TECHNICAL GUIDE
to access
Business Talk and BTIP
IPBX Avaya AURA

version addressed in this guide : 7.1

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 28/03/2017

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

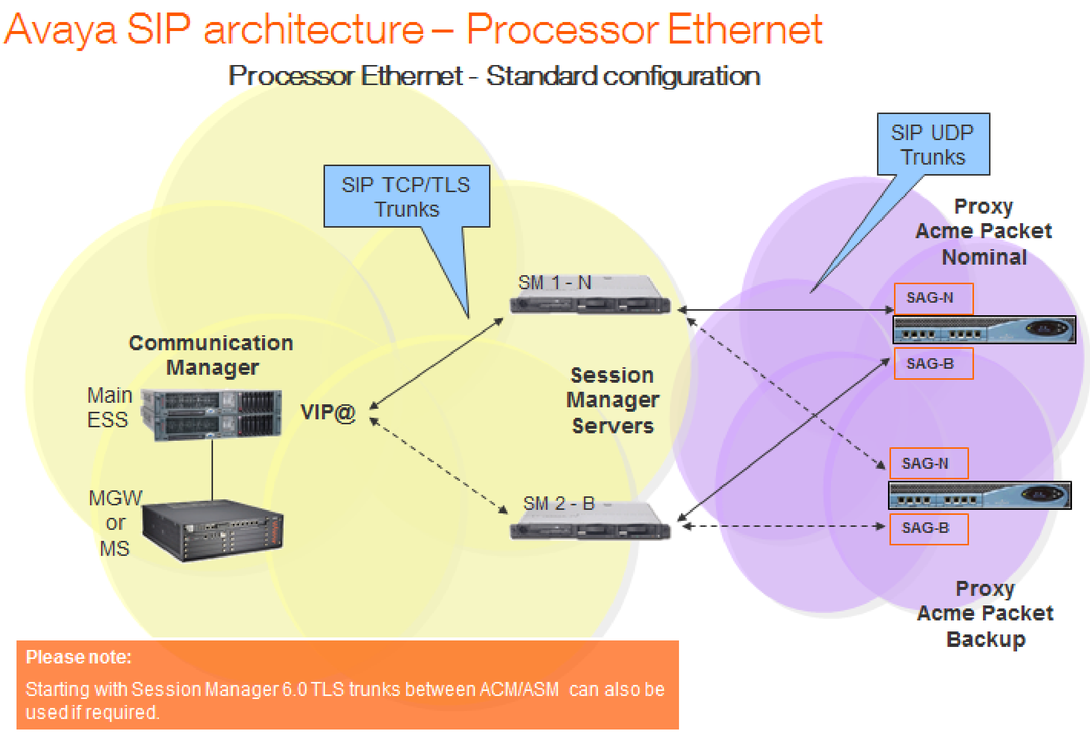
3.1 Supported architecture components

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 : Communication Manager Messaging
- Avaya Aura Session Border Controller for Enterprise (ASBCE)

3.2 Architecture ACM + SM

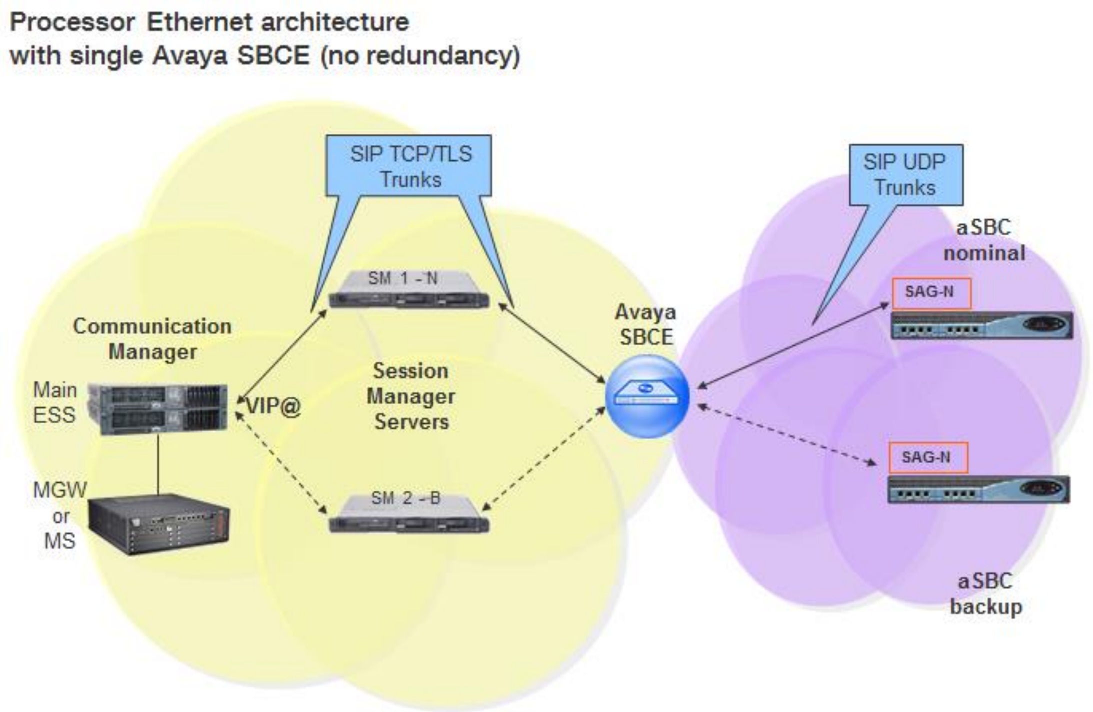
On a Session Manager, ACM will be considered as a single SIP entity. SIP entity toward ACM will be configured as single IP address representing Processor Ethernet. SBCs are in Nominal/Backup mode (there is no load balancing), they will be created as separate SIP entities on ASM (one being the alternate destination of the other).



