Business Services

Business Talk & BTIP for Avaya AURA

version addressed in this guide : 8.0

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 31/01/2020

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 Supported architecture components

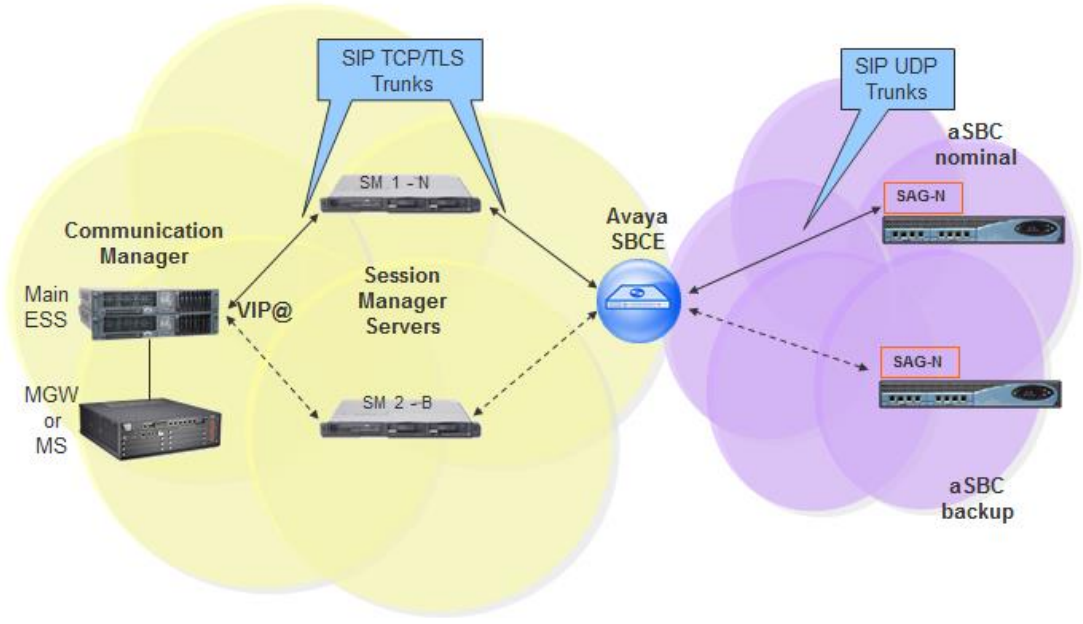
The IP Telephony Avaya Aura has been validated on Business Talk IP / Business Talk with the following architecture components :

- 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)

