



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 Telenor SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Telenor SIP Trunk 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.

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

Telenor is a member of the DevConnect Service Provider program. 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 Telenor SIP Trunk 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); Endpoints as described in Section 3. 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 Telenor SIP Trunk 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 Telenor SIP Trunk 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 Telenor SIP Trunk, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via Telenor SIP Trunk to PSTN destinations, calls made from SIP and H.323 telephones.
- Inbound and outbound PSTN calls to/from an Avaya one-X® Communicator and Avaya Communicator for Windows soft phones .
- Calls using the G.711A and G.711MU Law 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 Telenor SIP Trunk requiring Avaya response and sent by Avaya requiring Telenor response.

2.2. Test Results

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

- Intermittent faults were observed with media transmission. These were assumed to be the result of network issues at the time of testing and not due to interoperability issues with the Telenor SIP trunk.
- When dialling in from an EC500 mobile to a Feature Name Extension (FNE) for an idle appearance, on-net calls were successful but off-net weren't. This was thought to be due to network issues at the time and DTMF digits being missed.
- When making outbound calls from a one-X Communicator softphone connected via SIP and in "Other Phone" mode, no ring back was heard. This was assumed to be a one-X Communicator issue as ring back was heard when connected via H.323.
- When attempting to redirect to a busy phone using REFER, the call is cleared immediately from the network. There is no NOTIFY message for busy.
- When the SIP Trunk is busy and an incoming call is attempted, the Avaya equipment sends 503 Service Unavailable. The network repeatedly re-attempts the call set-up for a period of around 2 minutes before an announcement is played.
- When the signalling link is down and an incoming call is attempted, the Avaya equipment sends 408 Request Timeout then 503 Service Unavailable. The network repeatedly re-attempts the call set-up for a period of around 2 minutes before an announcement is played.
- The re-INVITE without SDP sent from Communication Manager to change media path to include Media Gateway caused an error in the Telenor network. This was resolved by configuring the Avaya SBCE to include an SDP in these re-INVITE messages as described in **Section 7.4**.
- When testing call forwarding to the PSTN, the INVITE for leg 2 of the call was not received by the network due to fragmentation of the message. This was resolved by removing the P-Asserted-Identity header to reduce the size of the Message as described in **Section 6.4**. This header is not used by the Telenor network.
- Though initial incoming T.38 fax calls were successful, there were numerous T.30 error messages in the signalling. This was thought to be due to network issues as opposed to interoperability issues. ECM was turned off on Communication Manager and subsequent T.38 fax calls were successful and didn't contain T.30 error messages.

Items not tested include the following:

- No Inbound Toll-Free access available for testing
- No test call was made to Directory Enquiries as access was not available from the test environment
- No test call was made to Emergency Services as a test call was not booked with the Emergency Services Operator.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

For technical support on Telenor products please contact the following website: <http://www.telenor.com/>

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Telenor SIP Trunk 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 telephones (with SIP and H.323 firmware), Avaya 16xx series IP telephones (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.

