



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R7.0, Avaya Aura® Session Manager R7.0 and Avaya Session Border Controller for Enterprise R7.0 to support Proximus SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Proximus SIP Trunking service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server. Proximus, previously Belgacom, is a member of the DevConnect Service Provider program.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in Section 2.1 as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Proximus SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R7.0 (Communication Manager); Avaya Aura® Session Manager R7.0 (Session Manager); Avaya Session Border Controller for Enterprise R7.0 (Avaya SBCE). Note that the shortened names shown in brackets will be used throughout the remainder of the document. Customers using this Avaya SIP-enabled enterprise solution with the Proximus SIP Trunking service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Avaya SBCE. The enterprise site was configured to connect to the Proximus SIP Trunking service.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using the Proximus SIP Trunking service, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the Proximus SIP Trunking service to PSTN destinations, calls made from SIP and H.323 telephones.
- Calls using the G.711A and G.729A codecs.
- Fax calls to/from a Group 3 fax machine to a PSTN connected fax machine using T.38.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media between the Avaya SBCE and the SIP and H.323 telephones.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by the Proximus SIP Trunking service requiring Avaya response and sent by Avaya requiring Proximus response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Proximus SIP Trunking service with the following observations:

- Outbound calls failed with Initial IP-IP Direct Media set to “y” on Communication Manager. This was because of an Avaya proprietary parameter “+Avaya-cm-keep-mpro=no” in the Contact header. This was removed using a Sigma script in Avaya SBCE.
- When there was no matching codec between Communication Manager and the network for an outgoing call, the network returned 482 “Merged Request”. Though the call failed as expected and a tone was heard on the calling phone, it is listed as an observation because the commonly used response is 488 “Not Accepted Here”.
- Inbound access from Toll-Free numbers was not tested as it is not part of the Proximus service.
- Outbound international access was not tested as it is not available from the Proximus Lab environment.
- Emergency calls were not tested as a test call was not booked with the Emergency Services Operator.
- Operator and Directory Enquiries were not tested as the short numbers were not available from the Proximus Lab environment
- When forwarding calls off-net, the network did not respond to the SIP INVITE message for leg 2. This was resolved by removing the “Recv-Info” header from the INVITE using a Session Manager Adaptation.
- A number of errors were observed when sending fax, this was retested with ECM turned Without ECM, the fax transmission was faster and a visual inspection showed that the fax was of satisfactory quality.
- When calling a Communication Manager extension DDI from a number configured as EC500 for another extension, no ringback was heard. Due to Lab equipment constraints, these calls were made from a VoIP user. As the signalling was correct, this was considered to be a fault in the VoIP network and not an interworking issue.
- When transferring an outbound PSTN call on a one-X® Communicator softphone to an internal extension, a failure announcement was heard from the PSTN as well as ringing from the extension. The call was successfully transferred.
- When making outbound calls using one-X® Communicator in “Other phone” mode, no ringback was heard when the “Other Phone” was a Communication Manager H.323 extension forwarded from a Belgian national number. This was considered to be specific to the test environment. During this test, the Alert-Info header was removed using an SM Adaptation.
- During testing of Consultative transfer to internal extension by Avaya one-X® Communicator in “Other Phone” Mode, audio was lost to the VoIP user being used as the “Other phone”. This was a fault with the VoIP user as there was also no audio when ringing from a PSTN phone. Testing continued with signalling checked to determine whether or not a call was a success, and some tests were repeated successfully with a different type of “Other phone”

- When testing failure of the SIP Trunk, the network sent numerous re-INVITEs in response to error messages from Session Manager. This resulted in 45 seconds of silence before a failure tone was heard.
- During testing, two softphone clients were used that were registered to the Proximus IMS. These were not part of the tested solution, but were used for test cases that required outgoing calls to the PSTN. To make these clients work effectively, **Delayed SDP** was used in the Avaya SBCE configuration to prevent the sending of empty INVITE messages as described in **Section 7.4**. This resolved an issue where Communication Manager cleared calls that were put on hold. When there was no SDP in the INVITE, the 200 OK from the soft clients included an SDP that was not accepted by Communication Manager.

2.3. Support

For technical support on Proximus products please contact Proximus on 0800 55200 or visit their website at http://www.proximus.be/en/id_zwpl_s/large-companies-and-public-sector/support.html

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Proximus SIP Trunking service. Located at the Enterprise site is an Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP deskphones (with SIP and H.323 firmware), Avaya 16xx series IP deskphones (with H.323 firmware), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Avaya Communicator for Windows running on laptop PCs.

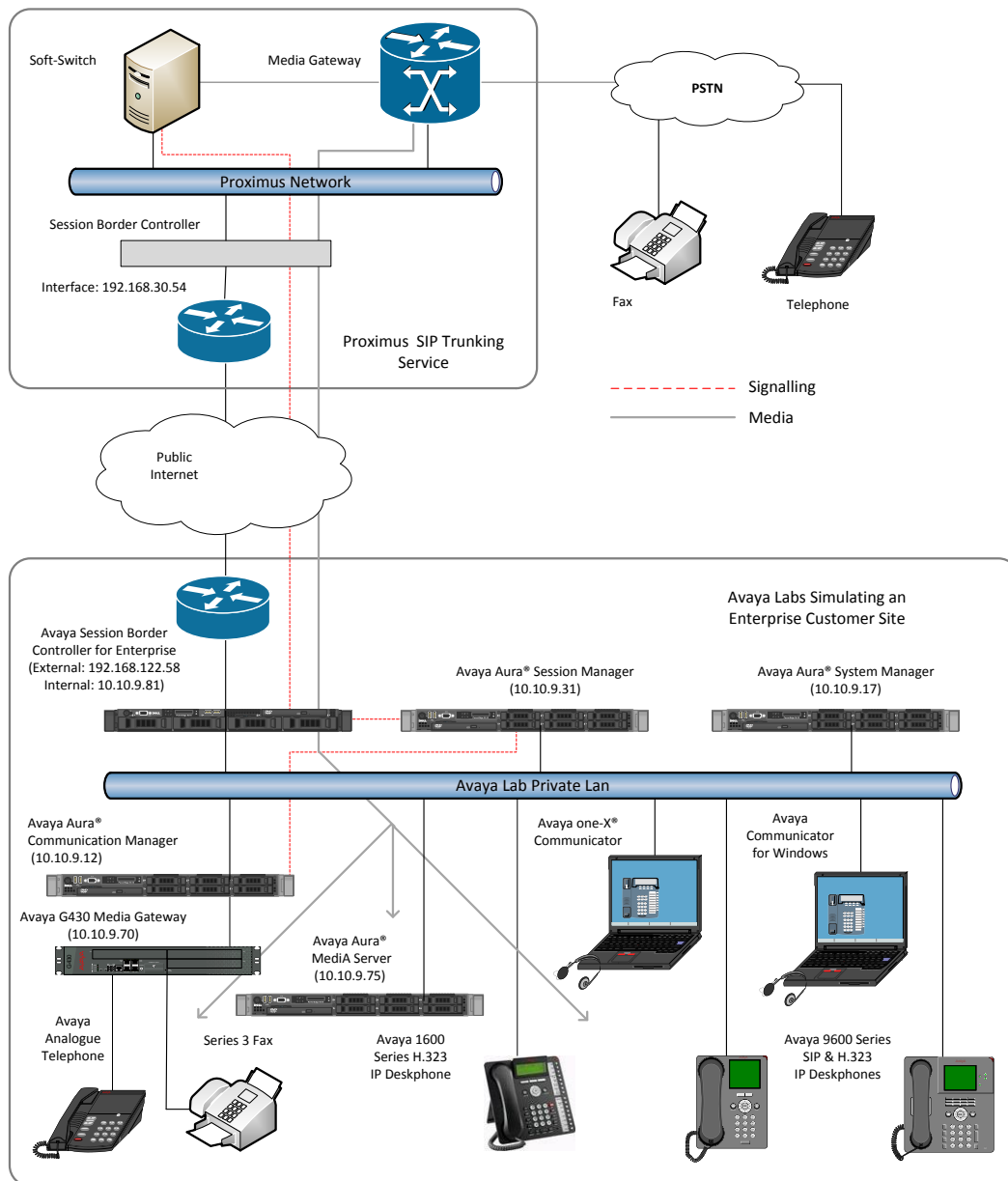


Figure 1: Test Setup Proximus SIP Trunking service to Avaya Enterprise

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Session Manager	7.0.0.1.700102
Avaya Aura® System Manager	7.0.0.1.4212
Avaya Aura® Communication Manager	7.0-441 Build 0.22684
Avaya Session Border Controller for Enterprise	7.0.0-21-6602 Patch sbc700-p001-20151005-7.0.0-21.x86_64.rpm
Avaya G430 Media Gateway	37.19.0
Avaya Aura® Media Server	7.7.0.236_2015.07.24
Avaya 96x0 Deskphone (SIP)	2_6_14_5
Avaya 9608 Deskphone (SIP)	7.0.0 R39
Avaya 96x0 Deskphone (H.323)	3.230A
Avaya 9608 Deskphone (H.323)	6.3116
Avaya 1616 Deskphone (H.323)	1.380B
Avaya One-X Communicator	6.2.7.03-SP7
Avaya Communicator for Windows	2.1.2.75
Avaya 2400 Series Digital Handsets	N/A
Analogue Handset	N/A
Analogue Fax	N/A
Proximus	
Alcatel-Lucent IMS Solution	Version 10.1

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP signalling associated with the Proximus SIP Trunking Service. For incoming calls, Session Manager receives SIP messages from the Avaya SBCE and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to Session Manager. Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Proximus network. Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the Servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorised Avaya sales representative to add additional capacity. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the Proximus SIP Trunking service and any other SIP trunks used.

