
  - For G.711 inband fax transmission, customers may implement any inband fax configuration, including, but not limited to, autonomous mode, passthrough mode, and voice mode. V.152 is explicitly excluded and is not supported.
  - Customers are solely responsible for configuring their own fax equipment. Orange does not recommend any specific G.711 inband fax configuration, as fax transmission performance may depend on the behaviour of fax gateways and on any transcoding operations performed within the core network.
  - Consequently, Orange does not provide technical support for issues related to G.711 inband fax transmission.
- **T.38 fax transport mode**
  - SIP endpoint SHALL support "image t38" as SDP media description information.
  - If the call is established with a codec different from T38, when the FAX is detected, a media session modification MUST be operated as described below.

Main T.38 configuration in following chapters

5.9.1 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.

5.9.2 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.

5.9.3 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.

5.9.4 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

5.9.5 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

5.9.6 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.

5.9.7 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.

5.9.8 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.

5.9.9 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 (DigiCert Global Root G2, 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 TLS Mutual Authentication Mechanism support regarding public certificate Extended Key Usage (EKU) change

Since mid-2026 public Certificate Authorities (CA's) have progressively issued TLS certificates with the **Server Authentication Extended Key Usage only (EKU),** removing Client Authentication EKU by default, in all end-entity public certificate.

This change follows the **Google Chrome Root Program requirement** (decision made in last October 2024) that publicly **trusted TLS x.509 certificates must no longer support both Server Authentication and Client Authentication purposes, leaving only Server Authentication EKU in.**

Some CAs, such as DigiCert, offer a **grace period** during which End- Entity certificates with both Server Authentication and Client Authentication EKUs can still be requested.

By default, DigiCert issues certificates with Server Authentication EKU only. This dual-EKU option is available on request until 1 March 2027. After that date, only Server Authentication EKU will be included. Source: https://knowledge.digicert.com/alerts/sunsetting-client-authentication-eku-from-digicert-public-tls-certificates

Please check your CA provider current policy:

5. Grace period available: dual-EKU certificates remain supported for a limited period of time

6. No grace period: both the Orange aSBC and the customer eSBC/IPBX are oblige using Server Authentication EKU–only in their respective End- Entity certificates.

In the 2nd scenario, where both endpoints use public certificates with the Server Authentication EKU only, Orange validates mutual TLS interoperability through testing.

The impact on mutual authentication may depend on:

- which endpoint acts as the TLS client or TLS server.
- and the vendor capabilities for handling certificates without the Client Authentication EKU

Case 1: Oracle eSBC initiates the TLS handshake:

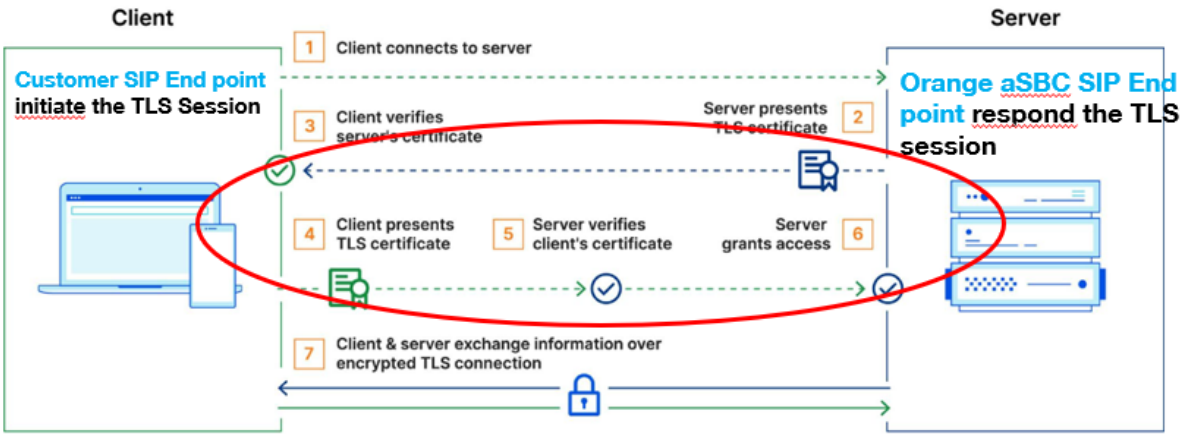
In this scenario:

- The Oracle eSBC acts as the TLS client.
- The Orange aSBC acts as the TLS server.
- The Oracle eSBC initiates the TLS handshake.