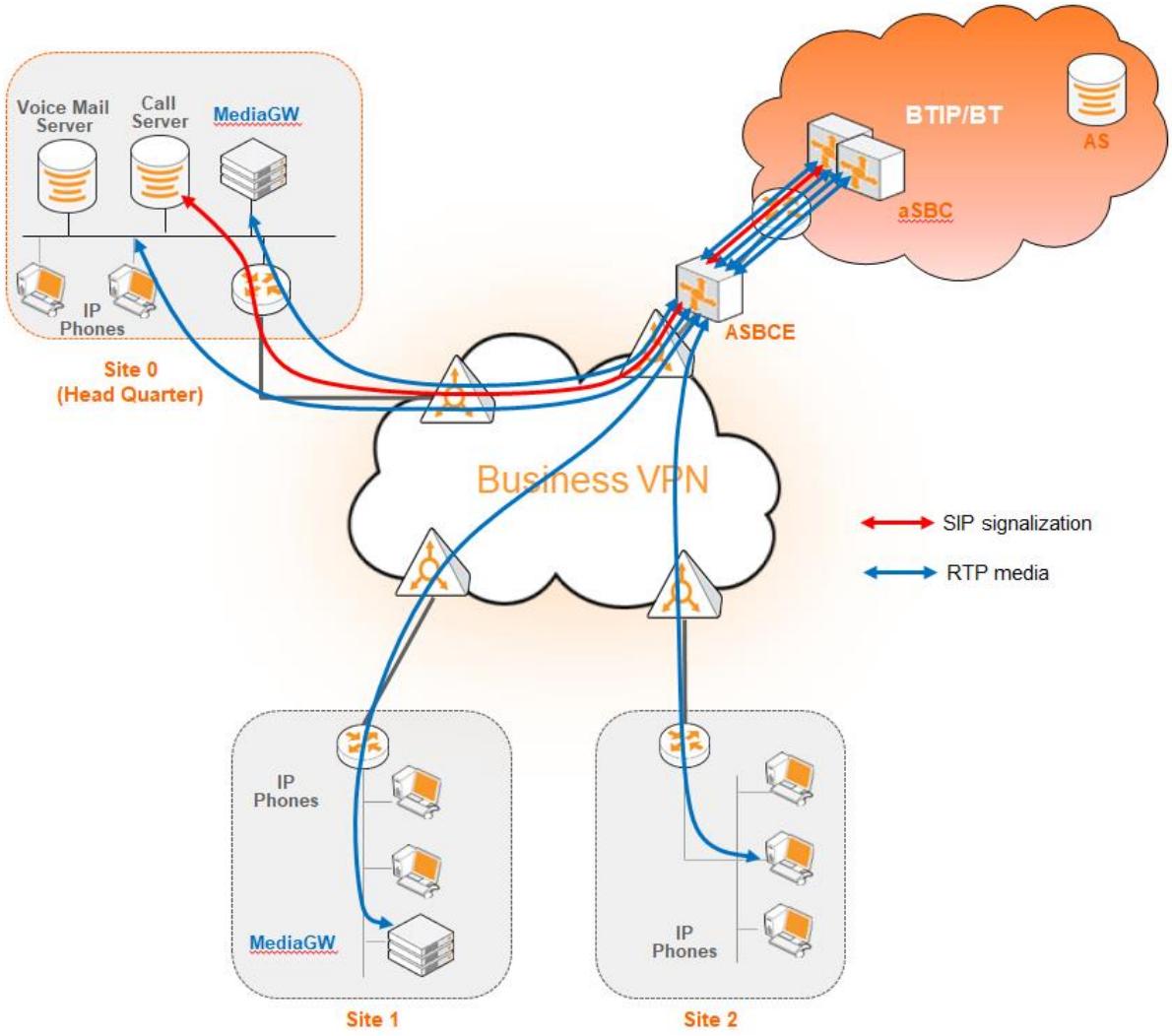
3.2 Architecture: ACM + SM + ASBCE

On a Session Manager, ACM will be considered as a single SIP entity. SIP entity toward ACM will be configured as a single IP address representing Processor Ethernet. SIP entity toward ASBCE will be configured as a single IP address representing internal ASBCE IP address. Avaya Session Border Controller for Enterprise (ASBCE) is used as an intermediate point between Avaya Session Manager located in customer's site and 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).

Processor Ethernet architecture with single Avaya SBCE (no redundancy)



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



	Call scenario	Nb of Voice channels/media resources used on :		
		Media Gateway Voice Channels	**Bandwidth g711 on bt/btip**	**Bandwidth g729 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

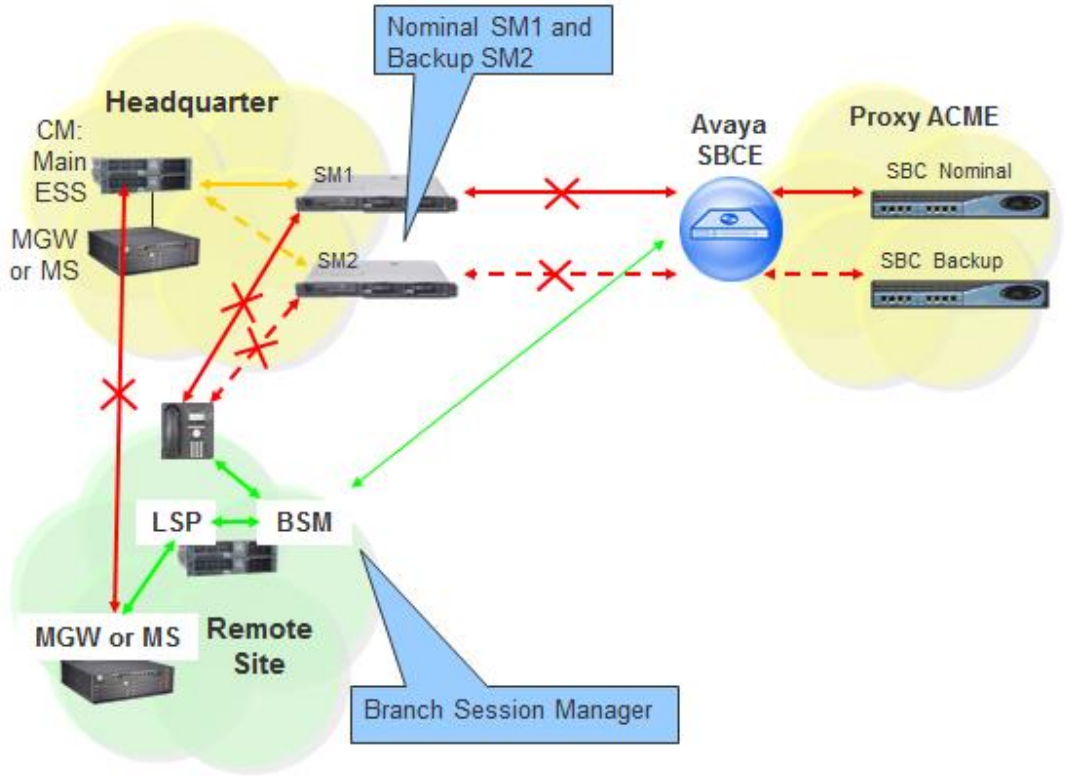
(1) sites 0 & 1 with IP phones and media resources, site 2 with IP phones only

3.3 Architecture: Survivability in Remote Site with ASBCE

Below architecture diagram 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.