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		4000	0
Maximum Concurrently Registered IP Stations:		2400	3
Maximum Administered Remote Office Trunks:		4000	0
Maximum Concurrently Registered Remote Office Stations:		2400	0
Maximum Concurrently Registered IP eCons:		68	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		2400	0
Maximum Video Capable IP Softphones:		2400	0
Maximum Administered SIP Trunks:		4000	20
Maximum Administered Ad-hoc Video Conferencing Ports:		4000	0
Maximum Number of DS1 Boards with Echo Cancellation:		80	0

On **Page 5**, verify that **IP Trunks** field is set to **y**.

```
display system-parameters customer-options                                     Page 5 of 12
                                OPTIONAL FEATURES

Emergency Access to Attendant? y                                           IP Stations? y
  Enable 'dadmin' Login? y
  Enhanced Conferencing? y
    Enhanced EC500? y
Enterprise Survivable Server? n
Enterprise Wide Licensing? n
  ESS Administration? y
  Extended Cvg/Fwd Admin? y
  External Device Alarm Admin? y
  Five Port Networks Max Per MCC? n
    Flexible Billing? n
  Forced Entry of Account Codes? y
  Global Call Classification? y
    Hospitality (Basic)? y
  Hospitality (G3V3 Enhancements)? y
    IP Trunks? y

IP Attendant Consoles? y
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for Session Manager. In this case, **Session_Manager** and **10.10.9.31** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** IP address as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```
display node-names ip
                                IP NODE NAMES

Name      IP Address
AMS       10.10.9.75
Session_Manager  10.10.9.31
default   0.0.0.0
procr      10.10.9.12
procr6    ::
```


5.3. Administer IP Network Region

Use the **change ip-network-region n** command where **n** is the chosen value of the configuration for the SIP Trunk. Set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the Avaya SBCE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **2** is used.
- The rest of the fields can be left at default values.

```
change ip-network-region 2                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 2
Location:      Authoritative Domain: avaya.com
Name: Trunk    Stub Network Region: n
MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes
Codec Set: 2   Inter-region IP-IP Direct Audio: yes
                IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5    AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS        RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

Note: In the test configuration, ip-network-region 1 was used within the enterprise and ip-network-region 2 was used for the SIP Trunk. In the configuration of the G430 (not shown) ip-network-region 1 was selected so that the G430 is used for calls within the enterprise and for analogue and digital endpoints. In the configuration of the Avaya Media Server (not shown), ip-network-region 2 was selected so that the Avaya Media Server (AMS) is used for the SIP Trunk.

5.4. Administer IP Codec Set

Open the IP Codec Set form for the codec set specified in the IP Network Region form in **Section 5.3** by typing **change ip-codec-set n** where **n** is the chosen value of the configuration for the SIP Trunk. Enter the list of audio codecs eligible to be used in order of preference. For the interoperability test the codecs supported by Proximus were configured, namely **G.711A** and **G.729A**.

```
change ip-codec-set 2                                     Page 1 of 2
```

IP CODEC SET

Codec Set: 2

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711A	n	2	20
2: G.729A	n	2	20
3:			
4:			

The Proximus SIP Trunking service supports T.38 for transmission of fax. Navigate to **Page 2** and define T.38 fax as follows:

- Set the **FAX - Mode** to **t.38-standard**
- Leave **ECM** at default value of **y**