The Orange aSBC requests a certificate from the Oracle eSBC in order to perform mutual TLS authentication.

TLS handshake sequence

7. The Orange aSBC requests the customer certificate (TLS message “Certificate request”)
8. The Oracle eSBC presents its certificate with Server Authentication (serverAuth) EKU only [4].
9. The Orange aSBC verifies the certificate [5] and grants access [6].



Result: Mutual TLS continues to work when the Oracle eSBC initiates the connection, even if the customer public certificate contains the serverAuth EKU only.

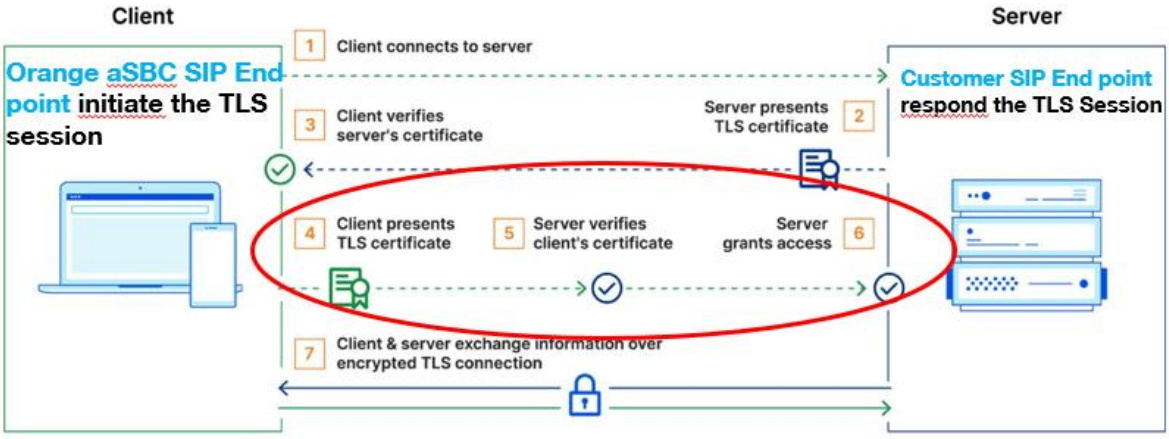
No specific Oracle configuration change is required for this scenario.

Case 2: mTLS supported by Oracle eSBC without considering missing Client Auth EKU in Orange SBC public certificate.

In this scenario:

- The Orange aSBC acts as the TLS client.
- The Oracle eSBC acts as the TLS server.
- The Orange aSBC initiates the TLS handshake.

The Oracle eSBC requests a certificate from Orange in order to perform mutual TLS authentication. Orange presents its public certificate containing the serverAuth EKU only.
Result: Mutual TLS continues to work when the Orange aSBC initiates the connection, even if the Orange public certificate contains the serverAuth EKU only.
No specific Oracle configuration change is required for this scenario.



6.2.6 License

- No license is required

6.2.7 User Agent

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

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

6.2.8 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	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**
S0p1	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**

- **Network interface configuration**

Interface	Configuration
Wancom0	Configured at first initial boot
S0p0 **To Teams**	OracleSBC1# **configure terminal** OracleSBC1 (configure)# **system** OracleSBC1 (system)# **network-interface** OracleSBC1 (network-interface)# **name s0p0** OracleSBC1 (network-interface)# **hostname *<SBC FQDN>*** OracleSBC1 (network-interface)# **ip-address *<SBC Public IP>*** OracleSBC1 (network-interface)# **netmask *<Netmask>*** OracleSBC1 (network-interface)# **gateway *<GW IP>*** OracleSBC1 (network-interface)# **dns-ip-primary *<Primary Public DNS>*** OracleSBC1 (network-interface)# **dns-ip-backup1 *<Backup Public DNS>*** OracleSBC1 (network-interface)# **dns-domain *<DNS Domain>*** OracleSBC1 (network-interface)# **add-hip-ip *<SBC Public IP>*** OracleSBC1 (network-interface)# **add-icmp-ip *<SBC Public IP>***