3.3 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).

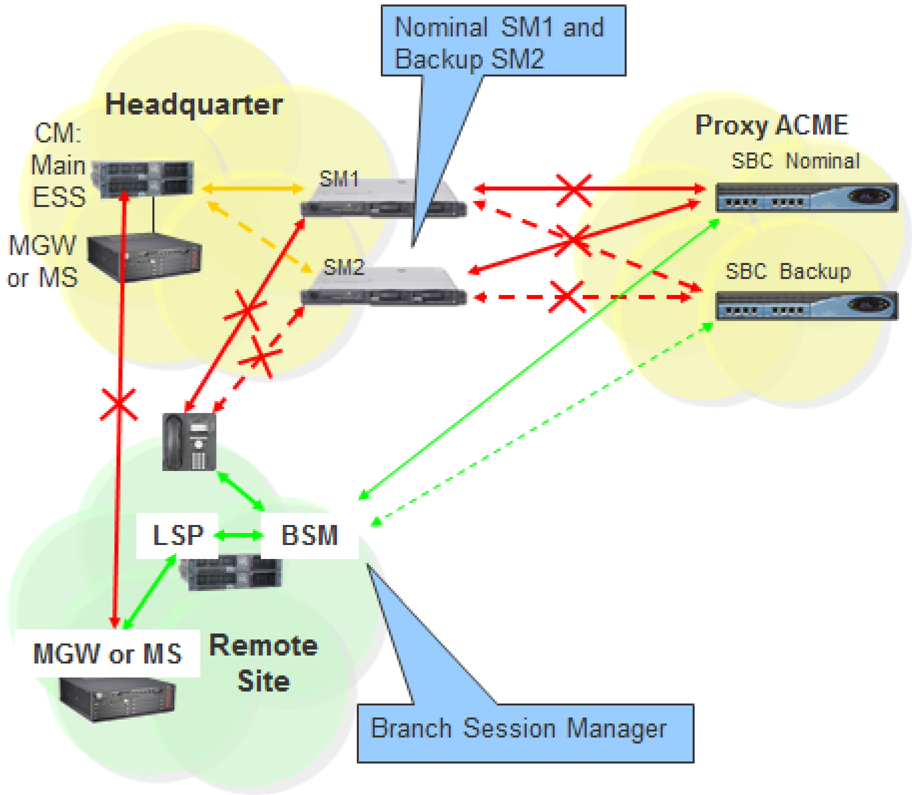


3.4 Architecture Survivability in Remote Site

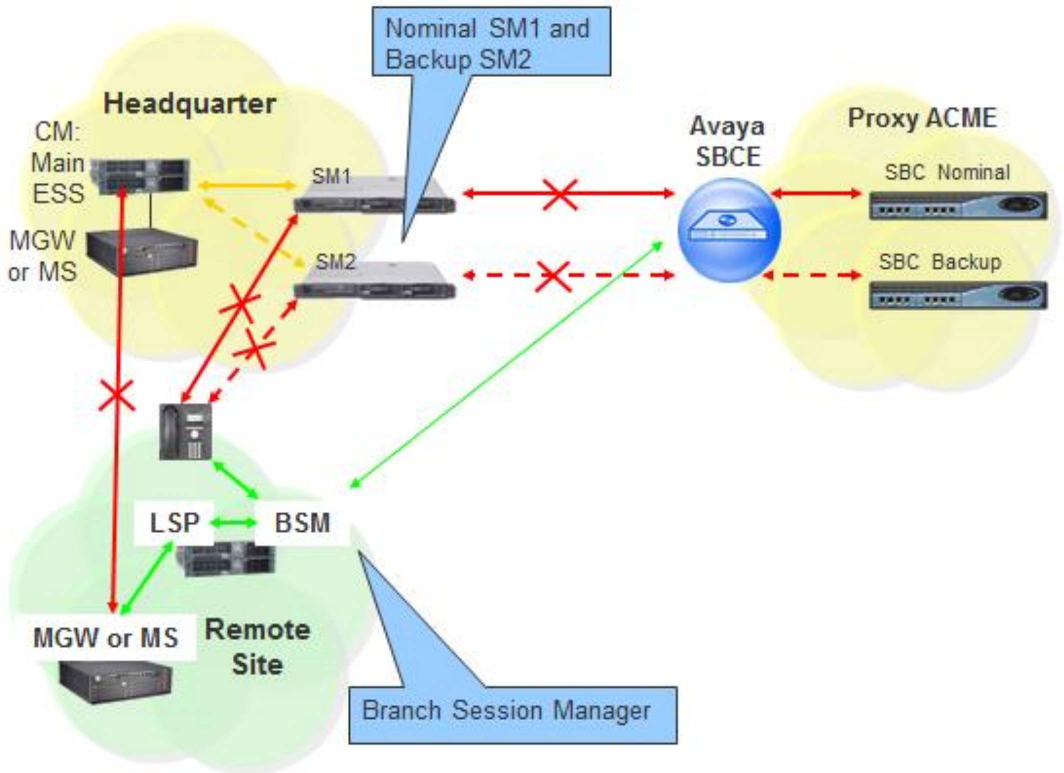
Below architecture shows multisite environment: Headquarter with BT/BTIP SIP trunk and Remote Site controlled by this HQ. In case there is a WAN failure between Remote Site and Headquarter:

- 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



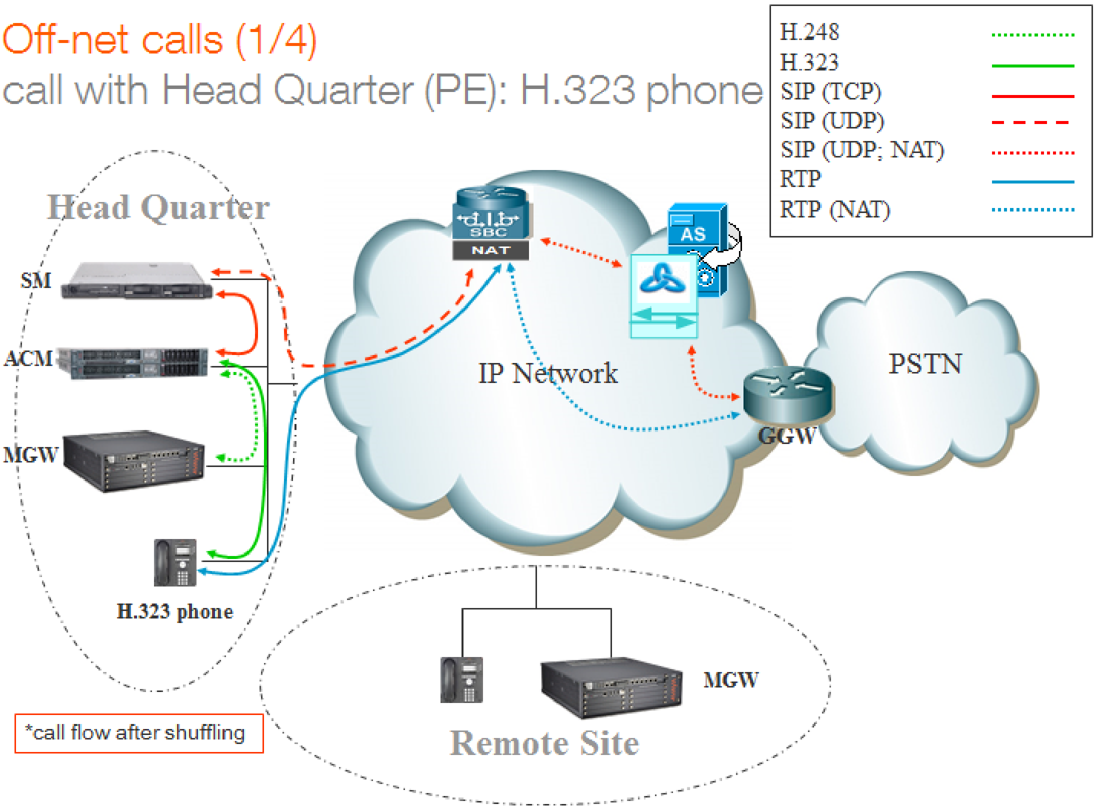
3.4.2 LSP and BSM in Remote Site and ASBCE