```
change ip-codec-set 2                                     Page 2 of 2
```

IP CODEC SET

Allow Direct-IP Multimedia? n

	Mode	Redundancy	ECM: y	Packet Size (ms)
FAX	t.38-standard	0		
Modem	off	0		
TDD/TTY	US	3		
H.323 Clear-channel	n	0		
SIP 64K Data	n	0		20

Note: Fax was also successfully tested with G.711 fallback (**t.38-G711-fallback**); however Communication Manager always changes to G.711 on incoming faxes.

During testing, transmission of fax was unreliable due to network issues. Retesting was carried out with **ECM** set to **n** as described in **Section 2.2**. Fax transmission was faster and there were no visible quality issues.

Redundancy can be used to send multiple copies of T.38 packets which can help the successful transmission of fax over networks where packets are being dropped. This was not experienced in the test environment and **Redundancy** was left at the default value of **0**.

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Proximus SIP Trunking service. During test, this was configured to use TCP and port 5062 though it's recommended to use TLS and port 5061 in the live environment to enhance security.

Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to **tcp**.
- Set **Peer Detection Enabled** to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Far-end Node Name** to the Session Manager (node name **Session_Manager** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** as required. The standard value for TCP is **5060**, though **5062** was used in test to separate the SIP Trunk from the SIP endpoints on the Session Manager (See **Section 6.5**).
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3** (logically establishes the far-end for calls using this signalling group as network region 2).
- Leave **Far-end Domain** blank (allows Communication Manager to accept calls from any SIP domain on the associated trunk).
- Set **Direct IP-IP Audio Connections** to **y**.
- Set **Initial IP-IP Direct Media** and **H.323 Station Outgoing Direct Media** to **y**. This initiates direct media when the call is set up without the need for shuffling.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).

change signaling-group 2		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: Session_Manager	
Near-end Listen Port: 5062	Far-end Listen Port: 5062	
	Far-end Network Region: 2	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? y	Initial IP-IP Direct Media? y	
	Alternate Route Timer(sec): 6	

Note: The default values for the other fields may be used.

5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group n** command, where **n** is an available trunk group for the SIP Trunk. On **Page 1** of this form:

- Set the **Group Type** field to **sip**.
- Choose a descriptive **Group Name**.
- Specify a trunk access code (**TAC**) consistent with the dial plan.
- The **Direction** is set to **two-way** to allow incoming and outgoing calls.
- Set the **Service Type** field to **public-ntwrk**.
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**.
- Specify the **Number of Members** supported by this SIP trunk group.

add trunk-group 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: SIP_Trunk	COR: 1	TN: 1	TAC: 102
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 2		
	Number of Members: 10		

On **Page 2** of the trunk-group form, the Preferred **Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Proximus to prevent unnecessary SIP messages during call setup. During testing, a value of **900** was used that sets Min-SE to 1800 in the SIP signalling.

add trunk-group 2		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 900			
Disconnect Supervision - In? y Out? y			

On **Page 3**, set the **Numbering Format** field to **private**. This allows delivery of CLI in formats other than E.164 with leading “+”. In test, CLIs were sent as Communication Manager extension numbers and were reformatted by Session Manager in an Adaptation described in **Section 6.4**. This format was successfully verified in the network.

add trunk-group 2	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	
	UI Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n

On **Page 4** of this form:

- Set **Send Diversion Header** and **Support Request History** to **n** as these headers are not supported in the Proximus SIP trunk.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Proximus (this Payload Type is not applied to calls from SIP end-points).
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on Communication Manager extension.

add trunk-group 2	Page 4 of 21
PROTOCOL VARIATIONS	
	Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? n	
Support Request History? n	
Telephone Event Payload Type: 101	
	Convert 180 to 183 for Early Media? n
	Always Use re-INVITE for Display Updates? n
Identity for Calling Party Display: From	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
	Enable Q-SIP? n

Note: - The above screenshot shows **Network Call Redirection** set to **y**. This was temporarily set to **y** for some of the last tests that involved testing of 302 Moved Temporarily and REFER messages. When set, REFER messages are sent that are not acted on by the Proximus SIP Trunking service and so are unnecessary additional signalling.

5.7. Administer Calling Party Number Information

Use the **change private-unknown-numbering** command to configure Communication Manager to send the calling party number in the format required. In test, calling party numbers were sent as Communication Manager extension numbers to be modified in Session Manager. Adaptations are used in Session Manager to format the number as described in **Section 6.4**. These calling party numbers are sent in the SIP From, Contact and PAI headers. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
4	2	1-2		4	Total Administered: 2
					Maximum Entries: 540

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the Proximus SIP Trunking service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *69		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 8		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 2**.

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
	0	8	12	2	pubu		n
	00	13	15	2	pubu		n
	1	3	3	2	pubu		n
	118	5	6	2	pubu		n
	7000	4	4	1	pubu		n

Use the **change route-pattern n** command, where **n** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **2** is used to route calls to trunk group **2**. **Numbering Format** is applied to CLI and is used to set TDM signalling parameters such as type of number and numbering plan indicator. This doesn't have the same significance in SIP calls and during testing it was set to **lev0-pvt** to ensure that calling party number was not prefixed with a leading "+".

change route-pattern 2														Page 1 of 3															
Pattern Number: 2														Pattern Name: SIP_Endpoints															
SCCAN? n														Secure SIP? n		Used for SIP stations? n													
Grp FRL NPA Pfx Hop Toll No.														Inserted		DCS/ IXC													
No														Mrk Lmt List Del		Digits		QSIG											
														Dgts		Intw													
1: 2														0		n		user											
2:																n		user											
3:																n		user											
4:																n		user											
5:																n		user											
6:																n		user											
BCC VALUE														TSC		CA-TSC		ITC BCIE		Service/Feature		PARM		Sub		Numbering		LAR	
0 1 2 M 4 W																Request								Dgts		Format			
1: y y y y y n														n		rest								lev0-pvt		none			
2: y y y y y n														n		rest										none			
3: y y y y y n														n		rest										none			
4: y y y y y n														n		rest										none			
5: y y y y y n														n		rest										none			
6: v v v v v n														n		rest										none			

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to Communication Manager extensions. The incoming digits sent in the INVITE message from Proximus can be manipulated as necessary to route calls to the desired extension. During test, the incoming DDI numbers were changed in Session Manager to Communication Manager extension numbers using an Adaptation as described in **Section 6.4**. When done this way, there is no requirement for any incoming digit translation in Communication Manager. If incoming digit translation is required, use the **change inc-call-handling-trmt trunk-group x** command where **x** is the Trunk Group defined in **Section 5.6**.

change inc-call-handling-trmt trunk-group 2				Page	1 of	3
INCOMING CALL HANDLING TREATMENT						
Service/	Number	Number	Del	Insert		
Feature	Len	Digits				
public-ntwrk						
public-ntwrk						

Note: One reason for configuring the enterprise in this way is to allow the use of the extension number as a common identifier with other network elements within the enterprise such as voice mail.

5.10. EC500 Configuration

When EC500 is enabled on a Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2391. Use the command **change off-pbx-telephone station-mapping x** where **x** is Communication Manager station.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** if required by the routing configuration.
- For the **Phone Number** enter the phone that will also be called (e.g. **02797nnnn**).
- Set the **Trunk Selection** to **ars** so that the ARS table will be used for routing.
- Set the **Config Set** to **1**.

change off-pbx-telephone station-mapping 2391							Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual		
Extension		Prefix			Selection	Set	Mode		
2391	EC500	-		02797nnnn	ars	1			

Note: The phone number shown is for a VoIP user registered with the Proximus IMS system independently of the test environment. To use facilities for calls coming in from EC500 mobile phones, the calling party number received in Communication Manager must exactly match the number specified in the above table.

Save the Communication Manager configuration by entering **save translation**.

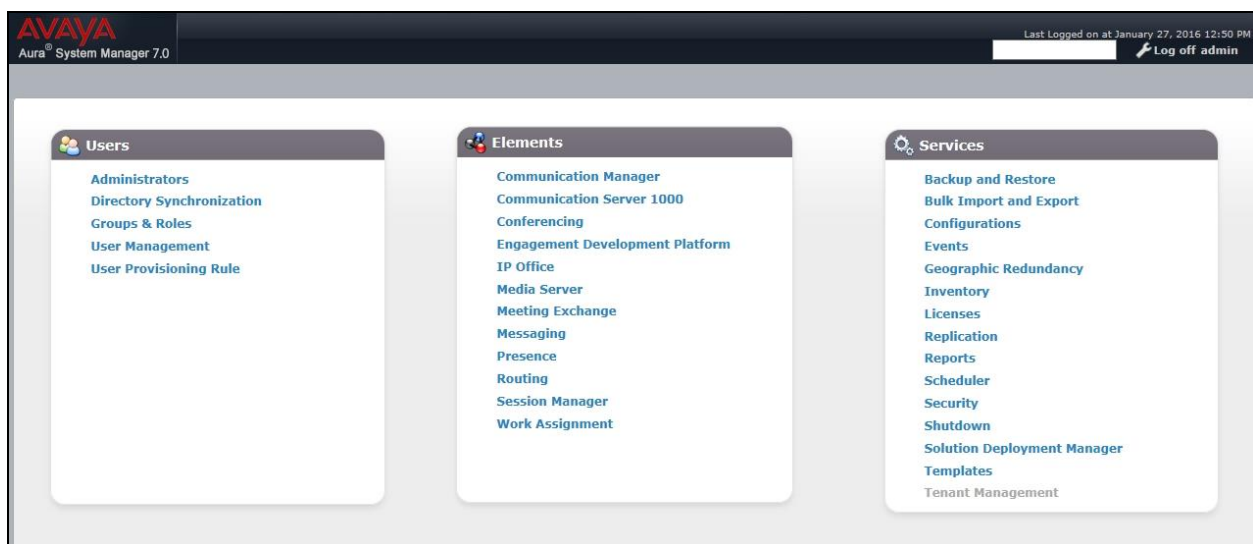
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured by opening a web browser to System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager
- Administer SIP Extensions

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a web browser and entering **http://<FQDN>/SMGR**, where <FQDN> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** tab will be presented with menu options shown below.



6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name of the enterprise site or a name agreed with Proximus; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on Communication Manager. Refer to **Section 5.3** for details. In test, **avaya.com** was used. Optionally, a description for the domain can be entered in the Notes field (not shown). Click **Commit** to save changes.

The screenshot shows the Avaya Session Manager web interface. The top navigation bar has 'Home' and 'Routing' tabs. The left sidebar is expanded to 'Routing', and 'Domains' is selected. The main content area is titled 'Domain Management' and includes buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below these is a table with one item, 'avaya.com', of type 'sip'. The table has columns for 'Name', 'Type', and 'Notes'. A 'Select' dropdown is at the bottom of the table, showing 'All, None'.

Name	Type	Notes
avaya.com	sip	

Note: If the existing domain name used in the enterprise equipment does not match that used in the network, Topology Hiding in the Avaya SBCE can be used to change it (see **Section 7.8**).

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu (not shown). Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the test enterprise.

Home / Elements / Routing / Locations

Help ?

Location Details

CommitCancel

General

* Name:

Galway

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

2000 Kbit/Sec

* Minimum Multimedia Bandwidth:

64 Kbit/Sec

* Default Audio Bandwidth:

80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold:

80 %

Multimedia Alarm Threshold:

80 %

* Latency before Overall Alarm Trigger:

5 Minutes

* Latency before Multimedia Alarm Trigger:

5 Minutes

Location Pattern

AddRemove

1 Item

Filter: Enable

☐ IP Address Pattern

Notes

☐ *10.10.9.x

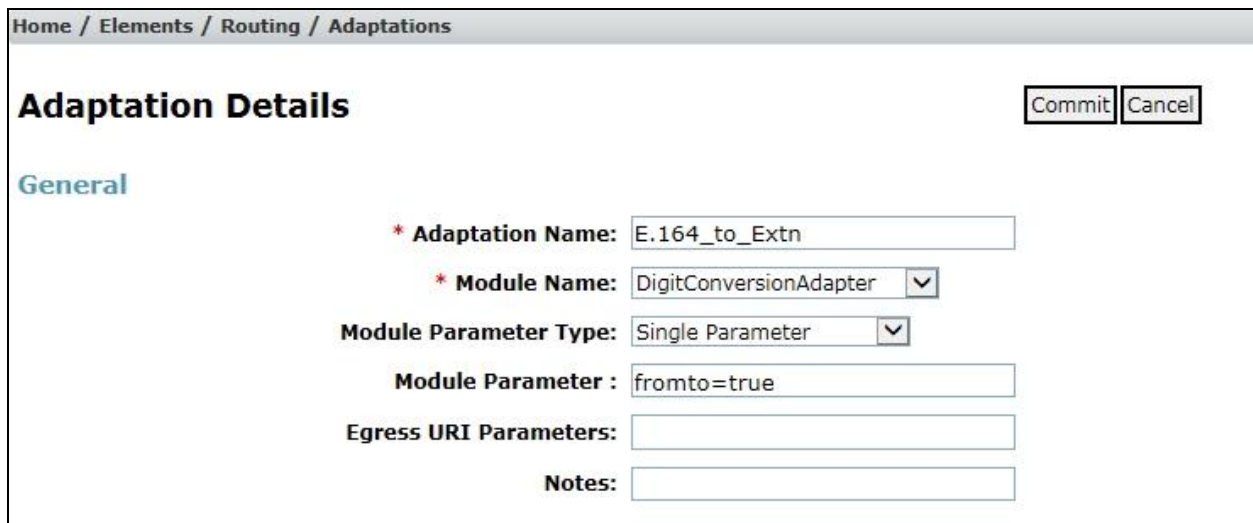
Select : All, None

6.4. Administer Adaptations

Calls from Proximus are received at the enterprise in E.164 format with leading “+” on the Request URI. An Adaptation specific to Communication Manager is used to convert the called party number to a pre-defined extension number before onward routing to the Communication Manager SIP Entity, removing the requirement for incoming digit manipulation on Communication Manager.

On the **Routing** tab select **Adaptations** from the left-hand menu. Click on **New** (not shown).

- In the **Adaptation name** field, enter a descriptive title for the adaptation.
- In the **Module name** drop down menu, select **DigitConversionAdapter**. This is used for simple digit conversion adaptations.
- In the **Module Parameter Type** drop down menu, select **Single Parameter**.
- In the Module Parameter box (not shown), type **fromto=true**. This will apply the adaptation to the From and To headers as well as the Request URI.



Home / Elements / Routing / Adaptations

Adaptation Details

General

* **Adaptation Name:**

* **Module Name:**

Module Parameter Type:

Module Parameter :

Egress URI Parameters:

Notes:

Scroll down and in the section **Digit Conversion for Outgoing Calls from SM**, click on **Add**. An additional row will appear (not shown). This allows information to be entered for the manipulation of numbers coming from the network. This is where the called party number is translated from E.164l format to the extension number for termination of calls on Communication Manager. In addition, the calling party number is adapted to diallable format for display on Communication Manager extensions.

The screenshot below shows a translation for each called party number. This is not normally necessary where the extension number forms part of the national number. When this is the case, a simple deletion of the leading digits is required.

- Under **Matching Pattern** enter the DDI number as received from the network.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the incoming DDI number.
- Under **Delete Digits** enter the number of digits to delete to leave only the extension number remaining, during test all had to be deleted as the extension number did not form part of the national number.
- Under **Insert Digits** enter digits to be inserted. During test, this was the full extension number. If the extension number forms part of the DDI number, there will be no entry required here.
- Under **Address to Modify** choose **destination** from the drop down box to apply this rule to the To and Request-Line headers only.

Digit Conversion for Outgoing Calls from SM

Add Remove

12 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* +	* 11	* 15		* 1	00	origination		
<input type="checkbox"/>	* +32	* 11	* 11		* 3	0	origination		
<input type="checkbox"/>	* +32279nnnn0	* 11	* 11		* 11	2000	destination		
<input type="checkbox"/>	* +32279nnnn1	* 11	* 11		* 11	2391	destination		
<input type="checkbox"/>	* +32279nnnn2	* 11	* 11		* 11	2291	destination		
<input type="checkbox"/>	* +32279nnnn3	* 11	* 11		* 11	2316	destination		
<input type="checkbox"/>	* +32279nnnn4	* 11	* 11		* 11	2400	destination		
<input type="checkbox"/>	* +32279nnnn5	* 11	* 11		* 11	2401	destination		
<input type="checkbox"/>	* +32279nnnn6	* 11	* 11		* 11	7000	destination		
<input type="checkbox"/>	* +32279nnnn7	* 11	* 11		* 11	6002	destination		
<input type="checkbox"/>	* +32279nnnn8	* 11	* 11		* 11	2290	destination		
<input type="checkbox"/>	* +32279nnnn9	* 11	* 11		* 11	2396	destination		

Select : All, None

Commit Cancel

Note: In the above screenshots the DDI numbers are partially obscured. If the number is to be changed to diallable format for display on Communication Manager extensions, additional rows may be required. These would replace a leading “+” with “00” for international calling party numbers and “+32” would be replaced by “0” for national calling party numbers.

An additional Adaptation is required to convert extension numbers to national format. Calls from Communication Manager are received at Session Manager with the extension number in the From header. An Adaptation specific to Proximus is used to convert the calling party number to national format with no leading “0” before onward routing to the Proximus SIP Trunking service. This Adaptation is also used to remove unnecessary and Avaya proprietary headers from SIP messages outbound to the Proximus SIP trunk.

On the **Routing** tab select **Adaptations** from the left-hand menu. Click on **New** (not shown).

- In the **Adaptation name** field, enter a descriptive title for the adaptation.
- In the **Module name** drop down menu, select **DigitConversionAdapter**. This is used for simple digit conversion adaptations.
- In the **Module parameter Type** drop down menu, select **Name-Value Parameter**.
- In the **Name** field, type eRHdrs to remove SIP headers.
- In the **Value** field, type the names of the headers to be removed. During testing, the headers removed were as follows: "**P-AV-Message-Id, P-Charging-Vector, Av-Global-Session-ID, P-Location, Endpoint-View, Recv-Info, P-Conference, Alert-Info**".
- Click on **Add** to specify an additional parameter.
- In the **Name** field, type **fromto**.
- In the **Value** field, type **true**. This will apply the adaptation to the From and To headers as well as the Request URI.

Home / Elements / Routing / Adaptations

Adaptation Details Commit Cancel Help ?

General

* Adaptation Name:

* Module Name:

Module Parameter Type:

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	eRHdrs	"P-AV-Message-Id, P-Charging-Vector, Av-Global-Session-ID, P-Location, Endpoint-View, Recv-
<input type="checkbox"/>	fromto	true

Select : All, None

Egress URI Parameters:

Notes:

Scroll down and in the section **Digit Conversion for Outgoing Calls from SM**, click on **Add**. An additional row will appear (not shown). This allows information to be entered for the manipulation of numbers coming from Communication Manager. This is where the calling party number is translated from the extension number to E.164 format with leading “+” for display on the terminating PSTN phones as the diallable DDI number assigned to the extension.

The screenshot below shows a translation for each calling party number. This is not normally necessary where the extension number forms part of the national number. When this is the case, a simple additional of the leading digits to build up the national format is required.

- Under **Matching Pattern** enter the extension number as received from Communication Manager.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the incoming DDI number.
- Under **Delete Digits** enter the number of digits to delete to remove any digits that will not form part of the national number, during test all had to be deleted as the extension number did not form part of the national number.
- Under **Insert Digits** enter digits to be inserted. During test, this was the E.164 number with leading “+”. If the extension number forms part of the DDI number, only the necessary prefix digits will be required.
- Under **Address to Modify** choose **origination** from the drop down box to apply this rule to the From header only.

Digit Conversion for Outgoing Calls from SM

Add Remove

11 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*0	*9	*10		*1	+32	destination		
<input type="checkbox"/>	*00	*11	*17		*2	+	destination		
<input type="checkbox"/>	*2000	*4	*4		*4	+32279nnnn0	origination		
<input type="checkbox"/>	*2001	*4	*4		*4	+32279nnnn7	origination		
<input type="checkbox"/>	*2290	*4	*4		*4	+32279nnnn8	origination		
<input type="checkbox"/>	*2291	*4	*4		*4	+32279nnnn2	origination		
<input type="checkbox"/>	*2316	*4	*4		*4	+32279nnnn4	origination		
<input type="checkbox"/>	*2391	*4	*4		*4	+32279nnnn1	origination		
<input type="checkbox"/>	*2396	*4	*4		*4	+32279nnnn9	origination		
<input type="checkbox"/>	*2400	*4	*4		*4	+32279nnnn4	origination		
<input type="checkbox"/>	*2401	*4	*4		*4	+32279nnnn5	origination		

Select : All, None

Commit Cancel

Note: In the above screenshots the DDI numbers are partially obscured. Also, the called party number is converted to E.164 format with leading “+”. This wasn’t strictly necessary during testing as the network is able to do the conversion, but it’s shown here for use if required. Add additional lines for destination numbers starting with “0” or “00”. If the number starts with “0”, it is a national number and the leading “0” must be replaced with “+32”. If the number starts with “00”, it is an international number and the leading “00” must be replaced with “+”.

6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu, and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **General**:

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **SIP Trunk** for the Avaya SBCE SIP entity.
- In the **Adaptation** field (not available for the Session Manager SIP Entity), select the appropriate Adaptation from the drop down menu.
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity.

In this configuration there are four SIP Entities:

- Avaya Aura® Session Manager SIP Entity.
- Avaya Aura® Communication Manager SIP Entity for the SIP Endpoints
- Avaya Aura® Communication Manager SIP Entity for the SIP Trunk
- Avaya Session Border Controller for Enterprise (Avaya SBCE) SIP Entity.

6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface.

The screenshot shows the 'SIP Entity Details' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'General' selected. In the top right corner, there are 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields: 'Name' (text box with 'Session_Manager'), 'FQDN or IP Address' (text box with '10.10.9.31'), 'Type' (dropdown menu with 'Session Manager' selected), 'Notes' (text box), 'Location' (dropdown menu with 'Galway' selected), 'Outbound Proxy' (dropdown menu), 'Time Zone' (dropdown menu with 'Europe/Dublin' selected), and 'Credential name' (text box). Below the 'General' section is the 'SIP Link Monitoring' section, which contains a 'SIP Link Monitoring' dropdown menu with 'Use Session Manager Configuration' selected.

Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field enter the port number on which the system listens for SIP requests.
- In the **Protocol** field enter the transport protocol to be used for SIP requests.
- In the **Default Domain** field, from the drop down menu select the domain added in **Section 6.2** as the default domain.

Listen Ports

TCP Failover port:

TLS Failover port:

Add Remove

4 Items Filter: Enable

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	
<input type="checkbox"/>	5060	UDP	avaya.com	
<input type="checkbox"/>	5061	TLS	avaya.com	
<input type="checkbox"/>	5062	TCP	avaya.com	

Select : All, None

6.5.2. Avaya Aura® Communication Manager SIP Entities

The following screen shows one of the SIP entities for Communication Manager which is configured as an Evolution Server. This SIP Entity is used for the SIP Trunk. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the **Location** to that defined in **Section 6.3**.

Home / Elements / Routing / SIP Entities Help ?

SIP Entity Details Commit Cancel

General

* Name: CM Trunk

* FQDN or IP Address: 10.10.9.12

Type: CM

Notes:

Adaptation: E.164_to_Extn

Location: Galway

Time Zone: Europe/Dublin

* SIP Timer B/F (in seconds): 4

Credential name:

Securable: ☐

Call Detail Recording: none

