Business Talk & BTIP for Avaya AURA

version addressed in this guide : 8.1 and 10.1 and 10.2

Information included in this document is dedicated to customer equipment (IPBX, TOIP ecosystems) connection to Business Talk IP service : it shall not be used for other goals or in another context.

Document Version

Version of 20/02/2025

1 Table of Contents

2 Goal of this document

The aim of this document is to list technical requirements to ensure the interoperability between Avaya AURA IPBX with OBS service Business Talk IP SIP, hereafter so-called “service”.

3 Architectures

3.1 Introduction to architecture components and features

This document describes “only” the main supported architectures either strictly used by our customers or that are used as reference to add specific usages often required in enterprise context (specific ecosystems, redundancy, multi-codec and/or transcoding, recording…)

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

- fax servers connected to the IPBX* -and sharing same dial plan-, or as sperate ecosystems -and separate dial plan-
- analog fax machines, usually connected on specific gateways* (seen as IPBX ecosystem or not)

Fax flows are handled via T.38 transport only through BTIP and Business Talk.
Note: Fax communications via Business Talk (International) will still be allowed but will no longer be officially supported by the Orange support teams from April 2023 for new customer implementations.
***Warning !** Fax transport with Avaya Aura and associated G430/450 gateways is NOT fully supported. Fax transmissions MAY fail depending on the termination carrier.

Concerning the Quality of Service, Business VPN and BTIP/Btalk networks trust the DSCP (Differenciated Services Code Point) values sent by customer voice equipment. That’s why Orange strongly recommends to set the IPBX, IP phones and other voice applications with a DiffServ/TOS value** = 46 (or PHB value = EF) at least for media.

**cf QoS parameters in the:

ACM Configuration Checklist → “Network Regions: DIFFSERV/TOS PARAMETERS: Call Control PHB Value / Audio PHB Value” **Note: H.323 phone** series 9600 uses DSCP values for signaling an media from a network region the phone is within.

SM Configuration Checklist → “Session Manager / Device and Location / Device Settings Group”. **Note: SIP softphone** (Equinox and Workplace) uses DSCP values for signaling and media set on SM through SMGR. Softphone must be installed with a special parameter to activate DSCP.

ASBCE Configuration Checklist → “Domain Policies / Media Rules” and “Domain Policies / Signaling Rules” sections.

46xxsettings.txt file Configuration Checklist → “SET DSCPAUD / SET DSCPSIG”. **Note: SIP phone** series 9600 and J.100 and Vantage K.100 uses DSCP values for signaling and media set on 46xxsettings.txt file.

‘BTIP DROM’ architectures are now supported. Dedicated aSBC pairs have been installed in Caribbean and Indian Ocean zones for local calls. For a trunking point of view, the mechanism is similar to ‘BTIP out of France’, the IPBX must support international dial plans and route local calls to the dedicated aSBC pair.

3.2 Supported architecture components

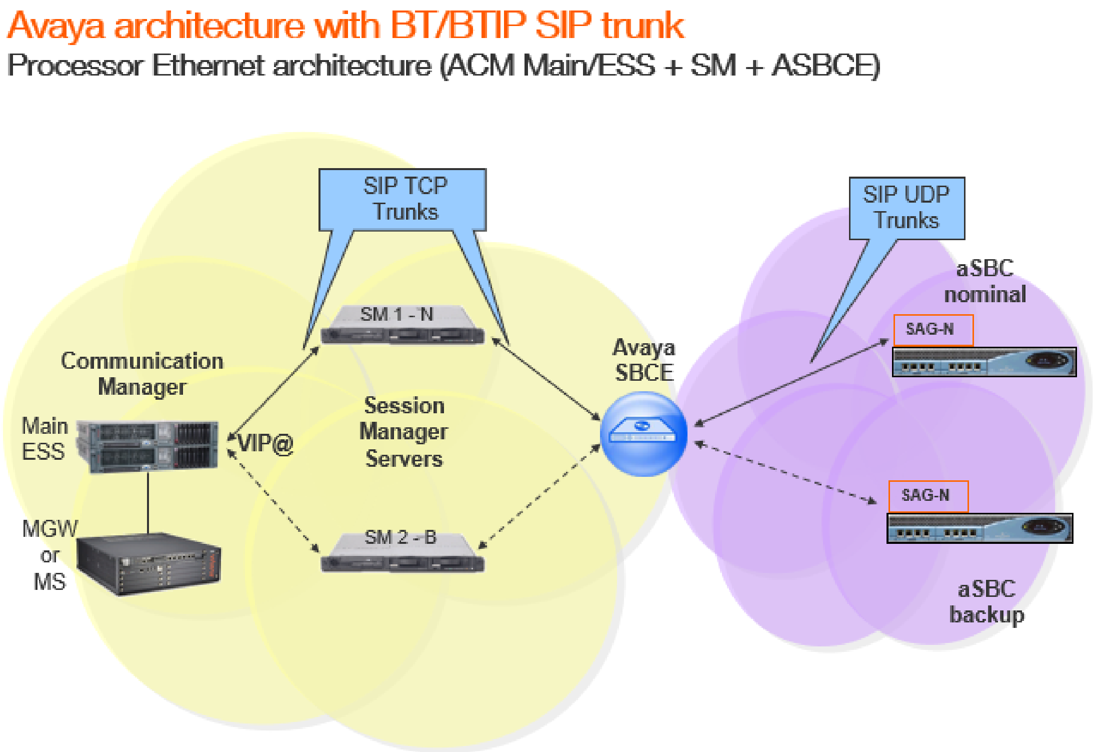
The IP Telephony Avaya Aura has been validated on Business Talk IP / Business Talk with the following architecture components :

- Avaya Aura Communiaction Manager (ACM)
- Avaya Aura Session Manager (ASM)
- Avaya Aura System Manager (SMGR)
- Voice Mails : Avaya Aura Messaging (AAM)
- Avaya Aura Session Border Controller for Enterprise (ASBCE)

3.3 Architecture: ACM + SM + ASBCE

This solution consists of a G430/G450 gateways or Media Servers and a call controlling server configured as a Processor Ethernet.

On a Session Manager (SM), Avaya Communication Manager (ACM) will be considered as a single SIP entity. SIP entity towards ACM will be configured as a single IP address representing Processor Ethernet. SIP entity towards Avaya Session Border Controller for Enterprise (ASBCE) will be configured as a single IP address representing internal ASBCE IP address. ASBCE is used as an intermediate point between SM located in customer's site and Acme Session Border Controller (SBC) in Business Talk / Business Talk IP. SBCs are in Nominal/Backup mode (there is no load balancing and one is being the alternate destination of the other).

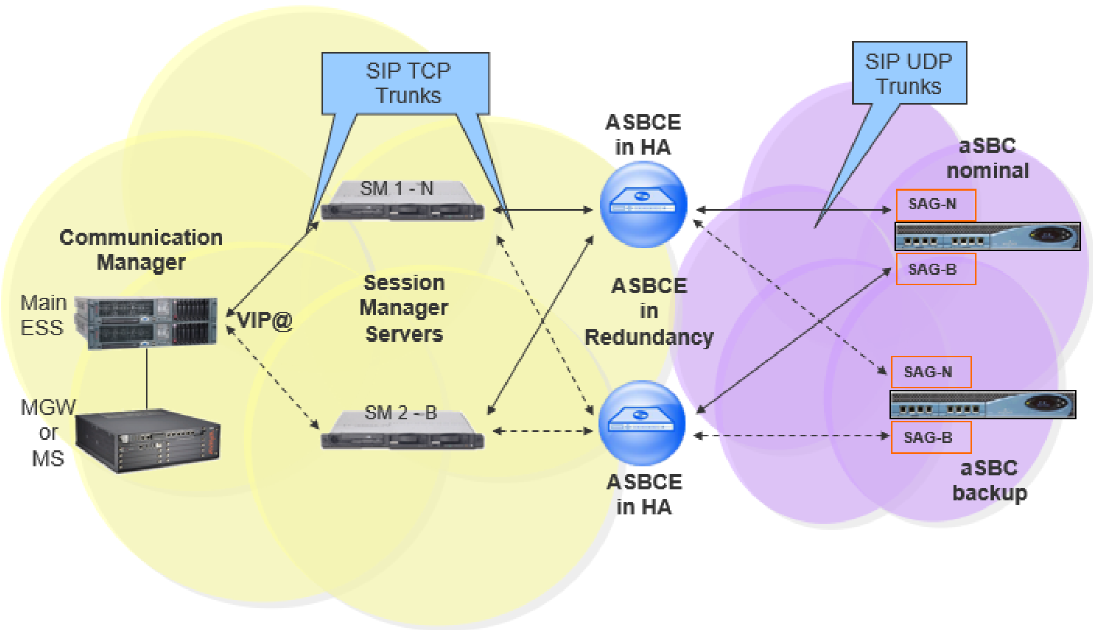


Orange SA, with a share capital of 10,640,226,396 euros,
111 Quai du Président Roosevelt, 92130 Issy-les-Moulineaux, France,
Trade Register No. 380.129.866 Nanterre

When the Survivable Core Server (ESS) is implemented in the architecture and the communication to the Primary Controller (main ACM server) is lost then all the IP telephones and Media Gateways and Media Servers register to a Survivable Core Server (ESS).

ASBCE architecture in High Availability and Redundancy

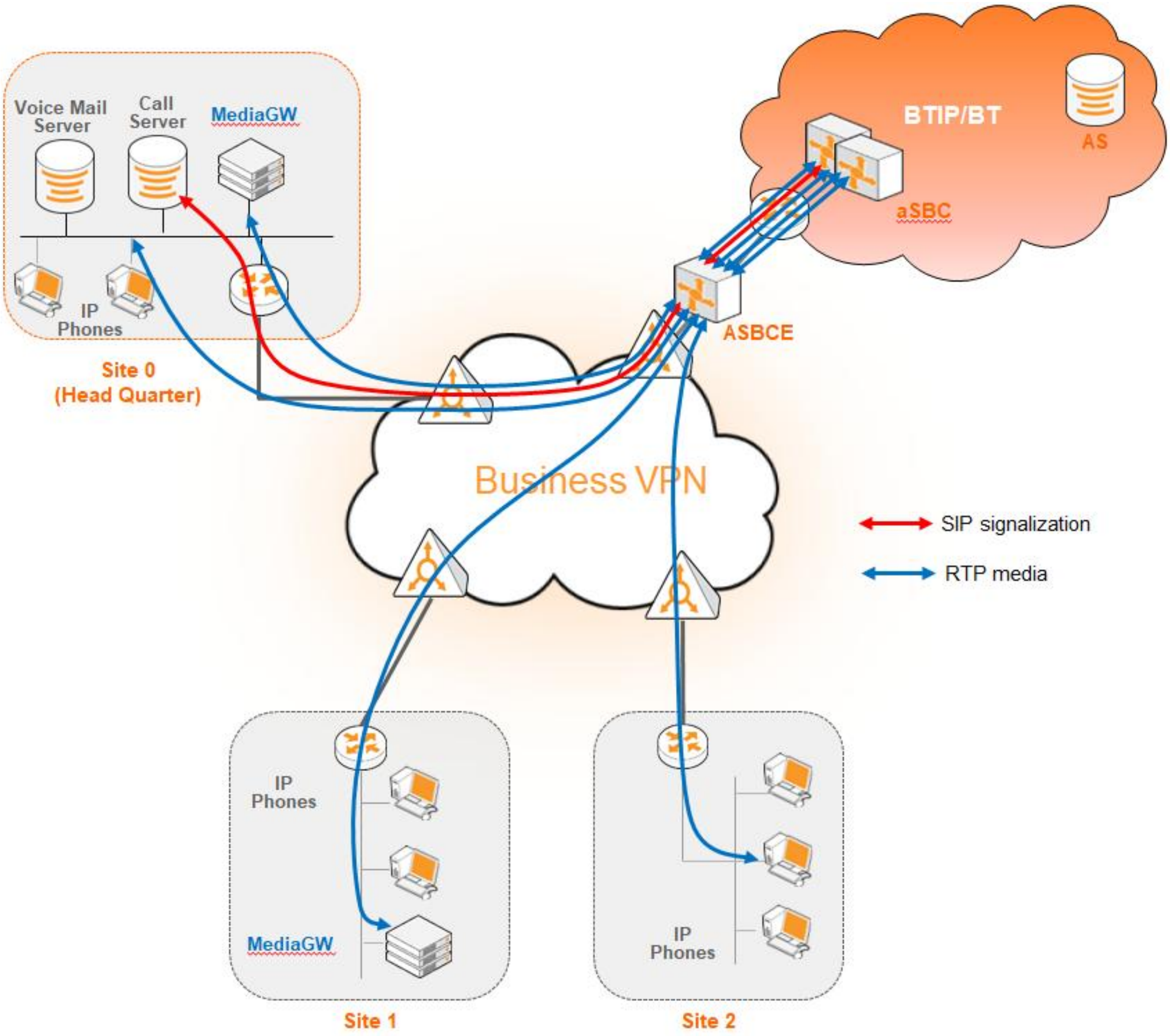
Processor Ethernet architecture (ACM Main/ESS + SM + ASBCE)



ASBCE in Redundancy mode deployment (Geographic-redundant deployment) is a multiple ASBCE deployment. ASBCE in redundancy can be deployed in the HA (High Availability) or non-HA mode. ASBCEs in redundancy are available at the same time and the calls can be routed over them depending on the dialplan on ACM/SM or AS (Application Server).

Call Admission Control analysis

Here below is a table with a Call Admission Control analysis, for the architecture with ASBCE.



