



Application Notes for Configuring Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise R6.2 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 Telenor SIP Trunk service and an Avaya SIP enabled Enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise R6.2. Telenor is a member of the DevConnect Service Provider program.

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

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

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Telenor SIP Trunk service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise (Avaya SBCE). 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 data 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 use the SIP Trunk service provided by Telenor.

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using the SIP Trunk provided by Telenor, calls made to SIP, H.323, Digital and Analogue telephones at the enterprise.
- Outgoing calls from the enterprise site completed via Telenor's SIP Trunk to PSTN destinations, calls made from SIP, H.323, Digital and Analogue telephones.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator and Avaya Flare Experience for Windows softphones.
- Calls using G.711A and G.711MU codecs.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using T.38 transmission.
- Caller ID Presentation and Caller ID Restriction.
- DTMF transmission using RFC 2833.
- Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer and conference.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Off-net call forwarding and EC5000 mobile twinning.
- Transmission and response of SIP OPTIONS messages sent by Telenor 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:

- G729 codec is not supported by Telenor.
- No inbound toll free numbers were tested as none were available from the Service Provider.
- No Emergency Services numbers tested as test calls to these numbers should be pre-arranged with the 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 96xx, 16xx Series IP Deskphones (with SIP and H.323 firmware), Avaya Digital Deskphones, Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was Avaya one-X® Communicator and Avaya Flare Experience for Windows softphones running on a laptop PC configured for SIP & H.323.

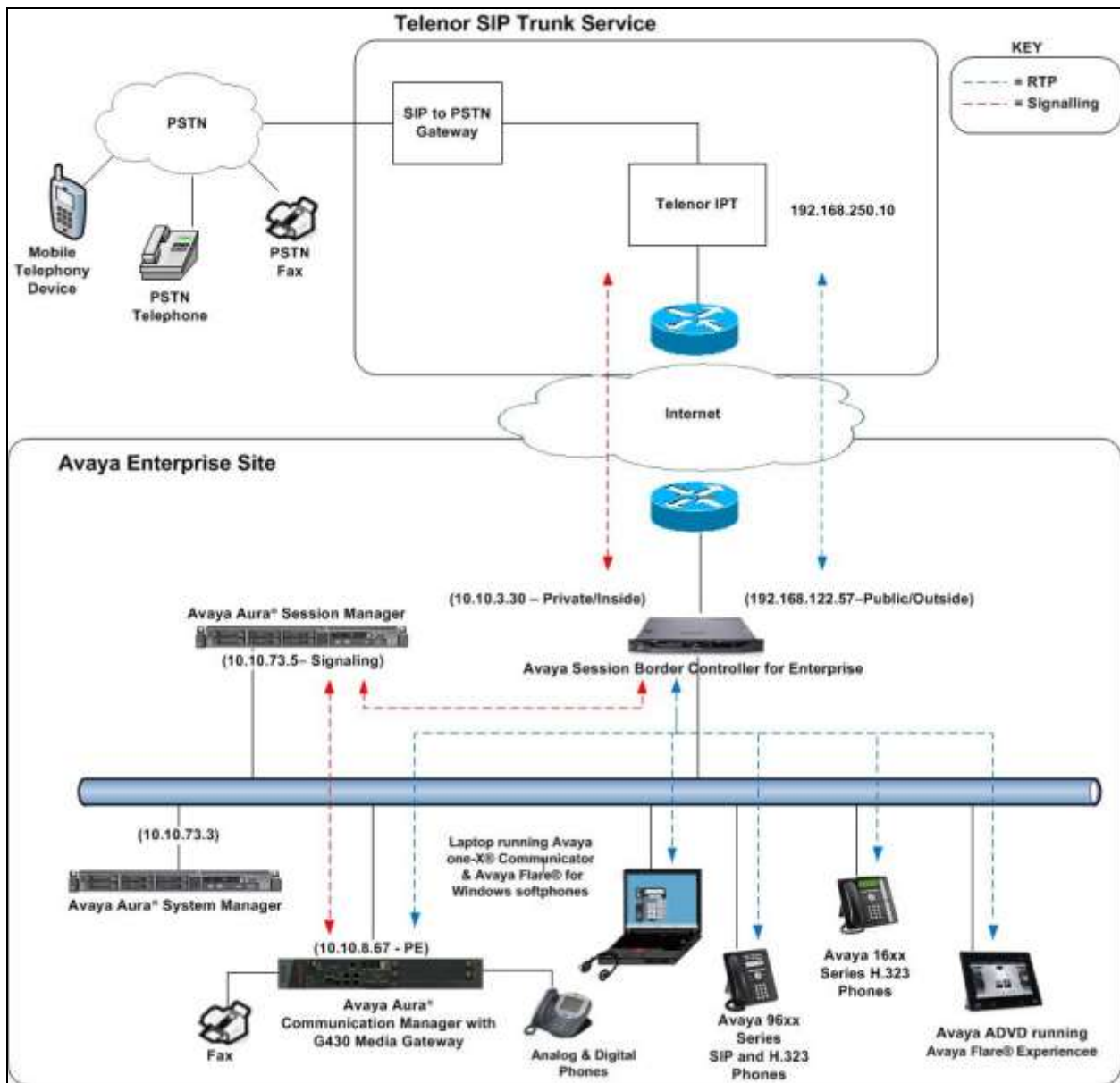


Figure 1: Test Setup Telenor SIP Trunk service to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Dell PowerEdge R620 running Avaya Aura® Session Manager on VM Version 8	R6.3.11 - 6.3.11.0.631103
Dell PowerEdge R620 running Avaya Aura® System Manager on VM Version 8	R6.3.11 - Build No. - 6.3.0.8.5682-6.3.8.4411 Software Update Revision No: 6.3.11.8.1.2871
Avaya S8800 Server running Avaya Aura® Communication Manager	R016x.03.0.124.0-21754
Avaya Session Border Controller for Enterprise	6.2.1.Q18
Avaya 16xx IP DeskPhone (H.323)	1.3
Avaya 9670 IP DeskPhone (H.323)	6.4
Avaya 96x0 IP DeskPhone (H.323)	6.4
Avaya 96x1 IP DeskPhone (H.323)	6.4
Avaya 96x0 IP DeskPhone (SIP)	6.4.1
Avaya 96x1 IP DeskPhone (SIP)	6.4.1
Avaya A175 Desktop Video Device with Avaya Flare® Experience	1.1.3
Avaya one-X® Communicator (H.323) on Lenovo T510 Laptop PC	6.2.4.07-FP4
Avaya Flare Experience for Windows	1.1.4.23
Avaya Digital Deskphone	Rel 12.0
Analogue Telephone	N/A
Telenor	
Telenor SIP Trunk Service	Telenor IPT Version 11.0.138