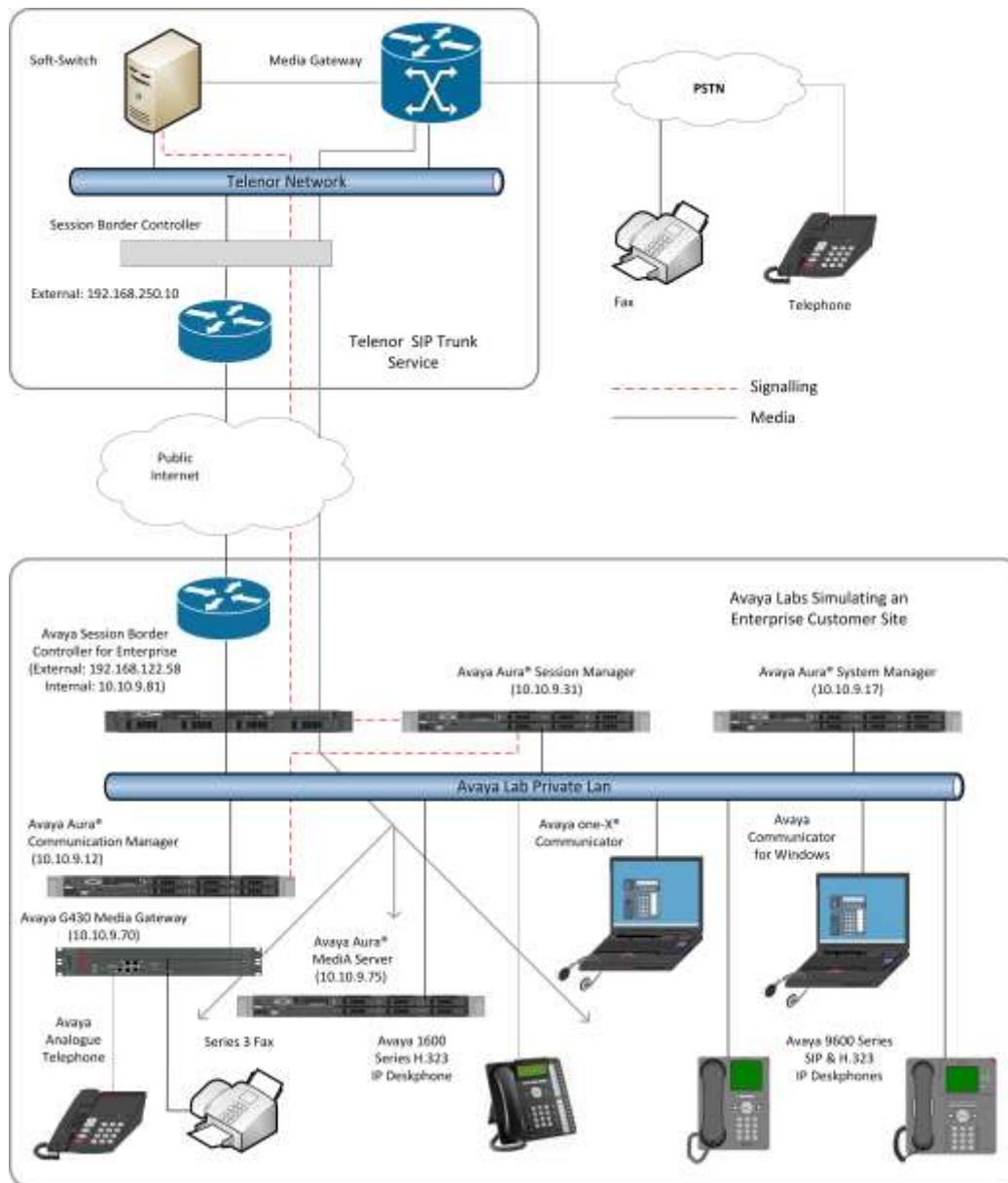


Figure 1: Test Setup Telenor SIP Trunk Service to Avaya Enterprise

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	7.0.0.2.700201
Avaya Aura® System Manager	7.0.0.2.4416
Avaya Aura® Communication Manager	7.0-441 0-22856
Avaya Session Border Controller for Enterprise	7.0.1-03-8739
Avaya G430 Media Gateway	37.21.0
Avaya Aura® Media Server	7.7.0.236_2015.07.24
Avaya 9600 series Handsets: SIP 96x0 SIP 9608 H.323 96x0 H.323 9608 H.323 1616	2_6_15_0 7.0.0 R39 3.2.6A 6.6.1.15 V474 1.380B
Avaya One-X Communicator	6.2.10.03-FP10
Avaya Communicator for Windows	2.1.3.80
Analogue Handset	N/A
Telenor	
Telenor IPT3	version 13.3

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 Telenor SIP Trunk 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. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Telenor 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 authorized 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 Telenor SIP Trunk 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

                                ISDN Feature Plus? n
                                ISDN/SIP Network Call Redirection? y
                                ISDN-BRI Trunks? y
                                ISDN-PRI? y
                                Local Survivable Processor? n
                                Malicious Call Trace? y
                                Media Encryption Over IP? n
                                Mode Code for Centralized Voice Mail? n
                                Multifrequency Signaling? y
                                Multimedia Call Handling (Basic)? y
                                Multimedia Call Handling (Enhanced)? y
                                Multimedia IP SIP Trunking? 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 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 direct media is used on a PSTN call, 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
UDP Port Min: 2048 IP Audio Hairpinning? n
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 and Avaya Media Server (not shown) ip-network-region 1 was used in such a way that either one could be selected at call set-up.

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 codec's eligible to be used in order of preference. For the interoperability test the codecs supported by Telenor were configured, namely **G.711A** and **G.711MU**.

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.711MU	n	2	20		
3: 4:					

Telenor SIP Trunk 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**. Note that during testing, this was set to **n** to avoid unnecessary retransmission.

change ip-codec-set 2				Page 2 of 2	
IP CODEC SET					
Allow Direct-IP Multimedia? n					
	Mode	Redundancy	ECM: n	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: **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 Telenor SIP Trunk 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 Session Manager interface (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 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 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** to avoid unnecessary use of MGW resources
- Set **Initial IP-IP Direct Media** to **n** to facilitate the use of Early Media to avoid ring back issues.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).

The default values for the other fields may be used.

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? n		Initial IP-IP Direct Media? n
		Alternate Route Timer(sec): 6

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** if the Diversion header is to be supported.
- 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 Telenor 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 **public**. This allows delivery of CLI in E.164 format with leading “+” as required by Telenor.

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

On **Page 4** of this form:

- Set **Mark Users as Phone** to **y** as required by Telenor
- Set **Network Call Redirection** to **y** to allow the use of REFER messages for call flows such as blind call transfer.
- Set **Send Diversion Header** to **y** so that the DDI number assigned to the extension is passed for forwarded calls.
- Set **Support Request History** to **n** as this header is not supported by Telenor.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Telenor (this Payload Type is not applied to calls from SIP end-points).
- Set **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? y		
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? y		
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		

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number in the format required. During testing, calling party numbers were sent as E.164 numbers with leading "+". 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 public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	2	1		4	Total Administered: 7
4	2000	2	47223nnnn3	10	Maximum Entries: 240
4	2291	2	47223nnnn1	10	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
4	2316	2	47223nnnn4	10	
4	2391	2	47223nnnn2	10	
4	2400	2	47223nnnn5	10	
4	2401	2	47223nnnn5	10	

Note: During testing the extension numbers were reformatted to E.164 numbers for Trunk Group 2 only. The numbers were analysed for Trunk Group 1 but not reformatted.

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 Telenor network. 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. In the Norwegian number plan, there is no preceding 0 for national numbers. The national numbers should be analysed as required to specify routing and number length.

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 international numbers beginning 00 and national numbers beginning with area code. 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	
00	13	15	2	pubu		n	
0035391	13	13	2	pubu		n	
1	3	4	2	pubu		n	
118	5	6	2	pubu		n	
223	8	8	2	pubu		n	
241	8	8	2	pubu		n	
671	8	8	2	pubu		n	
675	8	8	2	pubu		n	
7000	4	4	1	pubu		n	
800	8	8	2	pubu		n	
820	8	8	2	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 **unk-unk**.

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 No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC					
			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						
1:	y	y	y	y	y	n	n	rest				unk-unk	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:	y	y	y	y	y	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 Telenor can be manipulated as necessary to route calls to the desired extension. Use the **change inc-call-handling-trmt trunk-group x** command where **x** is the Trunk Group defined in **Section 5.6**. In the example shown, 10 digits are received along with a preceding “+”. All digits are deleted and the extension number is inserted. Note that some of the DDI digits have been obscured.

change inc-call-handling-trmt trunk-group 2					Page	1 of	3
INCOMING CALL HANDLING TREATMENT							
Service/ Feature	Number Len	Number Digits	Del	Insert			
public-ntwrk	11	+47223nnnn1	11	2291			
public-ntwrk	11	+47223nnnn2	11	2391			
public-ntwrk	11	+47223nnnn3	11	2000			
public-ntwrk	11	+47223nnnn4	11	2316			
public-ntwrk	11	+47223nnnn5	11	7000			
public-ntwrk							
public-ntwrk							

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 2291. 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, none was required during testing.
- For the **Phone Number** enter the phone that will also be called (e.g. **003538941nnnn7**).
- 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 2291							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
2291	OPS	-		2291	aar	1	
2291	EC500	-		003538941nnnn7	ars	1	

Note: The phone number shown is for a mobile phone in the Avaya Lab. To use facilities such as Feature Name Extension (FNE) 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.

The additional line in the previous screenshot with **Application** of **OPS** is standard on SIP endpoints where the phone is registered to the Session Manager and is essentially “Off PBX”.