	Call scenario	Nb of Voice channels/media resources and bandwidth used on :		
		Media Gateway Voice Channels	Bandwidth G.711A on BT/BTIP G.711MU on BT	Bandwidth G.729 on BT/BTIP
Basic calls	1 BTIP offnet call from/to site 1 [1]	**0** in site 0 **0** in site 1 **0** in site 2	0kbit/s in site 0 86kbit/s in site 1 0kbit/s in site 2	0kbit/s in site 0 30kbit/s in site 1 0kbit/s in site 2
	1 onnet call from site 1 to site 2 [1]	**0** in site 0 **0** in site 1 **0** in site 2	0kbit/s in site 0 86kbit/s in site 1 86kbit/s in site 2	0kbit/s in site 0 30kbit/s in site 1 30kbit/s in site 2
	1 onnet call from site 2 to site 1 through BTIP (“**forced-onnet**”)	**0** in site 0 **0** in site 1 **0** in site 2	0kbit/s in site 0 86kbit/s in site 1 86kbit/s in site 2	0kbit/s in site 0 30kbit/s in site 1 30kbit/s in site 2
	1 BTIP offnet call **to IVR**	**1** in site 0 **0** in site 1 **0** in site 2	86kbit/s in site 0 0kbit/s in site 1 0kbit/s in site 2	30kbit/s in site 0 0kbit/s in site 1 0kbit/s in site 2
	1 BTIP offnet call from/to site 1 **with put on hold**	**0** in site 0 **1** in site 1 **0** in site 2	0kbit/s in site 0 86kbit/s in site 1 0kbit/s in site 2	0kbit/s in site 0 30kbit/s in site 1 0kbit/s in site 2
Transfers	1 BTIP offnet call from/to site 1 **with put on hold + 1 onnet call to site 2**	**0** in site 0 **1** in site 1 **0** in site 2	0kbit/s in site 0 172kbit/s in site 1 86kbit/s in site 2	0kbit/s in site 0 60kbit/s in site 1 30kbit/s in site 2
	1 BTIP offnet call from/to site 1 **after transfer to site 2**	**0** in site 0 **0** in site 1 **0** in site 2	0kbit/s in site 0 0kbit/s in site 1 86kbit/s in site 2	0kbit/s in site 0 0kbit/s in site 1 30kbit/s in site 2
	1 BTIP offnet call from/to site 1 **with put on hold + 1 offnet call to BTIP**	**0** in site 0 **1** in site 1 **0** in site 2	0kbit/s in site 0 172kbit/s in site 1 0kbit/s in site 2	0kbit/s in site 0 60kbit/s in site 1 0kbit/s in site 2
	1 BTIP offnet call from/to site 1 **after transfer to BTIP**	**0** in site 0 **0** in site 1 **0** in site 2	0kbit/s in site 0 0kbit/s in site 1 0kbit/s in site 2	0kbit/s in site 0 0kbit/s in site 1 0kbit/s in site 2
Forwards	1 BTIP offnet call to site 1 **forwarded to Voicemail**	**0** in site 0 **0** in site 1 **0** in site 2	86kbit/s in site 0 0kbit/s in site 1 0kbit/s in site 2	30kbit/s in site 0 0kbit/s in site 1 0kbit/s in site 2
	1 BTIP offnet call to site 1 **forwarded to site 2**	**0** in site 0 **0** in site 1 **0** in site 2	0kbit/s in site 0 0kbit/s in site 1 86kbit/s in site 2	0kbit/s in site 0 0kbit/s in site 1 30kbit/s in site 2
	1 BTIP offnet call to site 1 **forwarded to BTIP**	**0** in site 0 **0** in site 1 **0** in site 2	0kbit/s in site 0 0kbit/s in site 1 0kbit/s in site 2	0kbit/s in site 0 0kbit/s in site 1 0kbit/s in site 2

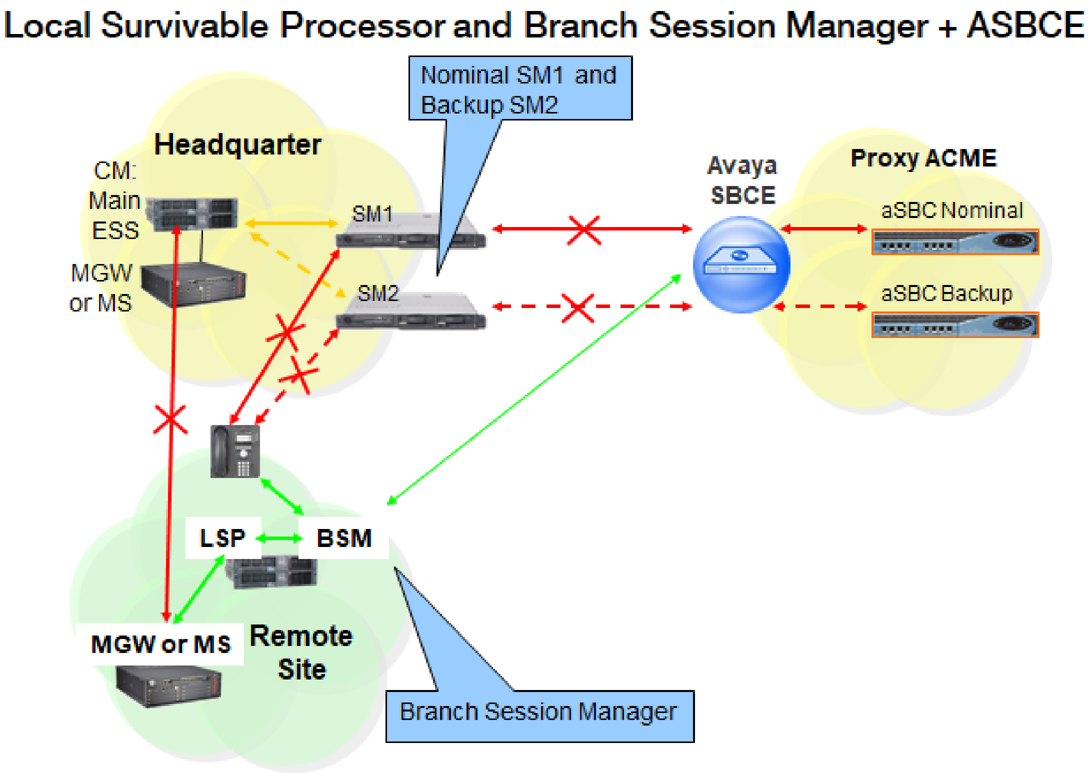
[1] sites 0 & 1 with IP phones and media resources, site 2 with IP phones only

3.4 Architecture: Survivability in Remote Site with ASBCE

Below architecture shows multisite environment: Headquarter with BT/BTIP SIP trunk and Remote Site controlled by this HQ. In case there is a WAN failure between Remote Site and Headquarter:

- Branch Session Manager (also called Survivable Remote Session Manager) provides a SIP survivability solution and service to SIP users in Remote Site
- Local Survivable Processor (also called Survivable Remote Server) is a survivable processor for the Remote Site Media Gateway/Media Server. LSP provides telephony features to SIP users via application sequencing.
- Remote Site Media Gateway/Media Server provides media services such as conferencing, tones and announcements.

3.4.1 LSP and BSM in Remote Site and ASBCE



When communication from Remote Site to the Primary Controller (main ACM server) and Survivable Core Server (ESS) is lost then the Remote Site's IP telephones and Media Gateways and Media Servers register to the Survivable Remote Server (LSP) and SIP telephones register to the Branch Session Manager (BSM).

3.4.2 Media unanchoring on ASBCE

It is a feature available on Avaya Session Border Controller for Enterprise. Unanchoring media benefits in:

- Reducing media (RTP) delay as the direct media (RTP) is passing by ASBCE.
- Media (RTP) is decentralized resulting in bandwidth saving on Headquarter site as the media (RTP) flow to/from Remote Site call over VISIT SIP trunk is passing by the ASBCE placed in Headquarter.
- Reducing resource consumption on ASBCE as the only signaling messages are going through ASBCE.

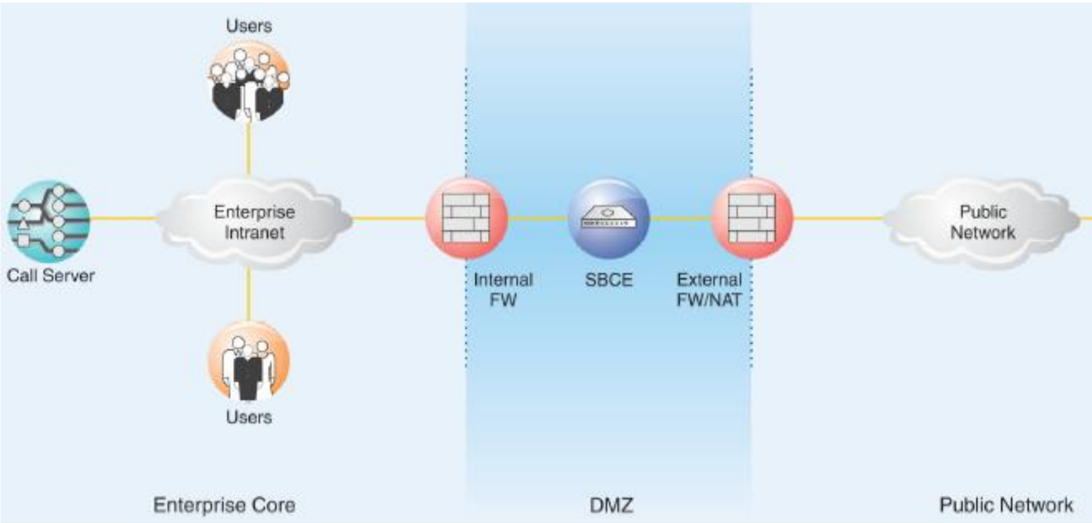
3.5 Business Talk over Internet(BToI) / Business Talk IP over Internet(BTIPoI). Architecture overview for TLS and SRTP over SIP Trunk.

Note: To avoid any security risk the clients should always install on ASBCE the latest mandatory patch/hotfix released by the Avaya vendor.

The two-wire topology, also referred to as inline, is the simplest and most basic deployment of the ASBCE.

Avaya SBCE is positioned at the edge of the network in the DMZ. Avaya SBCE is directly inline with the call servers, and protects the enterprise network against all inadvertent and malicious intrusions and attacks.

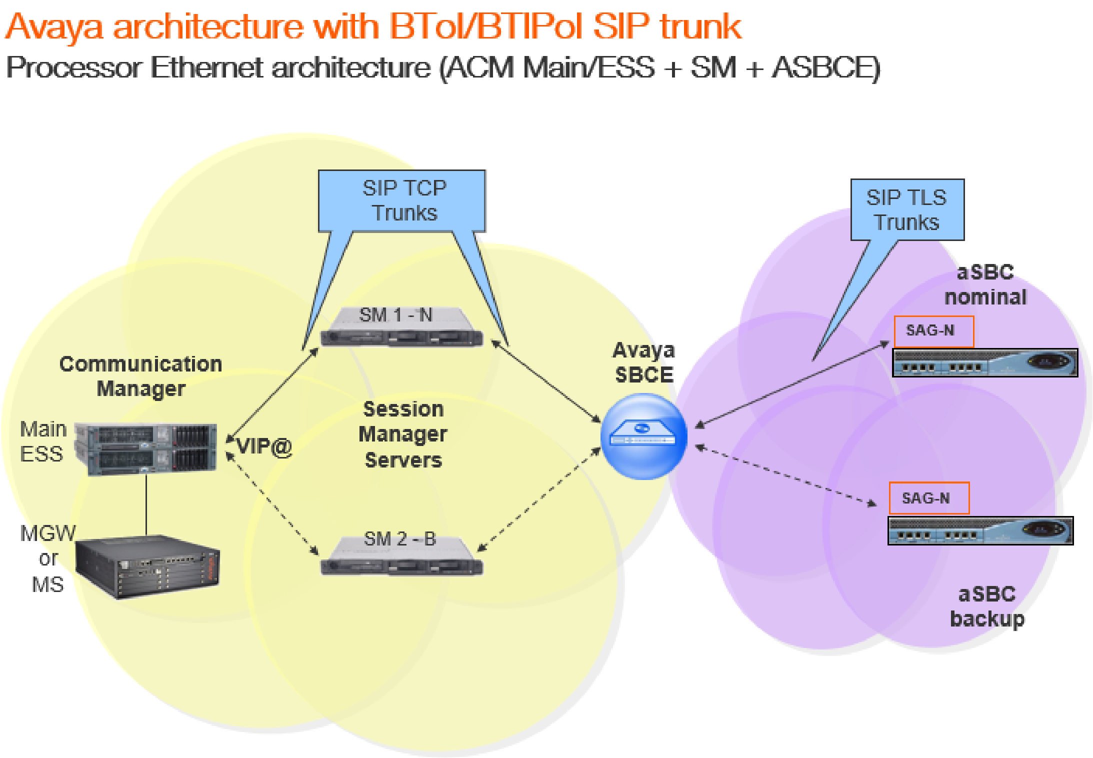
In this configuration, the Avaya SBCE performs border access control functionality such as internal and external Firewall or Network Address Translation (FW/NAT) traversal, access management and control. These functions are based on domain policies that the user can configure, and intrusion functionality to protect against DoS, spoofing, stealth attacks, and voice SPAM.



The two-wire Avaya SBCE deployment enables TLS encryption of the signaling traffic and SRTP encryption of the media traffic carried over public internet between ASBCE and Orange A-SBC.

An X.509 v3 public key certificate is used to identify the Avaya SBCE when performing a TLS handshake for incoming and outgoing connections.

Media must be anchored on ASBCE to perform media transcoding between internal RTP and external SRTP.



3.5.1 Prerequisites

In order to establish the connection with public interface of A-SBC, several preliminary configuration steps have to be performed. These involve the following:

- Public IP address assignment
- Public DNS record
- Firewall updates
- Certificate updates
- TLS v1.3 or v1.2 cypher suites compliance
- SRTP encryption
- Supported codecs on BTIPoI/BToI

3.5.2 Public IP address assignment

The certified solution is using a public IP address directly configured on ASBCE interface placed within DMZ. It is possible to use NAT address translation since public IP addresses can be limited, however this is not part of standard configuration and require additional modifications to be included on ASBCE. Such setup would require a study and validation on customer's request.

3.5.3 Public DNS record

Orange A-SBC can be reached via Fully Qualified Domain Name (FQDN) type SRV or type A deployed on public DNS. Customer premise ASBCE requires a record on public DNS that enables to reach it using FQDN via public internet. BTIPoI can be reached using FQDN only, whereas BToI can be reached either via public IP address or FQDN.

- BTIPoI supports type SRV & type A for DNS resolution and do not support direct public IP connections.
- BToI supports both public IP and type A for DNS resolution and do not provide any type SRV record connections.

3.5.4 Firewall updates

Firewalls in the way of traffic between ASBCE and A-SBC have to be updated in order to open required ports. BToI and BTIPoI vary concerning the UDP port range.

The media UDP port ranges required by Orange BTIPoI SIP Trunk is 6000-38000 and for Orange BToI SIP Trunk is 6000-20000.

BTIPoI/BToI port matrix				
Source device	Source ports	Destination device	Destination ports	Purpose
ASBCE public @IP	Defined Signaling port range on ASBCE: Network & Flows -> Advanced Options e.g. TCP 51001-55000 Depending on customer context or needs.	A-SBC public @IP	TCP 5061	TLS SIP signaling
A-SBC public @IP	TCP Any	ASBCE public @IP	TCP 5061	
ASBCE public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	A-SBC public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	SRTP media
A-SBC public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	ASBCE public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	

3.5.5 Certificate updates

In order to ensure the security of traffic, public root & intermediate certificates need to be exchanged between ASBCE and Orange A-SBC. ASBCE would require an identity certificate signed by a public root CA certificate (including any intermediate certificates in the path). The customer should send public Root & Intermediate certificates which signed ASBCE identity certificate to OBS to be uploaded on Orange A-SBC in case of using a different Public Certificate Authority on their side. This is described in details in following chapters of ASBCE secure configuration.

In case of different public Root & intermediate certificates used by Orange (Digicert) Customer should retrieve ours which signed Orange A-SBC's certificates and upload them to ASBCE. The **Root and the Intermediate Orange CA** are included in the DigiCert CA by following the procedure described below. Connect to the Digicert site : https://www.digicert.com/digicert-root-certificates.htm then download and import (pem format):

- the Root CA: **DigiCert Global Root CA**
- the Intermediate CA: **DigiCert TLS RSA SHA256 2020 CA1**

Upload of the Root and Intermediate Orange CA to ASBCE is described in detail in following chapters of ASBCE secure configuration.

3.5.6 TLS v1.3 and v1.2 cipher suites compliance

The following cipher suites are supported by Orange SBC for TLS 1.3 and TLS 1.2. Compliant cypher suites with Orange SBC are marked in bold.