	OracleSBC1 (network-interface)# **add-ssh-ip** ***<SBC Public IP>*** OracleSBC1 (network-interface)# **gw-heartbeat** OracleSBC1 (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**
S0p1 **To BTIP**	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**

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 (DigiCert Global Root G2 for Teams SIP proxy)

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

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

Step 1 – Creating the certificate

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

Element	Configuration
Certificate-record **SBCCertificate**	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**

Certificate-record **IntermediateCA**	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**
Certificate-record **DigiCert Global Root G2**	OracleSBC1# **configure terminal** OracleSBC1 (configure)# **security** OracleSBC1 (security)# **certification-record** OracleSBC1 (certificate-record)# **name GlobalRootG2** 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 "DigiCert Global Root G2"** 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**

Step 2 – Generating a certificate signing request

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

Element	Configuration
Certificate signing **request**	OracleSBC1# **generate-certification-request SBCCertificate** Should return something like this :

	-----BEGIN CERTIFICATE REQUEST----- MIIC7zCCAdcCAQAwgYsxCzAJBgNVBAYTAkZSMQ4wDAYDVQQIEwVQYXJpczEOMAwG A1UEBxMFUGFyaXMxDzANBgNVBAoTBk9yYW5nZTEhMB8GA1UECxMYT3Jhbmdl IEJ1 c2luZXNzIFNlcnZpY2VzMSgwJgYDVQQDEx9ocTYwNmd3Lm1zdmlzaXQ2Lm9uZS5l cXVhbnQubmV0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv/NxxJUw 2JeNE3NBvYFkYC0kniJkaB3r4Y+QCPolgkL5qK9bsVTwop7mHmpon4NlgZQwfKqA UigABDIVwiSOavpLpo98FM5fCFg0J1GZXe/E9UReK9g4NV8D1yyDgZoeDWBtuq6h S/n1ob96NjuHO+wSaxWviOeQk0icB+7+o9YZ1tCS gym7WAy7UKyJ 7b6FQ7DYJifsd6hAfASx9xfnDRW9RaWr1QnlkjXeFXwJRSLALaWVn6vaFznAkXGL 5thaEi3MirbinRJQXdtmBqd5hF4wZxIQpZS4qVtVS0O+EjQ7+mxvXyBQo08mzmSy vSmWu3Yw3jZREwIDAQABoB4wHAYJKoZIhvcNAQkOMQ8wDTALBgNVHQ8EBAMCBaAw DQYJKoZIhvcNAQELBQADggEBALZliCeQjm0ovxprVjFf2NPnVEbYUcs2t8vJnCZr 1a6NxdBT5sF/lOOfss67X/X8TAIgOWX1It81xC7ydoItohpUtiII4R1zL6nJC5oP brCHHnqFRJbQxdnCFpWYDV3Rff8HsmicizHNv3cYbGyTWwbySuOpiA+RCTPST1Rg vr1hdSVuCrzRCrt51nEE5X+Vmb0RK2nJ+4CGgNGy6MLyRQOaIFxnRF/wCWdr+zjQ rDjrRknTc0tB/QaQk1VgpcvZG3XJ90Q3toqXpo6F2Fq8q99/75aUg1680G8J3CMu mZ5K+yldScQuS6Dq1EJt0RZ8IUrNYcn8sB/uhGWxm4Qy79c= -----END CERTIFICATE REQUEST-----