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. 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 Avaya S8800 Server 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 network, and any other SIP trunks used.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	25
Maximum Concurrently Registered IP Stations:		18000	4
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		113	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		41000	0
Maximum Video Capable IP Softphones:		10	7
Maximum Administered SIP Trunks:		24000	54
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
Maximum TN2501 VAL Boards:		128	0
Maximum Media Gateway VAL Sources:		250	1
Maximum TN2602 Boards with 80 VoIP Channels:		128	0
Maximum TN2602 Boards with 320 VoIP Channels:		128	0
Maximum Number of Expanded Meet-me Conference Ports:		0	0

On **Page 4**, verify that **IP Trunks** field is set to **y**.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y		IP Stations? y
Enable 'dadmin' Login? y		
Enhanced Conferencing? y		ISDN Feature Plus? y
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y
Enterprise Wide Licensing? n		ISDN-PRI? y
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? y	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
IP Trunks? y		
IP Attendant Consoles? y		

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for Session Manager. In this case, **SM100** and **10.10.73.5** are the **Name** and **IP Address** for Session Manager SIP interface. Also note the **procr** name 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	
SM100	10.10.73.5	
default	0.0.0.0	
procr	10.10.8.67	
procr6	::	

5.3. Administer IP Network Region

Use the **change ip-network-region 1** command to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the Avaya SBCE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** is used.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1
Location: 1           Authoritative Domain: avaya.com
Name:
MEDIA PARAMETERS           Intra-region IP-IP Direct Audio: yes
      Codec Set: 1         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
H.323 IP ENDPOINTS           AUDIO RESOURCE RESERVATION PARAMETERS
                                RSVP Enabled? n
      H.323 Link Bounce Recovery? y
      Idle Traffic Interval (sec): 20
      Keep-Alive Interval (sec): 5
      Keep-Alive Count: 5
```


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

change ip-codec-set 1				Page 1 of 2
IP Codec Set				
Codec Set: 1				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)	
1: G.711A	n	2	20	
2: G.711MU	n	2	20	

Telenor SIP Trunk service supports T.38 for transmission of fax. Navigate to **Page 2** to configure T.38 by setting the **FAX - Mode** to **t.38-standard** as shown below.

change ip-codec-set 1				Page 2 of 2
IP Codec Set				
Allow Direct-IP Multimedia? y				
FAX	Mode	Redundancy	ECM: y	
Modem	t.38-standard	0		
TDD/TTY	off	0		
Clear-channel	UK	3		
	n	0		

5.5. Administer SIP Signalling 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 **5060** to facilitate tracing and fault analysis. It is recommended however, to use TLS (Transport Layer Security) and the default TLS port of **5061** for security. Configure the **Signaling Group** using the **add signaling-group x** 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 (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (commonly used TCP port value).