TLS 1.3

- **TLS_AES_256_GCM_SHA384** (0x1302)
- **TLS_AES_128_GCM_SHA256** (0x1301)
- **TLS_CHACHA20_POLY1305_SHA256** (0x1303)

TLS 1.2

- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** (0xc030)
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** (0xc02f)
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384** (0xc028)
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256** (0xc027)

Cipher suites supported by ASBCE version 10.2 for TLS 1.3 and TLS 1.2 are listed below. Compliant cipher suites with Orange SBC are marked in bold. At least one ASBCE cipher suite must be compliant with BToI/BTIPoI to work.

- **TLS_AES_256_GCM_SHA384** (0x1302)
- **TLS_CHACHA20_POLY1305**_SHA256 (0x1303)
- **TLS_AES_128_GCM_SHA256** (0x1301)
- TLS_AES_128_CCM_SHA256 (0x1304)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** (0xc030)
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)

- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** (0xc02f)
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384** (0xc028)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256** (0xc027)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)

ASBCE and A-SBC will negotiate the TLS 1.3 secure matched cipher suite (**TLS_AES_256_GCM_SHA384** (0x1302)) to establish TLS connection.

Cipher suites supported by ASBCE version 8.1.2 hotfix1 and 10.1 hotfix 1 for TLS 1.2 are listed below. Compliant cipher suites with Orange SBC are marked in bold. At least one ASBCE cipher suite must be compliant with BToI/BTIPoI to work.

- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** (0xc030)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384** (0xc028)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** (0xc02f)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256** (0xc027)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)

- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)

ASBCE and A-SBC will negotiate the most secure matched cipher suite (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(0xc030)) to establish TLS connection.

Note: The Avaya "ASBCE encryption license" is required to activate TLS on ASBCE SIP trunk.

3.5.7 SRTP encryption on BTIPoI/BToI

Media encryption preferred format: AES_CM_128_HMAC_SHA1_80

Note: The Avaya "ASBCE encryption license" is required to activate SRTP (media encryption) on ASBCE SIP trunk.

3.5.8 Supported codecs on BTIPoI/BToI

Supported codec is G.711A (20ms) for BTIPoI and BToI.

G.711u (20ms) can be requested on specific case for BToI.

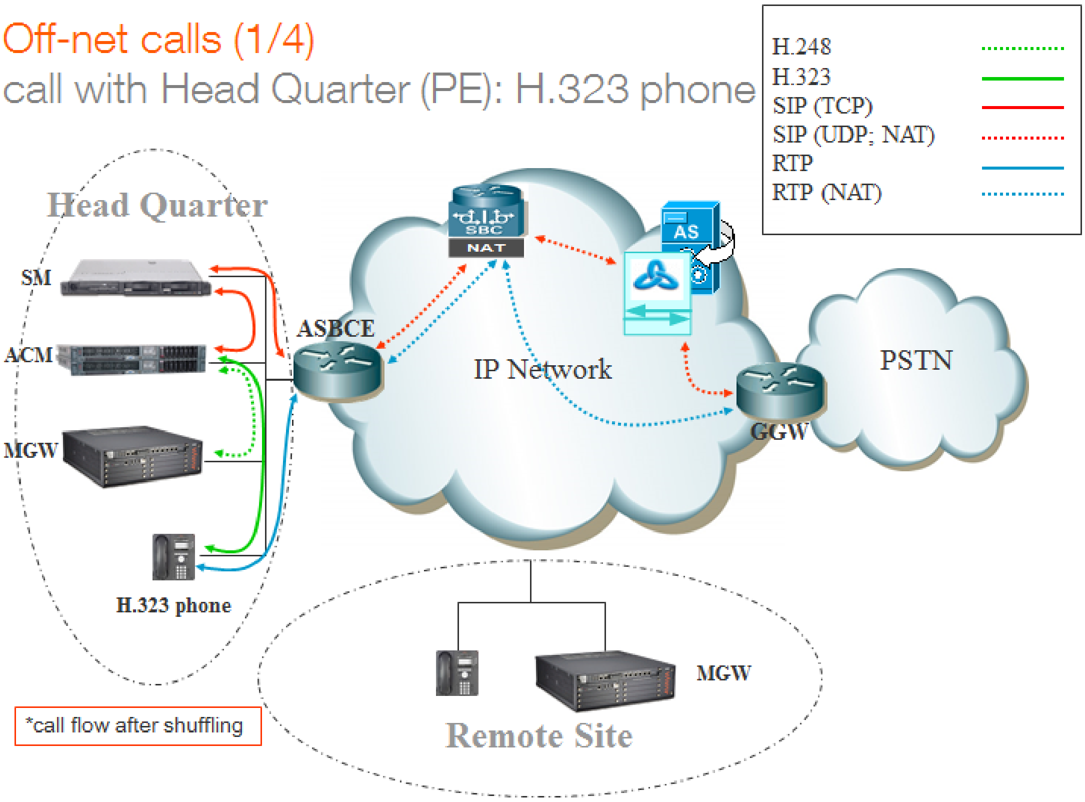
Enable appropriate codec on ACM (Avaya Communication Manager).

4 Call Flows

4.1 Call flows with media anchoring on ASBCE

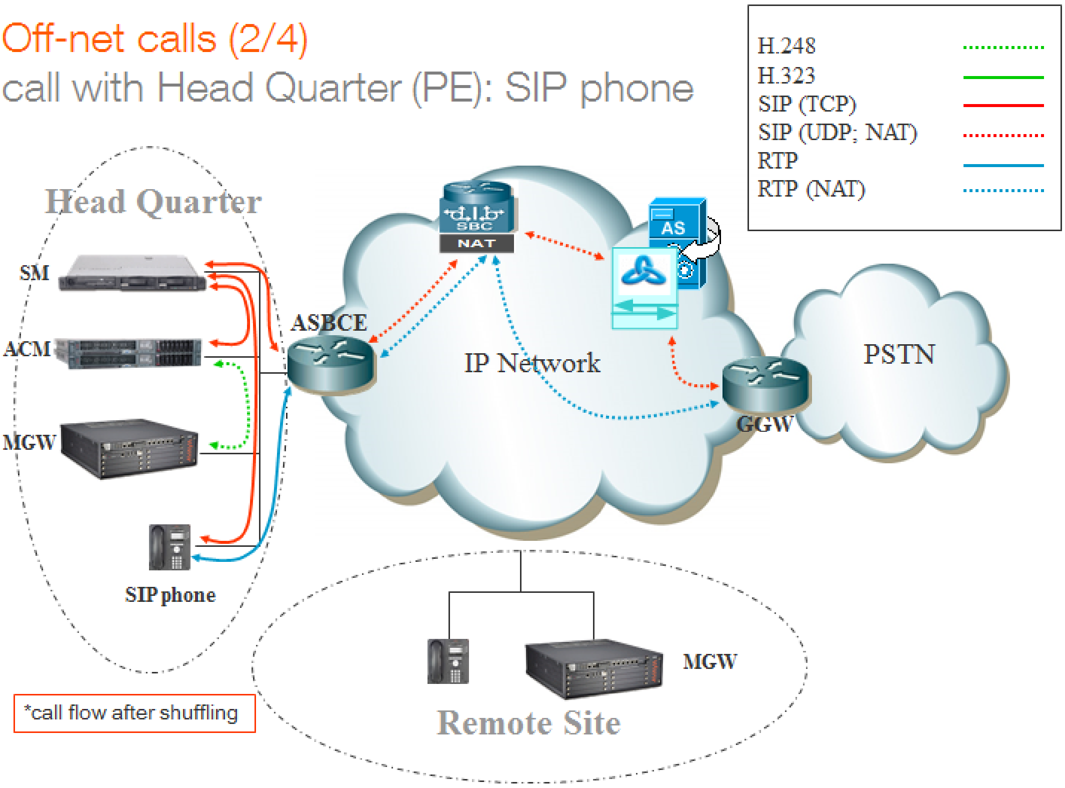
Off-net calls (1/4)

call with Head Quarter (PE): H.323 phone



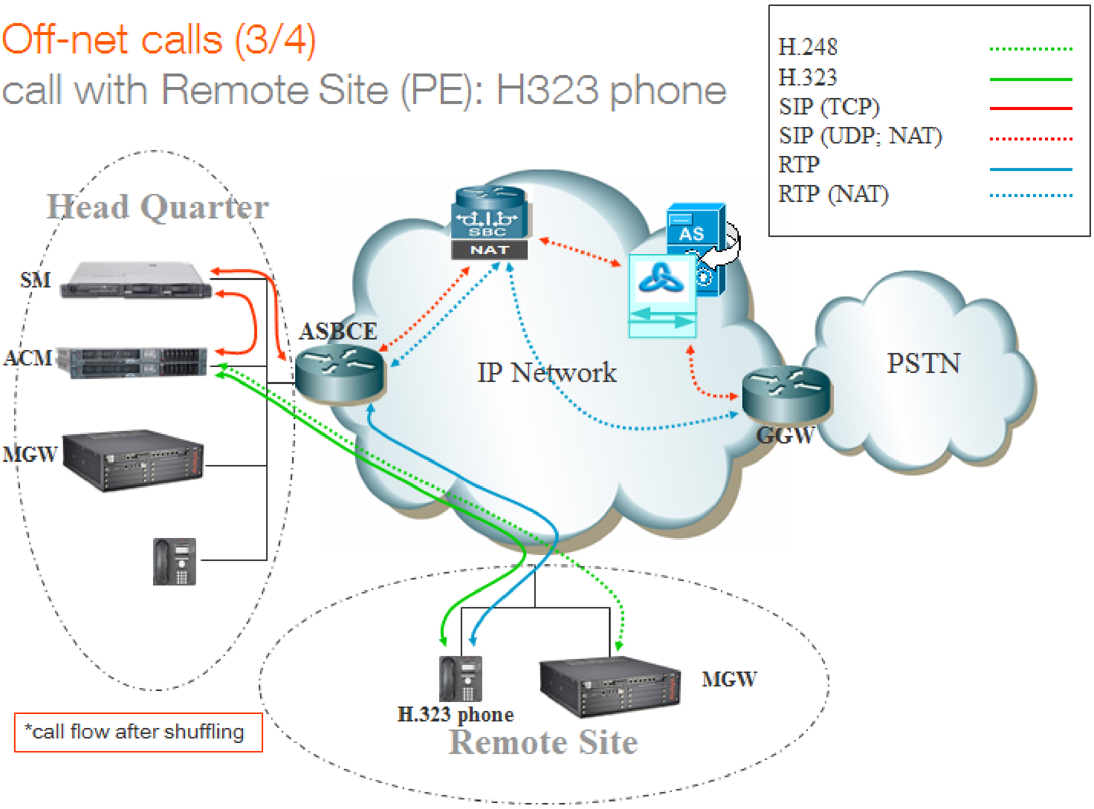
Off-net calls (2/4)

call with Head Quarter (PE): SIP phone



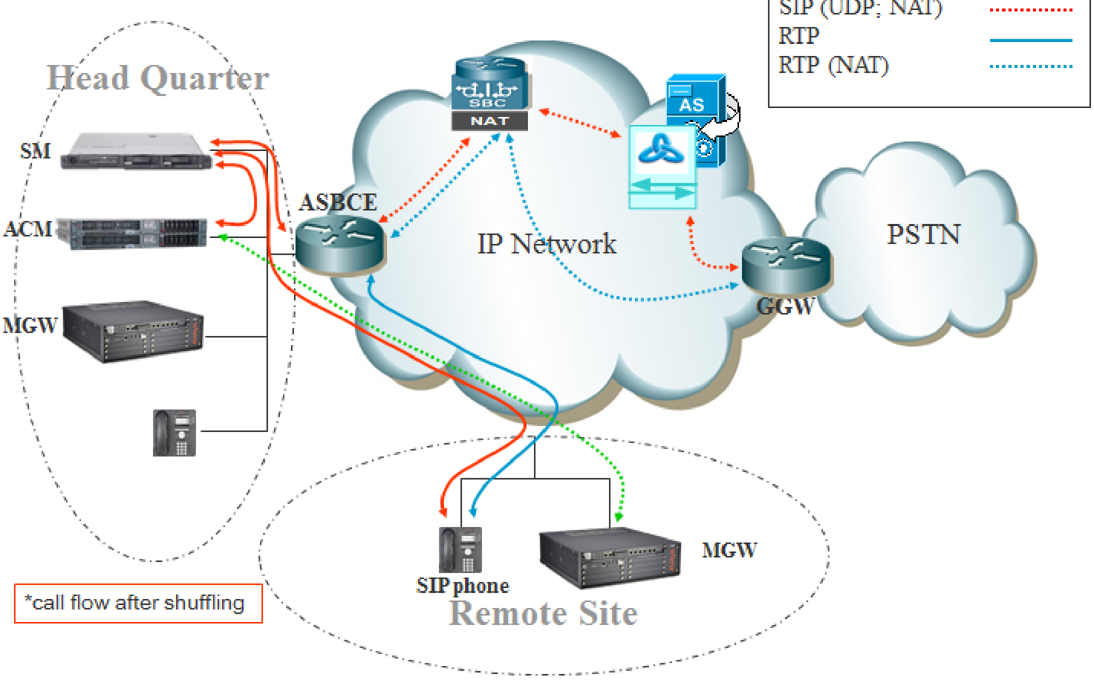
Off-net calls (3/4)

call with Remote Site (PE): H323 phone



Off-net calls (4/4)