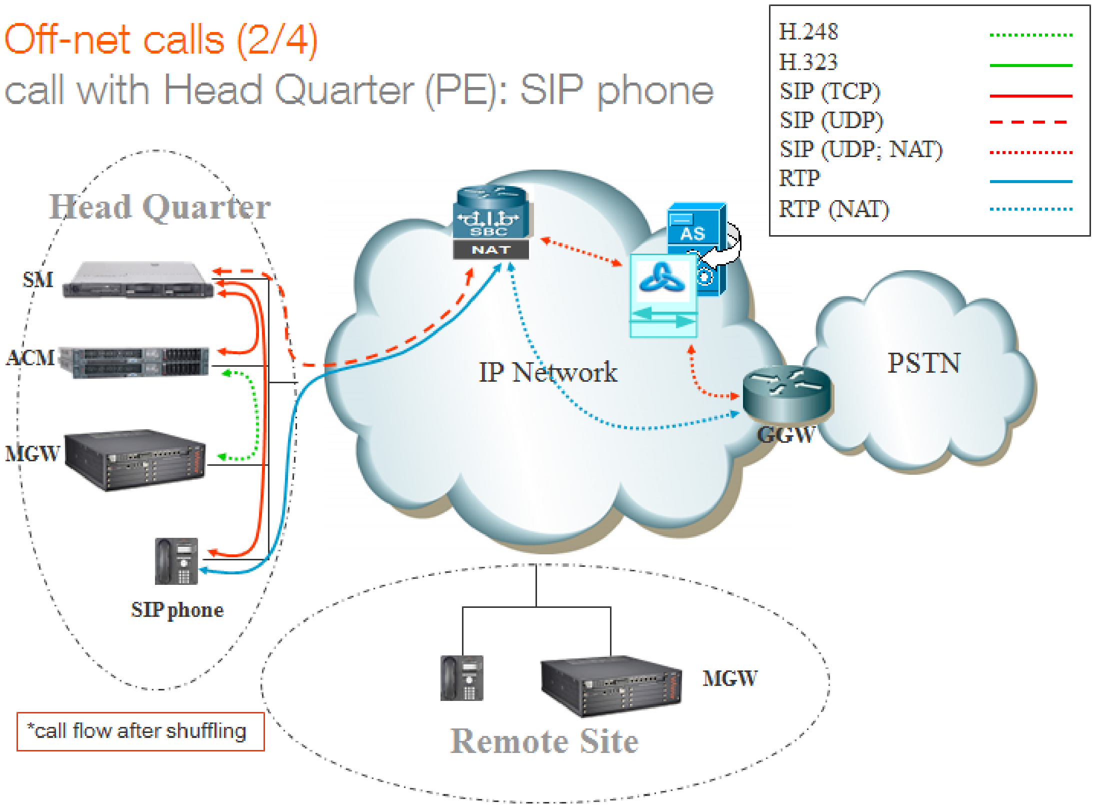
4 Call Flows

4.1 Call flows for architecture ACM + SM

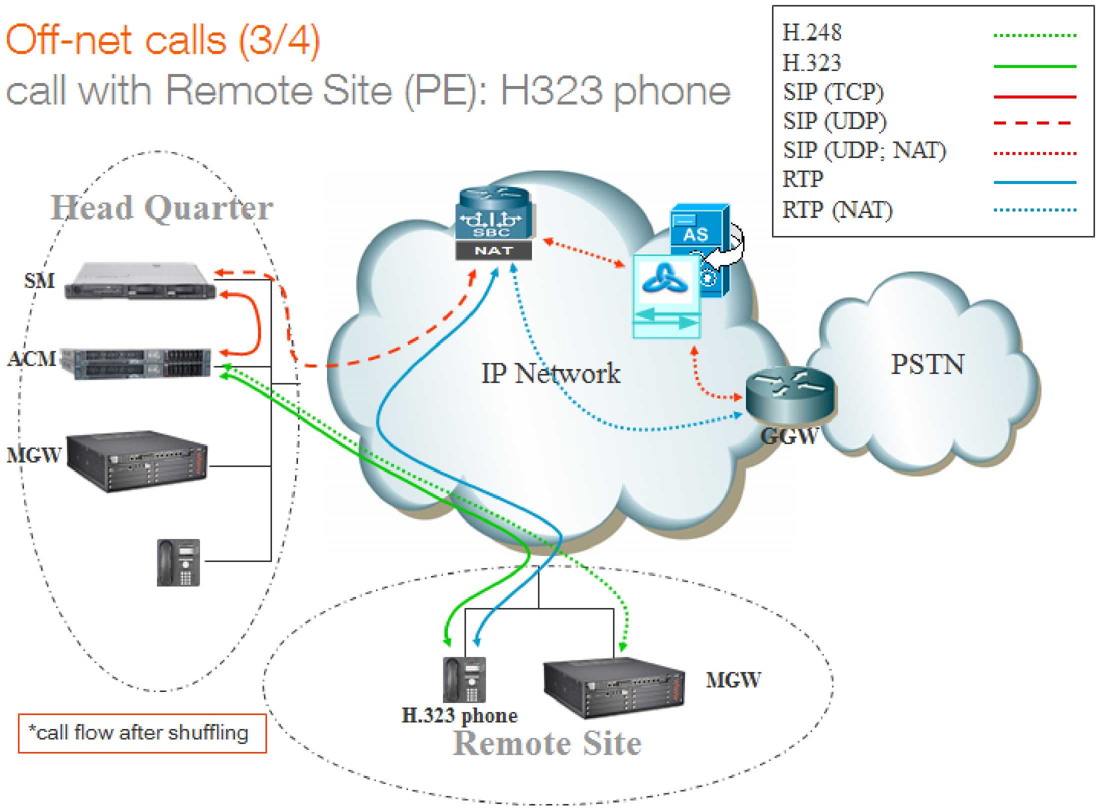
Off-net calls (1/4)
call with Head Quarter (PE): H.323 phone