3.3.1 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.

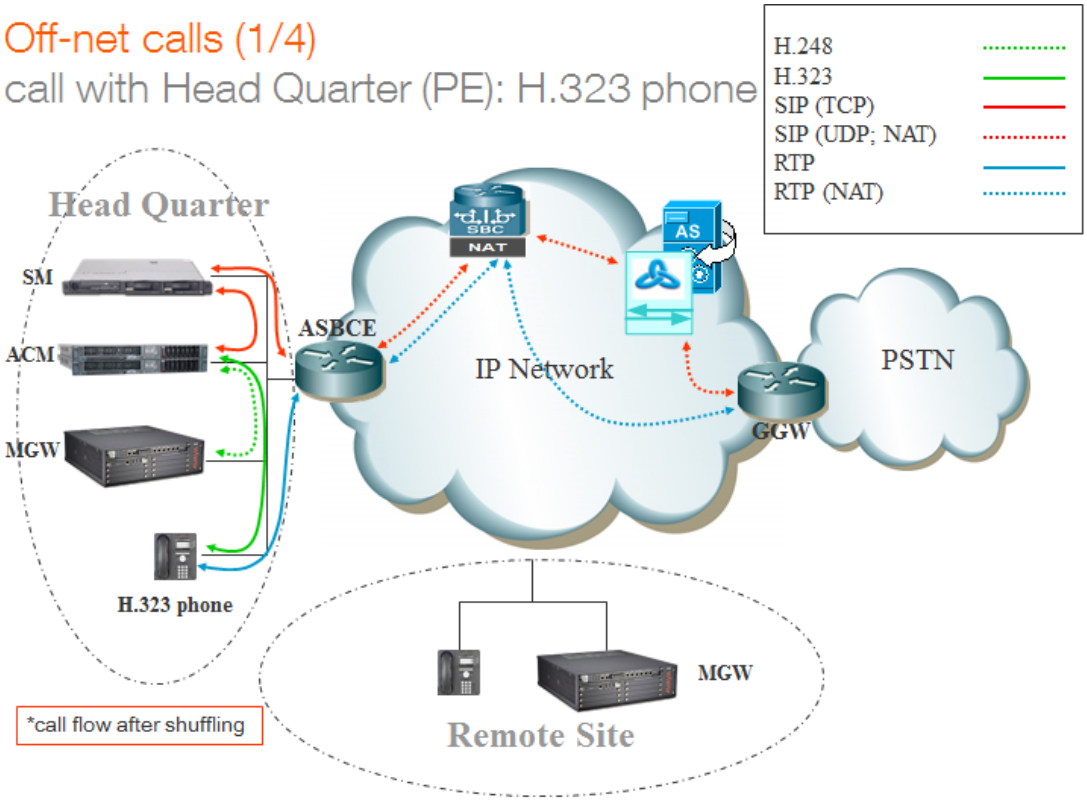
3.3.2 Media unanchoring on ASBCE

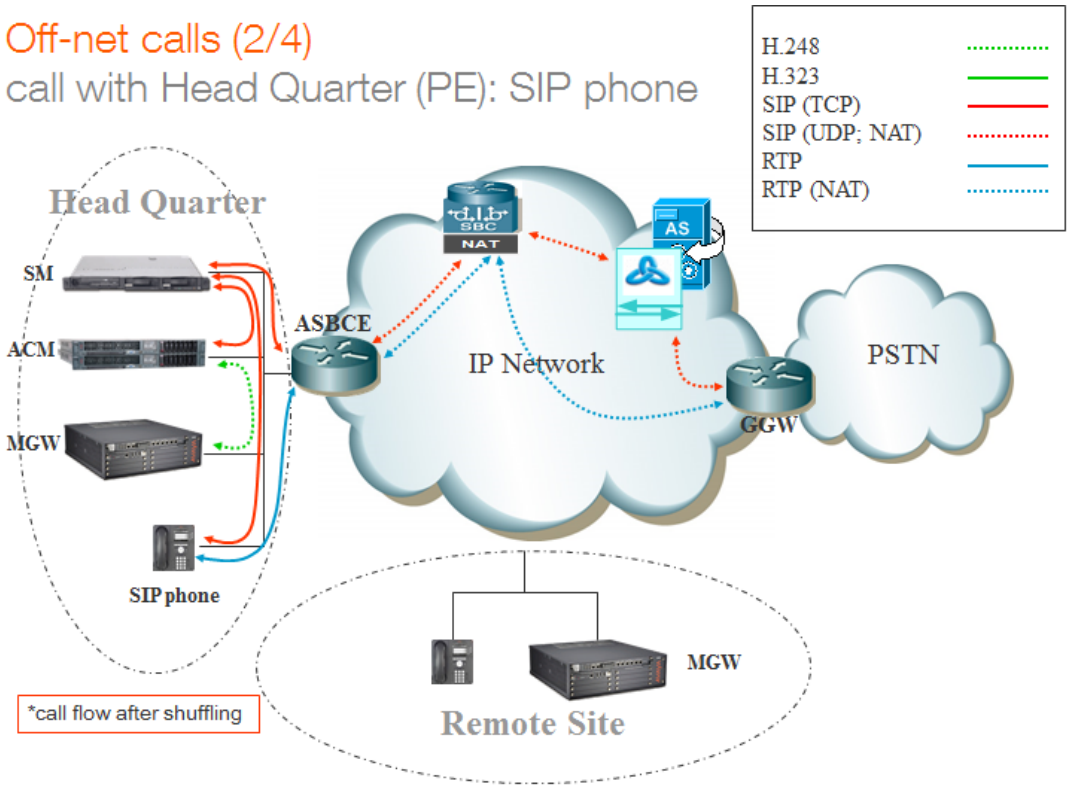
It is a feature available on Avaya Session Border Controller for Enterprise. Unanchoring media benefits in:

- 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.