call with Remote Site (PE): SIP phone

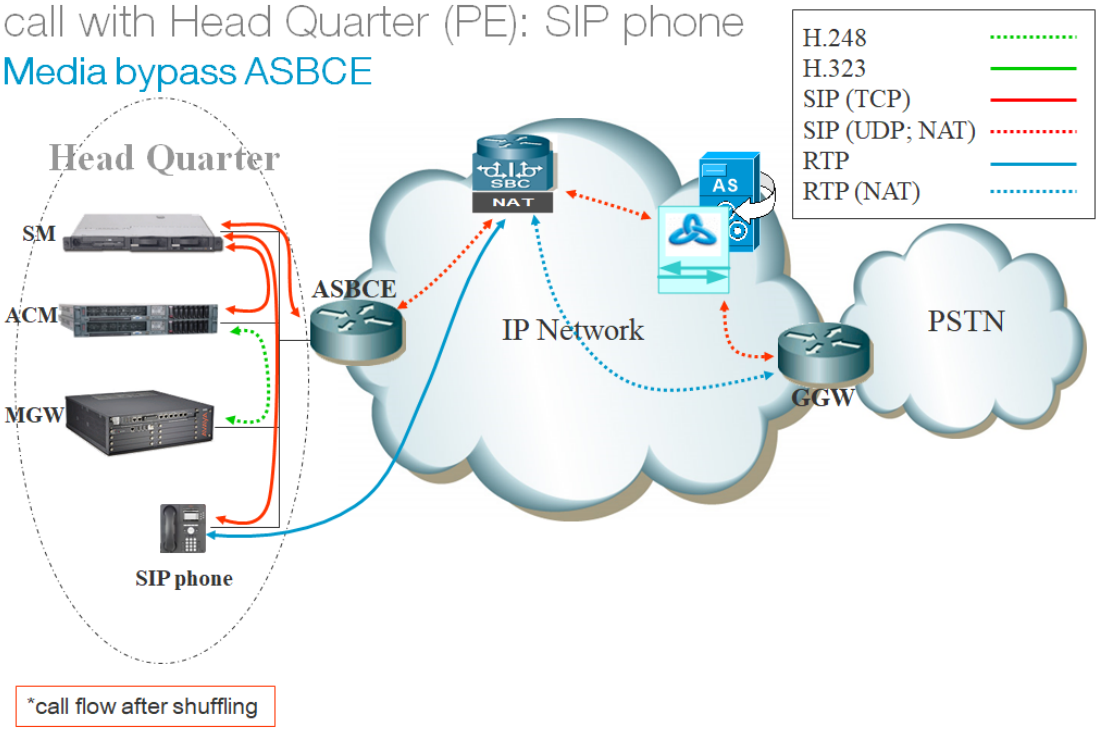


4.2 Call flows with media bypass

Off-net call with media unanchoring on ASBCE

call with Head Quarter (PE): SIP phone

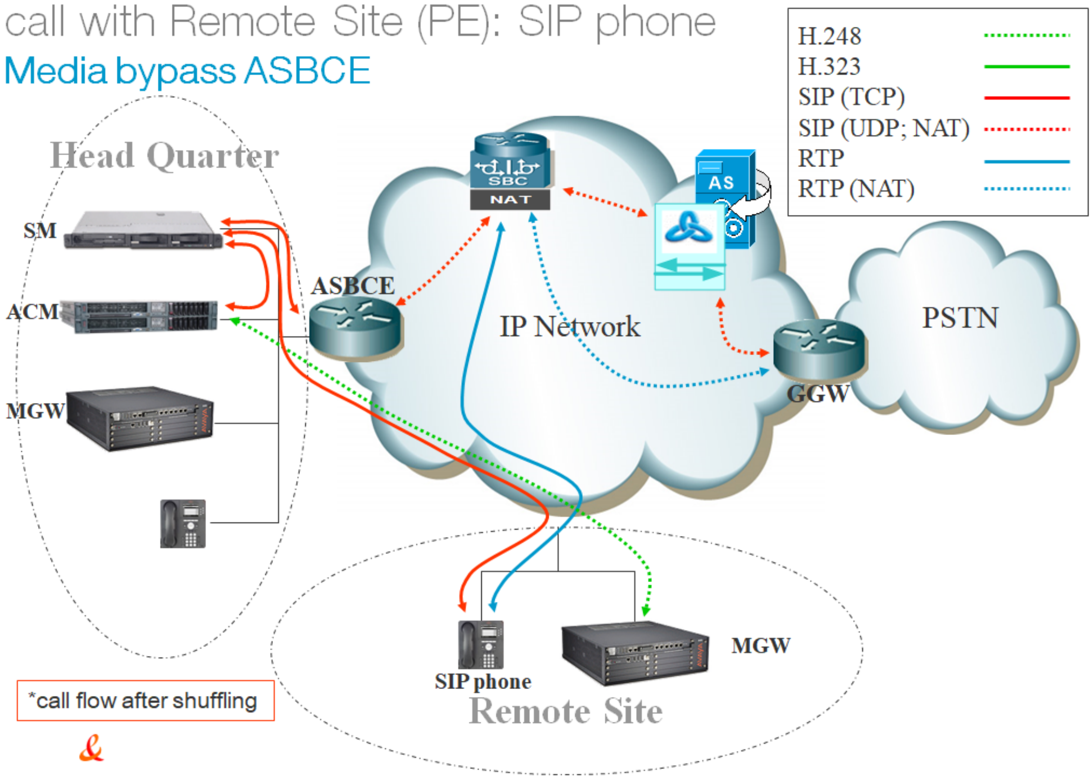
Media bypass ASBCE



Off-net call with media unanchoring on ASBCE

call with Remote Site (PE): SIP phone

Media bypass ASBCE



5 Integration Model

IP addresses marked in red have to be indicated by the Customer, depending on Customer architecture scenario.

Integration model applicable to Avaya Aura + ASBCE with: BT/BTIP (ASBCE IP@)

Head Quarter (HQ)	Level of Service	a-SBC			AS
		SAG Nominal	SAG Backup	Associated T1T7	Site Access
ACM + Single Session Manager (SM)	No redundancy	ASBCE IP@	N/A	T1T7 HQ	T1T7 HQ
ACM + ESS + 2 Session Managers **warning:** - Site access capacity to be sized adequately on the site carrying the 2nd SM in case both SMs are based on different sites	**- ACM redundancy by ESS server in Head Quarter** **- Local redundancy** if both Session Managers (SM) are hosted by the same site OR **- Geographical redundancy** if each SM is hosted by 2 different sites (SM1 + SM2) - Both SMs must be in the same region	ASBCE1 IP@	ASBCE2 IP@	T1T7 HQ	T1T7 HQ

Remote Site (RS) architecture**	Level of Service	a-SBC			AS
		SAG Nominal	SAG Backup	SAG Nominal	SAG Backup
Remote site without survivability	No survivability, no trunk redundancy	ASBCE IP@	N/A	T1T7 HQ	T1T7 HQ
LSP	Local site survivability and trunk redundancy via PSTN only	N/A	N/A	T1T7 RS	T1T7 RS
Branch Session Manager	Local site survivability and SIP trunk redundancy	ASBCE IP@	N/A	T1T7 RS	T1T7 RS

All architectures with ASBCE	Level of Service	a-SBC		AS	a-SBC
		SAG Nominal	SAG Backup	SAG Nominal	SAG Backup
Single ASBCE	No redundancy	ASBCE IP@	N/A	T1T7 HQ	T1T7 HQ
ASBCE in **High Availability**: a pair of ASBCE consisting of one SBCE server acting as primary (active) and another one server acting as secondary (standby). Both SBCE servers share the same IP@ (ASBCE VIP@).	Local vendor redundancy with nominal/backup behavior. The 2 SBCE servers can be located on two different geographic sites but Layer 2 connection between servers 150 ms max round Trip is required. Loss of audio for all active calls on primary SBCE by only 1 second when it fails and its connection with the secondary ASBCE server is up. Loss of audio for all active calls on primary SBCE by 15 seconds when it fails and its connection with the secondary ASBCE server is down.	ASBCE VIP@	N/A	T1T7 HQ	T1T7 HQ
Multiple ASBCE: two ASBCE (ASBCE1 and ASBCE2) **in Nominal/Backup mode on vendor side.**	Local vendor redundancy with nominal/backup behavior. Both ASBCE are hosted on the same site. Nominal/Backup mode on Orange a-SBC side for incoming trafic to the customer ASBCE. Loss of active calls handled by the ASBCE that fails. Geographical vendor redundancy with nominal/backup behavior.	ASBCE1 IP@	ASBCE2 IP@	T1T7 HQ	T1T7 HQ

	The two ASBCE are hosted on 2 different geographic sites. Nominal/Backup mode on Orange a-SBC side for incoming trafic to the customer ASBCE. Loss of active calls handled by the ASBCE that fails.				
Multiple ASBCE in High Availability: two ASBCE pairs in **High Availabity and in Nominal/Backup mode on vendor side**. One ASBCE1 pair (2 ASBCE servers) with shared ASBCE1 VIP@ and one ASBCE2 pair (2 ASBCE servers) with shared ASBCE2 VIP@).	Local/geographical redundancy. The two ASBCE pairs are hosted on the same site or on 2 different geographic sites. Nominal/Backup mode on Orange a-SBC side for incoming trafic to the customer ASBCE pairs. If a full ASBCE pair fails, active calls are lost. Loss of audio for all active calls on primary SBCE of a pair by only 1 second when it fails and its connection with the secondary ASBCE server is up. Loss of audio for all active calls on primary SBCE of a pair by 15 seconds when it fails and its connection with the secondary ASBCE server is down.	ASBCE1 VIP@	ASBCE2 VIP@	T1T7 HQ	T1T7 HQ

Integration model applicable to Avaya Aura + ASBCE with: BT over Internet (ASBCE public IP@ or public FQDN type A)

Head Quarter (HQ)	Level of Service	a-SBC			AS
		SAG Nominal	SAG Backup	Associated T1T7	Site Access
ACM + Single Session Manager (SM)	No redundancy	ASBCE public IP@ or public FQDN type A	N/A	T1T7 HQ	T1T7 HQ
ACM + ESS + 2 Session Managers **warning:** - Site access capacity to be sized adequately on the site carrying the 2nd SM in case both SMs are based on different sites	**- ACM redundancy by ESS server in Head Quarter** **- Local redundancy** if both Session Managers (SM) are hosted by the same site OR **- Geographical redundancy** if each SM is hosted by 2 different sites (SM1 + SM2) - Both SMs must be in the same region	ASBCE1 public IP@ or public FQDN type A	ASBCE2 public IP@ or public FQDN type A	T1T7 HQ	T1T7 HQ

Remote Site (RS) architecture**	Level of Service	a-SBC			AS
		SAG Nominal	SAG Backup	SAG Nominal	SAG Backup
Remote site without survivability	No survivability, no trunk redundancy	ASBCE public IP@ or public FQDN type A	N/A	T1T7 HQ	T1T7 HQ
LSP	Local site survivability and trunk redundancy via PSTN only	N/A	N/A	T1T7 RS	T1T7 RS
Branch Session Manager	Local site survivability and SIP trunk redundancy	ASBCE public IP@ or public FQDN type A	N/A	T1T7 RS	T1T7 RS

All architectures with ASBCE	Level of Service	a-SBC		AS	a-SBC
		SAG Nominal	SAG Backup	SAG Nominal	SAG Backup
Single ASBCE	No redundancy	ASBCE public IP@ or public FQDN type A	N/A	T1T7 HQ	T1T7 HQ
ASBCE in **High Availability**: a pair of ASBCE consisting of one SBCE server acting as primary (active) and another one server acting as secondary (standby). Both SBCE servers share the same IP@ (ASBCE VIP@).	Local vendor redundancy with nominal/backup behavior. The 2 SBCE servers can be located on two different geographic sites but Layer 2 connection between servers 150 ms max round Trip is required. Loss of audio for all active calls on primary SBCE by only 1 second when it fails and its connection with the secondary ASBCE server is up. Loss of audio for all active calls on primary SBCE by 15 seconds when it fails and its connection with the secondary ASBCE server is down.	ASBCE public IP@ or public FQDN type A	N/A	T1T7 HQ	T1T7 HQ
Multiple ASBCE: two ASBCE (ASBCE1 and ASBCE2) **in Nominal/Backup mode on vendor side.**	Local vendor redundancy with nominal/backup behavior. Both ASBCE are hosted on the same site. Nominal/Backup mode on Orange a-SBC side for incoming trafic to the customer ASBCE. Loss of active calls handled by the ASBCE that fails. Geographical vendor redundancy with nominal/backup behavior. The two ASBCE are hosted on 2 different geographic sites. Nominal/Backup mode on Orange a-SBC side for incoming trafic to the customer ASBCE. Loss of active calls handled by the ASBCE that fails.	ASBCE1 public IP@ or public FQDN type A	ASBCE2 public IP@ or public FQDN type A	T1T7 HQ	T1T7 HQ
Multiple ASBCE in High Availability: two ASBCE pairs in **High Availabity and in Nominal/Backup mode on vendor side**. One ASBCE1 pair (2 ASBCE servers) with shared ASBCE1 VIP@ and one ASBCE2 pair (2 ASBCE servers) with shared ASBCE2 VIP@).	Local/geographical redundancy. The two ASBCE pairs are hosted on the same site or on 2 different geographic sites. Nominal/Backup mode on Orange a-SBC side for incoming trafic to the customer ASBCE pairs. If a full ASBCE pair fails, active calls are lost. Loss of audio for all active calls on primary SBCE of a pair by only 1 second when it fails and its connection with the secondary ASBCE server is up. Loss of audio for all active calls on primary SBCE of a pair by 15 seconds when it fails and its connection with the secondary ASBCE server is down.	ASBCE1 public IP@ or public FQDN type A	ASBCE2 public IP@ or public FQDN type A	T1T7 HQ	T1T7 HQ

Integration model applicable to Avaya Aura + ASBCE with: BTIP over Internet (ASBCE public FQDN type SRV or type A)

Head Quarter (HQ)	Level of Service	a-SBC			AS
		SAG Nominal	SAG Backup	Associated T1T7	Site Access
ACM + Single Session Manager (SM)	No redundancy	ASBCE public FQDN type SRV or type A	N/A	T1T7 HQ	T1T7 HQ
ACM + ESS + 2 Session Managers **warning:** - Site access capacity to be sized adequately on the site carrying the 2nd SM in case both SMs are based on different sites	**- ACM redundancy by ESS server in Head Quarter** **- Local redundancy** if both Session Managers (SM) are hosted by the same site OR **- Geographical redundancy** if each SM is hosted by 2 different sites (SM1 + SM2) - Both SMs must be in the same region	ASBCE1 public FQDN type SRV or type A	ASBCE2 public FQDN type SRV or type A	T1T7 HQ	T1T7 HQ

Remote Site (RS) architecture**	Level of Service	a-SBC			AS
		SAG Nominal	SAG Backup	SAG Nominal	SAG Backup
Remote site without survivability	No survivability, no trunk redundancy	ASBCE public FQDN type SRV or type A	N/A	T1T7 HQ	T1T7 HQ
LSP	Local site survivability and trunk redundancy via PSTN only	N/A	N/A	T1T7 RS	T1T7 RS
Branch Session Manager	Local site survivability and SIP trunk redundancy	ASBCE public FQDN type SRV or type A	N/A	T1T7 RS	T1T7 RS

All architectures with ASBCE	Level of Service	a-SBC		AS	a-SBC
		SAG Nominal	SAG Backup	SAG Nominal	SAG Backup
Single ASBCE	No redundancy	ASBCE public FQDN type SRV or type A	N/A	T1T7 HQ	T1T7 HQ
ASBCE in **High Availability**: a pair of ASBCE consisting of one SBCE server acting as primary (active) and another one server acting as secondary (standby). Both SBCE servers share the same IP@ (ASBCE VIP@).	Local vendor redundancy with nominal/backup behavior. The 2 SBCE servers can be located on two different geographic sites but Layer 2 connection between servers 150 ms max round Trip is required. Loss of audio for all active calls on primary SBCE by only 1 second when it fails and its connection with the secondary ASBCE server is up. Loss of audio for all active calls on primary SBCE by 15 seconds when it fails and its connection with the secondary ASBCE server is down.	ASBCE public FQDN type SRV or type A	N/A	T1T7 HQ	T1T7 HQ

Multiple ASBCE: two ASBCE (ASBCE1 and ASBCE2) **in Nominal/Backup mode on vendor side.**	Local vendor redundancy with nominal/backup behavior. Both ASBCE are hosted on the same site. Nominal/Backup mode on Orange a-SBC side for incoming trafic to the customer ASBCE. Loss of active calls handled by the ASBCE that fails.	ASBCE1 public FQDN type SRV or type A	ASBCE2 public FQDN type SRV or type A	T1T7 HQ	T1T7 HQ
	Geographical vendor redundancy with nominal/backup behavior. The two ASBCE are hosted on 2 different geographic sites. Nominal/Backup mode on Orange a-SBC side for incoming trafic to the customer ASBCE. Loss of active calls handled by the ASBCE that fails.				
Multiple ASBCE in High Availability: two ASBCE pairs in **High Availabity and in Nominal/Backup mode on vendor side**. One ASBCE1 pair (2 ASBCE servers) with shared ASBCE1 VIP@ and one ASBCE2 pair (2 ASBCE servers) with shared ASBCE2 VIP@).	Local/geographical redundancy. The two ASBCE pairs are hosted on the same site or on 2 different geographic sites. Nominal/Backup mode on Orange a-SBC side for incoming trafic to the customer ASBCE pairs. If a full ASBCE pair fails, active calls are lost. Loss of audio for all active calls on primary SBCE of a pair by only 1 second when it fails and its connection with the secondary ASBCE server is up. Loss of audio for all active calls on primary SBCE of a pair by 15 seconds when it fails and its connection with the secondary ASBCE server is down.	ASBCE1 public FQDN type SRV or type A	ASBCE2 public FQDN type SRV or type A	T1T7 HQ	T1T7 HQ

6 Certified software and hardware versions

6.1 Global Release Policy

Orange supports the last 2 major IPBX versions and will ensure Business Talk and BTIP infrastructure evolutions will rightly interwork with the related architectures. Orange will assist customers running supported IPBX versions and facing issues.