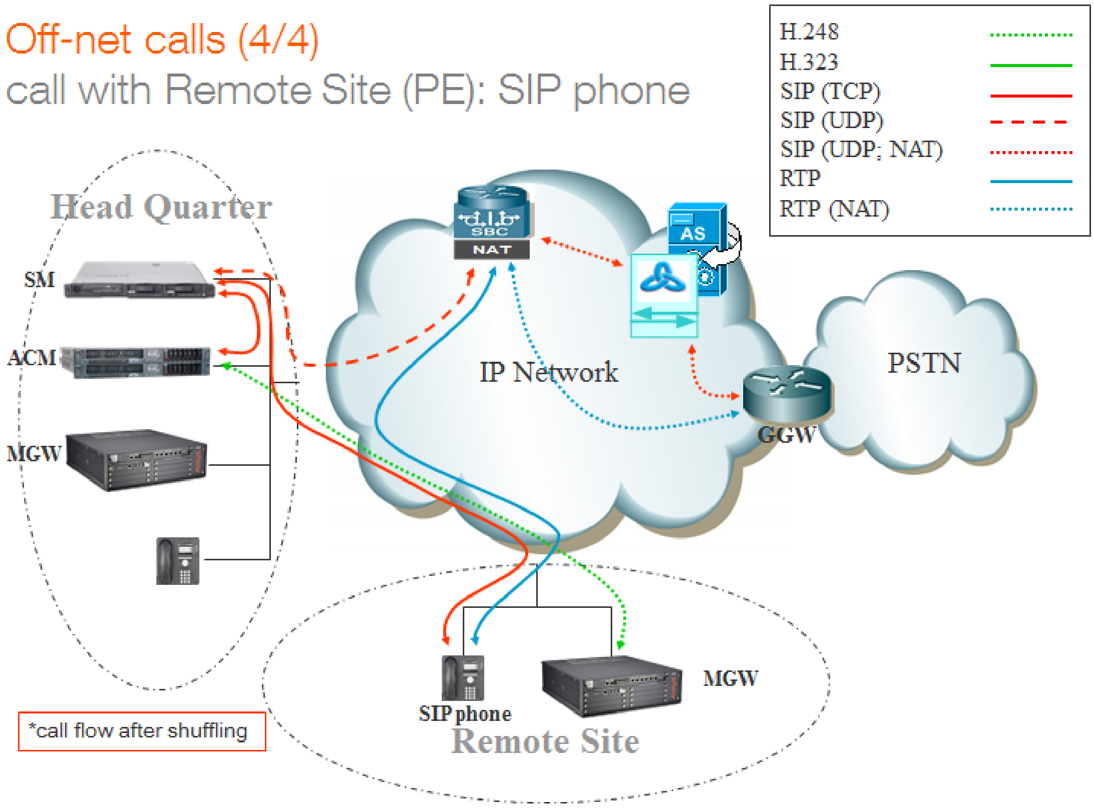


Off-net calls (2/4)
call with Head Quarter (PE): SIP phone

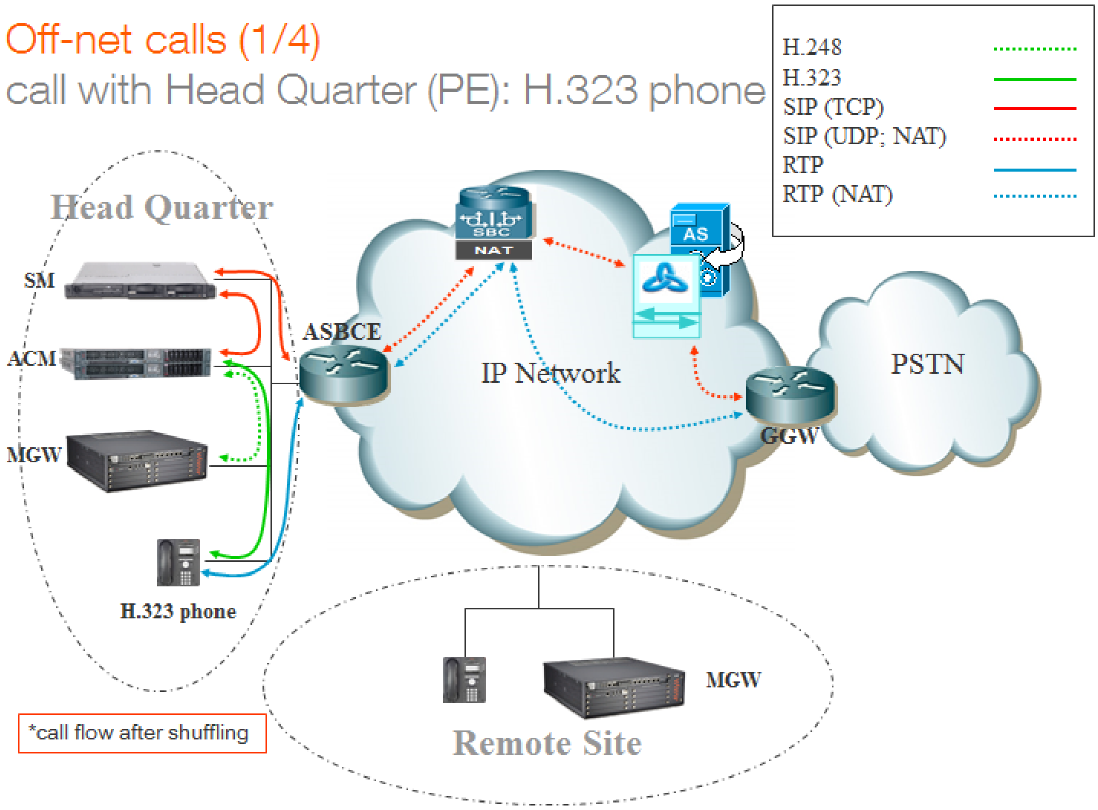


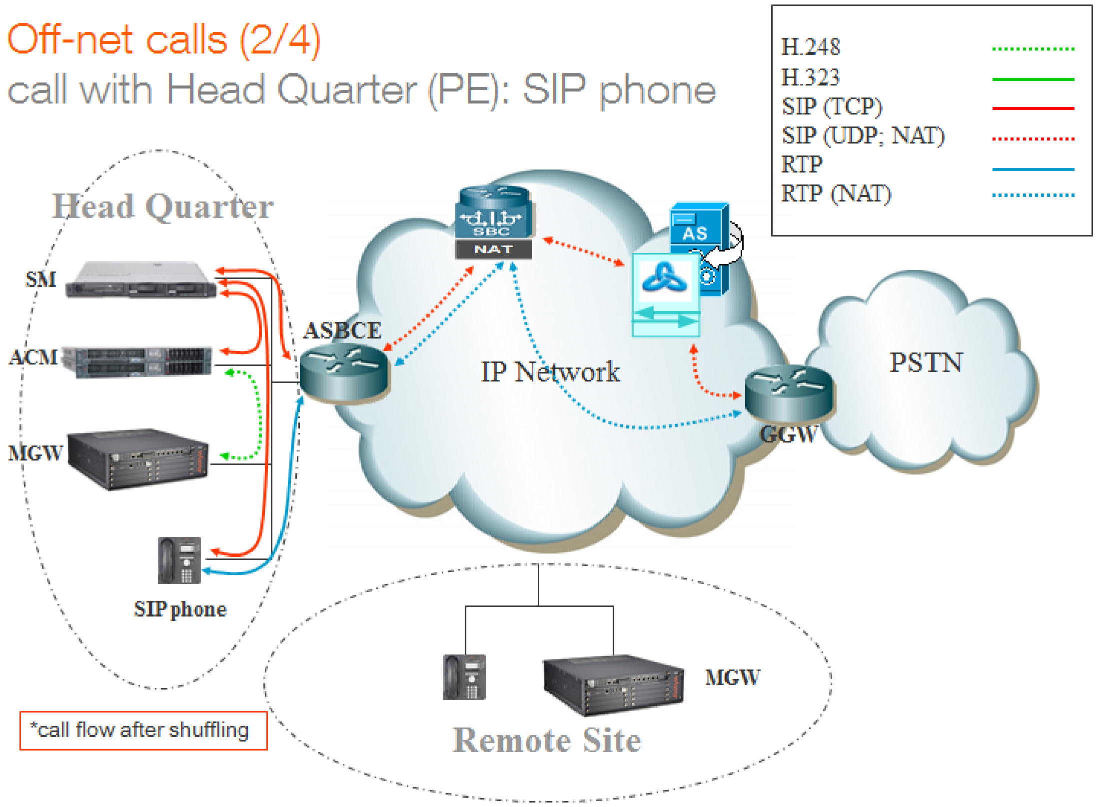
Off-net calls (3/4)
call with Remote Site (PE): H323 phone