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region 1).
- 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**.
- 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.

add signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	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		
Near-end Node Name: procr	Far-end Node Name: SM100	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
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 signalling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group x** command, where **x** is an available trunk group. On **Page 1** of this form:

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

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: OUTSIDE CALL	COR: 1	TN: 1	TAC: 101
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: 1	
		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.

Add trunk-group 1		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			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	

On **Page 3**, set the **Numbering Format** field to **public**. This allows delivery of CLI in E.164 format with a leading “+”.

add trunk-group 1	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
Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y	

On **Page 4** of this form:

- Set **Mark Users as Phone** to **y**.
- Set **Send Transferring Party Information** to **n**.
- Set **Network Call Direction** to **n**.
- Set **Send Diversion Header** to **y**.
- Set **Support Request History** to **n**.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Telenor.
- Set **Always Use re-INVITE for Display Updates** to **y**.
- Set the **Identity for Calling Party Display** to **P-Asserted-Identity**.

add trunk-group 1	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? 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? y
	Identity for Calling Party Display: P-Asserted-Identity
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 E.164 format. In the test configuration, individual stations were mapped to send numbers allocated from the Telenor DDI range supplied. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Note that the digits identifying the DDI range are not shown.

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	6010	1	4722nnnn31	10	Total Administered: 8
4	6011	1	4722nnnn32	10	Maximum Entries: 9999
4	6012	1	4722nnnn33	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	6013	1	4722nnnn34	10	
4	6102	1	4722nnnn35	10	
4	6101	1	4722nnnn36	10	
					Communication Manager automatically inserts a '+' digit in this case.

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 SIP Trunk service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line.

Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *69		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 7		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to two UK area codes and one international country code. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

change ars analysis 0							Page 1 of 2	
ARS DIGIT ANALYSIS TABLE							Percent Full: 2	
Location: all								
	Dialed String	Total Min	Max	Route Pattern	Call Type	Node Num	ANI Reqd	
0		8	15	1	pubu		n	
0		8	18	1	pubu		n	
00		8	15	1	pubu		n	

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**.

change route-pattern 1												Page 1 of 3		
Pattern Number: 1												Pattern Name: to ASM		
SCCAN? n												Secure SIP? n		
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits					QSIG		
Dgts												Intw		
1:	1	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	No. Numbering	LAR
0		1 2 M 4 W				Request						Dgts Format		
												Subaddress		
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 the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Telenor can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DDI numbers provided by Telenor correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DDI numbers **+47xxxxxx31**, **+47xxxxxx32** and **+47xxxxxx33** to a 4 digit extension by deleting all of the incoming digits and inserting an extension. Public DDI numbers have been masked for security purposes.

change inc-call-handling-trmt trunk-group 1				Page	1 of	3
INCOMING CALL HANDLING TREATMENT						
Service/ Feature	Number Len	Number Digits	Del	Insert		
public-ntwrk	11	+47xxxxxx31	all	6010		
public-ntwrk	11	+47xxxxxx32	all	6011		
public-ntwrk	11	+47xxxxxx33	all	6012		

5.10. EC500 Configuration

When EC500 is enabled on the 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 a sample EC500 configuration for the user with station extension 6102. Use the command **change off-pbx-telephone station-mapping x** where **x** is the Communication Manager station extension.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration.
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386xxxxxxx**).
- Set the **Trunk Selection** to the trunk group defined in **section 5.6** for the SIP Trunk, in test it was **1**.
- Set the **Config Set** to **1**.

change off-pbx-telephone station-mapping 6102						Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION								
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual	
Extension		Prefix			Selection	Set	Mode	
6102	EC500	-		0035386xxxxxxx	1	1		
		-						

Note: The phone number shown is for a mobile phone used for testing at Avaya Labs and is in international format. To use facilities for calls coming in from EC500 mobile phones, the number received in Communication Manager must exactly match the number specified in the above table.

Save Communication Manager changes by entering **save translation** to make them permanent.