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

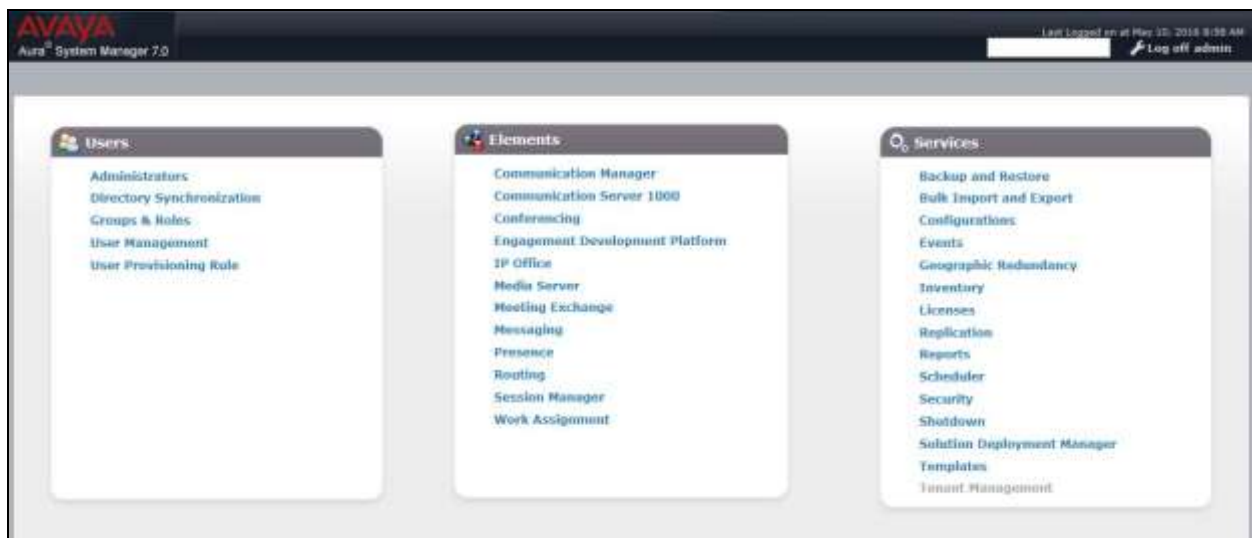
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured by opening a web browser to the 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 Telenor; 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 'Domain Management' interface. On the left is a navigation menu with 'Routing' expanded, showing sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, and Dial Patterns. The main area has a breadcrumb 'Home / Elements / Routing / Domains' and a title 'Domain Management'. Below the title are buttons: 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A table below shows '1 Item' with a refresh icon. The table has columns: Name, Type, and Notes. One row is visible with 'avaya.com' in the Name column and 'sip' in the Type column. At the bottom, there is a 'Select' dropdown with options 'All' and '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, a Session Manager Adaptation can be used to change it (see **Section 6.4**).

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.

The screenshot shows the 'Location Details' configuration page. At the top, there is a breadcrumb trail 'Home / Elements / Routing / Locations' and a 'Help ?' link. The page title is 'Location Details' with 'Commit' and 'Cancel' buttons. The 'General' section contains a 'Name' field with 'Galway' and a 'Notes' field. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox, a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field. The 'Overall Managed Bandwidth' section includes 'Managed Bandwidth Units' (set to 'Kbit/sec'), 'Total Bandwidth', 'Multimedia Bandwidth', and an 'Audio Calls Can Take Multimedia Bandwidth' checkbox. The 'Per-Call Bandwidth Parameters' section has fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', '* Minimum Multimedia Bandwidth', and '* Default Audio Bandwidth'. The 'Alarm Threshold' section includes 'Overall Alarm Threshold', 'Multimedia Alarm Threshold', '* Latency before Overall Alarm Trigger', and '* Latency before Multimedia Alarm Trigger'. The 'Location Pattern' section at the bottom has 'Add' and 'Remove' buttons, a table with one row containing '*10.10.9.x' under the 'IP Address Pattern' column, and a 'Select : All, None' option.

Home / Elements / Routing / Locations

Help ?

Location Details

Commit Cancel

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

Add Remove

1 Item Filter: Enable

IP Address Pattern	Notes
*10.10.9.x	

Select : All, None

6.4. Administer Adaptations

Communication Manager and Session Manager make use of Avaya proprietary SIP headers to facilitate the full suite of Avaya functionality within the enterprise. These are not required on the SIP trunk however, and are not recognized by the Telenor network. In addition, the called and calling party number formats passed between the Enterprise and the Telenor network are in E.164 format with leading “+”. A Session Manager Adaptation is used both to remove proprietary headers and to convert numbers to and from diallable format.

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** box, type **eRHdrs**.
- In the **Value** box, type the list of headers to be deleted. During testing, the following list was used: "**P-AV-Message-Id, P-Charging-Vector, Av-Global-Session-ID, P-Location, Endpoint-View, Recv-Info, P-Conference, Alert-Info, Reason, P-Asserted-Identity**".
- Click on Add.
- In the **Name** box, type **fromto**.
- In the **Value** box, type **true**. This will apply the number conversion rules to the From and To headers in the SIP messages.

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

Help ?

General

* Adaptation Name: Header_Removal

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
eRHdrs	P-AV-Message-Id, P-Charging-Vector, Av-Global-Session-ID, P-Location, Endpoint-View, Recv-Info, P-Conference, Alert-Info, Reason, P-Asserted-Identity
fromto	true

Select : All, None

Egress URI Parameters:

Notes:

Number analysis is used to apply the above Module Parameter rule and to convert the called and calling party numbers between E.164 with leading “+” and diallable format. Scroll down and in the section **Digit Conversion for Incoming Calls to 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.

The screenshot below shows analysis of called party numbers for incoming calls. The called party number is the DDI number associated with the Communication manager extensions.

- 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, in this case the DDI number length is fixed at **11**.
- Under **Delete Digits** enter 0 as the number is not to be modified.
- Leave the **Insert Digits** field blank as the number is not to be modified.
- Under **Address to Modify** choose **destination** from the drop down box to apply this rule to the called party number.

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
*+47223nnnn	11	11		0		destination		

Note: In the above screenshot the DDI numbers are partially obscured. If the calling party number is to be modified for display on Communication Manager extensions in diallable format, it should be done here. For international numbers, remove the leading “+” and replace with 00. For national numbers remove the leading “+47”. **Address to modify** would be **origination**.

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 going out to the network

The screenshot below shows analysis of called party numbers for outgoing calls. The called party number is the dialled public number.

- Under **Matching Pattern** enter the first dialled digits. For international calls, these will be **00**. For national calls, these may be the area code, for example **223**.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the dialled number. For international calls, the maximum would be that specified by E.164, i.e. 15 without the international dialling prefix, **17** in total. For the national number used during testing, the number length was **8** digits.
- Under **Delete Digits** enter **2** for international numbers to delete the international dialling prefix. For national numbers, enter **0** as the number is not to be modified.
- Under **Insert Digits**, enter the “+” used to indicate E.164 numbering in SIP and the country code where required i.e., national numbers.
- Under **Address to Modify** choose **destination** from the drop down box to apply this rule to the called party number.
- Click **Commit** to save changes.