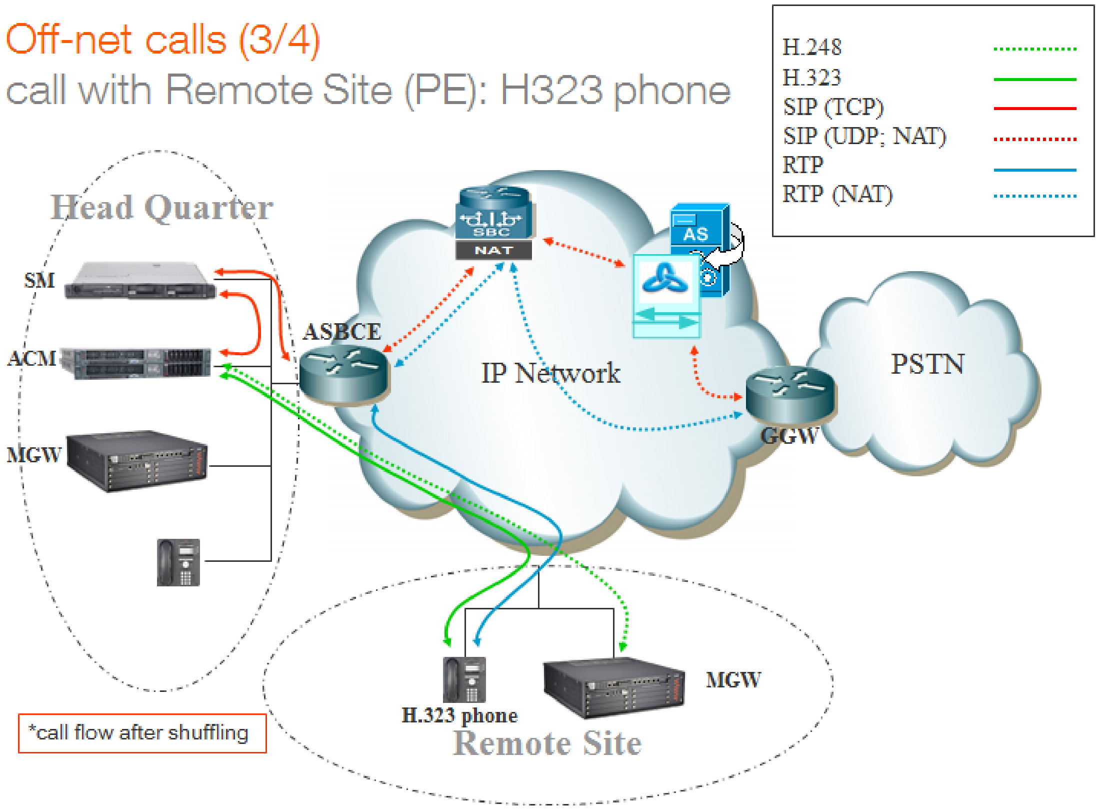


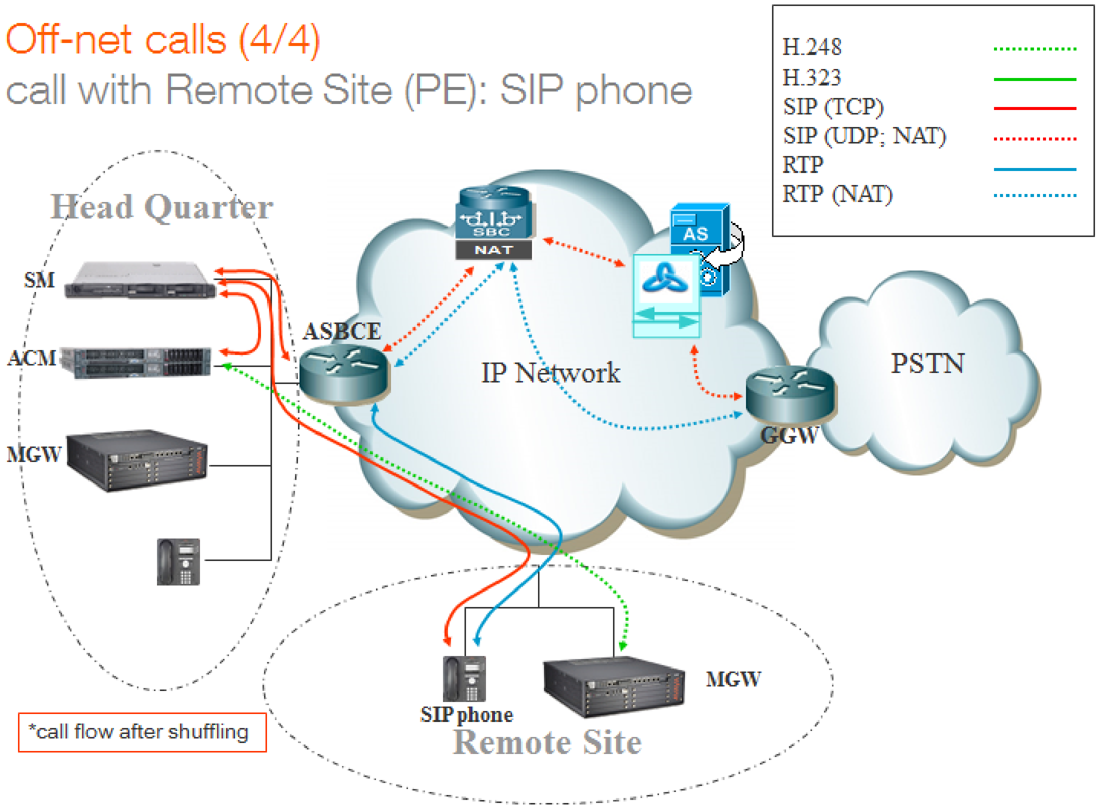

Off-net calls (4/4)
call with Remote Site (PE): SIP phone
H.248
H.323
SIP (TCP)
SIP (UDP)
SIP (UDP; NAT)
RTP
RTP (NAT)
Head Quarter
SM
ACM
MGW
SBC
NAT
AS
IP Network
GGW
PSTN
SIP phone
MGW
Remote Site
*call flow after shuffling

4.1.1 Call flows for architecture ACM + SM + ASBCE






Off-net calls (3/4)
call with Remote Site (PE): H323 phone
H.248
H.323
SIP (TCP)
SIP (UDP; NAT)
RTP
RTP (NAT)
Head Quarter
SM
ACM
MGW
ASBCE
SBC
NAT
AS
IP Network
GGW
PSTN
H.323 phone
MGW
Remote Site
*call flow after shuffling


Off-net calls (4/4)
call with Remote Site (PE): SIP phone
H.248
H.323
SIP (TCP)
SIP (UDP; NAT)
RTP
RTP (NAT)
Head Quarter
SM
ACM
MGW
ASBCE
SBC
NAT
AS
IP Network
GGW
PSTN
SIP phone
MGW
Remote Site
*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 SM 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	7.1 FP2	✓	Load 01.0.532.0
Avaya Aura System Manager	7.1 FP2	✓	N/A
Avaya Aura Session Manager	7.1 FP2	✓	7.1.2.0.712004
Avaya Aura Session Border Controller for Entreprise	7.2 FP1	✓	N/A

6.2 Certified applications and devices