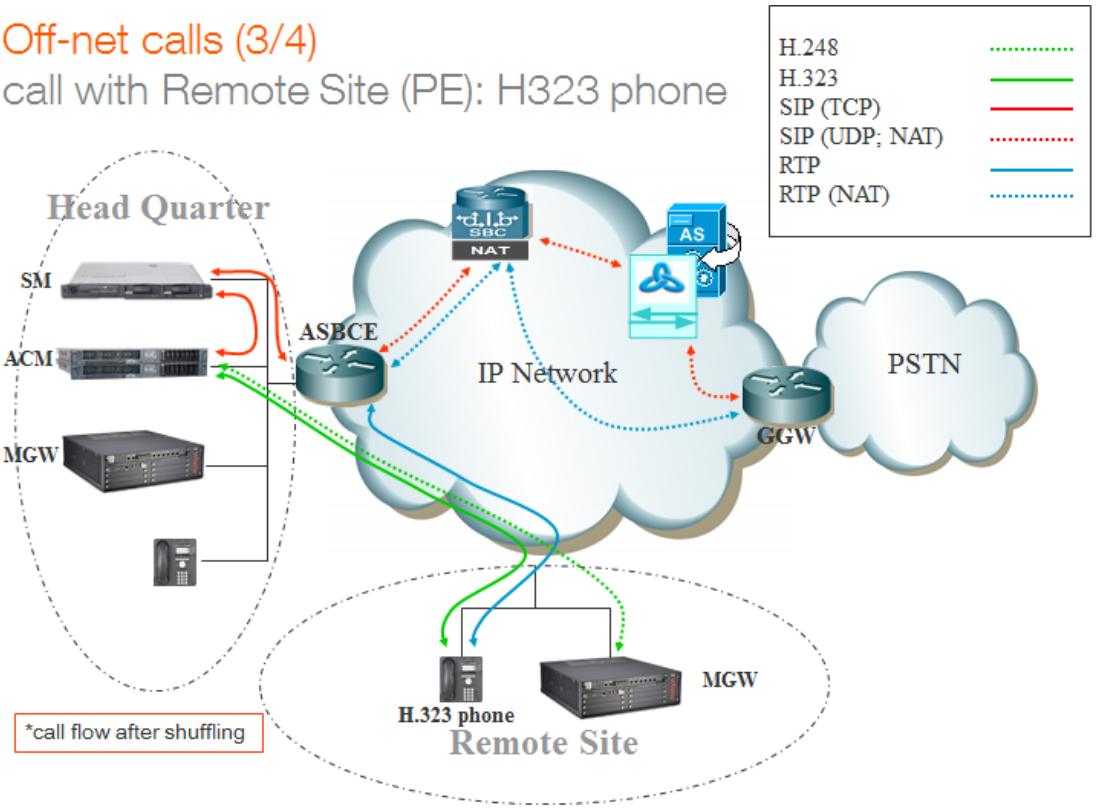
4 Call Flows

4.1 Call flows with media anchoring on ASBCE

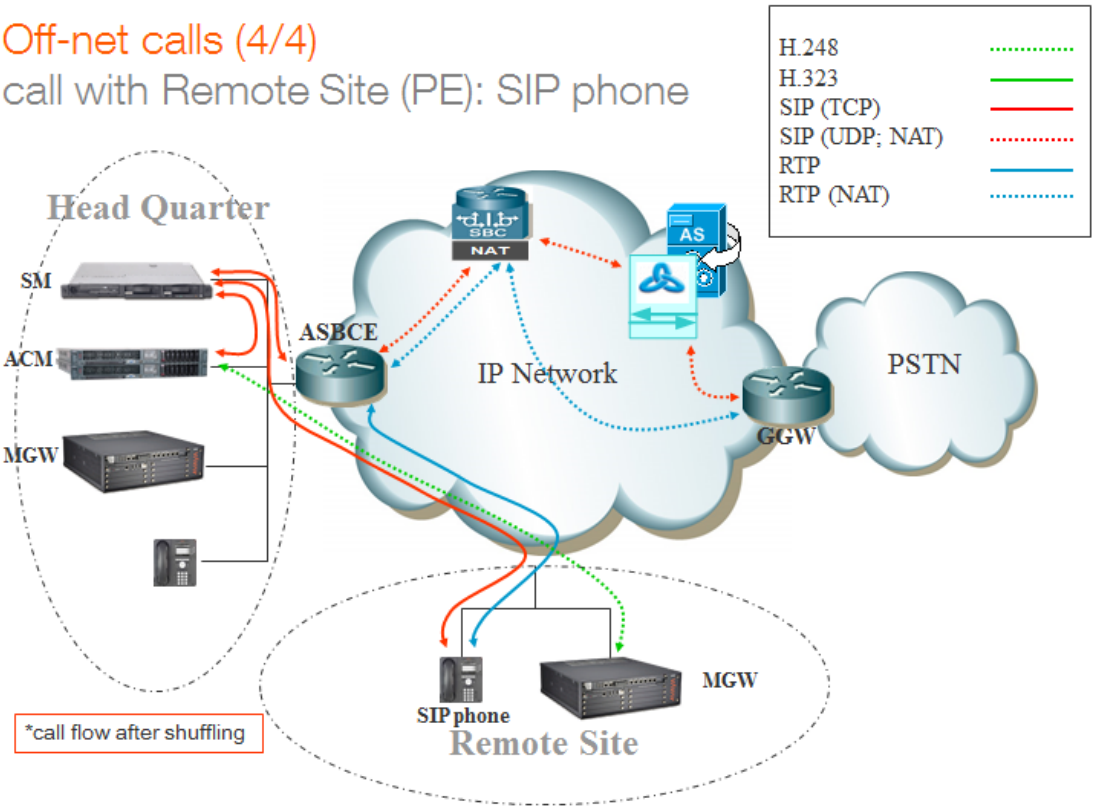




Off-net calls (3/4)
call with Remote Site (PE): H323 phone

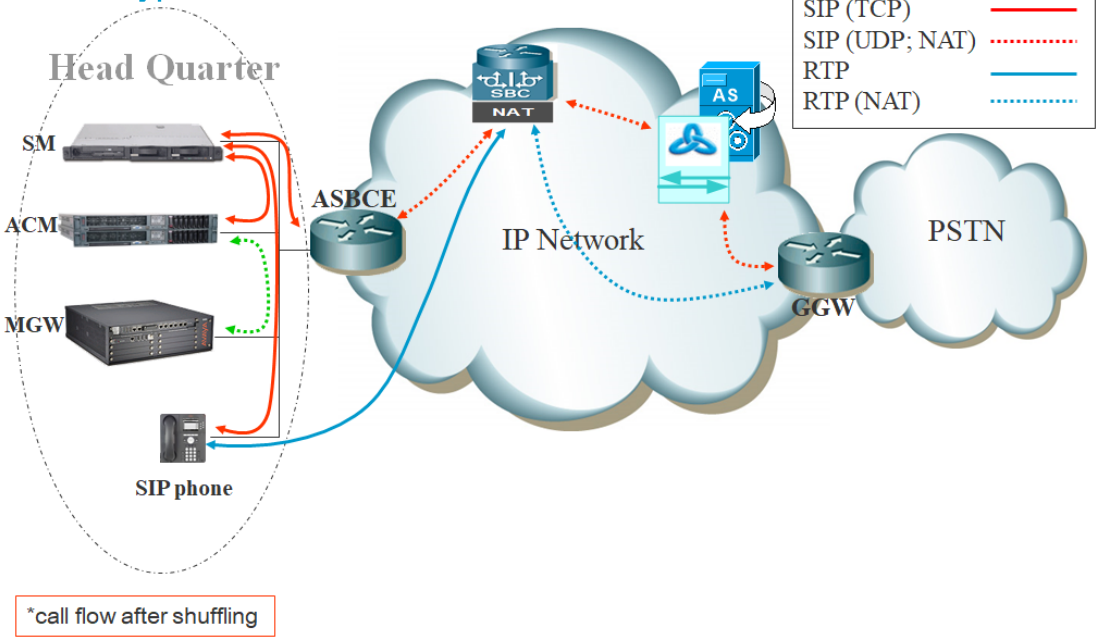


Off-net calls (4/4)
call with Remote Site (PE): SIP phone



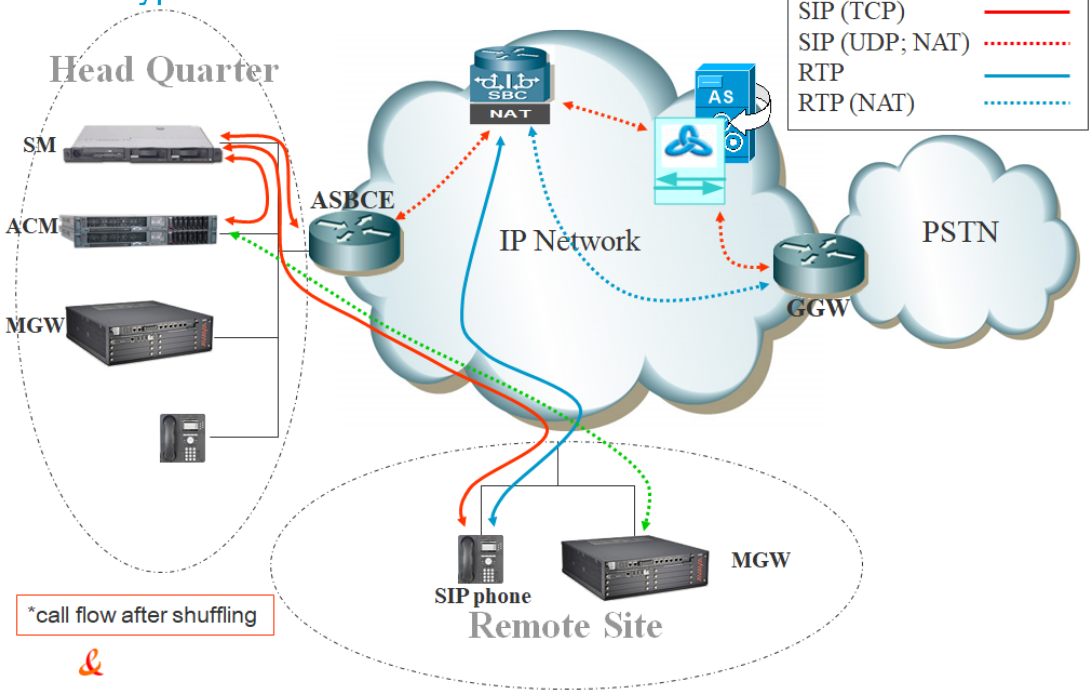
4.2 Call flows with media bypass

Off-net call with media unanchoring on ASBCE
call with Head Quarter (PE): SIP phone
Media bypass ASBCE



*call flow after shuffling

Off-net call with media unanchoring on ASBCE
call with Remote Site (PE): SIP phone
Media bypass ASBCE