Please refer to the Avaya web portal for more details about the supported versions.

6.2 Certified Avaya Aura versions

IPBX Avaya Aura – certified software versions Business Talk IP (SIP trunk) -

Equipment Reference	Software version	Certification pronounced	Certified Loads / Key Points
Avaya Aura Communication Manager Note: To avoid any security risk the clients should always install on ACM the latest mandatory patch/hotfix released by the Avaya vendor.	10.2.0.1.1	✓	02.0.229.0-28126
	10.1 FP3	✓	01.0.974.0-27867
	8.1 FP3 SP3	✓	01.0.890.0-27168
Avaya Aura System Manager Note: To avoid any security risk the clients should always install on ASM the latest mandatory patch/hotfix released by the Avaya vendor.	10.2.0.1	✓	10.2.0.1_r1020116918
	10.1 FP3	✓	10.1.3.0_r1013015713
	8.1 FP3 SP3 hotfix1	✓	R8.1.3.3_HotFix1_813313878
Avaya Aura Session Manager Note: To avoid any security risk the clients should always install on ASMGR the latest mandatory patch/hotfix released by the Avaya vendor.	10.2.0.1	✓	10.2.0.1.1020108
	10.1 FP3	✓	10.1.3.0.1013007
	8.1 FP3 SP3	✓	8.1.3.3.813310
Avaya Aura Session Border Controller for Entreprise Note: To avoid any security risk the clients should always install on ASBCE the latest mandatory patch/hotfix released by the Avaya vendor.	10.2.0.1	✓	10.2.0.1-89-24401
	10.1 hotfix 4	✓	10.1.0.0-34-23231-hotfix-04272023
	8.1.3.0 hotfix 3	✓	8.1.3.0-38-21467-hotfix-12302021

6.3 Certified applications and devices

IPBX Avaya Aura – Avaya ecosystems tested (SIP trunk) -

Equipment Reference		Software Version	Pronounced validation
Attendant	Equinox Attendant client and Equinox Attendant Snap-in on Breeze	5.2.13.0.18	✓
Breeze	Avaya Breeze	3.7.0.0	✓
File server	Avaya Aura Device Services	10.1.0.0	✓
Phones / Softphones	9600 SIP (9601, 9608, 9608G, 9611G, 9621G, 9641G, 9641GS)	7.1.15.0	✓
	9600 H.323 (9608, 9608G, 9611G, 9621G, 9641G, 9641GS)	6.8.3	✓
	1600 H.323 (1603, 1603C, 1603SW, 1603SW-I, 1603-I,1608, 1608-I,1616, 1616-I)	1.3.12	✓
	J100 SIP phone (J129, J139, J169, J179)	4.0.12.1	✓
	B169 DECT conference	2.0.0	✓
	B179 SIP conference	2.4.4.3	✓
	B189 H323 conference	6.8.3.04	✓
	IP DECT phones 37xx: (3725, 3745, 3749)	4.3.32	✓
	Vantage	3.8.5	✓
	Workplace for Windows	3.37.0.156	✓
	IX Workplace for Android (previously Equinox for Android)	3.8.5	✓
	IX Workplace for iOS (previously Equinox for iOS)	3.8.9	✓
	H200 SIP phone (H229, H239, H249)	2.5.6.5670	✓
IP DECT	IP DECT Base Station v2	10.2.9	✓
Voice Mail	Avaya Aura Messaging	7.1 SP3	✓
Media Gateway	G450	43.13.0	✓
		42.22.0	✓

		41.34.3	✓
	G430	43.13.0	✓
		42.22.0	✓
		41.34.3	✓
Fax	Analog media module MM711 on Avaya Media Gateway G450/G430 Remark: this card does not support V17 transmission but only V27 and V29 with max speed up to 9kbps in T.38 **WARNING !** Fax transport with Avaya Aura and associated G430/450 gateways is NOTfully supported, because it doesn't comply with the Business Talk/BTIP SIP profile. Fax transmissions MAY fail depending on the termination carrier. Therefore Orange Business Services strongly recommends to NOT deploy fax over IP with Avaya G430/450 analog gateways	HW 31 FW 103	✗
Media Server	Avaya Aura Media Server	10.1 SP7	✓
		10.1 SP2	✓
		8.0.2 SP1	✓

7 SIP trunking configuration checklist

7.1 Basic configuration

This chapter indicates the mandatory configuration steps on Avaya Communication Manager 8.1 + Avaya Session Manager 8.1 + Avaya Session Border Controller for Enterprise 8.1 for the SIP trunking with Business Talk IP / Business Talk.

7.2 Communication Manager

After the installation of ACM it does not have a translation (xln file under /etc/opt/defty) resulting in the add/change commands are not available on the Site Administration Terminal. It is a must to save translation and restart ACM to make that configuration commands available.

Note: To save translation and restart ACM log in to ACM through Site Administration Terminal (SAT) and type *save translation all* and *reset system 4.*

Processor Ethernet settings	
`add ip-interface procr`	Enable interface: y Network Region: 1
Media Gateway settings	
`add media-gateway 1`	Page 1 ▪ Type: g450 (in case g450) ▪ Name: HQ-REGION ▪ Serial No: (serial number of MG) ▪ Network Region: 1 Page 2 ▪ V1: MM710 DS1 MM ▪ V9:gateway-announcements ANN VMM Note: slots configuration will depend on physical location of modules
Node Names settings	
`change node-names ip`	Appropriate node names have to be set, it includes: ▪ ASM1, ASM2 Media Server 6.200.66.10 ASM 1 6.3.27.20 ASM2 6.3.27.30 ESS-HQ124 6.1.24.2 IPBS 6.1.24.214 LSP-RS66 6.200.66.1 default 0.0.0.0 procr 6.1.24.1
Codec Set settings – G711 offer (G.722 optional)	

`change ip-codec-set 1`	Audio codec 1 : G722-64K Frames Per Pkt 1: 2 Packet Size(ms) 1: 20 Audio codec 2 : G711A (or G711MU) Silence Suppression 2 : n Frames Per Pkt 2: 2 Packet Size(ms) 2: 20 Media Encryption 1: none
`change ip-codec-set 2`	Page 1: Audio codec 1: G722-64K Frames Per Pkt 1: 2 Packet Size(ms) 1: 20 Audio codec 2 : G711A (or G711MU) Silence Suppression 2 : n Frames Per Pkt 2: 2 Packet Size(ms) 2: 20 Media Encryption 1: none Note: To enable fax transmission edit the second page Page 2: FAX: - Mode: t.38 -standard - Redundancy : 2 - ECM : y
Codec Set settings – G729 offer	
`change ip-codec-set 1`	Audio codec 1: G722-64K Frames Per Pkt 1: 2 Packet Size(ms) 1: 20 Audio codec 2 : G711A (or G711MU) Silence Suppression 2 : n Frames Per Pkt 2: 2 Packet Size(ms) 2: 20 Audio codec 3 : G729a Silence Suppression 3 : n Frames Per Pkt 3: 2 Packet Size(ms) 3: 20 Media Encryption 1: none Note: Codec G.729a must be set as a third codec so as the system would correctly use resources for MOH and conference when call is established with SIP phone over sip trunk.
`change ip-codec-set 2`	Page 1: Audio codec 1 : G729a Silence Suppression 1 : n Frames Per Pkt 1: 2 Packet Size(ms) 1: 20 Media Encryption 1: none

	Note: To enable fax transmission edit the second page Page 2: FAX: ▪ Mode: t.38 -standard ▪ Redundancy : 2 ▪ ECM : y
Locations	
change locations *(number between 1-2000)*	configure appropriate locations: ▪ HQ – 1 ▪ RSxx – xx ▪ VoIP – 10 Note: to use multiple Locations enable parameter Multiple Locations on ACM web manager interface: Administration → Licensing → Feature Administration → Multiple Locations configure appropriate Loc Parm (Location Parameters) for each location: ▪ HQ – 1 ▪ RSxx – 1 ▪ VoIP – 1
Location Parameters	
change location-parameters *(number between 1-50)*	International Access Code: 00 Local E.164 Country Code: 33 Note: To use multiple Location Parameters enable parameter Multinational Locations on the ACM web manager interface: Administration → Licensing → Feature Administration → Multinational Locations
Network Regions	
change ip-network-region 1 (Used for HQ region)	Page 1: ▪ Region: 1 ▪ Location: 1 ▪ Name: HQ-REGION ▪ Authoritative Domain: e.g. labobs.com ▪ Codec Set: 1 ▪ Intra-region IP-IP Direct Audio: yes ▪ Inter-region IP-IP Direct Audio: yes ▪ UDP Port Min: 16384 ▪ UDP Port Max : 32767 DIFFSERV/TOS PARAMETERS ▪ Call Control PHB Value: **46** ▪ Audio PHB Value: **46** ▪ Video PHB Value: 34 Page 4: ▪ dst rgn: 10, codec set: 2, direct WAN: n, Intervening Regions: 250 ▪ dst rgn: 66, codec set: 2, direct WAN: n, Intervening Regions: 250 ▪ dst rgn: 250, codec set: 2, direct WAN: y

change ip-network-region 66 (Used for RS region)	Page 1: - Region: 66 - Location: 66 - Name: RS-REGION - Authoritative Domain: e.g. labobs.com - Codec Set: 1 - Intra-region IP-IP Direct Audio: yes - Inter-region IP-IP Direct Audio: yes - UDP Port Min: 16384 - UDP Port Max : 32767 DIFFSERV/TOS PARAMETERS - Call Control PHB Value: **46** - Audio PHB Value: **46** - Video PHB Value: 34 Page 4: - dst rgn: 1, codec set: 2, direct WAN: n, Intervening Regions: 250 - dst rgn: 10, codec set: 2, direct WAN: n, Intervening Regions: 250 - dst rgn: 250, codec set: 2, direct WAN: y
change ip-network-region 10 (Used for VoIP region)	Page 1: - Region: 10 - Location: 10 - Name: VOIP - Authoritative Domain: e.g. labobs.com - Codec Set: 2 - Intra-region IP-IP Direct Audio: yes - Inter-region IP-IP Direct Audio: yes - UDP Port Min: 16384 - UDP Port Max : 32767 DIFFSERV/TOS PARAMETERS - Call Control PHB Value: **46** - Audio PHB Value: **46** - Video PHB Value: 34 Page 4: - dst rgn: 1, codec set: 2, direct WAN: n, Intervening Regions: 250 - dst rgn: 66, codec set: 2, direct WAN: n, Intervening Regions: 250 - dst rgn: 250, codec set: 2, direct WAN: y

change ip-network-region 250 (Used for Intervening region) *consult “Configuration Guideline” for other network regions settings	Page 1: ▪ Region: 250 ▪ Location: 1 ▪ Name: HQ-REGION ▪ Authoritative Domain: e.g. labobs.com ▪ Codec Set: 2 ▪ Intra-region IP-IP Direct Audio: yes ▪ Inter-region IP-IP Direct Audio: yes ▪ UDP Port Min: 16384 ▪ UDP Port Max : 32767 DIFFSERV/TOS PARAMETERS ▪ Call Control PHB Value: **46** ▪ Audio PHB Value: **46** ▪ Video PHB Value: 34 Page 4: ▪ dst rgn: 1, codec set: 2, direct WAN: y ▪ dst rgn: 1, codec set: 2, direct WAN: y ▪ dst rgn: 66, codec set: 2, direct WAN: y
Network map	
change ip-network map	Assign IP network ranges to the appropriate network regions. See example below (Page 1): FROM: 6.1.24.0 Subnet Bits: /24 Network Region: 1 VLAN: n TO: 6.1.24.255 FROM: 6.200.66.0 Subnet Bits: /24 Network Region: 66 VLAN: n TO: 6.200.66.255
Signaling group	
change signaling-group (example: change signaling-group 10 add signaling-group 10)	▪ Group Type: sip ▪ Transport Method: TCP (or TLS) ▪ Near-end Node Name: procr ▪ Far-end Node Name: ASM1 ▪ Near-end Listen Port: 5060 (or 5061 if TLS) ▪ Far-end Listen Port: 5060 (or 5061 if TLS) ▪ Far-end Network Region: 10 ▪ Far-end Domain: e.g. labobs.com ▪ DTMF over IP: rtp-payload ▪ Enable Layer 3 Test?: y ▪ H.323 Station Outgoing Direct Media?: y ▪ Direct IP-IP Audio Connections?: y ▪ Initial IP-IP Direct Media?: y ▪ Alternate Route Timer(sec): 20 ▪ Prepend ‘+’ to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?: y ▪ Remove ‘+’ from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?: n

Numbering Plan	
change dialplan analysis	check if digits are correctly collected. Below example: - Dialed String: 0, Total Length: 1, Call Type: fac - Dialed String: 124, Total Length: 7, Call Type: ext - Dialed String: *8, Total Length: 4, Call Type: dac - Dialed String: 8, Total Length: 1, Call Type: fac
change feature-access-codes	check if on-net extensions are routed to AAR table. Example configuration: - Auto Alternate Routing (AAR) Access Code: 8 - Auto Route Selection (ARS) – Access Code 1: 0
change uniform-dialplan 0	Page 1: Matching Pattern: 124, Len: 7, Del: 0, Net: aar, conv: n
change aar analysis	Dialed string: 124, Min: 7, Max: 7, Route Pattern: 10, Call Type: unku
change ars analysis	Dialed string: 00, Min: 2, Max: 20, Route Pattern: 10, Call Type: pubu
Trunk group	
change trunk-group (example: change trunk-group 10/ add trunk-group 10)	Page 1: - Group Number: 10 - Group Type: sip - Group Name: PE-ASM - Direction: two-way - Service Type: tie - Member Assignment Method: auto - Signaling Group: 10 - Number of Members: 255 Page 3: - Numbering Format: private - Hold/Unhold Notifications? n Page 4: - Network Call Redirection? n - Support Request History?: y - Telephone Event Payload Type: 101 - Identity for Calling Party Display: P-Asserted-Identity Note: ACM trunk must have disabled option NCR “Network Call Redirection” to not send the REFER method but re-Invite to complete call transfer.
Route Pattern	
change route-pattern 10	Processor Ethernet: - Grp No: 10, FRL: 0, LAR: next - Grp No: 20, FRL: 0, LAR: next - Grp No: 1, FRL: 0, LAR: none