IPBX Avaya Aura – Avaya ecosystems tested (SIP trunk) -			
Equipment Reference		Software Version	Pronounced validation
Attendant	Equinox Attendant	5.0.0.644	✓
Phones / Softphones	96X1 SIP (9601, 9608, 9608G, 9611G, 9621G, 9641G, 9641GS)	7.1.1.0	✓
	96X1 H.323 (9608, 9608G, 9611G, 9621G, 9641G, 9641GS)	6.6.5	✓
	1603, 1603C, 1603SW, 1603SW-I, 1603-I,1608, 1608-I,1616, 1616-I	1.3.11	✓
	J129 SIP phone	1.1.0.1	✓
	B179 SIP conference	2.4.3.4	✓
	B189 H323 conference	6.6.6	✓
	IP DECT phones (3725, 3745)	4.3.32	✓
	Vantage	3.2.3	✓
	Equinox for Windows	3.2.2	✓
	Equinox for Android	3.3.0	✓
	ONE-X Mobile	6.2 SP10	✓
IP DECT	IP DECT Base Station v2	10.0.6	✓
Voice Mail	Aura Communication Manager Messaging	7.0 FP1 SP1	✓
Media Gateway	G450	38.20.1	✓
	G430	38.20.1	✓
Media Server	Avaya Aura Media Server	7.8	✓

7 SIP trunking configuration checklist

7.1 Basic configuration

This chapter indicates the mandatory configuration steps on Avaya Communication Manager 7.1 + Avaya Session Manager 7.1 + Avaya Session Border Controller for Enterprise 7.2 for the SIP trunking with Business Talk IP / Business Talk.