Digit Conversion for Outgoing Calls from SM

Add Remove

8 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	*8	*15		*1	+47	destination		
<input type="checkbox"/>	*00	*10	*17		*2	+	destination		
<input type="checkbox"/>	*223	*8	*8		*0	+47	destination		
<input type="checkbox"/>	*241	*8	*8		*0	+47	destination		
<input type="checkbox"/>	*671	*8	*8		*0	+47	destination		
<input type="checkbox"/>	*675	*8	*8		*0	+47	destination		
<input type="checkbox"/>	*800	*8	*8		*0	+47	destination		
<input type="checkbox"/>	*820	*8	*8		*0	+47	destination		

Select : All, None

Commit Cancel

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 for PSTN destinations.

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 window. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The window title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The form contains the following fields:

- Name:** Session_Manager
- FQDN or IP Address:** 10.10.9.31
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text area)
- Location:** Galway (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (empty text area)

Below the 'General' section is the 'SIP Link Monitoring' section, which contains a dropdown menu set to 'Use Session Manager Configuration'.

The 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	Protocol	Default Domain	Notes
5060	TCP	avaya.com	
5060	UDP	avaya.com	
5061	TLS	avaya.com	
5062	TCP	avaya.com	

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**.

SIP Entity Details

General

* Name: CM Trunk

* FQDN or IP Address: 10.10.9.12

Type: CM

Notes:

Adaptation:

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.

The screenshot shows two sections of a configuration form. The first section, titled "Loop Detection", contains three fields: "Loop Detection Mode" set to "On", "Loop Count Threshold" set to "5", and "Loop Detection Interval (in msec)" set to "200". The second section, titled "SIP Link Monitoring", contains five fields: "SIP Link Monitoring" set to "Use Session Manager Configuration", "Supports Call Admission Control" (unchecked), "Shared Bandwidth Manager" (unchecked), "Primary Session Manager Bandwidth Association" (empty), and "Backup Session Manager Bandwidth Association" (empty).

Note: A second SIP Entity for Communication Manager is required for SIP Endpoints. In the test environment this is named "CM_SIP_Endpoints".

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

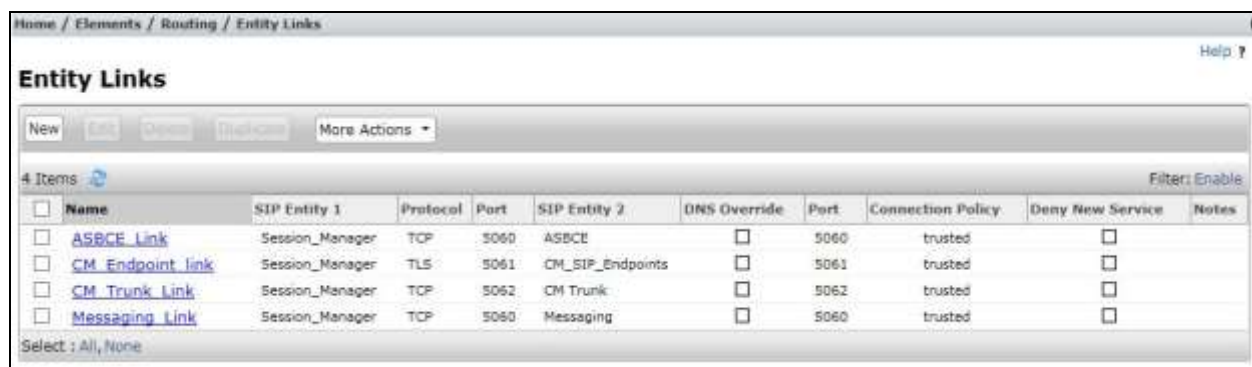
The following screen shows the SIP Entity for the Avaya SBCE used for PSTN destinations. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface used for PSTN fixed calls (see **Figure 1**). Set the **Adaptation** to that defined in **Section 6.4**, the **Location**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

The screenshot shows the "SIP Entity Details" configuration page for the "ASBCE" entity. The page has a breadcrumb trail "Home / Elements / Routing / SIP Entities" and "Commit" and "Cancel" buttons. The "General" tab is selected. The configuration fields are: "Name" (ASBCE), "FQDN or IP Address" (10.10.9.81), "Type" (SIP Trunk), "Notes" (empty), "Adaptation" (Header_Removal), "Location" (Galway), "Time Zone" (Europe/Dublin), "SIP Timer B/F (in seconds)" (4), "Credential name" (empty), "Securable" (unchecked), and "Call Detail Recording" (egress).

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.



<input type="checkbox"/>	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_Endpoint_Link	Session_Manager	TLS	5061	CM_SIP_Endpoints	<input type="checkbox"/>	5061	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"/>	

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

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

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 PSTN destinations via Telenor SIP Trunk.

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

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 to PSTN destinations via Telenor SIP Trunk.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Commit] [Cancel] [Help ?]

General

* Pattern: 223

* Min: 8

* Max: 8

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- ▼

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"/>	Galway		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: +47223nnnn 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 analyze 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

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 and select **Commit** to save the configuration.

Application Editor [Commit] [Cancel]

Application

* Name: CM_App x

* SIP Entity: CM_SIP_Endpoints

* CM System for SIP Entity: CM1_Element Refresh View/Add CM Systems

Description:

Note: The Application described here and the Application Sequence described in the next section are likely to have been defined during installation. The configuration is shown here for reference. Note also that the Communication Manager SIP Entity selected is that set up specifically for SIP endpoints. In the test environment there is also a Communication Manager SIP Entity that is used specifically for the SIP Trunk and is not to be used in this case.

6.10. Administer Application Sequence for Avaya Aura® Communication Manager

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**.

The screenshot shows the 'Application Sequence Editor' window. At the top, the breadcrumb navigation reads: 'Home / Elements / Session Manager / Application Configuration / Application Sequences'. The window title is 'Application Sequence Editor' with 'Commit' and 'Cancel' buttons. Below the title bar, there's a section for 'Application Sequence' with a 'Name' field containing 'CM_App_Seq' and a 'Description' field. Below this is a section titled 'Applications in this Sequence' with 'Move First', 'Move Last', and 'Remove' buttons. It shows '1 Item' in a table:

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

Below the table is a 'Select: All, None' option. Underneath is the 'Available Applications' section with a 'Filter: Enable' button and '1 Item' in a table:

	Name	SIP Entity	Description
+	CM_App	CM_SIP_Endpoints	

At the bottom left, there's a '*Required' label. At the bottom right, there are 'Commit' and 'Cancel' buttons.