*call flow after shuffling

&

5 Integration Model

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

Head Quarter (HQ)	Level of Service	Customer IP@ used by service	
		Nominal	Backup
ACM + Single Session Manager (SM)	No redundancy	N/A	N/A
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	N/A	N/A

Remote Site (RS) architecture**	Level of Service	Customer IP@ used by service	
		Nominal	Backup
Remote site without survivability	No survivability, no trunk redundancy	N/A	N/A
LSP	Local site survivability and trunk redundancy via PSTN only	N/A	N/A
Branch Session Manager	Local site survivability and SIP trunk redundancy	N/A	N/A

All architectures with ASBCE	Level of Service	Customer IP@ used by service	
		Nominal	Backup
ASBCE	No redundancy	ASBCE IP@	N/A

6 Certified software and hardware versions

6.1 Certified Avaya Aura versions

IPBX Avaya Aura – certified software versions Business Talk IP (SIP trunk) -			
Equipment Reference	Softvare version	Certification pronounced	Certified Loads / Key Points
Avaya Aura Communication Manager	8.0.1 FP1	✓	822.0-25031
Avaya Aura System Manager	8.0.1 FP1	✓	8.0.1.0.038826
Avaya Aura Session Manager	8.0.1 FP1	✓	8.0.1.0.801007
Avaya Aura Session Border Controller for Entreprise	7.2 FP2	✓	7.2.2.1-04-16104