6. Configuring Avaya Aura® Session Manager

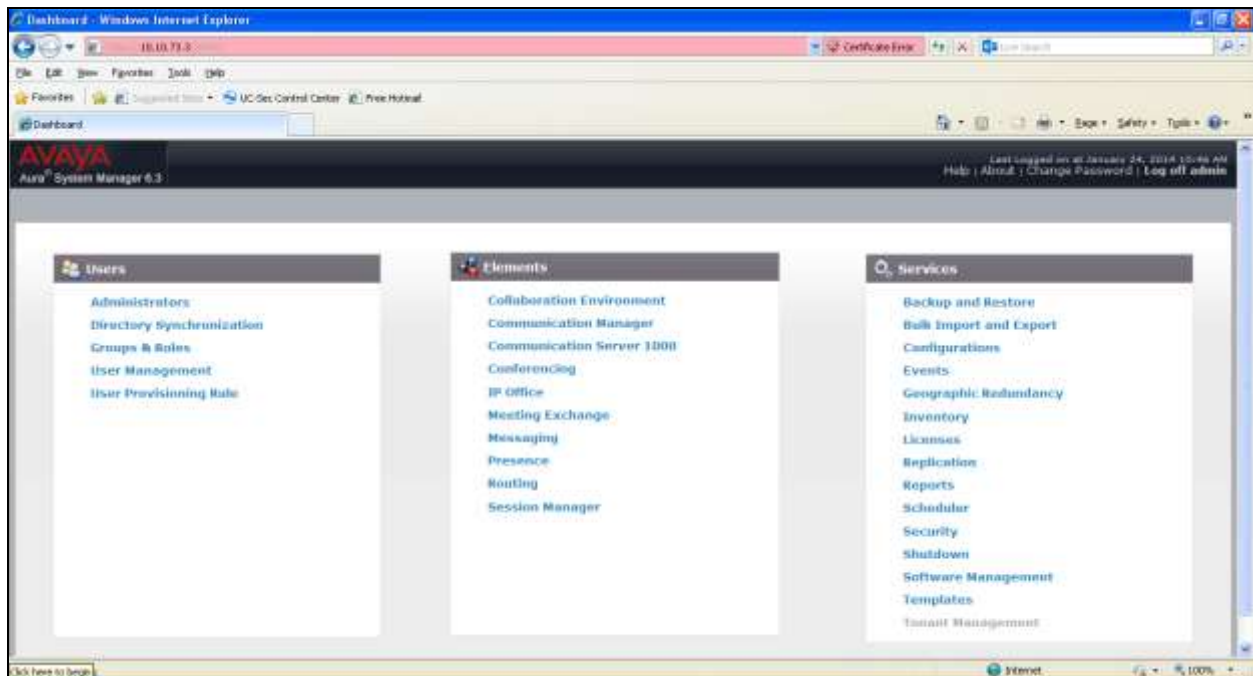
This section provides the procedures for configuring Session Manager. Session Manager is configured via the System Manager. The procedures include the following areas:

- 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

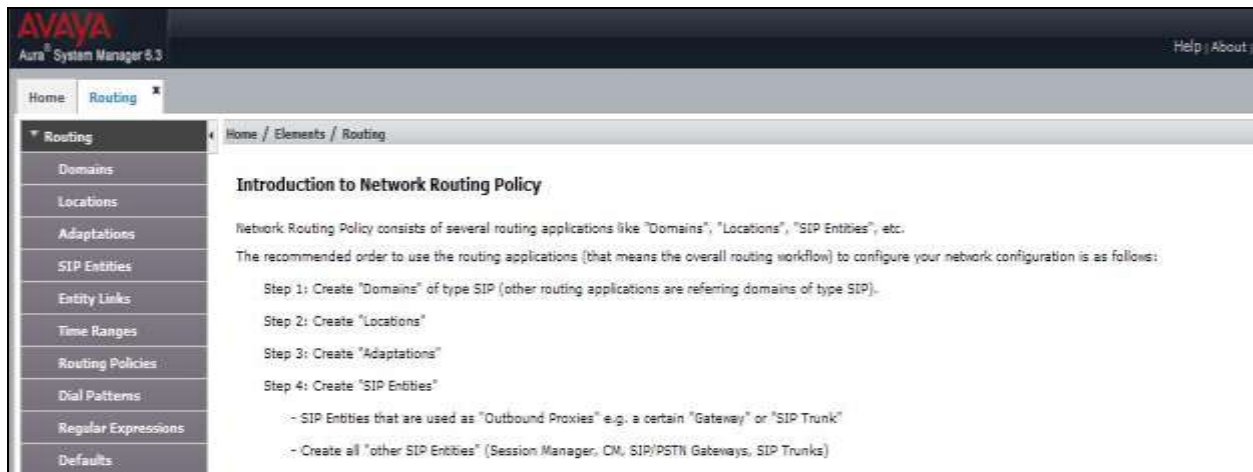
It may not be necessary to create all the items above when creating a connection to the Service Provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by 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.



Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown above to bring up the **Introduction to Network Routing Policy** screen.