Step 3 – Deploy SBC & root/intermediate certificates

SBCInter →
SBCCertificate →

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

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

➢ **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 (*<GlobalRootG2>*** ***<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-asymetric-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 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)# **mine-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**	OracleSBC1# **configure terminal** OracleSBC1 (configure)# **session-router** OracleSBC1 (session-router)# **sip-manipulation** OracleSBC1 (sip-manipulation)# **name KeepFirstCodec**
SIP Mime SDP rule	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**

MSR_ KeepFirstCodec	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.$2+" 101"** OracleSBC1 (sip-sdp-line-rules)# **done** OracleSBC1 (sip-sdp-line-rules)# **exit** OracleSBC1 (sip-sdp-media-rules)# **sdp-line-rule** OracleSBC1 (sip-sdp-line-rules)# **name LR_aLineFirstCodecOnly** OracleSBC1 (sip-sdp-line-rules)# **type a** OracleSBC1 (sip-sdp-line-rules)# **action delete** OracleSBC1 (sip-sdp-line-rules)# **comparison-type pattern-rule** OracleSBC1 (sip-sdp-line-rules)# **match-value (rtpmap\|fmtp):(?!({$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**

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,BYE,REFER** 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 \\ 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 StripVideo

Element	Configuration
SIP Manipulation **StripVideo**	OracleSBC1# **configure terminal** OracleSBC1 (configure)# **session-router** OracleSBC1 (session-router)# **sip-manipulation** OracleSBC1 (sip-manipulation)# **name StripVideo**
SIP Mime SDP rule **MSR_StripVideo**	OracleSBC1 (sip-manipulation)# **mine-sdp-rules** OracleSBC1 (sip-mime-sdp-rules)# **name MSR_StripVideo** OracleSBC1 (sip-mime-sdp-rules)# **msg-type request** OracleSBC1 (sip-mime-sdp-rules)# **methods INVITE** OracleSBC1 (sip-mime-sdp-rules)# **comparison-type manipulate** OracleSBC1 (sip-mime-sdp-rules)# **sdp-media-rule** OracleSBC1 (sip-sdp-media-rules)# **name MR_RemoveVideo** OracleSBC1 (sip-sdp-media-rules)# **media-type video** OracleSBC1 (sip-sdp-media-rules)# **action delete** OracleSBC1 (sip-sdp-media-rules)# **done** OracleSBC1 (sip-sdp-media-rules)# **exit** OracleSBC1 (sip-mime-sdp-rules)# **done** OracleSBC1 (sip-mime-sdp-rules)# **exit**

SIP Manipulation out-teams:

Element	Configuration
SIP manipulation **out-teams**	OracleSBC1# **configure terminal** OracleSBC1 (configure)# **session-router** OracleSBC1 (session-router)# **sip-manipulation** OracleSBC1 (sip-manipulation)# **name out-teams**
SIP Header rule **HR_CallFixCLineNAT**	OracleSBC1 (sip-manipulation)# **header-rules** OracleSBC1 (sip-header-rules)# **name 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**
SIP Header rule **KeepFirstCodec**	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**

SIP Manipulation in-teams:

Element	Configuration

SIP manipulation **in-teams**	OracleSBC1# **configure terminal** OracleSBC1 (configure)# **session-router** OracleSBC1 (session-router)# **sip-manipulation** OracleSBC1 (sip-manipulation)# **name in-teams**
SIP Header rule **CallRemovePrivacy**	OracleSBC1 (sip-manipulation)# **header-rules** OracleSBC1 (sip-header-rules)# **name CallRemovePrivacy** OracleSBC1 (sip-header-rules)# **header-name Privacy** OracleSBC1 (sip-header-rules)# **action sip-manip** OracleSBC1 (sip-header-rules)# **new-value RemovePrivacy** OracleSBC1 (sip-header-rules)# **done**
SIP Header rule **CallFixALineNATInbound**	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**
SIP Header rule **CallAddAnnexBNo**	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**
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 Header rule **CallStripVideo**	OracleSBC (sip-header-rules)# **name CallStripVideo** OracleSBC (sip-header-rules)# **header-name From** OracleSBC (sip-header-rules)# **action sip-manip** OracleSBC (sip-header-rules)# **new-value StripVideo** 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**