6.2 Certified applications and devices

IPBX Avaya Aura – Avaya ecosystems tested (SIP trunk) -			
Equipment Reference		Software Version	Pronounced validation
Attendant	Equinox Attendant and Attendant Snap-in	5.0.5.19	✓
Breeze	Avaya Breeze	3.6.0.0	✓
File server	Avaya Aura Device Services	7.1.3.2	✓
Phones / Softphones	9600 SIP (9601, 9608, 9608G, 9611G, 9621G, 9641G, 9641GS)	7.1.4.011	✓
	9600 H.323 (9608, 9608G, 9611G, 9621G, 9641G, 9641GS)	6.8.0.03	✓
	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)	4.0.0.0.21	✓
	B179 SIP conference	2.4.3.4	✓
	B189 H323 conference	6.6.6	✓
	IP DECT phones 37xx: (3725, 3745, 3749)	4.3.32	✓
	Vantage	3.5.0.53	✓
	Equinox for Windows	3.5.0.52	✓
	Equinox for Android	3.4.8.36	✓
	Equinox for iOS	3.5.1.10	✓
IP DECT	IP DECT Base Station v2	10.2.9	✓
Voice Mail	Avaya Aura Messaging	7.1 Patch 2	✓
Media Gateway	G450	40.20.0	✓
	G430	40.20.0	✓
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	8.0.0 SP2	✓

7 SIP trunking configuration checklist

7.1 Basic configuration

This chapter indicates the mandatory configuration steps on Avaya Communication Manager 8.0.1 + Avaya Session Manager 8.0.1 + Avaya Session Border Controller for Enterprise 7.2 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 Below please find example of configuration for G650: **ASM 6.3.53.20** **HQ353-g450 6.3.53.10** Below configuration for Processor Ethernet: **ASM1 6.3.53.20** default 0.0.0.0 **procr 6.3.53.1**
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** 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** 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 (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** 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): ▪ 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	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** ▪ Video PHB Value: **34** Page 4: ▪ dst rgn: **10**, codec set: **2**, direct WAN: **n**, Intervening Regions: **250** ▪ dst rgn: **119**, codec set: **2**, direct WAN: **n**, Intervening Regions: **250**

change ip-network-region 119 (Used for RS site)	Page 1: ▪ Region: **119** ▪ Location: **119** ▪ 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** ▪ 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**
change ip-network-region 250 *consult "Configuration Guideline" for other network regions settings	Page 4 (dst rgn 1): ▪ Codec set: **2** ▪ Direct WAN: **y** Page 4 (dst rgn 10): ▪ Codec set: **2** ▪ Direct WAN: **y**
change ip-network map	Assign IP network ranges to the appropriate network regions. See example below (Page 1): FROM: **6.3.53.0** Subnet Bits: **/24** Network Region: **1** VLAN: **n** TO: **6.3.53.255** FROM: **6.201.19.0** Subnet Bits: **/24** Network Region: **119** VLAN: **n** TO: **6.201.19.255**
Signaling group	
change signaling-group (example: change signaling-group 10)	▪ Group Type: **sip** ▪ Transport Method: **TCP (or TLS)** ▪ Near-end Node Name: **procr** ▪ Far-end Node Name: **ASM** ▪ 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: **353**, Total Length: **7**, Call Type: **ext** ▪ Dialed String: **446**, 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 cor 1	Calling Party Restriction: **none**
change uniform-dialplan 0	Page 1: Matching Pattern: **353**, Len: **7,** Del: **0,** Net: **aar,** conv: **n**
change aar analysis	Dialed string: **353,** 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)	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**

Calling number format	
change public-unknown-numbering 0	▪ Ext Len: 7, Ext Code: 353, Trk Grp(s) : 10, CPN Prefix: 33296097560, Total CPN Len: 11 ▪ Ext Len: 7, Ext Code: 353, Trk Grp(s) : 20, CPN Prefix: 33296097560, Total CPN Len: 11
change private-numbering 0	▪ Ext Len: 7, Ext Code: 353, Trk Grp(s) : 10, Private Prefix: empty, Total CPN Len: 7 ▪ Ext Len: 7, Ext Code: 353, Trk Grp(s) : 20, Private Prefix: empty, Total CPN Len: 7
Music on Hold configuration	
change location-parameters 1	Companding Mode: A-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)`

Add announcement 3530666	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 353-0666 moh
Disconnect tone enabling 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.