Calling number format	
change public-unknown-numbering 0	▪ Ext Len: 7, Ext Code: 124, Trk Grp(s) : 10, CPN Prefix: 33296097560, Total CPN Len: 11 ▪ Ext Len: 7, Ext Code: 124, Trk Grp(s) : 20, CPN Prefix: 33296097560, Total CPN Len: 11
change private-numbering 0	▪ Ext Len: 7, Ext Code: 124, Trk Grp(s) : 10, Private Prefix: empty, Total CPN Len: 7 ▪ Ext Len: 7, Ext Code: 124, Trk Grp(s) : 20, Private Prefix: empty, Total CPN Len: 7
Music on Hold configuration	
change location-parameters 1	Companding Mode: A-Law (or Mu-Law)
change media-gateway 1	V9: gateway-announcements ANN VMM
enable announcement-board 001V9	Issue command fo the rest of gateways if applicable: Enable announcement-board <gw_nrV9>

change audio-group 1	`Group Name:` **`MOH`**
	`1:` **`001V9`**
	`2:` **`002V9`** `(if second gateway is configured on CM)`
	`3: M1 (if media server is configured)`

Add announcement 1240666	Issue command with extension on the end: Add announcement <ann_nr> • COR: 1 • Annc Name: moh • TN: 1 • Annc Type: integ-mus • Source: G1 • Protected? N • Rate: 64
change music-sources	1:music Type: ext 124-0666 moh
Enable Disconnect tone for H.323 phones	
change system-parameters features	Station Tone Forward Disconnect: busy
Recovery timers configuration on H.248 Media Gateway	
set reset-times primary-search	Strict value is not defined for Primary Search Timer (H.248 PST). PST is the acceptable maximum time of network disruption i.e. Max. network outage detection time. Could be 4 or 5 min.
set reset-times total-search	Total Search Timer (H.248 TST) recommended value is: H.248 TST = H.248 PST + 1-2 minutes In case of no alternate resources usage it could be: H.248 TST = H.248 PST
Recovery timers configuration on ACM	

`change system-parameters ip-options`	**H.248 Media Gateway Link Loss Delay Timer (H.248 LLDT)** recommended value is: H.248 LLDT = H.248 PST + 1 minute
`change system-parameters ip-options`	**H.323 IP Endpoint Link Loss Delay Timer (H.323 LLDT)** recommended value is: H.323 LLDT = H.248 PST + 1 min
`change system-parameters ip-options`	**H.323 IP Endpoint Primary Search Time (H.323 PST)** recommended value is: H.323 PST = H.248 PST + 30 sec
`change system-parameters ip-options`	Periodic Registration Timer. No strict value defined. Could be 1 min.
`change ip-network-region`	H.323 IP Endpoints • H.323 Link Bounce Recovery **y** • Idle Traffic Interval (sec) **20** • Keep-Alive Interval (sec) **5** • Keep-Alive count (sec) **5**
SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING	
`change system-parameters coverage-forwarding`	Configure mandatory parameter for Voice mail: • QSIG/SIP Diverted Calls Follow Diverted to Party's Coverage Path? **Y**
display system-parameters customer-options	
display system-parameters customer-options	On page 6 Multiple Locations? **Y** To enable this option log in to ACM through web manager and go to Administration → Licensing → Feature administration → Current Settings → Display Under the feature administration menu select ON for the feature "**Multiple Locations?**" then submit this change
System-parameters features	
change system-parameters features	On page 1 to enable transfer over sip trunk set: Trunk-to-Trunk Transfer: **all** On page 19 for transfer initiated by SIP endpoint to force ACM to use re-Invite not Refer method over sip trunk: SIP Endpoint Managed Transfer? **n**
Class of Restriction	
change cor 1	Calling Party Restriction: **none** Called Party Restriction: **none** Note: Fresh installation by default restricts outgoing calls for calling party.

Class of Service	
change cos 1	Enable/disable appropriate services under the Class Of Service 1: e.g. to to allow transfer over the trunk: Trk-to-Trk Transfer Override: y

7.3 Session Manager architecture with ASBCE

Menu	Settings
Network Routing Policy **SIP Domains**	check if correct SIP domain is configured (You need to choose and configure a SIP domain for which a Communication Manager and a Session Manager will be a part of)
Network Routing Policy **Locations**	check if Locations are correctly configured (Session Manager uses the origination location to determine which dial patterns to look at when routing the call if there are dial patterns administered for specific locations)
Network Routing Policy **Adaptations**	check if Adaptation for ASBCE is configured ASBCEAdapter should be used with parameters: odstd=<@IP_ASBCE> iodstd=<SIP Domain> fromto=true eRHdrs=P-AV-Message-ID,Endpoint-View,P-Charging-Vector,Alert-Info,P-Location,AV-Correlation-ID,P-Conference,Accept-Language

Menu	Settings
`Network Routing Policy` `SIP Entities: SM`	Check if SIP Entity for Session Manager is correctly configured. Ensure that following settings are applied: ▪ Type: Session Manager Make sure that for Session Manager's SIP Entity ports and protocols are correctly set. ▪ 5060, TCP (or 5061 if TLS) TCP protocol (or TLS) is used for communication between SM & ASBCE and SM & CMs Make sure under Listen Ports there are correctly set ports, protocols and domain and select the box under the Endpoint tab to "Enable Listen Port for Endpoint Connections" ▪ 5060, UDP, e.g. labobs.com ▪ 5060, TCP, e.g. labobs.com ▪ if used: 5061, TLS, e.g. labobs.com Beside each of the protocol there is also a checkbox under the Endpoint tab to enable listen port for endpoint connections. When checkbox is selected the SIP endpoint can use this protocol for signalization. Protocol priority order (from highest to lowest) is: TLS, TCP, UDP.
`Network Routing Policy` `SIP Entities: ASBCE`	Check if SIP Entity for ASBCE is correctly configured. Ensure that following settings are applied: ▪ Type: SIP Trunk ▪ Adaptation: adaptation module created for ASBCE has to be selected ▪ Location: Location created for ASBCE has to be selected Make sure that for ASBCE SIP Entity ports and protocols are correctly set. ▪ 5060, TCP (or 5061 if TLS) TCP protocol (or TLS) is used for communication between SM & ASBCE..

Menu	Settings
Network Routing Policy **SIP Entities: CM**	Check if SIP Entity for Communication Manager is correctly configured. Ensure that following settings are applied: - Type: CM - Location: Location created for Communication Manager has to be selected Make sure that for Communication Manager SIP Entity ports and protocols are correctly set. - 5060, TCP (or 5061 if TLS) Only TCP protocol (or TLS) is used for communication between CMs & SM.
Network Routing Policy: **Entity Links**	check if all needed Entity Links are created (An entity link between a Session Manager and any entity that is administered is needed to allow a Session Manager to communicate with that entity directly. Each Session Manager instance must know the port and the transport protocol of its entity link to these SIP entities in the network)
Network Routing Policy **Time Ranges**	check if at last one Time Range is configured covering 24/7 (Time ranges needs to cover all hours and days in a week for each administered routing policy. As time based routing is not planned we need to create only one time range covering whole week 24/7)
Network Routing Policy **Routing Policies**	check if routing policies are configured: - towards ASBCE - towards each Communication Manager hub
Network Routing Policy **Dial Patterns**	check if proper dial patterns are configured (Routing policies determine a destination where the call should be routed. Session Manager uses the data configured in the routing policy to find the best match (longest match) against the number of the called party)
Session Manager **Device and Location** **Device Settings Group**	DIFFSERV / QOS Parameters Call Control PHB Value: 46 Audio PHB Value: 46

7.4 Avaya Session Border Controller for Enterprise

7.4.1 BT/BTIP SIP trunk configuration

Below table presents ASBCE configuration required to set up BT/BTIP SIP trunk.

Device Management → Licensing		
External WebLM Server URL	https://<SMGR_server_IP>:52233/WebLM/LicenseServer or https://<SMGR_server_domain_name>:52233/WebLM/LicenseServer e.g. https://6.5.53.232:52233/WebLM/LicenseServer or https://smgr80.warsaw.lab:52233/WebLM/LicenseServer	
Device Management -> Devices -> select appropriate asbce -> Edit -> Next -> Next -> Dynamic License Settings		
Since version 10.2.1 of ASBCE, Avaya implemented license pool management. Licenses must be allocated on each ASBCE for features to allow calls over SIP trunk.		
Displayed "Available" value is acquired from WebLM and depends on the purchased licenses quantity available on WebLM	MIN License Allocation (must be allocated at least one if available quantity is higher than 0)	MAX License Allocation (can be allocated up to available quantity)
Standard Session Available: e.g. 60	1	60
Advanced Session Available: e.g. 30	1	30
Transcoding Session Available: e.g. 30	1	30
Premium Session Available: e.g. 6	1	6
Encryption Available: Yes/No	Checked / Unchecked	
Device Management → Devices → Install		
Device Configuration Appliance Name	This name will be referenced in other configuration e.g. avaya-sbce	
DNS Configuration Primary	e.g. 6.3.14.10	
Network Configuration Name	Interface name toward Session Manager e.g. Int-SBCE-SM	
Network Configuration Default Gateway	e.g. 6.3.27.254	

Network Configuration Subnet Mask or Prefix Length	e.g. 255.255.255.0
Network Configuration Interface	A1 Note: Interface must be enabled on ASBCE virtual machine on ESXi host after installation is complete.
Ip Address 1#	Ip address of the internal ASBCE interface e.g. 6.5.27.61
Network & Flows → Network Management → Networks → Add	
Name	Interface name toward Orange A-SBC e.g. Ext-SBCE-BTIP
Default Gateway	e.g. 172.22.235.30
Network Prefix or Subnet Mask	e.g. 255.255.255.0
Interface	B1 Note: Interface must be enabled on SBCE virtual machine on ESXi host after configuration is complete.
IP Address	Ip address of the external ASBCE interface e.g. 172.22.235.23 Note: Reboot of the ASBCE is required after configuration of the ip addresses.
Network & Flows → Signaling Interface → Add	
Name	Create a signaling interface for the internal side of the ASBCE e.g. Sign_Int_SBCE-SM
Ip Address	Select ASBCE internal interface and associated ip address defined in previous step. Int_SBCE-SM (A1, VLAN 0) 6.5.27.61
TCP port	This is the port on which ASBCE will listen to SIP messages from Session Manager. 5060 Remark: TCP protocol is used for communication between ASBCE & Session Manager.
Network & Flows → Signaling Interface → Add	
Name	Create a signaling interface for the external side of the ASBCE e.g. Sign_Ext_SBCE-BTIP
Ip Address	Select ASBCE external interface and associated ip address defined in previous step. Ext_SBCE-BTIP (B1, VLAN 0) 172.22.235.23
UDP port	This is the port on which ASBCE will listen to SIP messages from Orange A-SBC. 5060 Remark: UDP protocol is used for communication between ASBCE & Orange A-SBC.
Network & Flows → Advanced Options → Port Ranges	
Signaling Port Range	Decrease default ASBCE port range to allocate them to required by Orange BTIP SIP Trunk. Set: 12000-16000

Config Proxy Internal Signaling Port Range	Remove default ASBCE port range to allocate them to required by Orange BTIP SIP Trunk. Set: 50001-51000
Network & Flows → Media Interface → Add	
Name	Create a media interface for the internal side of the ASBCE e.g. Media_Int_SBCE-SM
IP Address	Select ASBCE internal interface and corresponding ip address configured in previous step. Int_SBCE-SM (A1, VLAN 0) 6.5.27.61
Port Range	The Orange BTIP SIP Trunk service specifies that customers use RTP ports in the range of 16384 – 32767. Set this internal media port range to: 16384-32767
Network & Flows → Media Interface → Add	
Name	Create a media interface for the external side of the ASBCE e.g. Media_Ext_SBCE-BTIP
IP Address	Selec ASBCE external interface and corresponding ip address configured in previous step. Ext_SBCE-BTIP (B1, VLAN 0) 172.22.235.23
Port Range	The Orange BTIP SIP Trunk service specifies that customers use RTP ports in the range of 16384 – 32767. Set this external media port range to: 16384-32767
Configuration Profiles → Server Interworking → Add	
Profile Name	SBCE-SM
General Leave default parameters and ensure following parameters are selected:	
Hold Support	None
T.38 Support For fax transmission over VISIT SIP trunk enable T.38 support.	Checked
URI Scheme	SIP
Via Header Format	RFC3261
SIP Timers Leave default parameters.	
Privacy Leave default parameters.	
Interworking Profile Advanced parameters	
Record Routes	Both Sides
Extensions	Avaya
DTMF	
DTMF Support	Avaya sip phones or Avaya Gateways G430/450 send DMFs over RTP according to RFC4733 (obsolete RFC2833). Avaya Session Border Controller Enterprise terminates RTP flow so to not change DTMFs to SIP Info or SIP Notify Methods the option None must be selected in order to indicate the support of DTMF through RFC2833.