➢ **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 foreplaceTeams** 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)# **srtp-auth enabled** OracleSBC1 (sdes-profile)# **srtp-encrypt enabled**

	OracleSBC1 (sdes-profile)# **srtcp-encrypt enabled** OracleSBC1 (sdes-profile)# **mki disabled** OracleSBC1 (sdes-profile)# **egress-offer-format same-as-ingress** OracleSBC1 (sdes-profile)# **srtp-rekey-on-re-invite disabled** OracleSBC1 (sdes-profile)# **done**

➢ RTCP policy

Element	Configuration
RTCP policy	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**

➢ Net Management Control

Element	Configuration
Net-Management-Control	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**

➢ Session constraint

Element	Configuration
Session-constraint	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**

- Media sec policy

Element	Configuration
Media sec policy	OracleSBC1# **configure terminal** OracleSBC1 (configure)# **security** OracleSBC1 (security)# **media-security** OracleSBC1 (media-security)# **media-sec-policy** OracleSBC1 (media-sec-policy)# **name RTP** OracleSBC1 (media-sec-policy)# **pass-through disabled** OracleSBC1 (media-sec-policy)# **inbound** OracleSBC1 (inbound)# **mode rtp** OracleSBC1 (inbound)# **protocol none** OracleSBC1 (inbound)# **hide-egress-media-update enabled** 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	OracleSBC1# **configure terminal**

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

➢ **SIP interface**

Element	Configuration
SIP interface **ToTeams**	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 foreplaceTeams** 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**

6.3.4 BTIP configuration

- Enable SIP config

Element	Configuration
SIP config	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** OracleSBC1 (sip-config)# **options +multiple-dialogs-enhancement**

- SIP Profile

Element	Configuration
SIP profile	OracleSBC1# **configure terminal** OracleSBC1 (configure)# **session-router** OracleSBC1 (session-router)# **sip-profile** OracleSBC1 (sip-profile)# **name foreplaceBTIP** 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 disabled** OracleSBC1 (sip-profile)# **done**

- Codec policy

Element	Configuration
Codec policy : CodecBTIP	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**

Element	Configuration
Codec policy : CodecBT	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**

➢ Session agent

Element	Configuration
Session agent **active**	OracleSBC1# **configure terminal** OracleSBC1 (configure)# **session-router** OracleSBC1 (session-router)# **session-agent** OracleSBC1 (session-agent)# **hostname *<@IP aSBC 1>*** OracleSBC1 (session-agent)# **port 5060** OracleSBC1 (session-agent)# **transport-method StaticTCP** OracleSBC1 (session-agent)# **realm-id ToBTIP** OracleSBC1 (session-agent)# **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