Other parameters can be set for the SIP Entity as shown in the following screenshot, but for test, these were left at default values.

Loop Detection

Loop Detection Mode: On ▼

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration ▼

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association: ▼

Backup Session Manager Bandwidth Association: ▼

Note: An identical SIP Entity for Communication Manager is required for SIP Endpoints. In the test environment, the name of this SIP Entity is **CM_SIP_Endpoints**, and it is differentiated by use of port number

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set the **Adaptation** to that defined in **Section 6.4**, the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel Help ?

General

* Name: ASBCE

* FQDN or IP Address: 10.10.9.81

Type: SIP Trunk ▼

Notes:

Adaptation: Extn_to_E164 ▼

Location: Galway ▼

Time Zone: Europe/Dublin ▼

* SIP Timer B/F (in seconds): 4

Credential name:

Securable: ☐

Call Detail Recording: none ▼

6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **Session Manager**.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Select the **Trusted** tick box to make the other system trusted.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.

Click **Commit** to save changes. The following screen shows the Entity Links used in this configuration.

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	ASBCE_Link	Session_Manager	TCP	5060	ASBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM_Entity_Link	Session_Manager	TCP	5060	CM_SIP_Endpoints	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM_Trunk_Link	Session_Manager	TCP	5062	CM Trunk	<input type="checkbox"/>	5062	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Messaging_Link	Session_Manager	TCP	5060	Messaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

Note: There are two Entity Links for Communication Manager, one for the SIP Endpoints and the other for the SIP Trunk. These are differentiated by port number. The **Messaging_Link** Entity Link is used for the Avaya Aura ® Messaging system and is not described in this document.

6.7. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- Enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies
- Under **Time of Day**, click **Add**, and then select the time range

The following screen shows the routing policy for calls inbound from the SIP Trunk to Communication Manager.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM Trunk	10.10.9.12	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed to the PSTN via the Proximus SIP Trunking service.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE	10.10.9.81	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

6.8. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- In the **Pattern** field enter a dialled number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialled number.
- In the **Max** field enter the maximum length of the dialled number.
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**.

Under **Originating Locations and Routing Policies**:

- Click **Add**, in the resulting screen (not shown).
- Under **Originating Location**, select the location defined in **Section 6.3** or **ALL**.
- Under **Routing Policies** select one of the routing policies defined in **Section 6.7**.
- Click **Select** button to save.

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the PSTN via the Proximus SIP Trunking service.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	PSTN_Outbound	0	<input type="checkbox"/>	ASBCE		

Select : All, None

The following screen shows the test dial pattern configured for Communication Manager.

Dial Pattern Details [Commit] [Cancel] Help ?

General

* Pattern: +32279nnnn x

* Min: 10

* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- v

Notes:

Originating Locations and Routing Policies

[Add] [Remove]

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name ^	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		CM_Inbound	0	<input type="checkbox"/>	CM Trunk	

Select : All, None

Note: The above configuration is used to analyse the DDI numbers assigned to the extensions on Communication Manager. Some of the digits of the pattern to be matched have been obscured.

6.9. Administer Application for Avaya Aura® Communication Manager

The Application for Communication Manager would normally be defined at system installation, but is shown here for reference. From the **Home** tab select **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration → Applications** and click **New** (not shown).

- In the **Name** field enter a name for the application.
- In the **SIP Entity** field select the SIP entity for Communication Manager.
- In the **CM System for SIP Entity** field select the SIP entity for Communication Manager SIP Endpoints and select **Commit** to save the configuration.

Application Editor [Commit] [Cancel]

Application

* Name: CM_App

* SIP Entity: CM_SIP_Endpoints

* CM System for SIP Entity: CM1_Element [Refresh] [View/Add CM Systems](#)

Description:

6.10. Administer Application Sequence for Avaya Aura® Communication Manager

The Application Sequence for Communication Manager would normally be defined at system installation, but is shown here for reference. From the left panel navigate to **Session Manager** → **Application Configuration** → **Application Sequences** and click on **New** (not shown).

- In the **Name** field enter a descriptive name.
- Under **Available Applications**, click the + sign in front of the appropriate application instance. When the screen refreshes the application should be displayed under the **Applications in this Sequence** heading. Select **Commit**.

Home / Elements / Session Manager / Application Configuration / Application Sequences [Help ?](#)

Application Sequence Editor

Application Sequence

*Name:

Description:

Applications in this Sequence

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		CM_App	CM_Entity	<input checked="" type="checkbox"/>	

Select : All, None

Available Applications

1 Item [Filter: Enable](#)

	Name	SIP Entity	Description
	CM_App	CM_Entity	

6.11. Administer SIP Extensions

SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the **Home** tab select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields.
- In the **Login Name** field enter a unique system login name in the form of user@domain e.g. 2291@avaya.com which is used to create the user's primary handle.
- The **Authentication Type** should be **Basic**.
- In the **Password/Confirm Password** fields enter an alphanumeric password.
- Set the **Language Preference** and **Time Zone** as required.

Home / Routing / Session Manager / User Management / Manage Users

New User Profile

Commit & Continue Commit

Identity * Communication Profile Membership Contacts

User Provisioning Rule

User Provisioning Rule: [v]

Identity

* Last Name: SIP
Last Name (Latin Translation): SIP

* First Name: 9608
First Name (Latin Translation): 9608

Middle Name: [v]
Description: [v]

* Login Name: 2291@avaya.com
Authentication Type: Basic [v]
Password: [masked]
Confirm Password: [masked]
Localized Display Name: [v]
Endpoint Display Name: [v]
Title: [v]
Language Preference: English (United Kingdom) [v]
Time Zone: (0:0)GMT : Dublin, Edinburgh, L [v]
Employee ID: [v]
Department: [v]
Company: [v]

On the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it.


The screenshot shows the 'Communication Profile' tab in a configuration window. It includes fields for 'Communication Profile Password' and 'Confirm Password', both masked with dots. Below these are buttons for 'New', 'Delete', 'Done', and 'Cancel'. A section titled 'Name' contains a radio button for 'Primary' and a 'Select : None' dropdown. Below this is a field for 'Name' with the value 'Primary' and a 'Default' checkbox which is checked. A section titled 'Communication Address' contains buttons for 'New', 'Edit', and 'Delete'. Below these is a table with columns 'Type', 'Handle', and 'Domain'. The table is empty, showing 'No Records found'. Below the table is a scroll bar.

Expand the **Communication Address** section and click **New**. For the **Type** field select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.

The screenshot shows the 'Communication Address' section expanded. It includes buttons for 'New', 'Edit', and 'Delete'. Below these is a table with columns 'Type', 'Handle', and 'Domain'. The table is empty, showing 'No Records found'. Below the table is a scroll bar. Below the scroll bar are fields for 'Type' (set to 'Avaya SIP') and 'Fully Qualified Address' (set to '2291 @ avaya.com'). There are 'Add' and 'Cancel' buttons at the bottom right.

Expand the **Session Manager Profile** section.


- Make sure the **Session Manager Profile** check box is checked.
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field.
- Select the appropriate application sequence from the drop-down menu in the **Origination Sequence** field configured in **Section 6.10**.
- Select the appropriate application sequence from the drop-down menu in the **Termination Sequence** field configured in **Section 6.10**.
- Select the appropriate location from the drop-down menu in the **Home Location** field.

☒ **Session Manager Profile** 


SIP Registration
* Primary Session Manager



Secondary Session Manager



Survivability Server

Max. Simultaneous Devices 

Block New Registration When Maximum Registrations Active? ☐

Primary	Secondary	Maximum
4	0	4
		

Application Sequences
Origination Sequence 
Termination Sequence 

Call Routing Settings
* Home Location 
Conference Factory Set 

Call History Settings
Enable Centralized Call History? ☐

Expand the **Endpoint Profile** section.

- Select Communication Manager Element from the **System** drop-down menu.
- Select **Endpoint** from the drop-down menu for **Profile Type**.
- Enter the extension in the **Extension** field.
- Select the desired template from the **Template** drop-down menu.
- In the **Port** field **IP** is automatically inserted.
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box.
- Select **Commit** (Not Shown) to save changes and System Manager will add the Communication Manager user configuration automatically.

☒ **CM Endpoint Profile** ▼

* System

CM1_Element ▼

* Profile Type

Endpoint ▼

Use Existing Endpoints ☐

* Extension

Q 2291

Endpoint Editor

* Template

9608SIP_DEFAULT_CM_7_0 ▼

Set Type

9608SIP

Security Code

Port

IP

Voice Mail Number

Preferred Handle

(None) ▼

Calculate Route Pattern ☐

Sip Trunk

aar

Enhanced Callr-Info display for 1-line phones ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User ☒

Override Endpoint Name and Localized Name ☒

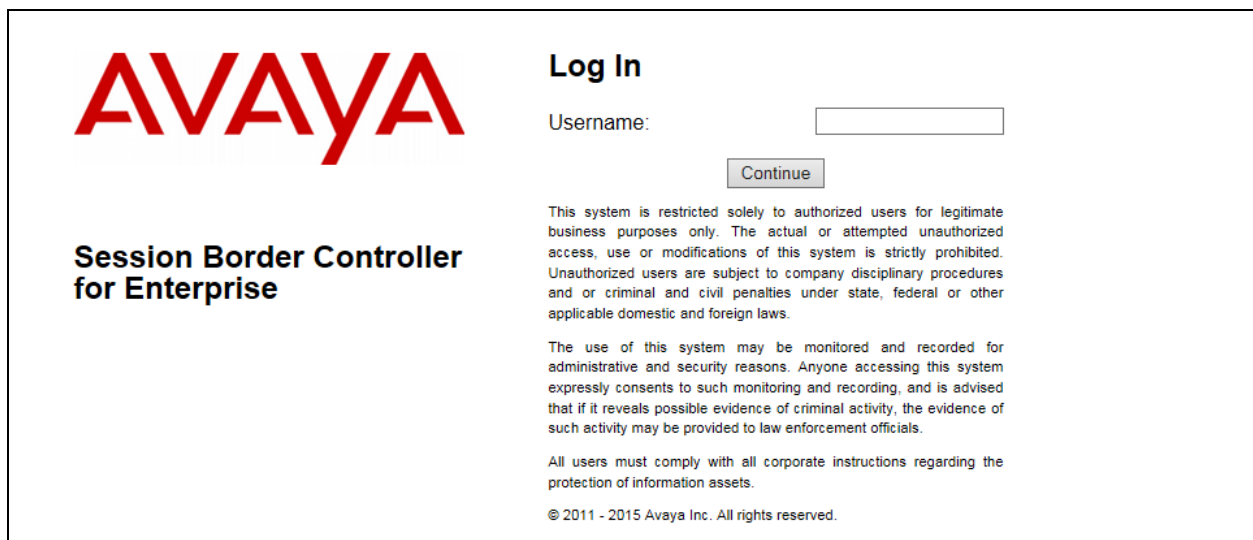
Allow H.323 and SIP Endpoint Dual Registration ☐

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

7.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using the appropriate username and password.



The login screen features the Avaya logo in red on the left. To the right, under the heading "Log In", is a "Username:" label followed by a text input field and a "Continue" button. Below the input field, there are two paragraphs of legal disclaimer text. At the bottom, it states "© 2011 - 2015 Avaya Inc. All rights reserved."

AVAYA

Session Border Controller for Enterprise

Log In

Username:

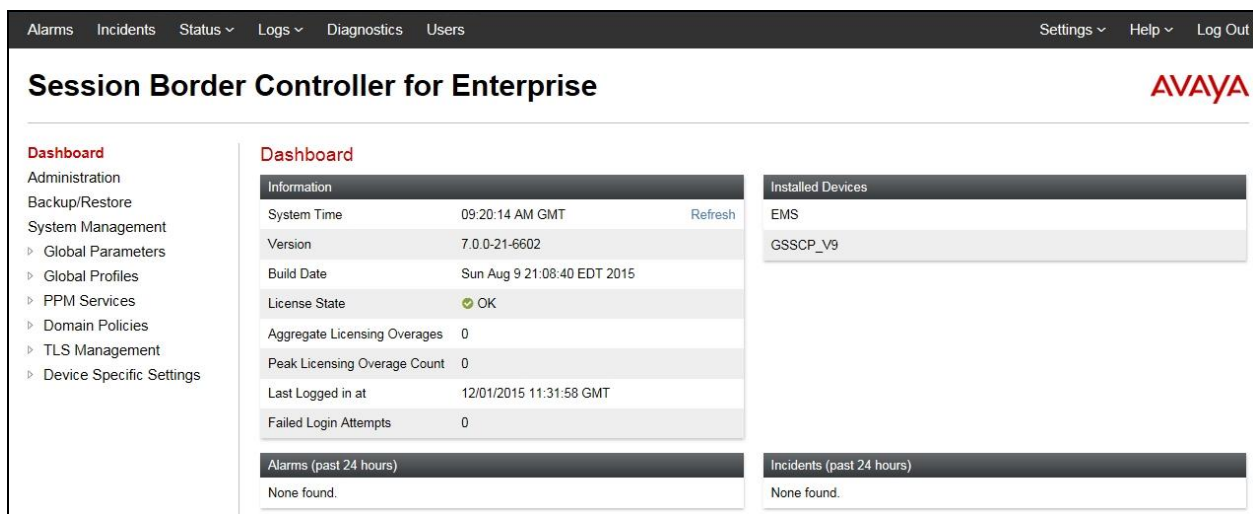
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2015 Avaya Inc. All rights reserved.

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



The dashboard has a top navigation bar with links: Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. On the left is a sidebar menu with "Dashboard" selected, and sub-items: Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is divided into three sections: "Information" (System Time, Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count, Last Logged in at, Failed Login Attempts), "Installed Devices" (EMS, GSSCP_V9), and "Alarms (past 24 hours)" and "Incidents (past 24 hours)" (both showing "None found").