6.11. Administer SIP Extensions

The SIP extensions are likely to have been defined during installation. The configuration shown in this section is for reference. SIP extensions are registered with 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.

The screenshot shows the 'New User Profile' form in the Avaya User Management interface. The form is divided into tabs: Identity, Communication Profile, Membership, and Contacts. The Identity tab is active, showing fields for User Provisioning Rule, Last Name, First Name, Login Name, Authentication Type, Password, Confirm Password, Localized Display Name, Endpoint Display Name, Title, Language Preference, Time Zone, Employee ID, Department, and Company. The form is pre-filled with example data: Last Name: SIP, First Name: 9608, Login Name: 2291@avaya.com, Authentication Type: Basic, Password: 9608, Confirm Password: 9608, Language Preference: English (United Kingdom), Time Zone: (0:0)GMT : Dublin, Edinburgh, L.

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


The screenshot shows the 'Communication Profile' tab selected in a multi-tabbed interface. The 'Communication Profile' section contains two password fields: 'Communication Profile Password' and 'Confirm Password', both masked with dots. Below these is a 'Name' section with a 'New' button, a 'Delete' button, a 'Done' button, and a 'Cancel' button. The 'Name' list shows 'Primary' selected. Below the list, the 'Name' field is set to 'Primary' and the 'Default' checkbox is checked. The 'Communication Address' section is expanded, showing a 'New' button, an 'Edit' button, and a 'Delete' button. Below these is a table with columns 'Type', 'Handle', and 'Domain'. The table is empty, with the text 'No Records found' displayed. Below the table, the 'Type' field is set to 'Avaya SIP' and the 'Fully Qualified Address' field is set to '2291 @ avaya.com'.

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 contains a 'New' button, an 'Edit' button, and a 'Delete' button. Below these is a table with columns 'Type', 'Handle', and 'Domain'. The table is empty, with the text 'No Records found' displayed. Below the table, the 'Type' field is set to 'Avaya SIP' and the 'Fully Qualified Address' field is set to '2291 @ avaya.com'. The 'Add' and 'Cancel' buttons are visible 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

Primary	Secondary	Maximum
4	0	4
		


Secondary Session Manager


Survivability Server

Max. Simultaneous Devices 


Block New Registration When Maximum Registrations Active? ☐


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 the System Manager will add 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.

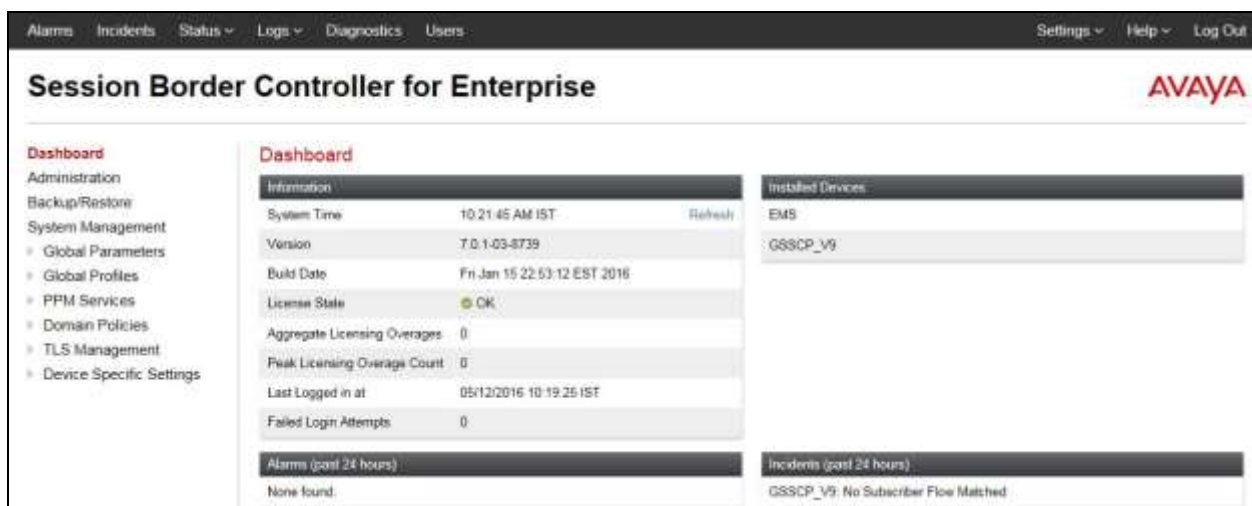
7.1. Access Avaya Session Border Controller for Enterprise

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 screenshot shows the login interface for the Avaya Session Border Controller for Enterprise. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right, under the heading "Log In", there is a "Username:" label followed by a text input field and a "Continue" button. Below the login fields, there are three paragraphs of legal disclaimer text and a copyright notice at the bottom: "© 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 screenshot displays the main dashboard of the Avaya Session Border Controller for Enterprise. At the top, there is a navigation bar with links for "Alarms", "Incidents", "Status", "Logs", "Diagnostics", "Users", "Settings", "Help", and "Log Out". The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand sidebar menu lists various configuration options: "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles", "PPM Services", "Domain Policies", "TLS Management", and "Device Specific Settings". The main content area is titled "Dashboard" and contains several sections: "Information" with fields for System Time, Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count, Last Logged in at, and Failed Login Attempts; "Installed Devices" showing a list of devices; "Alarms (past 24 hours)" showing "None found"; and "Incidents (past 24 hours)" showing "GSSCP_V9: No Subscriber Flow Matched".

7.2. Define Network Management

Network information is required on the Avaya SBCE to allocate IP addresses and 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**.



Enter details for the external interfaces in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external physical 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 of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

The screenshot shows the 'Add Network' dialog box. It contains fields for 'Name' (set to 'External'), 'Default Gateway' (192.168.122.7), 'Subnet Mask' (255.255.255.128), and 'Interface' (B1). Below these fields is an 'Add' button. At the bottom, there is a table with three columns: 'IP Address' (192.168.122.58), 'Public IP' (Use IP Address), and 'Gateway Override' (Use Default). A 'Delete' button is next to the 'Gateway Override' field. A 'Finish' button is at the bottom center.

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 interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the internal physical 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 for the Avaya SBCE 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:



Select the **Interface Configuration** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.



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 that will indicate when the restart is complete.

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 Telenor SIP Trunk. Two signalling and two media interfaces were required on both the internal and external sides of the Avaya SBCE to handle on-net and off-net traffic. 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 IP address **192.168.122.58** for the Avaya SBCE interface on the SIP Trunk.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for the Telenor SIP Trunk.