Configuration Profiles → Server Interworking → Add	
Profile Name	SBCE-BTIP
General Leave default parameters and ensure following parameters are selected:	
Hold Support	None
T.38 Support For fax transmission over VISIT SIP trunk enable T.38 support.	Checked
URI Scheme	SIP
Via Header Format	RFC3261
SIP Timers Leave default parameters except:	
Trans Expire	We recommend to set Trans Expire parameter to15 seconds to enable rerouting to second sip trunk by ASBCE, in case of unavailability of the first one. ACM has a timeout set on sip signaling group to 20 seconds after it reroutes to second ASM in case of no answer on firs sip trunk. 15
Transport Timers Leave default parameters.	
Privacy Leave default parameters.	
Interworking Profile Advanced parameters	
Record Routes	Both Sides
Extensions	None
DTMF	
DTMF Support	Avaya sip phones or Avaya Gateways G430/450 send DMFs over RTP according to RFC4733 (obsolete RFC2833). Avaya Session Border Controller Enterprise terminates RTP flow so to not change DTMFs to SIP Info or SIP Notify Methods the option None must be selected in order to indicate the support of DTMF through RFC2833.
Configuration Profiles → Server Interworking → SBCE-BTIP → Header Manipulation → Add	
Header	Select Contact
Action	Select Remove Parameter w/ [Value]
Parameter	gsid
Value **Leave blank for wildcard**	Leave blank
Configuration Profiles → Server Interworking → SBCE-BTIP → Header Manipulation → Add	
Header	Select Contact
Action	Select Remove Parameter w/ [Value]
Parameter	asm

Value **Leave blank for wildcard**	Leave blank
Configuration Profiles → Server Interworking → SBCE-BTIP → Header Manipulation → Add	
Header	Select Contact
Action	Select Remove Parameter w/ [Value]
Parameter	epv
Value **Leave blank for wildcard**	Leave blank
Services → SIP Servers → Add	
Profile Name	Define profile for far away server: Session Manager. Prof_SBCE-SM
General	
Server Type	Call Server
SIP Domain	Leave empty
TLS Client Profile	none
IP Address / FQDN	Add all Session Managers (Primary and Backup and Branch Session Manager if exists). e.g. 6.5.53.20 e.g. 6.5.53.30 e.g. 6.202.81.20
Port	This is the port on which Session Manager will listen to SIP messages from Avaya SBCE. 5060
Transport	Protocol used for SIP signaling between Session Manager and the Avaya SBCE. TCP
Authentication Leave all fields blank.	
Heartbeat Configure Heartbeat to send Options to monitor status of a trunk toward Session Manager server (Primary and Backup and Branch Session Manager if exists) defined in previous step.	
Enable Heartbeat	Checked
Method	OPTIONS
Frequency	90
From URI	ping@6.5.27.61
To URI	ping@warsaw.lab
Ping Leave all fields blank.	
Advanced Leave default fields except following:	
Enable Grooming	With Grooming enabled the system can reuse the same connections for the same subscriber or port. Select checkbox

Interworking Profile	Select the Interworking Profile for Session Manager defined previously. SBCE-SM
Services → SIP Servers → Add	
Profile Name	Define profile for far away server: Orange A-SBC. Prof_SBCE-BTIP
Server Type	Trunk Server
TLS Client Profile	none
IP Address / FQDN	Add all Orange A-SBC servers (primary and backup if exists). e.g. 172.22.246.33 e.g. 172.22.246.73
Port	This is the port on which Orange A-SBC will listen to SIP messages from Avaya SBCE. 5060
Transport	Protocol used for SIP signaling between Orange BTIP SIP trunk service (i.e. Orange SBC primary and backup) and the Avaya SBCE. UDP
Authentication Leave all fields blank.	
Heartbeat Configure Heartbeat to send Options to monitor status of a trunk toward the Orange A-SBC (Primary and Backup if exists) defined in previous step.	
Enable Heartbeat	Checked
Method	OPTIONS
Frequency	90
From URI	ping@172.22.235.23
To URI	ping@orange.sbc
Ping Leave all fields blank.	
Advanced	Leave default fields except following:
Enable Grooming	Unchecked
Interworking Profile	Select the Interworking Profile for Orange BTIP SIP trunk service defined previously. SBCE-BTIP
Configuration Profiles → Signaling Manipulation → Add	
Title	Remove parameter from Contact

```
/*Script to remove attribute (+avaya-cm-keep-mpro) from Contact Header */
within session "INVITE"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
   {
     if (exists(%HEADERS["Contact"][1].PARAMS["+avaya-cm-keep-mpro"])) then
      {
        remove(%HEADERS["Contact"][1].PARAMS["+avaya-cm-keep-mpro"]);
      }
   }
}
```

Services → SIP Servers → Prof_SBCE-BTIP → Advanced → Edit	
Interworking Profile	Interworking Profile for Orange BTIP SIP trunk service. SBCE-BTIP
Signaling Manipulation Script	Select created previously script name: Remove parameter from Contact
Domain Policies → Application Rules → default-trunk → Application Rule	
Audio	Regulate the number of audio sessions that are allowed for each trunk server, or a call server. Select checkboxes: In Out
Domain Policies → Media Rules → default-low-med → Encryption	
Audio Encryption	
Preferred Formats	RTP
Interworking	Checked
Domain Policies → Media Rules → default-low-med → Advanced	
Leave all checkboxes unselected.	
Domain Policies →Media Rules → default-low-med → QoS → Edit	
Media QoS Marking	
Enabled	Checked
QoS Type	DSCP
Audio QoS	
Audio DSCP	EF
Domain Policies → Signaling Rules → Add	
Rule Name	e.g. SigR_SBCE-SM
Inbound Leave default parameters.	
Outbound Leave default parameters.	
Content-Type Policy	
Enable Content-Type Checks	**Checked**
Action	**Allow**

Multipart Action	Allow
Domain Policies → Signaling Rules → SigR_SBCE-SM → Response Headers → Add In Header Control	
Proprietary Response Header	Checked
Header Name	Av-Global-Session-ID
Response Code	1XX
Method Name	ALL
Header Criteria	Forbidden
Presence Action	Remove header
Domain Policies → Signaling Rules → SigR_SBCE-SM → Response Headers → Add In Header Control	
Proprietary Response Header	Checked
Header Name	Av-Global-Session-ID
Response Code	2XX
Method Name	ALL
Header Criteria	Forbidden
Presence Action	Remove header
Domain Policies → Signaling Rules → SigR_SBCE-SM → Response Headers → Add In Header Control	
Proprietary Response Header	Checked
Header Name	Av-Global-Session-ID
Response Code	4XX
Method Name	ALL
Header Criteria	Forbidden
Presence Action	Remove header
Domain Policies → Signaling Rules → SigR_SBCE-SM → Response Headers → Add In Header Control	
Proprietary Response Header	Unchecked
Header Name	User-Agent
Response Code	1XX
Method Name	INVITE

Header Criteria	Forbidden
Presence Action	Remove header
Domain Policies → Signaling Rules → SigR_SBCE-SM → Response Headers → Add In Header Control	
Proprietary Response Header	Unchecked
Header Name	User-Agent
Response Code	2XX
Method Name	INVITE
Header Criteria	Forbidden
Presence Action	Remove header
Domain Policies → Signaling Rules → SigR_SBCE-SM → Signaling QoS	
Enabled	Checked
DSCP	Selected
Value	EF
Domain Policies → Signaling Rules → SigR_SBCE-SM → UCID	
Enabled	Unchecked
Node ID	Leave default field blank.
Protocol Discriminator	Leave default field.
Domain Policies → Signaling Rules → SigR_SBCE-SM → Requests → Add In Request Control	
Proprietary Request	Unchecked
Method Name	OPTIONS
In Dialog Action	Allow
Out of Dialog Action	Select Block with and type in first field 200 then in next field OK
Domain Policies → Signaling Rules → Add	
Rule Name	e.g. SigR_SBCE-BTIP
Inbound Leave default parameters.	
Outbound Leave default parameters.	
Content-Type Policy	
Enable Content-Type Checks	Checked

Action	Allow
Multipart Action	Allow
Domain Policies → Signaling Rules → SigR_SBCE-BTIP → Request Headers → Add Out Header Control	
Proprietary Request Header	Checked
Header Name	Av-Attendant
Method Name	INVITE
Header Criteria	Forbidden
Presence Action	Remove header
Domain Policies → Signaling Rules → SigR_SBCE-BTIP → Request Headers → Add Out Header Control	
Proprietary Request Header	Checked
Header Name	Av-Global-Session-ID
Method Name	ALL
Header Criteria	Forbidden
Presence Action	Remove header
Domain Policies → Signaling Rules → SigR_SBCE-BTIP → Request Headers →Add Out Header Control	
Proprietary Request Header	Checked
Header Name	Max-Breadth
Method Name	INVITE
Header Criteria	Forbidden
Presence Action	Remove header
Domain Policies → Signaling Rules → SigR_SBCE-BTIP → Request Headers → Add Out Header Control	
Proprietary Request Header	Checked
Header Name	P-Location
Method Name	ALL
Header Criteria	Forbidden
Presence Action	Remove header
Domain Policies → Signaling Rules → SigR_SBCE-BTIP → Request Headers → Add Out Header Control	

Proprietary Request Header	Unchecked
Header Name	Reason
Method Name	INVITE
Header Criteria	Forbidden
Presence Action	Remove header
Domain Policies → Signaling Rules → SigR_SBCE-BTIP → Signaling QoS	
Enabled	Checked
DSCP	Selected
Value	EF
Domain Policies → Signaling Rules → SigR_SBCE-BTIP → UCID	
Enabled	Unchecked
Node ID	Leave default field blank.
Protocol Discriminator	Leave default value.
Domain Policies → Signaling Rules → SigR_SBCE-BTIP → Request → Add In Request Control	
Proprietary Request	Unchecked
Method Name	OPTIONS
In Dialog Action	Allow
Out of Dialog Action	Select Block with and type in first field 200 then in next field OK
Domain Policies → End Point Policy Groups → Add	
Group Name	e.g. EPPG_SBCE-SM
Domain Policies → End Point Policy Groups → EPPG_SBCE-SM → Edit Policy Set	
Application Rule	default-trunk
Border rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	select created previously: SigR_SBCE-SM
Domain Policies → End Point Policy Groups → Add	
Group Name	e.g. EPPG_SBCE-BTIP

Domain Policies → End Point Policy Groups → EPPG_SBCE-BTIP → Edit Policy Set	
Application Rule	default-trunk
Border rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	select created previously: SigR_SBCE-BTIP
Configuration Profiles → Routing → Add	
Profile name	e.g. Routing-to-SM
Configuration Profiles → Routing → Routing-to-SM	
Uri Group	*
Load Balancing	Priority
Transport	None
Next Hop In-Dialog	Unchecked
ENUM	Unchecked
Time of Day	default
NAPTR	Unchecked
Next Hop Priority	Checked
Ignore Route Header	Unchecked
ENUM Suffix	Leave this field blank.
Priority / Weight	1
SIP Server Profile	Select previously created: Prof_SBCE-SM
Next Hop Address	Select IP address of the Session Manager Primary e.g. 6.5.53.20: 5060 (TCP)
Priority / Weight	2
SIP Server Profile	Select previously created: Prof_SBCE-SM
Next Hop Address	Select IP address of the Session Manager Backup if exists e.g. 6.5.53.30: 5060 (TCP)
Priority / Weight	3
SIP Server Profile	Select previously created: Prof_SBCE-SM
Next Hop Address	Select IP address of the Branch Session Manager if exists e.g. 6.202.81.20: 5060 (TCP)

Configuration Profiles → Routing → Add	
Profile	e.g. Routing-to-BTIP
Configuration Profiles → Routing → Routing-to-BTIP	
Uri Group	*
Load Balancing	Priority
Transport	None
Next Hop In-Dialog	Unchecked
ENUM	Unchecked
Time of Day	default
NAPTR	Unchecked
Next Hop Priority	Checked
Ignore Route Header	Unchecked
ENUM Suffix	Leave this field blank.
Priority / Weight	1
SIP Server Profile	Select previously created: Prof_SBCE-BTIP
Next Hop Address	Select IP address of the Orange A-SBC Primary e.g. 172.22.246.33: 5060 (UDP)
Priority / Weight	2
SIP Server Profile	Select previously created: Prof_SBCE-BTIP
Next Hop Address	Select IP address of the Orange A-SBC Backup if exists e.g. 172.22.246.73: 5060 (UDP)
Configuration Profiles → Topology Hiding → Add	
Profile Name	This profile will be applied for the traffic from the Avaya SBCE to Session Manager. e.g. THP_SBCE-SM
Configuration Profiles → Topology Hiding → Topology Hiding Profile → Add Header	
Header	For all headers set the following parameters:
Criteria	IP/Domain
Replace Action	Auto
Configuration Profiles → Topology Hiding → Add	
Profile Name	This profile will be applied for the traffic from the Avaya SBCE to Orange Business Services. e.g. THP_SBCE-BTIP

Configuration Profiles → Topology Hiding → Topology Hiding Profile → Add Header	
Header	For all headers set the following parameters except the header From:
Criteria	IP/Domain
Replace Action	Auto
Replace Action for the header **From**	Overwrite
Overwrite Value for the header **From**	e.g. warsaw.lab
Network & Flows → End Point Flows → Server Flows → Add	
Flow Name	Traffic from Orange A-SBC through Avaya SBCE toward Session Manager: e.g. EPF_SBCE-SM
SIP Server Profile	Select previously configured profile: Prof_SBCE-SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Select the external signaling interface Sign_Ext_SBCE-BTIP
Signaling Interface	Select the internal signaling interface Sign_Int_SBCE-SM
Media Interface	Select the internal media interface Media_Int_SBCE-SM
Secondary Media Interface	None
End Point Policy Group	Select the endpoint policy group defined previously EPPG_SBCE-SM
Routing Profile	Select the routing profile to direct traffic to BTIP SIP trunk Routing-to-BTIP
Topology Hiding Profile	Select the topology hiding profile defined for Session Manager THP_SBCE-SM
Signaling Manipulation Script	None
Remote Branch Office	Any
Network & Flows → End Point Flows → Server Flows → Add	
Flow Name	Traffic from Session Manager through Avaya SBCE toward Orange A-SBC: e.g. EPF_SBCE-BTIP
SIP Server Profile	Select previously configured profile: Prof_SBCE-BTIP
URI Group	*
Transport	*
Remote Subnet	*

Received Interface	Select the internal signaling interface Sign_Int_SBCE-SM
Signaling Interface	Select the external signaling interface Sign_Ext_SBCE-BTIP
Media Interface	Select the external media interface Media_Ext_SBCE-BTIP
Secondary Media Interface	None
End Point Policy Group	Select the endpoint policy group defined previously EPPG_SBCE-BTIP
Routing Profile	Select the routing profile to direct traffic to Session Manager Routing-to-SM
Topology Hiding Profile	Select the topology hiding profile defined for BTIP SIP trunk THP_SBCE-BTIP
Signaling Manipulation Script	None
Remote Branch Office	Any

Media Unanchoring	
Domain Policies → Session Policies → default → clone	
Name	Change name to e.g. UnAnchor for media bypass or Anchor for media anchoring
Media Anchoring	Unchecked for media bypass or Checked for media anchoring
Media Forking Profile	None
Converged Conferencing	Unchecked
Call Type for Media Unanchoring	All
Network & Flows → Session Flows → Add	
Flow Name	e.g. UnAnchor for media bypass e.g. Anchor for media anchoring
URI Group#1	*
URI Group#2	*
Subnet#1 **Ex: 192.168.0.1/24**	*
SBC IP Address	* *
Subnet#2 **Ex: 192.168.0.1/24**	*
SBC IP Address	* *

Session Policy	Select previously configured Session Policy e.g. UnAnchor or Anchor
Has Remote SBC	Unchecked

7.4.2 BToI/BTIPoI SIP trunk configuration

Below table focuses on **BToI/BTIPoI** SIP trunk configuration on ASBCE indicating the required update of configuration in addition to already implemented **BT/BTIP** configuration described in previous chapter.