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise **AVAYA**

Dashboard

Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ PPM Services
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings

Dashboard

Information	
System Time	09:20:14 AM GMT Refresh
Version	7.0.0-21-6602
Build Date	Sun Aug 9 21:08:40 EDT 2015
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	12/01/2015 11:31:58 GMT
Failed Login Attempts	0

Installed Devices

EMS
GSSCP_V9

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

7.2. Define Network Management

Network information is required on the Avaya SBCE to allocate IP addresses and subnet masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one physical interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** in the main menu on the left hand side and click on **Add**.

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ PPM Services
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings
‣ **Network Management**

Network Management: GSSCP_V9

Devices
GSSCP_V9

Interfaces
Networks

Add

Name	Gateway	Subnet Mask	Interface	IP Address
------	---------	-------------	-----------	------------

Enter details for the external interface in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interface in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external interface to be used from the **Interface** drop down menu. In the test environment, this was **B1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

Add Network X

Name External

Default Gateway 192.168.122.7

Subnet Mask 255.255.255.128

Interface B1

Add

IP Address	Public IP	Gateway Override
192.168.122.58 x	Use IP Address	Use Default

Delete

Finish

Click on **Add** to define the internal interface. Enter details in the dialogue box (not shown):

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interface in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the internal interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

The following screenshot shows the completed Network Management configuration:

Network Management: GSSCP_V9

Devices: GSSCP_V9

Interfaces | **Networks**

Add

Name	Gateway	Subnet Mask	Interface	IP Address	Edit	Delete
Internal	10.10.9.1	255.255.255.0	A1	10.10.9.81	Edit	Delete
External	192.168.122.7	255.255.255.128	B1	192.168.122.58	Edit	Delete

Select the **Interface Configuration** tab and click on the **Status** of the physical interface to toggle it. A status of **Disabled** will be changed to **Enabled**.

Network Management: GSSCP_V9

Devices: GSSCP_V9

Interfaces | Networks

Add VLAN

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on **System Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box will appear (not shown) that will indicate when the application has restarted.

7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces. Testing was carried out with TCP used for transport of signalling between Session Manager and the Avaya SBCE, and UDP for transport of signalling between the Avaya SBCE and the Proximus SIP Trunking service. This document shows the configuration for TCP and UDP, if additional security is required, it's recommended to use TLS and port 5061.

7.3.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** (not shown) in the main menu on the left hand side. Details of transport protocol and ports for the external and internal SIP signalling are entered here.

- Select **Add** and enter details of the external signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was a single IP address **192.168.122.58**.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for the Proximus SIP Trunking service.

The screenshot shows the 'Session Border Controller' web interface. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. The 'Device Specific Settings' menu is expanded, showing 'Signaling Interface' as the selected option. On the right, a dialog box titled 'Add Signaling Interface' is open. The dialog contains the following fields: 'Name' (text input with 'External' entered), 'IP Address' (a dropdown menu showing 'External (B1, VLAN 0)' and a sub-dropdown showing '192.168.122.58'), 'TCP Port' (text input with 'Leave blank to disable' below it), 'UDP Port' (text input with '5060' entered and 'Leave blank to disable' below it), 'TLS Port' (text input with 'Leave blank to disable' below it), 'TLS Profile' (dropdown menu with 'None' selected), 'Enable Shared Control' (checkbox, currently unchecked), and 'Shared Control Port' (text input). A 'Finish' button is at the bottom right of the dialog.

The internal signalling interface is defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal signalling interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.
- Select **TCP** port number, **5060** is used for Session Manager.

The following screenshot shows details of the signalling interfaces:

Signaling Interface: GSSCP_V9

Devices

GSSCP_V9

Signaling Interface

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Internal	10.10.9.81 Internal (A1, VLAN 0)	5060	---	---	None	Edit Delete
External	192.168.122.58 External (B1, VLAN 0)	---	5060	---	None	Edit Delete

Note. In the test environment, the internal IP address was **10.10.9.81**.

7.3.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** in the main menu on the left hand side. Details of the RTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

- Select **Add** and enter details of the external media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was a single IP address **192.168.122.58**.
- Define the **RTP Port Range** for the media path with the Proximus SIP Trunking service, during testing this was set to **1000 – 10019** which were the port values opened up in the Proximus firewall.

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

PPM Services

Domain Policies

TLS Management

Device Specific Settings

Network Management

Media Interface

Media Interface: GSSCP_V9

Devices

GSSCP_V9

Add Media Interface

Name

External

IP Address

External (B1, VLAN 0)

192.168.122.58

Port Range

10000 - 10019

Finish

The internal media interface is defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.

The following screenshot shows details of the media interfaces:

Media Interface: GSSCP_V9

Devices

GSSCP_V9

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP Network	Port Range	
Internal	10.10.9.81 Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
External	192.168.122.58 External (B1, VLAN 0)	10000 - 10019	Edit Delete

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the Proximus SIP Trunking service is connected as the Trunk Server and Session Manager is connected as the Call Server.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. To define Server Interworking for the Proximus SIP trunk, click on **Add** (not shown). A pop-up menu is generated. In the **Name** field enter a descriptive name for Proximus and click **Next**.

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

Domain DoS

Server Interworking

Interworking Profiles: PRXMS

Interworking Profile

Profile Name

PRXMS

Next

OCS-Edge-Server	Hold Support	NONE
cisco-ccm		

Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

- In the General dialogue box, check the **Delayed SDP Handling** which ensures that an SDP is always included in the INVITE messages. This resolves an issue described in **Section 2.2** that was specific to the test environment, but could possibly be encountered in the live network.
- Check the **T.38 Support** box.

The screenshot shows the 'Interworking Profile' configuration window with the 'General' tab selected. The window contains various settings for SIP interworking. The 'Hold Support' is set to 'None'. '180 Handling', '181 Handling', '182 Handling', and '183 Handling' are all set to 'None'. 'Refer Handling' is unchecked. 'URI Group' is set to 'None'. 'Send Hold' and 'Delayed Offer' are checked. '3xx Handling' is unchecked. 'Diversion Header Support' is unchecked. 'Delayed SDP Handling' is checked. 'Re-Invite Handling' and 'Prack Handling' are unchecked. 'Allow 18X SDP' is unchecked. 'T.38 Support' is checked. 'URI Scheme' is set to 'SIP'. 'Via Header Format' is set to 'RFC3261'. At the bottom, there are 'Back' and 'Next' buttons.

Interworking Profile	
General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None ▼
Send Hold	<input checked="" type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input checked="" type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Note: During testing, the rest of the parameters were left at default values.

Click on **Next** and **Next** again to go through the next two dialogue boxes. During testing, these were left at default values.

In the final dialogue box, ensure that the **Both Sides** button is checked in the **Record Routes** field and the **Has Remote SBC** box is checked. Click on **Finish**

To define Server Interworking for the Session Manager, click on **Add** (not shown). A pop-up menu (not shown) is generated. In the **Name** field enter a descriptive name for the Session Manager and click **Next**. Check the **T.38** box.

Interworking Profile	
General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None ▼
Send Hold	<input checked="" type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
<input type="button" value="Back"/> <input type="button" value="Next"/>	

- Click on **Next** and **Next** again to go through the next two dialogue boxes (not shown). During testing, these were left at default values.
- Ensure the settings in the final dialogue box (not shown) are the same as those used for the Proximus SIP Trunking service.
- Click on **Finish**.

7.5. Define Signalling Manipulation

Signalling manipulation is required in cases where there is non-standard signalling between the Call Server and Trunk Server that can't be resolved by the Server Interworking described in the previous section. During testing, an issue was found with the handling of an Avaya specific parameter in the Contact header.

The Avaya proprietary parameter is "+avaya-cm-keep-mpro" and is present with a value of "no" when the Media Gateway is not used for call set-up i.e., when Initial IP-IP Direct Media is used on Communication Manager SIP Trunk. This can't be removed using the Header Manipulation tab in the Server Interworking profile described in the previous section, and a fault report AURORA-7477 has been raised to address this. During testing, Signalling Manipulation was used to remove the parameter

To define the signalling manipulation to remove the Avaya proprietary parameter, navigate to **Global Profiles → Signaling Manipulation** in the main menu on the left hand side. Click on **Add** which will open a script editor. Enter a title and the script.

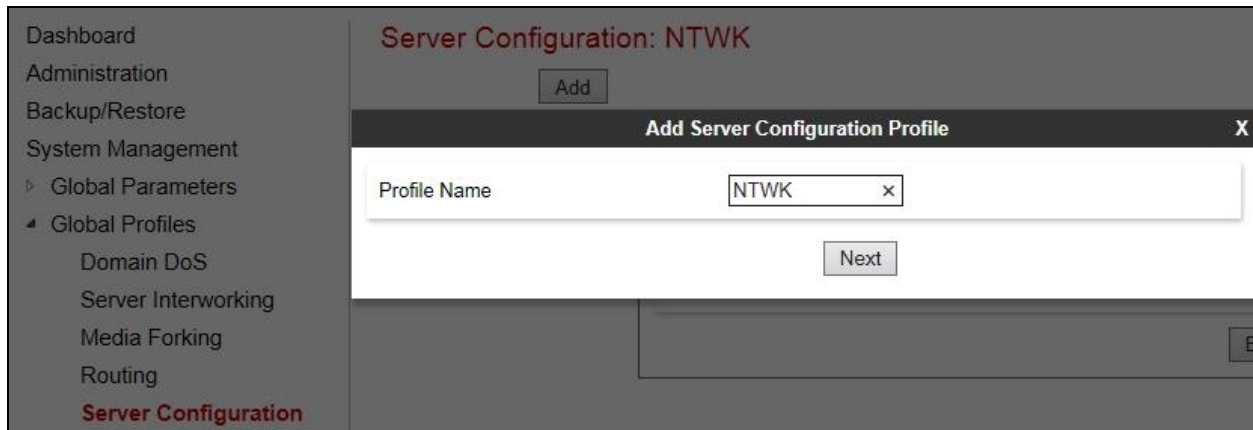
Click on **Save** (not shown). The script text is shown for clarity:

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

7.6. Define Servers

A server definition is required for each server connected to the Avaya SBCE. In this case, the Proximus SIP Trunking service is connected as the Trunk Server and Session Manager is connected as the Call Server.

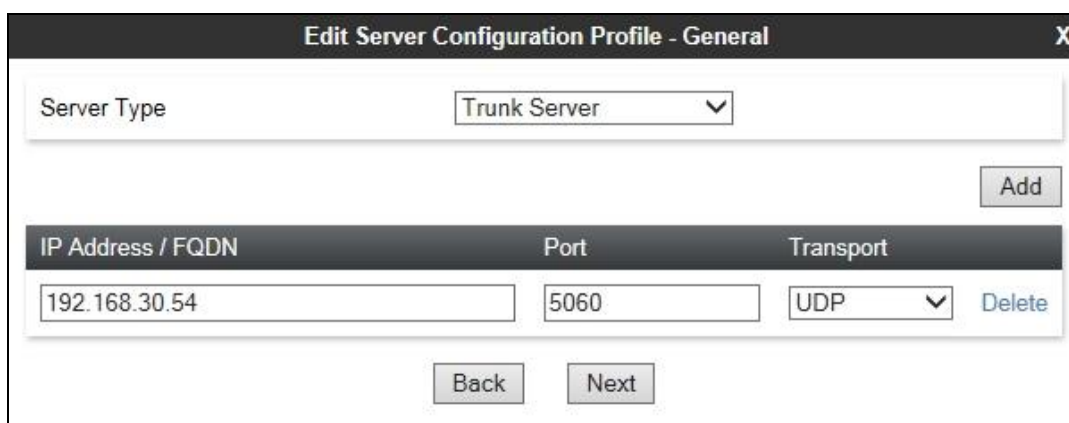
To define the Proximus SIP Trunk Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up menu.



The screenshot shows the 'Add Server Configuration Profile' dialog box. The 'Profile Name' field is populated with 'NTWK'. A 'Next' button is visible at the bottom right of the dialog. The background shows the 'Server Configuration: NTWK' page with a sidebar menu on the left containing options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Server Interworking, Media Forking, Routing, and Server Configuration (highlighted).