The screenshot shows the 'Add Signaling Interface' dialog box. On the left is a sidebar menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (expanded), Network Management, Media Interface, **Signaling Interface** (highlighted), End Point Flows, Session Flows, DMZ Services, and TURN/STUN Service. The main dialog box has a title bar 'Add Signaling Interface' with a close button 'X'. It contains the following fields:

- Name:** Text input field with 'External' entered.
- IP Address:** A dropdown menu showing 'External (B1, VLAN 0)' with a secondary dropdown showing '192.168.122.58'.
- TCP Port:** Text input field with the label 'Leave blank to disable' below it.
- UDP Port:** Text input field with '5060' entered and the label 'Leave blank to disable' below it.
- TLS Port:** Text input field with the label 'Leave blank to disable' below it.
- TLS Profile:** Dropdown menu with 'None' selected.
- Enable Shared Control:** A checkbox that is currently unchecked.
- Shared Control Port:** Text input field.
- Finish:** A button at the bottom right.

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 IP address **192.168.122.58**.
- Define the **RTP Port Range** for the media path with the Telenor SIP Trunk, during testing this was changed to **10000** to **10999** as specified in the Telenor SIP Specification.

System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management
- ▾ **Device Specific Settings**
 - Network Management
 - Media Interface**

Add Media Interface X

Name: External

IP Address: External (B1, VLAN 0) ▼
192.168.122.58 ▼

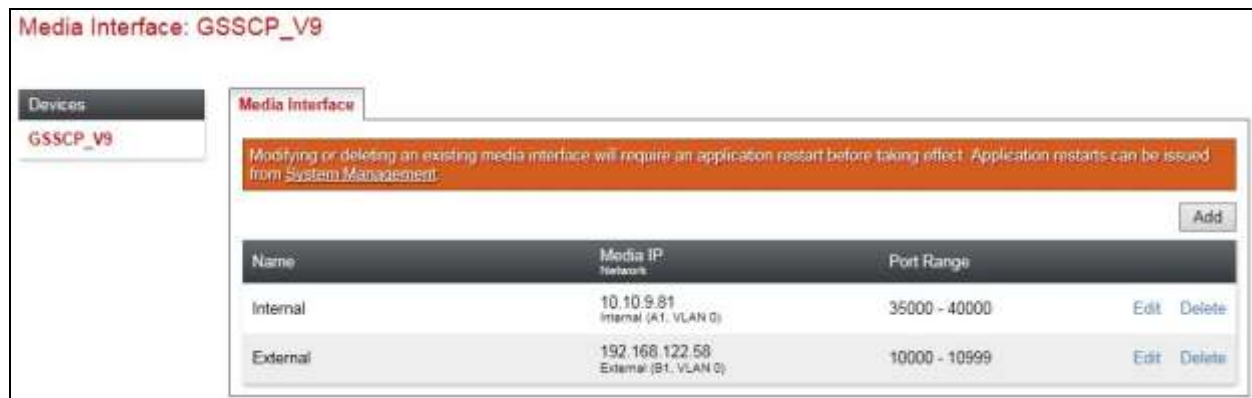
Port Range: 10000 - 10999

[Finish](#)

The internal media interfaces are 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:

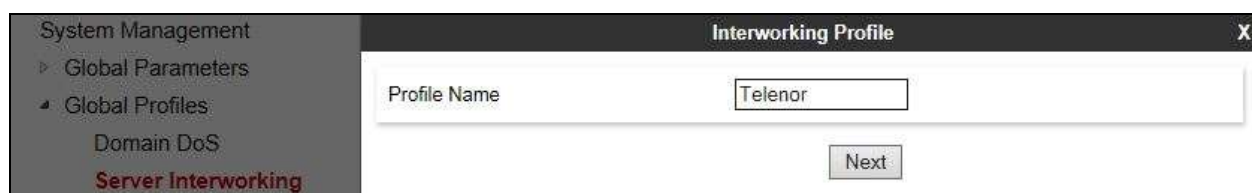


Note: In the test environment, the internal IP address was **10.10.9.81** and the port range was left at default values.

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the Telenor SIP Trunk is connected as the Trunk Server and the Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

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 Telenor SIP Trunk service, click on **Add** (not shown). A pop-up menu is generated. In the **Name** field enter a descriptive name for the Telenor network and click **Next**.



The Delayed SDP Handling in the Server Interworking is used to insert an SDP into a SIP INVITE that has no SDP. This is the case with Communication Manager shuffling and call hold. Shuffling is the Communication Manager function that changes the media path between a direct connection between the internal side of the SBC and the endpoint, and a connection via the Media Gateway or Media Server.

Check the **T.38 Support** and **Delayed SDP handling** boxes and click on **Next**.

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"/>	

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

Interworking Profile	
SIP Timers	
Min-SE	<input type="text"/> seconds, [90 - 86400]
Init Timer	<input type="text"/> milliseconds, [50 - 1000]
Max Timer	<input type="text"/> milliseconds, [200 - 8000]
Trans Expire	<input type="text"/> seconds, [1 - 64]
Invite Expire	<input type="text"/> seconds, [180 - 300]
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Interworking Profile	
Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	

In the final dialogue box, leave the **Record Routes** at the default setting of **None** and ensure that the **Has Remote SBC** box is checked. Note that Avaya extensions are not supported for the SIP Trunk. Click on **Finish**

The screenshot shows the 'Interworking Profile' dialog box with the following settings:

- Record Routes:** ☒ None, ☐ Single Side, ☐ Both Sides, ☐ Dialog-Initiate Only (Single Side), ☐ Dialog-Initiate Only (Both Sides)
- Include End Point IP for Context Lookup:** ☐
- Extensions:** None (dropdown)
- Diversion Manipulation:** ☐
- Diversion Condition:** None (dropdown)
- Diversion Header URI:** (empty text field)
- Has Remote SBC:** ☒
- Route Response on Via Port:** ☐
- DTMF:**
 - DTMF Support:** ☒ None, ☐ SIP NOTIFY, ☐ SIP INFO

Buttons at the bottom: Back, Finish

Repeat the process to define Server Interworking for Session Manager using the same parameter settings apart from **Delayed SDP Handling**. The following screenshot shows the **General** tab.

The screenshot shows the 'Interworking Profiles: ASM' configuration page. The left sidebar lists various profiles, with 'ASM' highlighted. The main area shows the 'General' tab for the 'ASM' profile.