TLS Management → Certificates → Create CSR	
Country Name	e.g. FR
State/Province Name	e.g. Bretagne
Locality Name	e.g. Rennes
Organization Name	e.g. Orange
Organizational Unit	e.g. Orange Business Services
Common Name	FQDN assigned to ASBCE public ip address. CN domain name must be resolved on public DNS. Allowed characters in the CN are alphanumeric and hypen [-]. Special characters must not be used. e.g. external.domain.com
Algorithm	SHA256
Key Size (Modulus Length)	e.g. 2046 bits
Key Usage Extension(s)	Checked Key encipherment Checked Non-Repudiation Checked Digital Signature
Extended Key Usage	Checked Server Authentication Checked Client Authentication
Subject Alt Name	FQDN for SAN is the same as for CN. e.g. DNS:external.domain.com
Passphrase **Confirm Passphrase**	Allowed characters are alphanumeric and special character but Avaya recommends not to use the dollar sign ($) in Key Passphrase Specify the passphrase to encrypt the private key.
Contact Name	e.g. Mike
Contact E-Mail	Email address
TLS Management → Certificates → Install	
Type	Select Certificate
Name	This field is optional. Can be left blank.
Overwrite Existing	Unchecked
Allow Weak Certificate/Key	Unchecked

Certificate File	Upload the Identity certificate file.
Trust Chain File	Upload Trust Chain file. If the third party CA provided separate Root CA and Intermediate certificates for ASBCE, you must combine both files into a single certificate file (trust chain file). To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end.
Key	Ensure that the Common Name used during generation of CSR matches with the file name of the identity certificate being installed. Select Use Existing Key
Key File	Select from a drop down list existing key file.
TLS Management → Certificates → Install	
Type	Select CA Certificate
Name	This field is optional. Can be left blank.
Overwrite Existing	Unchecked
Allow Weak Certificate/Key	Checked
Certificate File	Upload the public CA root & intermediate certificates file (trust chain file) of the remote entity (Orange A-SBC).
TLS Management → Server Profile → Add	
Profile Name	e.g. ThirdPartyServer
Certificate	Select installed ASBCE Identity certificate
SNI Options	None
Peer Verification	Required
Peer Certificate Authorities	Select public CA root & intermediate certificates file (trust chain file) of the remote entity (Orange A-SBC).
Verification Depth	Depends of the number of bundled certificates. In case the third party CA provided separate Root CA and Intermediate certificates for the Orange A-SBC that were bundled into one file the value will be set to number 2.
Version	Check TLS 1.3 or TLS 1.2
Ciphers	Select: Default
TLS Management → Client Profile → Add	
Profile Name	e.g. ThirdPartyClient
Certificate	Select installed ASBCE Identity certificate
SNI Options	Unchecked Enabled
Peer Certificate Authorities	Select public CA root & intermediate certificates file (trust chain file) of the remote entity (Orange A-SBC).

Verification Depth	Depends of the number of bundled certificates. In case the third party CA provided separate Root CA and Intermediate certificates for the Orange A-SBC that were bundled into one file the value will be set to number 2.
Extended Hostname Verification	Unchecked
Version	Check TLS 1.3 or TLS 1.2
Ciphers	Select: Default
Network & Flows → Network Management → Networks → Edit	
Name	Interface name toward Orange A-SBC e.g. Ext-SBCE-BTIP
Default Gateway	Public IP address.
Network Prefix or Subnet Mask	Network prefix or subnet mask.
Interface	B1
IP Address	Public Ip address of the external ASBCE interface.
Public IP	Leave blank
Gateway Override	Leave blank
Network & Flows → Signaling Interface → Edit	
Name	Signaling interface of the external side of the ASBCE. e.g. Sign_Ext_SBCE-BTIP
Ip Address	ASBCE external interface and associated public ip address defined in previous step. Ext_SBCE-BTIP (B1, VLAN 0) Public IP address
TLS port	This is the port on which ASBCE will listen to SIP messages from Orange A-SBC. 5061 Remark: TLS protocol is used for communication between ASBCE & Orange A-SBC.
TLS Profile	Select from a drop down list created previously server profile: ThirdPartyServer
Services → SIP Servers → Edit	
Profile Name	Edit/add profile for the far end server: Orange A-SBC. Prof_SBCE-BTIP
Server Type	Trunk Server
SIP Domain	Leave blank

DNS Query Type	DNS type Service Record (SRV) allows to query DNS server to receive hostname, priority, port of the target servers. Alternatively you can configure ip address or DNS Query Type A. SRV NONE/A BTIPoI supports type SRV & type A for DNS resolution and do not support direct public IP connections. BToI supports both public IP and type A for DNS resolution and do not provide any type SRV record connections.
TLS Client Profile	Select ThirdPartyClient
FQDN **IP Address / FQDN**	FQDN of the Orange A-SBC if DNS Query Type SRV was configured. IP Address or FQDN of the Orange A-SBC if DNS Query Type None/A was configured.
Port	This is the port on which Orange A-SBC will listen to SIP messages from Avaya SBCE. This value will be received from DNS server in SRV response. If DNS query type A was configured then insert port 5061. Leave blank if DNS Query Type SRV was configured. 5061 if DNS Query Type None/A was configured.
Transport	Protocol used for SIP signaling between ASBCE and Orange A-SBC. It will also result in the ASBCE will add by default SRV type query prefix "_sips._tcp." while querying DNS if DNS Query Type SRV was configured. TLS
Configuration Profiles → Routing → Routing-to-BTIP	
Uri Group	*
Load Balancing	DNS/SRV if DNS Query Type SRV was configured in previous step. Priority if DNS Query Type None/A was configured in previous step.
Transport	None
Next Hop In-Dialog	Unchecked
Time of Day	default
Next Hop Priority	Unchecked if Load Balancing DNS/SRV was configured. Checked if Load Balancing Priority was configured.
Ignore Route Header	Unchecked
ENUM	Unchecked
NAPTR	Unchecked
ENUM Suffix	Leave this field blank.
Priority / Weight	N/A if Load Balancing DNS/SRV was configured. 1 if Load Balancing DNS/A was configured.
SIP Server Profile	Select previously created: Prof_SBCE-BTIP
Next Hop Address	Select FQDN of the Orange A-SBC if Load Balancing DNS/SRV was configured. e.g. FQDN (TLS) Select IP address or FQDN of the Orange SBC Primary if Load Balancing DNS/A was configured. e.g. 172.22.246.33: 5061 (TLS) or FQDN: 5061 (TLS)

Priority / Weight	2 if Load Balancing Priority was configured.
SIP Server Profile	Select previously created: Prof_SBCE-BTIP
Next Hop Address	Select IP address or FQDN of the Orange SBC Backup if exists. e.g. 172.22.246.33: 5061 (TLS) or FQDN: 5061 (TLS)
Domain Policies → Media Rules → Add	
Rule Name	Orange-med-enc
Audio Encryption & Video Encryption	
Preferred Format #1	AES_CM_128_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	Checked
MKI	Unchecked
Lifetime Leave blank to match any value	Leave blank
Interworking	Checked
Symmetric Context Reset	Checked
Key Change in New Offer	Unchecked
Miscellaneous	
Capability Negotiation	Unchecked
Audio Codec & Video Codec	
Codec Prioritization	Unchecked
Transcode	Unchecked
Allow Preferred Codecs Only	Unchecked
Transrating	Unchecked
P-Time	20
Silencing	
Silencing Enabled	Unchecked
Binary Flow Control Protocol	
BFCP Enabled	Unchecked
Far End Camera Control	
FECC Enabled	Unchecked
ANAT	
ANAT Enabled	Unchecked
Local Preference	IP4

Use Remote Preference	Unchecked
Media Line Compliance	
Media Line Compliance Enabled	Unchecked
Media QoS Marking	
Enabled	Checked
QoS Type	DSCP
Audio QoS	
Audio DSCP	EF
Domain Policies → End Point Policy Groups → EPPG_SBCE-BTIP → Edit Policy Set	
Application Rule	default-trunk
Border rule	default
Media Rule	select created previously: Orange-med-enc
Security Rule	default-low
Signaling Rule	SigR_SBCE-BTIP
Network & Flows → Advanced Options → Port Ranges	
Signaling Port Range	Depending on customer context or need. ASBCE TLS/TCP/UDP source ports for the SIP signaling. Allocate e.g. range: 51001-55000
Config Proxy Internal Signaling Port Range	50001-51000
Listen Port Range	55001-55999
HTTP Port Range	40001-50000
Network & Flows → Media Interface	
Name	Edit/Add a media interface for the internal side of the ASBCE e.g. Media_Int_SBCE-SM
IP Address	ASBCE internal interface and corresponding ip address: Int_SBCE-SM (A1, VLAN 0) 6.5.27.61
Port Range	The Orange BTIPoI/BToI SIP Trunk service specifies media ports that customers use on the internal SIP trunk. ASBCE UDP ports for the RTP media: 6000-38000 for BTIPoI 6000-20000 for BToI
Network & Flows → Media Interface	
Name	Edit/Add media interface for the external side of the ASBCE e.g. Media_Ext_SBCE-BTIP
IP Address	ASBCE external interface and corresponding ip address: Ext_SBCE-BTIP (B1, VLAN 0) Public IP Address

Port Range	The Orange BTIPoI/BToI SIP Trunk service specifies media ports that customers use on the external SIP trunk. ASBCE UDP ports for the SRTP media: 6000-38000 for BTIPoI 6000-20000 for BToI
Configuration Profiles → Topology Hiding	
Profile Name	Edit/Add this profile will be applied for the traffic from the ASBCE to Orange Business Services BTIPoI/BToI. e.g. THP_SBCE-BTIP
Configuration Profiles → Topology Hiding → Topology Hiding Profile → Add Header	
Header	For all headers set the following parameters except the header From:
Criteria	IP/Domain
Replace Action	Auto
Replace Action for the header **From**	Overwrite
Overwrite Value for the header **From**	Public FQDN hostname of the ASBCE external interface.
Configuration Profiles → Server Interworking → Edit	
Profile Name	SBCE-SM
General	
SIPS Required	No
Configuration Profiles → Server Interworking → Edit	
Profile Name	SBCE-BTIP
General	
SIPS Required	No
Configuration Profiles → Server Interworking → SBCE-BTIP → Header Manipulation → Add	
Header	Select Contact
Action	Select Remove Parameter w/ [Value]
Parameter	gsid
Value **Leave blank for wildcard**	Leave blank
Configuration Profiles → Server Interworking → SBCE-BTIP → Header Manipulation → Add	
Header	Select Contact
Action	Select Remove Parameter w/ [Value]
Parameter	asm

Value Leave blank for wildcard	Leave blank
Configuration Profiles → Server Interworking → SBCE-BTIP → Header Manipulation → Add	
Header	Select Contact
Action	Select Remove Parameter w/ [Value]
Parameter	epv
Value Leave blank for wildcard	Leave blank
Configuration Profiles → Signaling Manipulation → Add	
Title	Remove parameter from Contact

/*Script to remove attribute (+avaya-cm-keep-mpro) from Contact Header */
within session "INVITE"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
if (exists(%HEADERS["Contact"][1].PARAMS["+avaya-cm-keep-mpro"])) then
{
remove(%HEADERS["Contact"][1].PARAMS["+avaya-cm-keep-mpro"]);
}
}
}	

Services → SIP Servers → Prof_SBCE-BTIP → Advanced → Edit	
Interworking Profile	Interworking Profile for Orange BTIP SIP trunk service. SBCE-BTIP
Signaling Manipulation Script	Select created previously script name: Remove parameter from Contact
Media anchoring	
Domain Policies → Session Policies → default	
Name	Media must be anchored on ASBCE. default
Media Anchoring	Checked for media anchoring
Media Forking Profile	None
Converged Conferencing	Unchecked
Recording Server	Unchecked
Media Server	Unchecked
Network & Flows → Session Flows	
Media must be anchored on ASBCE. Session Flows must be default. Remove any session flow if exists.	

8 Endpoints configuration

8.1 SIP endpoints

SIP endpoint configuration	
Home / Elements / Session Manager / Application Configuration / Applications	Create application for each HQ ie: hq353-app. To do so press "**New**" button and fill "**Name**" choose "**SIP Entity**" and select "CM System for SIP Entity" for your HQ. Next press "**Commit**" button. If you don't have "CM System for SIP Entity" configured then you need to press **"View/Add CM System"** and on a new tab you need to press **"New"** button. On **"Edit Communication Manager"** page you need to fill: **"Name"**, **"Type"** and type node IP address. On the second tab "Attributes" you need to fill below fields: **"Login"**, **"Password"** and **"Port"** number (5022). You should use the same login and password used to login to ACM.
Home / Elements / Session Manager / Application Configuration / Applications sequences	Click "**New**" button. Next fill "**Name**" field and from "**Available Applications**" filed choose application crated for your HQ. To finish creation click on "**commit**" button
Home / Users / User Management / Manage Users	To create new user click on "**new**" button. On first "*identity*" configuration page you need to fill below fields: "**Last Name**", "**First Name**", "**Login Name**", "**Authentication Type**", "**Password**" (here you should set password: "password"), and "**Time Zone**". On the second page "*Communication Profile*" you should fill "**Communication Profile Password**" (password used to log in the phone), then create "**Communication Address**" (this should be extension@domain). On "*Session Manager Profile"* fill below fields: "**Primary Session Manager**", "**Origination Application Sequence**", "**Termination Application Sequence**", "**Home Location**". Last thing is to fill fields in "*Endpoint Profile*" like: "**System**", "**Profile Type**", "**Extension**", "**Template**", "**Security Code**" (this should be password used to log in the phone "**Port**" (this should be set to: "IP"). To finish this configuration press "**commit**" button.

8.2 H.323 endpoints

H.323 endpoint configuration	
add station 3530001	To add station insert following command with extension you want to add: **add station <extension>** • Type: **9640** (according to phone model) • Security Code: **3530001** (this is the password to log in) • Name: **HQ353-ID1** (example for HQ353)

8.3 FAX endpoints

FAX endpoint configuration	
`add station 1230009`	To add station insert following command with extension you want to add: add station <extension> • Type: 2500 • Port i.e.: 001V301 (analog media module MM711 board number with a port, use *LIST CONFIGURATION ALL* command to view the card details) • Name: analog fax (example name for a fax device)

8.4 46xxsettings.txt files

File 46xxsettings.txt	
`set DTMF payload TYPE 101`	##DTMF_PAYLOAD_TYPE specifies the RTP payload type to be used for RFC4733 (obsolete RFC 2833) signaling. ## Valid values are 96 through 127; the default value is 120. SET DTMF_PAYLOAD_TYPE 101
`set SIP Controller`	SET SIP_CONTROLLER_LIST 6.5.27.20:5060;transport=tcp,6.5.27.30:5060;transport=tcp
`set SIP Domain`	SET SIPDOMAIN <SIP Domain> for example labobs.com
`set Config server secure mode`	Specifies whether HTTP or HTTPS is used to access the configuration server. 0 - use HTTP (default for 96x0 R2.0 through R2.5) 1 - use HTTPS (default for other releases and products). In case it is configured with 0 the phone will not use certificate for authentication. SET CONFIG_SERVER_SECURE_MODE <0 or 1> In case it is configured with 1 the phone will use certificate for authentication. The certificate "SystemManagerCA.cacert.pem" must be downloaded from SM and uploaded to http server where 46xxxsettings.txt file is. The following line must be added to 46xxxsettings.txt file: SET TRUSTCERTS SystemManagerCA.cacert.pem To obtain the certificate from SM go the System Manager GUI and navigate to Security → Certificates → Authority → Certificate Profiles and then clicking on the 'Download PEM file' link. It is also important to appropriately configure parameter "TLSSRVRID" which specifies whether a certificate will be trusted only if the identity of the device from which it is received matches the certificate, per Section 3.1 of RFC 2818. 0 Identity matching is not performed 1 Identity matching is performed (default) SET TLSSRVRID 0
`SET DSCPAUD`	DSCPAUD specifies the layer 3 Differentiated Services (DiffServ) Code Point for audio frames generated by the telephone. If this parameter is not activated the default value is 46. SET DSCPAUD 46

SET DSCPSIG	DSCPSIG specifies the layer 3 Differentiated Services (DiffServ) Code Point for signaling frames generated by the telephone. If this parameter is not activated the default value is 34. SET DSCPSIG 46