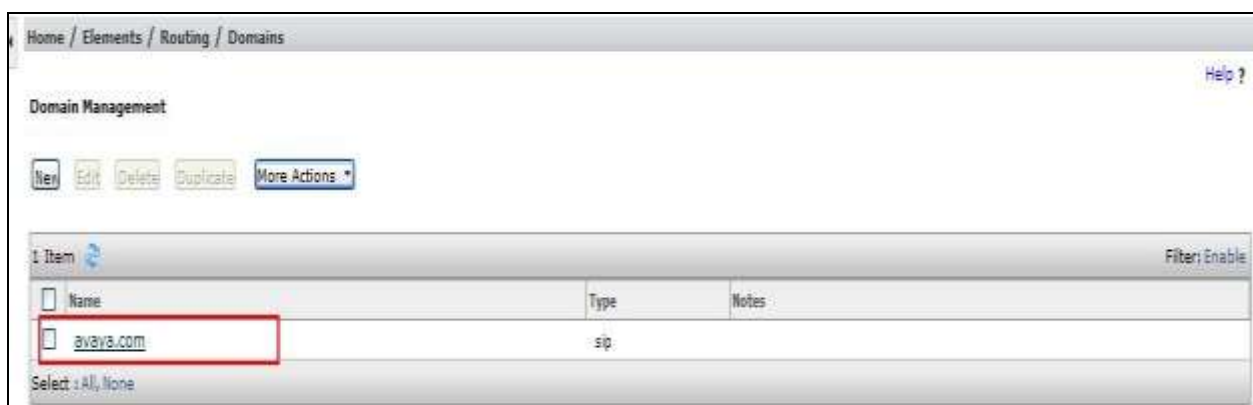


6.2. Administer SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. Expand **Elements** → **Routing** and select **Domains** from the left navigation menu, click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name** Enter a domain name. In the sample configuration, **avaya.com** was used.
- **Type** Verify **SIP** is selected.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screen below shows the SIP domain defined for the sample configuration (not shown).



6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screenshot below shows the Location **VM_SMGR** defined for the compliance testing.

The screenshot displays the Avaya Session Manager Administration console interface for configuring a location. The breadcrumb trail at the top reads: Home / Elements / Routing / Locations. The main section is titled "Location Details" and includes "Commit" and "Cancel" buttons in the top right corner. The "General" tab is selected, showing the following fields:

- Name:** VM_SMGR
- Notes:** (empty text area)
- Dial Plan Transparency in Survivable Mode:** Enabled: ☐
- Listed Directory Number:** (empty text field)
- Associated CM SIP Entity:** (dropdown menu with a selection icon)
- Overall Managed Bandwidth:**
 - Managed Bandwidth Units: Kbit/sec (selected)
 - Total Bandwidth: (empty text field)
 - Multimedia Bandwidth: (empty text field)
 - 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

Below the "General" section is the "Location Pattern" section, which includes "Add" and "Remove" buttons. It contains a table with the following columns: "IP Address Pattern", "Notes", and "Status/Enable". The table lists several IP address patterns, all of which are selected (checked in the first column):

IP Address Pattern	Notes	Status/Enable
10.10.2.		
10.10.3.		
10.10.5.		
10.10.7.		
10.10.8.		
10.10.9.		
*		

At the bottom of the "Location Pattern" section, there is a "Select: All, None" link and "Commit" and "Cancel" buttons.

6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the Digit Conversion in the Adaptation. The example below was applied to the Avaya SBCE SIP Entity and was used in test to convert numbers being passed between the Avaya SBCE and Session Manager.

To add an adaptation, under the **Routing** tab select **Adaptations** on the left hand menu and then click on the **New** button (not shown). Under **Adaption Details** → **General**:

- In the **Adaptation name** field enter an informative name.
- In the **Module name** field click on the down arrow and then select the **<click to add module>** entry from the drop down list and type **DigitConversionAdapter** in the resulting New Module Name field.
- **Module parameter** **MIME=no** strips MIME message bodies on egress from Session Manager.
fromto=true modifies from and to headers of a message.

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

Help ?

General

* Adaptation Name: Telenor

Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Add Remove

Name	Value
fromto	true
MIME	no

Select: All, None

Egress URI Parameters:

Notes:

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 **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field select the time zone for the SIP entity.

In this configuration there are three SIP entities.

- Session Manager SIP entity
- Communication Manager SIP entity
- Avaya SBCE SIP entity

6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface and **TYPE** is **Session Manager**. Set 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 window, specifically the 'General' tab. The breadcrumb navigation at the top is 'Home / Elements / Routing / SIP Entities'. There are 'Commit' and 'Cancel' buttons at the top right, and a 'Help ?' link. The 'SIP Entity Details' section has a 'General' sub-tab. The fields are as follows:

- * Name: Session Manager
- * FQDN or IP Address: 10.10.73.5
- Type: Session Manager (dropdown)
- Notes: (empty text box)
- Location: VM_SMGR (dropdown)
- Outbound Proxy: (empty dropdown)
- Time Zone: Europe/Dublin (dropdown)
- Credential name: (empty text box)

At the bottom, there is a 'SIP Link Monitoring' section with a checkbox 'SIP Link Monitoring:' and a dropdown 'Use Session Manager Configuration'.

