TECHNICAL GUIDE to access Business Talk IP SIP IPBX Avaya AURA

version addressed in this guide : 7.0

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 30/06/2017

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

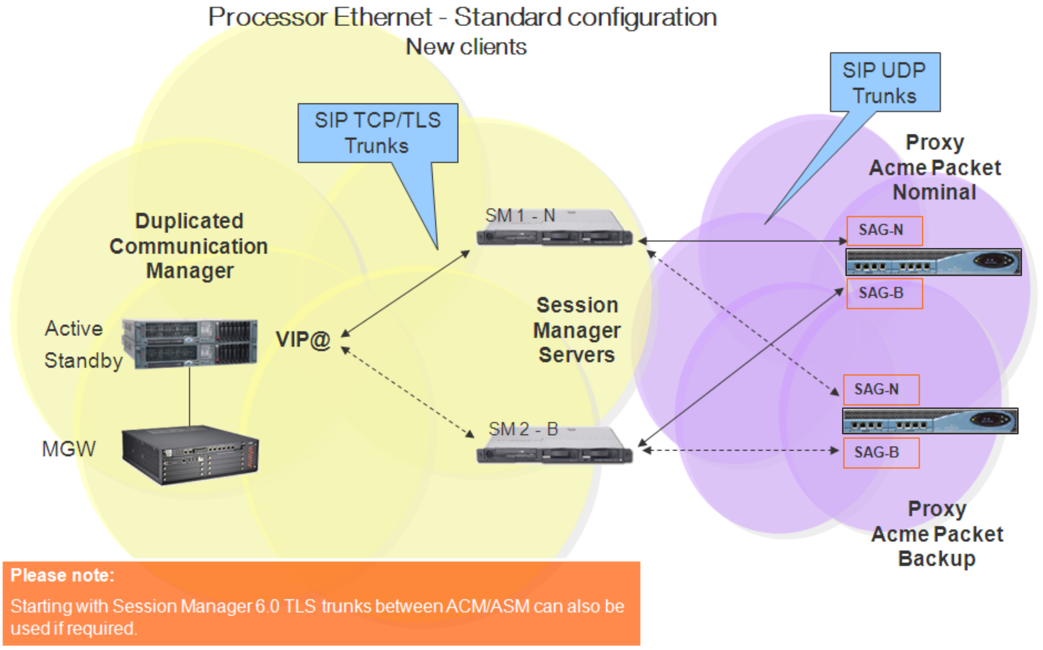
The IP Telephony Avaya Aura has been validated on Business Talk IP / Business Talk with the following architecture components :

- Avaya Aura Communiaction Manager (ACM)
- Avaya Aura Session Manager (ASM)
- Avaya Aura System Manager (SMGR)
- Messageries vocales Avaya Modular Messaging, Avaya Aura Messaging, Communication Manager Messaging
- Avaya Aura Session Border Controller for Enterprise (ASBCE)

3.2 Standard 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).

Avaya SIP architecture – Processor Ethernet

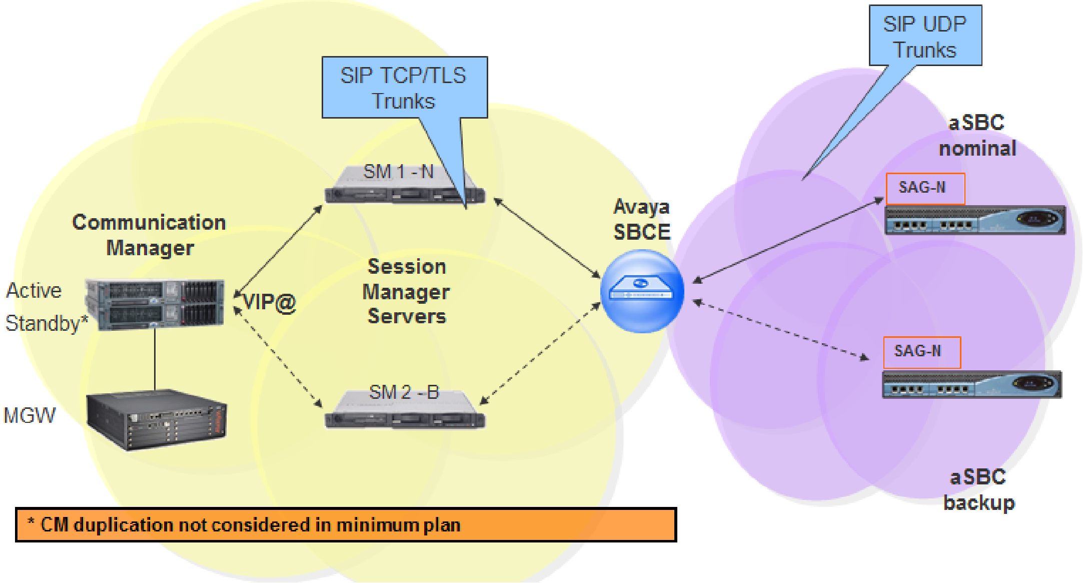


Please note:
Starting with Session Manager 6.0 TLS trunks between ACM/ASM can also be used if required.

3.3 Standard architecture ACM + SM + SBCE

Avaya Session Border Controller for Enterprise (SBCE) 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.