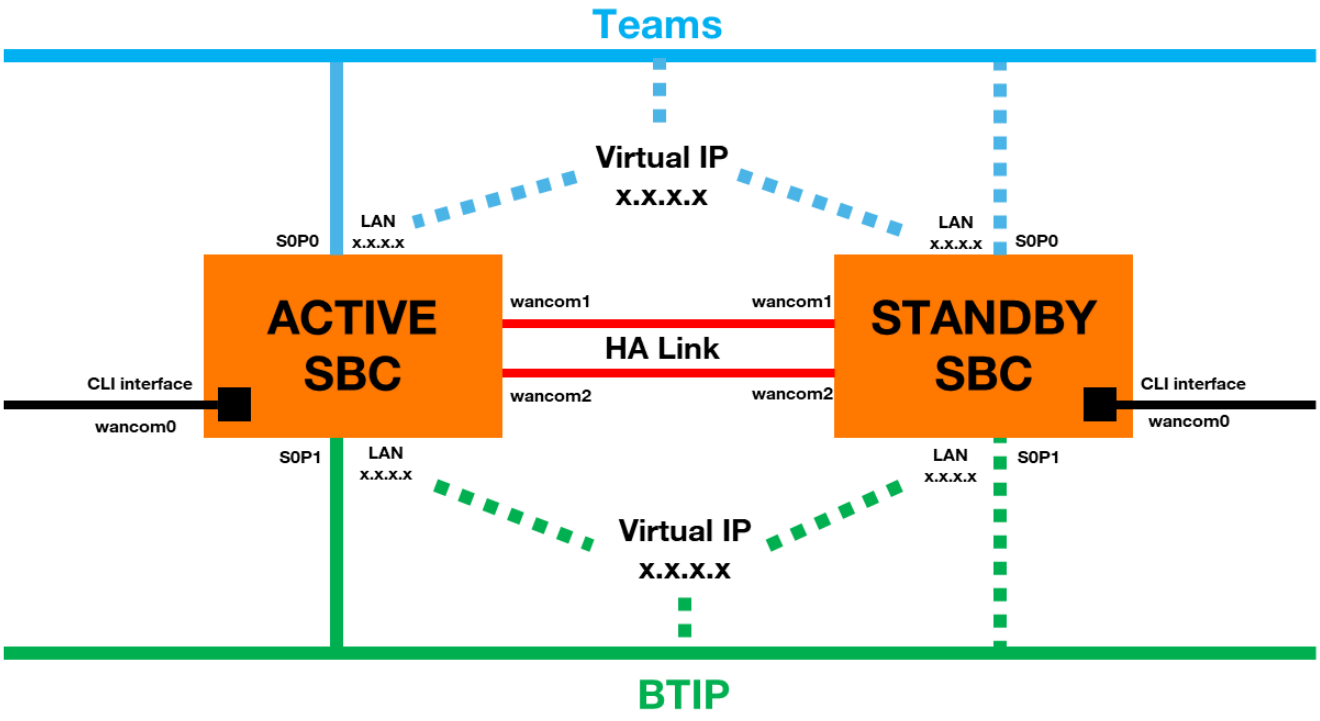
Element	Configuration
Realm **ToBTIP**	OracleSBC1# **configure terminal** OracleSBC1 (configure)# **media-manager** OracleSBC1 (media-manager)# **realm-config** OracleSBC1 (realm-config)# **identifier ToBTIP** OracleSBC1 (realm-config)# **network-interfaces s0p1:0** OracleSBC1 (realm-config)# **mm-in-realm 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)# **merge-early-dialog enable** OracleSBC1 (realm-config)# **hide-egress-media-update enabled** OracleSBC1 (realm-config)# **constraint-name SessionConstraintEmergency** OracleSBC1 (realm-config)# **ringback-trigger refer** OracleSBC1 (realm-config)# **ringback-file *<ringback file .raw>**** OracleSBC1 (realm-config)# **done**

➢ 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)# **sip-profile foreplaceBTIP** OracleSBC1 (sip-interface)# **initial-inv-trans-expire 6** OracleSBC1 (sip-interface)# **out-manipulationid out-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
  - NTP synchronization
  - Virtual MAC address
  - Primary & Secondary utility address
  - Wancom1 & Wancom2 physical configuration
  - Wancom1 & Wancom2 network configuration
  - Redundancy
- Secondary SBC configuration

6.4.1 First SBC configuration

➢ **NTP synchronization**

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

➢ **Virtual MAC address**

Element	Configuration
Virtual MAC address	OracleSBC1# **show interfaces**

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	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**

➢ 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	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**

➢ Wancom1 & Wancom2 physical configuration

Element	Configuration
Wancom1 physical configuration	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**
Wancom2 physical configuration	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**

➢ Wancom1 & Wancom2 network configuration

Element	Configuration

Wancom1 network configuration	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**
Wancom2 network configuration	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**

➢ Redundancy

Element	Configuration
Redundancy	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** 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	OracleSBC**2**# **ping *<Wancom0 SBC1 @IP>*** OracleSBC**2**# **acquire-config *<Wancom0 SBC1 @IP>*** OracleSBC**2**# **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	OracleSBC**1**# **show health** OracleSBC**1**# **display-current-cfg-version** OracleSBC**2**# **show health** OracleSBC**2**# **display-current-cfg-version**

```
Redundancy Protocol Process (v3):
        State                            Active
        Health
        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
        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
```