Interworking Profiles: ASM

Buttons: Add, Rename, Clone, Delete

Click here to add a description

General | Timers | Privacy | URI Manipulation | Header Manipulation | Advanced

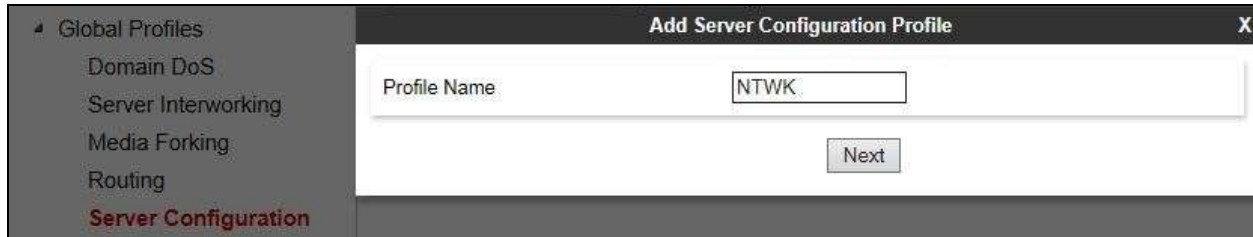
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Buttons: Edit

7.5. Define Servers

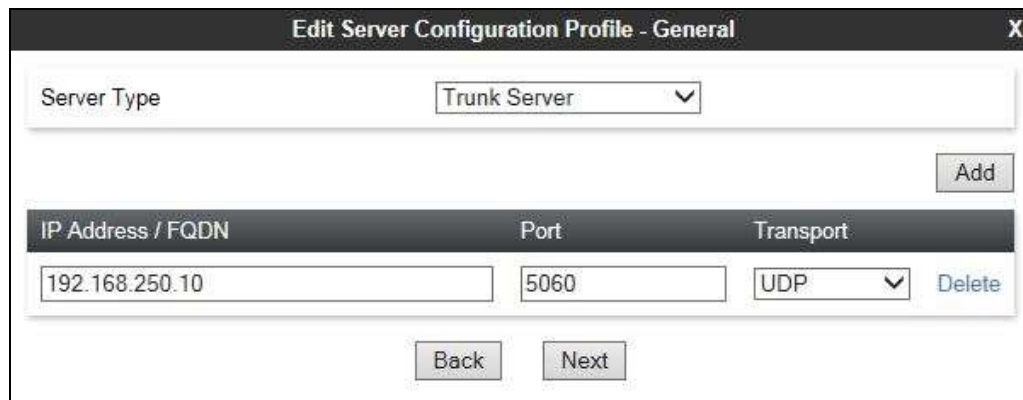
A server definition is required for each server connected to the Avaya SBCE. The Telenor SIP Trunk is connected as a Trunk Server. Session Manager is connected as a Call Server.

To define the Telenor 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.



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 Telenor SIP Trunk IP 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**.



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

Add Server Configuration Profile - Authentication	Add Server Configuration Profile - Heartbeat
Enable Authentication <input type="checkbox"/>	Enable Heartbeat <input type="checkbox"/>
User Name <input type="text"/>	Method <input type="text" value="OPTIONS"/>
Realm (Leave blank to detect from server challenge) <input type="text"/>	Frequency <input type="text" value="30"/> seconds
Password <input type="text"/>	From URI <input type="text"/>
Confirm Password <input type="text"/>	To URI <input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	<input type="button" value="Back"/> <input type="button" value="Next"/>

Click on **Next** again to get to the final dialogue box. This contains the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for Telenor SIP Trunk defined in **Section 7.4**.
- Leave the other fields at default settings.
- Click **Finish**.

Add Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	<input type="text" value="Telenor"/>
Signaling Manipulation Script	<input type="text" value="None"/>
Connection Type	<input type="text" value="SUBID"/>
Securable	<input type="checkbox"/>
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

Use the process above to define the Call Server configuration for 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 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:

The screenshot shows the 'Server Configuration: CPE' window with the 'General' tab selected. The left sidebar shows 'Server Profiles' with 'CPE' and 'NTWK' listed. The main area has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab contains a 'Server Type' dropdown set to 'Call Server'. Below it is a table with columns 'IP Address / FQDN', 'Port', and 'Transport'. The table has one row with values '10.10.9.31', '5060', and 'TCP'. An 'Edit' button is at the bottom right of the table. At the top right of the window are 'Rename', 'Clone', and 'Delete' buttons.

IP Address / FQDN	Port	Transport
10.10.9.31	5060	TCP

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

The screenshot shows the 'Server Configuration: CPE' window with the 'Advanced' tab selected. The left sidebar is the same. The main area has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'Advanced' tab contains several settings: 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (dropdown set to 'ASM'), 'Signaling Manipulation Script' (dropdown set to 'None'), 'Connection Type' (dropdown set to 'SUBID'), and 'Securable' (checkbox). An 'Edit' button is at the bottom right.

7.6. Define Routing

Routing information is required for routing to the Telenor SIP Trunk 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 Telenor 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 Profile' dialog box. The left sidebar shows 'Global Profiles' with 'Domain DoS', 'Server Interworking', 'Media Forking', and 'Routing' listed. The main area has a 'Profile Name' text box containing 'WAN' and a 'Next' button.

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

- During testing, **Load Balancing** was not required and was left at the default value of **Priority**.
- Click on **Add** to specify an IP address for the SIP Trunk.
- Assign a priority in the **Priority / Weight** field, during testing **1** was used.
- Select the Server Configuration defined in **Section 7.5** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.

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

7.7. 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.

To define Topology Hiding for Telenor SIP Trunk, 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** to configure Topology Hiding for each header as required:

The screenshot shows the 'Global Profiles' menu on the left with 'Topology Hiding' highlighted. The main area displays 'cisco_th_profile' and a table with headers 'Header', 'Criteria', and 'Replace Action'. Below this, a 'Topology Hiding Profile' dialog box is open, showing 'Profile Name' as 'Telenor' and a 'Next' button.

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

- 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. During testing the default **IP/Domain** was used for all headers that hides both domain names and IP addresses.
- Leave the **Replace Action** at the default value of **Auto** unless a specific domain name is required. In this case, select **Overwrite** and define a domain name in the **Overwrite Value** field.
- Topology hiding was defined for all headers where the function is available.

The screenshot shows the 'Topology Hiding Profile' dialog box with a table for configuration. The table has four columns: 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The first row shows 'Request-Line' selected for Header, 'IP/Domain' for Criteria, 'Auto' for Replace Action, and an empty field for Overwrite Value. There is an 'Add Header' button in the top right, and 'Back' and 'Finish' buttons at the bottom.

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

The following screenshot shows the completed **Topology** Hiding configuration for the Telenor SIP Trunk.

Topology Hiding Profiles: Telenor

Click here to add a description.

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

Edit

To define Topology hiding for Session Manager, follow the same process. This can be simplified by cloning the profile defined for Telenor SIP Trunk. Do this by highlighting the profile defined for Telenor and clicking on **Clone**. Enter an appropriate name for Session Manager and click on **Next** (not shown). Make any changes where required, in the test environment the settings were left at the same values.