7.2 Communication Manager

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 Etherenet: **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 1 : **n** Frames Per Pkt 1: **2** Packet Size(ms) 1: **20** Media Encryption 1: **none**
`change ip-codec-set 2`	Audio codec 1: **G722-64K** Frames Per Pkt 1: **2** Packet Size(ms) 1: **20** Audio codec 2 : **G711A** Silence Suppression 1 : **n**

	Frames Per Pkt 1: **2** Packet Size(ms) 1: **20** Media Encryption 1: **none**
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 1 : **n** Frames Per Pkt 1: **2** Packet Size(ms) 1: **20** Audio codec 3 : **G729a** Silence Suppression 1 : **n** Frames Per Pkt 1: **2** Packet Size(ms) 1: **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`	Audio codec 1 : **G729a** Silence Suppression 1 : **n** Frames Per Pkt 1: **2** Packet Size(ms) 1: **20** Media Encryption 1: **none**
Locations	
`change locations`	configure appropriate locations: ▪ HQ – **1** ▪ RSxx – **xx** ▪ VoIP – **10** Note: to enable multi-location go to ACM web manager interface: Administration -> Licensing -> Feature Administration -> Multiple Locations

<table>
<tr><th colspan="2">Network Regions</th></tr>
<tr><td><code>change ip-network-region 1</code></td><td>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</td></tr>
<tr><td><code>change ip-network-region 119</code>

<code>(Used for RS site)</code></td><td>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</td></tr>
<tr><td><code>change ip-network-region 250</code>

*consult “Configuration Guideline” for other network regions settings</td><td>Page 4 (dst rgn 1):
Codec set: 2
Direct WAN: y
Page 4 (dst rgn 10):
Codec set: 2
Direct WAN: y</td></tr>
<tr><td><code>change ip-network map</code></td><td>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</td></tr>
</table>

<table>
<tr><th colspan="2">Signaling group</th></tr>
<tr><td>change signaling-group

(example: change signaling-group 10)</td><td>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</td></tr>
<tr><th colspan="2">Trunk group</th></tr>
<tr><td>change trunk-group

(example: change trunk-group 10)</td><td>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.</td></tr>
<tr><th colspan="2">Route Pattern</th></tr>
<tr><td>change route-pattern 10</td><td>Processor Ethernet:
Grp No: 10, FRL: 0, LAR: next
Grp No: 20, FRL: 0, LAR: next
Grp No: 1, FRL: 0</td></tr>
</table>

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**
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**
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**

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	
system-parameters customer-options	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 select ON by 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 for architecture without 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 Adaptations for both Orange SBCs are configured **OrangeAdapter** should be used with parameters: odstd=<@IP_SBC> iodstd=<SIP Domain> fromto=true eRHdrs=P-AV-Message-ID,Endpoint-View,P-Charging-Vector,Alert-Info,AV-Global-Session-ID,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) ▪ 5060, UDP **TCP protocol (or TLS) is used for communication between SM & CMs** **UDP protocol is used for communication between SM & Orange SBC** 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

<table>
<tr><th>Menu</th><th>Settings</th></tr>
<tr><td>Network Routing Policy

SIP Entities – Orange SBC</td><td>Check if SIP Entity for Orange SBC is correctly configured.

Ensure that following settings are applied:
Type: Other
Adaptation: adaptation module created for Orange SBC has to be selected
Location: Location created for Orange SBC has to be selected
Make sure that for Orange SBC SIP Entity ports and protocols are correctly set.
5060, UDP
Only UDP protocol is used for communication between SM & Orange SBC.</td></tr>
<tr><td>Network Routing Policy

SIP Entities – CM</td><td>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.</td></tr>
<tr><td>Network Routing Policy:

Entity Links</td><td>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.)</td></tr>
<tr><td>Network Routing Policy

Time Ranges</td><td>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.)</td></tr>
<tr><td>Network Routing Policy

Routing Policies</td><td>check if routing policies are configured:
towards Orange SBC1 and Orange SBC2
towards each Communication Manager hub</td></tr>
<tr><td>Network Routing Policy

Dial Patterns</td><td>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.)</td></tr>
</table>

7.4 Session Manager for architecture with ASBCE

<table>
<tr><th>Menu</th><th>Settings</th></tr>
<tr><td>Network Routing Policy
SIP Domains</td><td>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)</td></tr>
<tr><td>Network Routing Policy
Locations</td><td>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.)</td></tr>
<tr><td>Network Routing Policy
Adaptations</td><td>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,AV-Global-Session-ID,P-Location,AV-Correlation-ID,P-Conference,Accept-Language</td></tr>
<tr><td>Network Routing Policy
SIP Entities – SM</td><td>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</td></tr>
<tr><td>Network Routing Policy
SIP Entities – ASBCE</td><td>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..</td></tr>
</table>

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.)

7.5 Avaya Session Border Controller for Enterprise

To configure ASBCE 7.1 refer to OBS documentation.

Remark: UDP protocol is used for communication between ASBCE & Orange SBC.

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 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**