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 select 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.

The screenshot shows the 'Port' configuration section. At the top, there are input fields for 'TCP Failover port:' and 'TLS Failover port:', followed by 'Add' and 'Remove' buttons. Below this is a table with 3 items. The table has columns: Port, Protocol, Default Domain, and Notes. The 'Filter' is set to 'Enable'. The table contains three rows:

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

At the bottom, there is a 'Select' dropdown menu with options 'All', 'None'.

6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling and **Type** is **CM**. Set 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' window for 'Communication Manager'. The 'General' tab is selected. The 'Name' field is 'Communication Manager'. The 'FQDN or IP Address' field is '10.10.8.67'. The 'Type' field is 'CM'. The 'Location' field is 'VN_SMGR'. The 'Time Zone' field is 'Europe/Dublin'. The 'SIP Timer B/F (in seconds)' field is '4'. The 'Credential name' field is empty. The 'Call Detail Recording' field is 'none'. The 'Loop Detection Mode' field is 'Off'.

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set **Type** to **SIP Trunk** and **Adaptation** to that defined in **Section 6.4**. Set 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' window for 'Avaya SBCE'. The 'General' tab is selected. The 'Name' field is 'Avaya SBCE'. The 'FQDN or IP Address' field is '10.10.3.30'. The 'Type' field is 'SIP Trunk'. The 'Location' field is 'VN_SMGR'. The 'Time Zone' field is 'Europe/Dublin'. The 'SIP Timer B/F (in seconds)' field is '4'. The 'Credential name' field is empty. The 'Call Detail Recording' field is 'egress'. The 'Loop Detection Mode' field is 'Off'. The 'SIP Link Monitoring' field is 'Use Session Manager Configuration'.

6.6. Administer Entity Links

A SIP trunk between 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 **Protocol** field select the transport protocol to be used to send SIP requests.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field select 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.
- In the **Connection Policy** field, select **trusted** from the drop-down menu.

Click **Commit** to save changes. The following screen shows the entity link for Communication Manager.

The screenshot shows the 'Entity Links' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Entity Links'. Below this, there are 'Commit' and 'Cancel' buttons. The main area contains a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DRS Override, Port, Connection Policy, Deny New Service, and Notes. A single row is displayed, representing the entity link for Communication Manager. The values in this row are: Name: '*Communication M...', SIP Entity 1: '*Session Manager', Protocol: 'TCP', Port: '*5060', SIP Entity 2: '*Communication Manager', DRS Override: (checkbox), Port: '*5060', Connection Policy: 'trusted', Deny New Service: (checkbox), and Notes: (empty). A red box highlights the row. At the bottom, there are 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DRS Override	Port	Connection Policy	Deny New Service	Notes
*Communication M...	*Session Manager	TCP	*5060	*Communication Manager	<input type="checkbox"/>	*5060	trusted	<input type="checkbox"/>	

The following screen shows the entity link for the Avaya SBCE.

The screenshot shows the 'Entity Links' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Entity Links'. Below this, there are 'Commit' and 'Cancel' buttons. The main area contains a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DRS Override, Port, Connection Policy, Deny New Service, and Notes. A single row is displayed, representing the entity link for Avaya SBCE. The values in this row are: Name: '*Avaya SBCE', SIP Entity 1: '*Session Manager', Protocol: 'TCP', Port: '*5060', SIP Entity 2: '*Avaya SBCE', DRS Override: (checkbox), Port: '*5060', Connection Policy: 'trusted', Deny New Service: (checkbox), and Notes: (empty). A red box highlights the row. At the bottom, there are 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DRS Override	Port	Connection Policy	Deny New Service	Notes
*Avaya SBCE	*Session Manager	TCP	*5060	*Avaya SBCE	<input type="checkbox"/>	*5060	trusted	<input type="checkbox"/>	

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 Communication Manager.

The screenshot shows the 'Routing Policy Details' form for a policy named 'to_Communication Manager'. The 'General' tab is active. The 'Name' field contains 'to_Communication Manager'. The 'Disabled' checkbox is unchecked. The 'Retries' field is set to 0. The 'Notes' field is empty. Under the 'SIP Entity as Destination' section, the 'Select' button is visible. Below it, a table lists the selected entity: 'Communication Manager' with IP address '10.10.8.87' and type 'CM'. Under the 'Time of Day' section, the 'Add' button is visible. Below it, a table lists the selected time range: '24/7' with start time '00:00' and end time '23:59', labeled 'Time Range 24/7'.

Name	FQDN or IP Address	Type	Notes
Communication Manager	10.10.8.87	CM	

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

The following screen shows the routing policy for the Avaya SBCE.