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
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.

Menu	Settings
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..**
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.)

7.4 Avaya Session Border Controller for Enterprise

System 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
System 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 SBCE virtual machine on ESXi host after installation is complete.
Ip Address 1#	Ip address of the internal SBCE interface e.g. 6.5.27.61
Device Specific Settings -> Network Management - > Networks -> Add	
Name	Interface name toward Orange 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 SBCE interface e.g. 172.22.235.23 Note:Reboot of the SBCE is required after configuration of the ip addresses.
Device Specific Settings -> Signaling Interface -> Add	
Name	Create a signaling interface for the internal side of the SBCE e.g. Sign_Int_SBCE-SM

Ip Address	Select ASBCE internal interface andassociated ip address defined in previous step. Int_SBCE-SM (A1, VLAN 0) 6.5.27.61
TCP port	This is the port on which SBCE will listen to SIP messages from Session Manager. 5060 Remark: TCP protocol is used for communication between ASBCE & Session Manager.
Device Specific Settings -> Signaling Interface -> Add	
Name	Create a signaling interface for the external side of the SBCE e.g. Sign_Ext_SBCE-SM
Ip Address	Selec 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 SBCE will listen to SIP messages from Orange SBC. 5060 Remark: UDP protocol is used for communication between ASBCE & Orange SBC.
Device Specific Settings -> 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
Device Specific Settings -> Media Interface -> Add	
Name	Create a media interface for the internal side of the SBCE 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
Device Specific Settings -> Media Interface -> Add	
Name	Create a media interface for the external side of the SBCE 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
Global 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. 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.
Global 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 unavaiability 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. 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.
Global Profiles -> Server Configuration -> 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
Global Profiles -> Server Configuration -> Add	

Profile Name	Define profile for far away server: Orange SBC. Prof_SBCE-BTIP
Server Type	Trunk Server
TLS Client Profile	none
IP Address / FQDN	Add all Orange 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 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 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
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 Headres -> 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 Headres -> 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 Headres -> 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 Headres -> 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 Headres -> 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	
Enebled	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 Headres -> 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 Headres -> 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 Headres -> 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 Headres -> 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 Headres -> 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	
Enebled	Checked
DSCP	Selected
Value	EF
Domain Policies -> Signaling Rules -> SigR_SBCE-BTIP -> UCID	
Enebled	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
Global Profiles -> Routing -> Add	
Profile name	e.g. **Routing-to-SM**
Global Profiles -> Routing -> Routing-to-SM	
Uri Group	*
Load Balancing	Priority
Transport	None
Next Hop In-Dialog	Unchacked
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
Server Configuration	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
Server Configuration	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
Server Configuration	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)
Global Profiles -> Routing -> Add	
Profile	e.g. Routing-to-BTIP
Global Profiles -> Routing -> Ruting-to-BTIP	
Uri Group	*
Load Balancing	Priority
Transport	None
Next Hop In-Dialog	Unchecked
ENUM	Unchecked
Time of Day	default
NAPTR	Unchecked
Next Hop Priorit	Checked
Ignore Route Header	Unchecked
ENUM Suffix	Leave this field blank.
Priority / Weight	1
Server Configuration	Select previously created: Prof_SBCE-BTIP
Next Hop Address	Select IP address of the Orange SBC Primary e.g. 172.22.246.33: 5060 (UDP)

Priority / Weight	2
Server Configuration	Select previously created: Prof_SBCE-BTIP
Next Hop Address	Select IP address of the Orange SBC Backup if exists e.g. 172.22.246.73: 5060 (UDP)
Global 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
Global Profiles -> Topology Hiding -> Toppology Hiding Profile -> Add Header	
Header	For all headers set the following parameters:
Criteria	IP/Domain
Replace Action	Auto
Global 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
Global Profiles -> Topology Hiding -> Toppology 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**	Overwite
Overwrite Value for the header **From**	e.g. warsaw.lab
Device Specific Settings -> End Point Flows -> Server Flows -> Add	
Flow Name	Traffic from Orange SBC through Avaya SBCE toward Session Manager: e.g. EPF_SBCE-SM
Server Configuration	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
Device Specific Settings -> End Point Flows -> Server Flows -> Add	
Flow Name	Traffic from Session Manager through Avaya SBCE toward Orange SBC: e.g. EPF_SBCE-BTIP
Server Configuration	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 Unachoring	
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
Device Specific Settings -> 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

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 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 ENABLE_PPM_SOURCED_SIPPROXYSRVR	Following additional configuration is required in 46xxsettings.txt file to force 96x1 SIP phone to register to SM over TCP: SET ENABLE_PPM_SOURCED_SIPPROXYSRVR **0**
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**