Click on **Next** and enter details in the dialogue box.

- In the **Server Type** drop down menu, select **Trunk Server**.
- Click on **Add** to enter an IP address
- In the **IP Addresses / FQDN** box, type the Proximus SIP trunk interface address.
- In the **Port** box, enter the port to be used for the SIP Trunk. This was left blank during testing which defaults to 5060 when UDP is used for transport.
- In the **Transport** drop down menu, select **UDP**.
- Click on **Next**.



The screenshot shows the 'Edit Server Configuration Profile - General' dialog box. The 'Server Type' dropdown is set to 'Trunk Server'. Below it, there is an 'Add' button. A table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The first row contains the values '192.168.30.54', '5060', and 'UDP'. A 'Delete' button is next to the first row. At the bottom, there are 'Back' and 'Next' buttons.

IP Address / FQDN	Port	Transport
192.168.30.54	5060	UDP

Click on **Next** and **Next** again. Leave the fields in the dialogue boxes at their default values.

Add Server Configuration Profile - Authentication	Add Server Configuration Profile - Heartbeat
<div>Enable Authentication <input type="checkbox"/></div> <div>User Name <input type="text"/></div> <div>Realm (Leave blank to detect from server challenge) <input type="text"/></div> <div>Password <input type="password"/></div> <div>Confirm Password <input type="password"/></div> <div><input type="button" value="Back"/> <input type="button" value="Next"/></div>	<div>Enable Heartbeat <input type="checkbox"/></div> <div>Method <input type="text" value="OPTIONS"/></div> <div>Frequency <input type="text"/> seconds</div> <div>From URI <input type="text"/></div> <div>To URI <input type="text"/></div> <div><input type="button" value="Back"/> <input type="button" value="Next"/></div>

Configure the Advanced Server Configuration Profile which is the final dialogue box.

- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for the Proximus SIP Trunking service defined in **Section 7.4**.
- In the **Signaling Manipulation Script** dialogue box, select the signalling manipulation script defined in **Section 7.5** to remove the Avaya proprietary parameter from the Contact header.
- Click **Finish**.

Add Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	<input type="text" value="PRXMS"/>
Signaling Manipulation Script	<input type="text" value="Remove mpro=no"/>
Connection Type	<input type="text" value="SUBID"/>
Securable	<input type="checkbox"/>
<div><input type="button" value="Back"/> <input type="button" value="Finish"/></div>	

Use the same process to define the Call Server configuration for the Session Manager if not already defined.

- Ensure that **Call Server** is selected in the **Server Type** drop down menu in the **General** dialogue box.
- Ensure that the Interworking Profile defined for the Session Manager in **Section 7.4** is selected in the **Interworking Profile** drop down menu in the Advanced dialogue box

The following screenshot shows the **General** tab of the completed Server Configuration:

Server Configuration: CPE

Add

Server Profiles

CPE

NTWK

General Authentication Heartbeat Advanced

Server Type Call Server

IP Address / FQDN	Port	Transport
10.10.9.31	5060	TCP

Edit

Rename Clone Delete

The next screenshot shows the **Advanced** tab.

Server Configuration: CPE

Add

Server Profiles

CPE

NTWK

General Authentication Heartbeat Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile ASM

Signaling Manipulation Script None

Connection Type SUBID

Securable ☐

Edit

Rename Clone Delete

Note that there is no **Signaling Manipulation Script** required for the Session manager server configuration.

7.7. Define Routing

Routing information is required for routing to the Proximus SIP Trunking service on the external side and Session Manager on the internal side. The IP addresses and ports defined here will be used as the destination addresses for signalling.

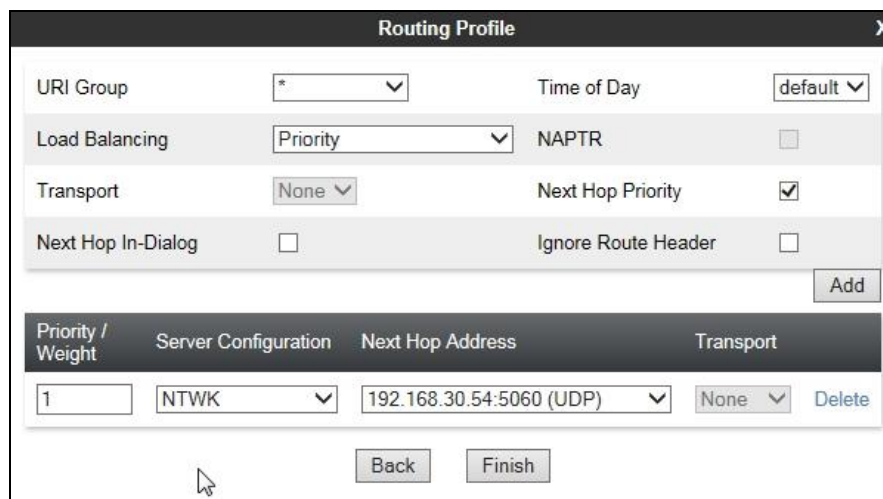
To define routing to the Proximus SIP Trunk, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the dialogue box.



The screenshot shows the 'Routing Profiles: WAN' configuration page. A sidebar on the left contains navigation links: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Server Interworking, Media Forking, and Routing. The main content area has a title 'Routing Profiles: WAN' and an 'Add' button. A 'Routing Profile' dialog box is open, with 'Profile Name' set to 'WAN'. The 'Next' button is visible.

Click on **Next** and enter details for the Routing Profile:

- In the **Load Balancing** drop down menu, select the method of load balancing required. During testing there was only one network interface provided for the Proximus SIP trunk so there was no load balancing required. This field was left at default value.
- Click on **Add** to specify the IP address for the Proximus SIP trunk.
- Assign a priority in the **Priority / Weight** field, during testing a value of **1** was used.
- Select the Server Configuration defined in **Section 7.6** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.



The screenshot shows the 'Routing Profile' configuration dialog box. The 'Add' button is visible. The 'Priority / Weight' field is set to 1, 'Server Configuration' is set to NTWK, 'Next Hop Address' is set to 192.168.30.54:5060 (UDP), and 'Transport' is set to None. The 'Back' and 'Finish' buttons are visible.

Repeat the process for the Routing Profile for Session Manager: The following screenshot shows the completed configuration:

Routing Profiles: LAN

Buttons: Add, Rename, Clone, Delete

Click here to add a description.

Routing Profile

Buttons: Update Priority, Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	10.10.9.31	TCP

Buttons: Edit, Delete

7.8. Topology Hiding

Topology Hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop or external interfaces. Topology Hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from Session Manager. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for the Proximus SIP Trunking service, navigate to **Global Profiles** → **Topology Hiding** in the main menu on the left hand side. Click on **Add** to bring up a dialogue box, assign an appropriate name and click on **Next**.

Topology Hiding Profiles: PRXMS

Buttons: Add

Click here to add a description.

Topology Hiding Profile

Buttons: X

Profile Name: PRXMS

Buttons: Next

From	IP/Domain	Auto
Via	IP/Domain	Auto
To	IP/Domain	Auto

Enter details in the **Topology Hiding Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Proximus SIP Trunking service and click **Next**.
- Click on **Add Header** and select from the **Header** drop down menu.
- Select **IP** or **IP/Domain** from the **Criteria** drop down menu depending on requirements.
- Leave the **Replace Action** at the default value of **Auto** unless a specific domain name is required. During testing, the domain name in the **Request-Line** was overwritten to that used by Proximus.
- Topology Hiding was defined for all headers where the function is available.

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	

The screenshot shows the completed Topology Hiding definition for the Proximus SIP trunk:

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	imst.belgacom.be
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---

To define Topology Hiding for Session Manager, follow the same process. This can be simplified by cloning the profile defined for the Proximus SIP Trunking service. Do this by highlighting the profile defined for the Proximus and clicking on **Clone**. Enter an appropriate name for the Session Manager profile and click on **Next**. Make any changes where required, in the test environment the **Replace Action** for **Request-Line** was left at the default value of **Auto**.

Topology Hiding Profiles: ASM

Add

Topology Hiding Profiles

default

cisco_th_profile

ASM

PRXMS

Rename

Clone

Delete

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---

Edit

7.9. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for the Proximus SIP Trunking service and another for Session Manager. These End Point Server Flows allow calls to be routed from Session Manager to the Proximus SIP Trunk and vice versa.

To define a Server Flow for the Proximus SIP Trunking service, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for the Proximus SIP Trunking service, in the test environment **Proximus** was used.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Proximus SIP Trunking service is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Proximus SIP Trunking service is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for the Proximus SIP Trunking service is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Proximus SIP Trunking service defined in **Section 7.8** and click **Finish**.

The screenshot shows a dialog box titled "Add Flow" with a close button (X) in the top right corner. The dialog contains the following fields and values:

Field	Value
Flow Name	Proximus
Server Configuration	NTWK
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal
Signaling Interface	External
Media Interface	External
End Point Policy Group	default-low
Routing Profile	LAN
Topology Hiding Profile	PRXMS
Signaling Manipulation Script	None
Remote Branch Office	Any

At the bottom of the dialog is a "Finish" button.

To define a Server Flow for Session Manager, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **CPE** was used.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Proximus SIP Trunking service defined in **Section 7.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.8** and click **Finish**.

Add Flow	
Flow Name	CPE
Server Configuration	CPE
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	External
Signaling Interface	Internal
Media Interface	Internal
End Point Policy Group	default-low
Routing Profile	WAN
Topology Hiding Profile	ASM
Signaling Manipulation Script	None
Remote Branch Office	Any
<div>Finish</div>	

The information for all Server Flows is shown on a single screen on the Avaya SBCE.

End Point Flows: GSSCP_V9

Devices
GSSCP_V9

Subscriber Flows

Server Flows

Add

Hover over a row to see its description.

Server Configuration: CPE

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	CPE	*	External	Internal	default-low	WAN	View Clone Edit Delete

Server Configuration: NTWK

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Proximus	*	Internal	External	default-low	LAN	View Clone Edit Delete

8. Configure the Proximus SIP Trunking service Equipment

The configuration of the Proximus equipment used to support the SIP Trunk is outside the scope of these Application Notes and will not be covered. To obtain further information on Proximus equipment and system configuration please contact an authorised Proximus representative.

9. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager **Home** tab click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entities from the list and observe if the **Conn Status** and **Link Status** are showing as **UP**.

The screenshot shows the 'Session Manager Entity Link Connection Status' page. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, and System Status. The main content area shows a table of entity links for 'Session_Manager'. The table has columns for SIP Entity Name, SIP Entity Resolved IP, Port, Proto, Deny, Conn. Status, Reason Code, and Link Status. All entries show 'UP' for both Conn. Status and Link Status.

SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
CM SIP Endpoints	10.10.9.12	5060	TCP	FALSE	UP	200 OK	UP
ASBCE	10.10.9.81	5060	TCP	FALSE	UP	200 OK	UP
CM Trunk	10.10.9.12	5062	TCP	FALSE	UP	200 OK	UP
Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP

2. From Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/idle**.