The screenshot shows the 'Routing Policy Details' form for a policy named 'to_AvayaSBCE'. The 'General' tab is active. The 'Name' field contains 'to_AvayaSBCE'. The 'Disabled' checkbox is unchecked. The 'Retries' field is set to 0. The 'Notes' field is empty. Under the 'SIP Entity as Destination' section, the 'Select' button is visible. Below it, a table lists the selected entity: 'Avaya SBCE' with IP address '10.10.3.30' and type 'SIP Trunk'. Under the 'Time of Day' section, the 'Add' button is visible. Below it, a table lists the selected time range: '24/7' with start time '00:00' and end time '23:59', labeled 'Time Range 24/7'.

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.10.3.30	SIP Trunk	

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

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** and under **Routing Policies** select one of the routing policies defined in **Section 6.7**. Click **Select** button to save. The following screen shows a sample dial pattern configured for the Avaya SBCE which will route calls out to the Telenor SIP Trunk service.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern: 00

* Min: 2

* Max: 16

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: ALL

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy	Routing Policy Destination	Routing Policy Notes
VM_SMOR		to_AvayaSBCE	0	Routing Policy Disabled	Avaya SBCE	

Select: All, None

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

Home / Elements / Routing / Dial Patterns help ?

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Rules	Routing Policy Name	Rank	Routing Policy	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	VM_SNDR		to_Communication Manager	0	<input checked="" type="checkbox"/> Disabled	Communication Manager	

Select:

7. Configure Avaya Session Border Controller for Enterprise

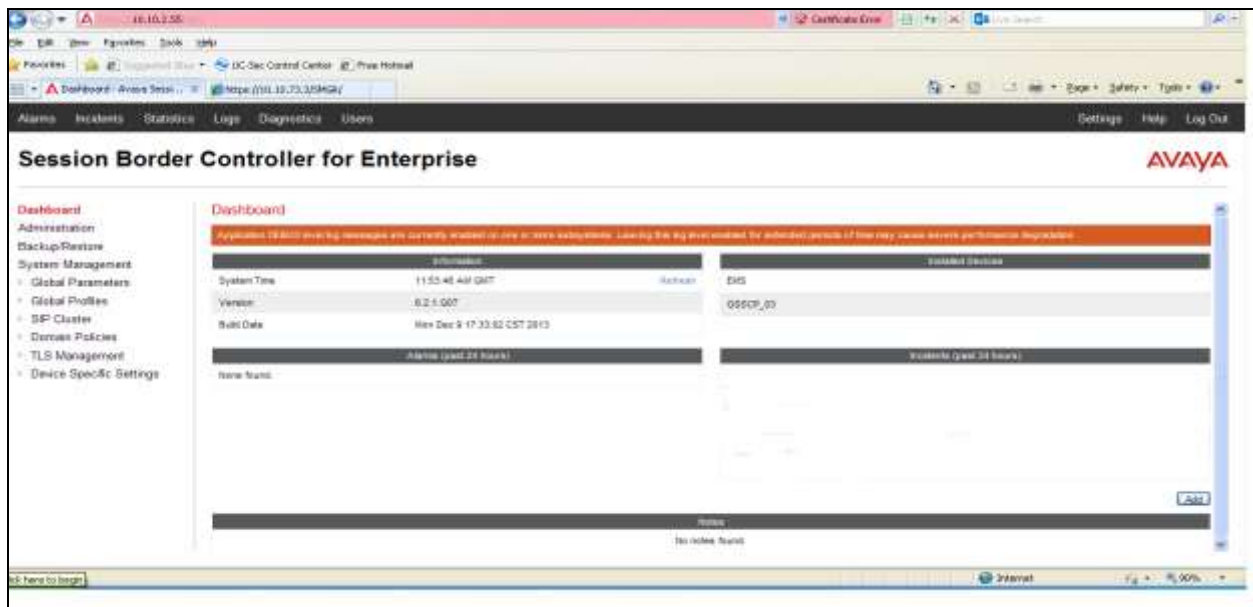
This section describes the configuration of the Avaya SBCE. The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary..