Topology Hiding Profiles: ASM

Click here to add a description.

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

Edit

7.8. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for the Session Manager and another for the Telenor SIP Trunk. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to the Telenor SIP Trunk and vice versa.

To define a Server Flow for the Telenor SIP Trunk, 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 **Flow Name** field enter a descriptive name for the server flow for the Telenor SIP Trunk, in the test environment **Telenor** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the Telenor SIP Trunk defined in **Section 7.5**.
- 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 SIP Trunk 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 SIP Trunk 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 SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Telenor SIP Trunk defined in **Section 7.7** and click **Finish**.

The screenshot shows a 'Add Flow' dialog box with the following fields and values:

Field	Value
Flow Name	Telenor
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	Telenor
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 **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **CPE** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.5**.
- 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 Telenor SIP Trunk defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.7** 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	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

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

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

Click here to add a row 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	Telenor	*	Internal	External	default-low	LAN	View Clone Edit Delete

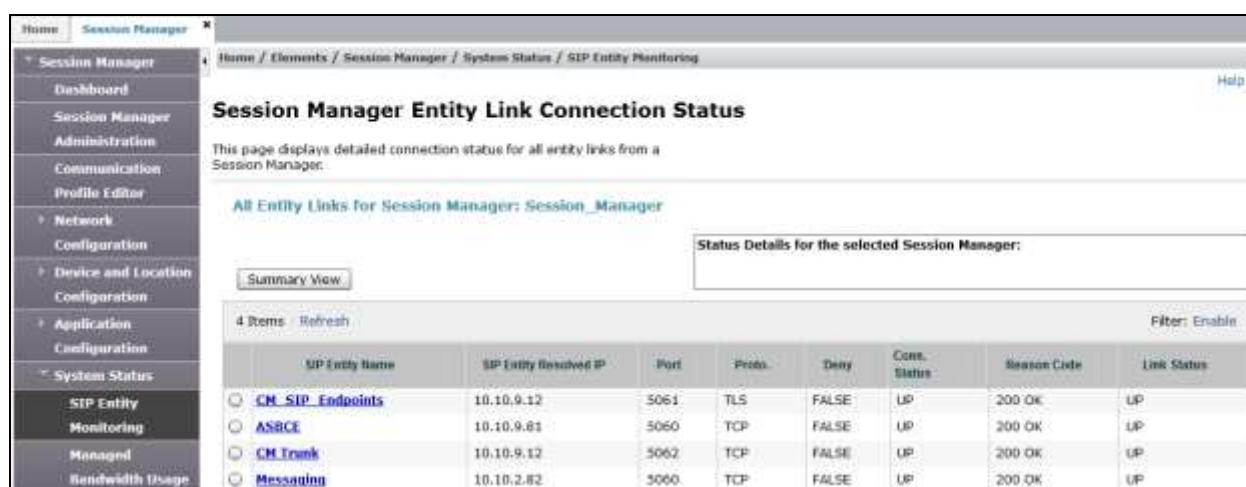
8. Configure the Telenor SIP Trunk Equipment

The configuration of the Telenor 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 Telenor equipment and system configuration please contact an authorized Telenor 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**.



SIP Entity Name	SIP Entity Resolved IP	Port	Proto	Deny	Conn. Status	Reason Code	Link Status
CM SIP Endpoints	10.10.9.12	5061	TLS	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 the 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

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 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.

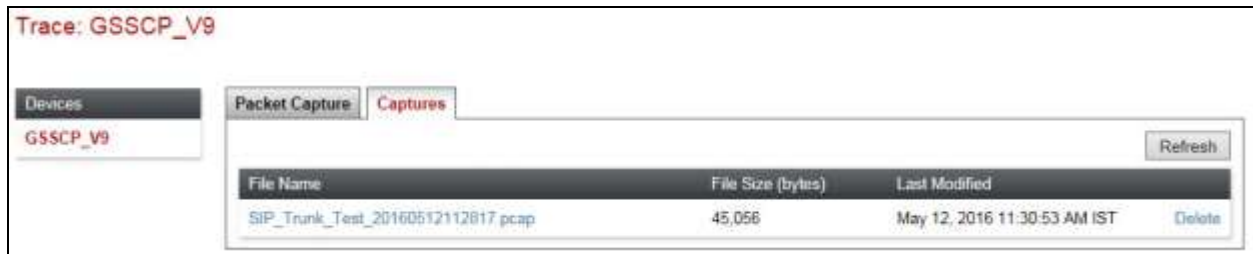
- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select the signalling interface IP address or **All** from the **Local Address** drop down menu.
- Enter the IP address of the network SBC in the **Remote Address** field or enter a * to capture all traffic.
- Specify the **Maximum 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**.

The screenshot displays the Avaya SBCE configuration interface for packet capture. The left-hand navigation pane lists various system management options, with 'Trace' highlighted under the 'Troubleshooting' category. The main content area, titled 'Trace: GSSCP_V9', features a 'Devices' dropdown menu currently set to 'GSSCP_V9'. Below this, the 'Packet Capture' configuration window is open, showing a 'Ready' status. The configuration parameters are as follows:

Field	Value
Status	Ready
Interface	B1
Local Address (IP Port)	All
Remote Address	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename	SIP_Trunk_Test.pcap

At the bottom of the configuration window, there are two buttons: 'Start Capture' and 'Clear'.

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



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 Telenor 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 Telenor SIP Trunk. The Telenor SIP Trunk 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. The Telenor SIP Trunk is described by the *Telenor SIP Specification – MBN* document provided by Telenor.

Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 7.0, Nov 2015.
- [2] *Upgrading and Migrating Avaya Aura® applications to 7.0*, Release 7.0, Nov 2015.
- [3] *Deploying Avaya Aura® applications*, Release 7.0, Oct 2015
- [4] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, August 2015
- [5] *Administering Avaya Aura® Communication Manager* Release 7.0, August 2015.
- [6] *Deploying Avaya Aura® System Manager* Release 7.0 Nov 2015
- [7] *Upgrading Avaya Aura® Communication Manager to Release 7.0*, Release 7.0, August 2015
- [8] *Upgrading Avaya Aura® System Manager to Release 7.0*, Nov 2015.
- [9] *Administering Avaya Aura® System Manager for Release 7.0* Release 7.0, Nov 2015
- [10] *Deploying Avaya Aura® Session Manager on VMware* , Release 7.0 August 2015
- [11] *Upgrading Avaya Aura® Session Manager* Release 7.0, August 2015
- [12] *Administering Avaya Aura® Session Manager* Release 7.0, August 2015,
- [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, Nov 2015
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2016 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.