Processor Ethernet architecture
with single Avaya SBCE (no redundancy)



* CM duplication not considered in minimum plan

4 Integration Model

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

Head Quarter (HQ) or Branch Office (BO) architecture	Level of Service	Customer IP@ used by service	
		Nominal	Backup
ACM + Single Session Manager (SM)	No redundancy	SM IP@	N/A
ACM + 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	- **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	SM1 IP@	SM2 IP@
Avaya Branch Edition	No redundancy	BE IP@	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 (embedded in Media Gateway)	Local site survivability and trunk redundancy via PSTN only	N/A	N/A
Branch Session Manager	Local site survivability and SIP trunk redundancy	BSM IP@	N/A

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

5 Certified software and hardware versions

5.1 Certified Avaya Aura versions

6 IPBX Avaya Aura – versions logicielles certifiées Business Talk IP (trunking SIP) -

Référence Équipement	Version Logicielle	Certification prononcée	"Loads" certifiés / Points clefs
Avaya Aura Communication Manager System Manager / Session Manager	6.0.1	✓	Load 00.1.510.1
	6.3	✓	Load 124.0
	7.0	✓	Load FP1
Avaya Session Border for Entreprise	7.1	✓	avec AURA 7.0 seulement

6.1 Certified application s and devices

IPBX Avaya Aura - écosystèmes Avaya testés (trunking SIP) **-**

Référence Équipement		Version Logicielle	validation prononcée	Version Avaya Aura	Load minimum requis et points clefs
Attendant	One-X Attendant	3.05	✓	6.0.1	-
		4.0 SP12	✓	7.0	7.0
Phones	9601 SIP	6.1	✓	6.0.1	-
	9601G/GS SIP	7.0.1.29	✓	7.0	7.0
	96X1 SIP (9608, 9611G, 9621G, 9641G)	6.0	✓	6.0.1	-
	One-X communicator-H323 mode	6.1	✓	6.0.1	-
	One-X communicator-SIP mode	6.1	✓	6.0.1	-
	DECT phones – Base station	V4.1.30	✓	6.0.1	-
	DECT phones – Base station V2	7.2.22	✓	7.0	7.0
	IP DECT phones (3720, 3725)	V3.2.23 V4.3.24	✓ ✓	6.0.1 7.0	- 7.0
	AIWS Avaya In-Building Wireless Server	V2.73	✓	6.0.1	-
	4602SW+,4601+, 4625SW,4610SW, 4621SW, 4622SW	2.9	✓	6.0.1	-
	9610, 9620, 9620C, 9620L, 9630, 9630G, 9640, 9640G, 9650, 9650C	3.1	✓	6.0.1	-
	1603, 1603C, 1603SW, 1603SW-I, 1603-I,1608, 1608-I,1616, 1616-I	1.3 1.3.9	✓ ✓	6.0.1 7.0	- 7.0
	4690	2.6.0	✓	6.0.1	-
	1692	1.4	✓	6.0.1	-
	96X1 H.323 (9608, 9611G, 9621G, 9641G) 96X1G/GS H.323	6.2 6.6302U	✓ ✓	6.0.1 7.0	- 7.0
	E129 SIP phone	1.25.2.34	✓	7.0	7.0
	B189 H323 conference B179 SIP conference	6.6.3 2.4.1.4	✓ ✓	7.0 7.0	7.0 7.0
Voice Mail	Modular Messaging-SIP	5.2	✓	6.0.1	-
	Aura Communication Manager Messaging	7.0 FP1 SP1	✓	7.0	7.0
MGW	G250	5.2	✓	6.0.1	-
	G350	5.2	✓	6.0.1	-
	G450	5.2	✓	6.0.1	
		37.38.0	✓	7.0	7.0
	G700	5.2	✓	6.0.1	
	G650	5.2	✓	6.0.1	
	G430	5.2	✓	6.0.1	
		37.38.0	✓	7.0	7.0
Unified Comms	One-X Mobile	6.2.SP10	✓	7.0	7.0

7 SIP trunking configuration checklist

7.1 Basic configuration

This chapter indicates the mandatory configuration steps on Avaya Communication Manager + Avaya Session Manager 7.0 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:S8300 ■ V2:MM712 ■ V8:MM711 ■ V9:gateway-announcements 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 -> Multinational Locations & Multiple 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

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:
	■ Support Request History?: y
	■ Telephone Event Payload Type: 101
	■ Identity for Calling Party Display: P-Asserted-Identity

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
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	Multinational 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 "Multinational Locations?" then submit this change

7.3 Session Manager

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>
	eRHdrs=P-AV-Message-ID,Endpoint-View,P-Charging-Vector,Alert-Info,AV-Global-Session-ID,P-Location,AV-Correlation-ID
	noar=404,486

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 Be sure that for Session Manager's SIP Entity ports, protocols and domain are correctly set. - 5060, UDP, e.g. labobs.com - 5060, TCP, e.g. labobs.com UDP protocol is used for communication between SM & Orange SBC. TCP protocol (or TLS) is used for communication between SM & CMs.
Network Routing Policy **SIP Entities – Orange SBC**	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 Be sure that for Orange SBC SIP Entity ports, protocols and domain are correctly set. - 5060, UDP, e.g. labobs.com Only UDP protocol is used for communication between SM & Orange SBC.

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 Be sure that for Communication Manager SIP Entity ports, protocols and domain are correctly set. ▪ 5060, TCP, e.g. labobs.com (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 SBC1 and SBC2 ▪ 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.)

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