```
status trunk 2
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0002/001	T00011	in-service/idle	no
0002/002	T00012	in-service/idle	no
0002/003	T00013	in-service/idle	no
0002/004	T00014	in-service/idle	no
0002/005	T00015	in-service/idle	no
0002/006	T00016	in-service/idle	no
0002/007	T00017	in-service/idle	no
0002/008	T00018	in-service/idle	no
0002/009	T00019	in-service/idle	no
0002/010	T00020	in-service/idle	no

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from the Session Manager via the Avaya SBCE to the network SBCs are receiving a response.

To define the trace, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main menu on the left hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select the signalling interface IP address or **All** from the **Local Address** drop down menu.
- Enter the IP address of the network SBC in the **Remote Address** field or enter a * to capture all traffic.
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example.
- Specify the filename of the resultant pcap file in the **Capture Filename** field.
- Click on **Start Capture**.

Trace: GSSCP_V9

Devices
GSSCP_V9

Packet Capture **Captures**

Packet Capture Configuration

Status	Ready
Interface	B1
Local Address <small>IP[:Port]</small>	All
Remote Address <small>*: *:Port, IP, IP:Port</small>	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	SIP_Trunk_Test.pcap

Start Capture **Clear**

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.

Trace: GSSCP_V9

Devices

GSSCP_V9

Packet Capture

Captures

Refresh

File Name	File Size (bytes)	Last Modified
SIP_Trunk_Test_20160127102857.pcap	24,576	January 27, 2016 10:29:10 AM GMT Delete

The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response to OPTIONS in the form of a 200 OK will be seen from the Proximus network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura ® Communication Manager R7.0, Avaya Aura ® Session Manager 7.0 and Avaya Session Border Controller for Enterprise R7.0 to the Proximus SIP Trunking service. The Proximus SIP Trunking service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 7.0.1, Aug 2016.
- [2] *Upgrading and Migrating Avaya Aura® applications to 7.0.1 from System Manager*, Release 7.0.1, Aug 2016.
- [3] *Deploying Avaya Aura® applications*, Release 7.0, Dec 2015
- [4] *Deploying Avaya Aura® Communication Manager*, Oct 2016
- [5] *Administering Avaya Aura® Communication Manager*, Release 7.0.1, May 2016.
- [6] *Deploying Avaya Aura® System Manager*, Release 7.0.1 Aug 2016
- [7] *Upgrading Avaya Aura® Communication Manager*, Release 7.0.1, Oct 2016
- [8] *Upgrading Avaya Aura® System Manager to Release 7.0.1*, Aug 2016.
- [9] *Administering Avaya Aura® System Manager for Release 7.0.1*, Nov 2016
- [10] *Deploying Avaya Aura® Session Manager*, Release 7.0.1 Nov 2016
- [11] *Upgrading Avaya Aura® Session Manager* Release 7.0.1, Nov 2016
- [12] *Administering Avaya Aura® Session Manager* Release 7.0.1, May 2016,
- [13] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015
- [14] *Upgrading Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015
- [15] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Jan 2016
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2017 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.