7.1. Access Avaya Session Border Controller for Enterprise

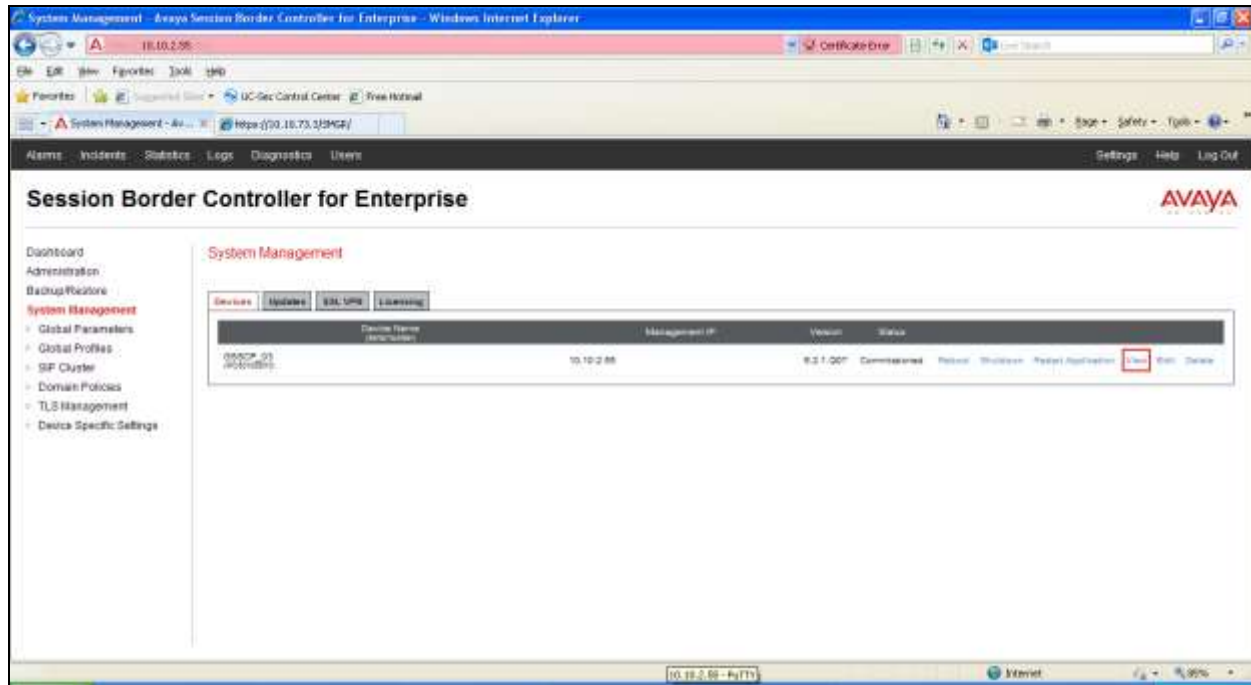
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



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.



To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP_03** is shown. To view the configuration of this device, click **View** (the third option from the right).



The **System Information** screen shows the **General Configuration**, **Device Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP** information.

System Information: GSSCP_03				
General Configuration		Device Configuration		
Appliance Name	GSSCP_03	HA Mode	No	
Box Type	SIP	Two Bypass Mode	No	
Deployment Mode	Proxy			
Network Configuration				
IP	Public IP	Netmask	Gateway	Interface
10.10.3.30	10.10.3.30	255.255.255.0	10.10.3.1	A1
192.168.122.55	192.168.122.55	255.255.255.128	192.168.122.7	B1
DNS Configuration		Management IP(s)		
Primary DNS	10.10.7.100	IP	10.10.2.55	
Secondary DNS	10.10.101.115			
DNS Location	DMZ			
DNS Client IP	10.10.3.30			

7.2. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.2.1. Server Interworking - Avaya

Server Interworking allows one to configure and manage various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles** → **Server Interworking** and click on **Add Profile**.

- Enter profile name such as **Avaya_SM** and click **Next** (not shown).
- Check **Delayed SDP Handling**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

Click on **Next** on the following screens and then **Finish**.

Profile: Avaya_SM

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
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input checked="" type="checkbox"/>
Re-Invite Handling	<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

Next

Default values can be used for the **Advanced Settings** window (not shown). Click **Finish**.

Profile: Avaya_SM X

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Finish

7.2.2. Server Interworking – Telenor

From the left-hand menu select **Global Profiles** → **Server Interworking** and click on **Add Profile** (not shown).

- Enter profile name such as **Telenor** and click **Next** (not shown).
- Check **180 Handling = No SDP**.
- Check **Delayed SDP Handling**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

Click on **Next** on the following screens and then **Finish**.

The screenshot shows the 'Profile: Telenor' configuration window with the 'General' tab selected. The settings are as follows:

Setting	Value
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 type="radio"/> None <input type="radio"/> SDP <input checked="" type="radio"/> No SDP
181 Handling	<input type="radio"/> None <input type="radio"/> SDP <input checked="" 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
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input checked="" type="checkbox"/>
Re-Invite Handling	<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

Next

Default values can be used for the **Advanced Settings** window (not shown). Click **Finish**.

Profile: Telenor X

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Finish

7.2.3. Routing

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by routing profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

Routing information is required for routing to Session Manager on the internal side and the Telenor addresses on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

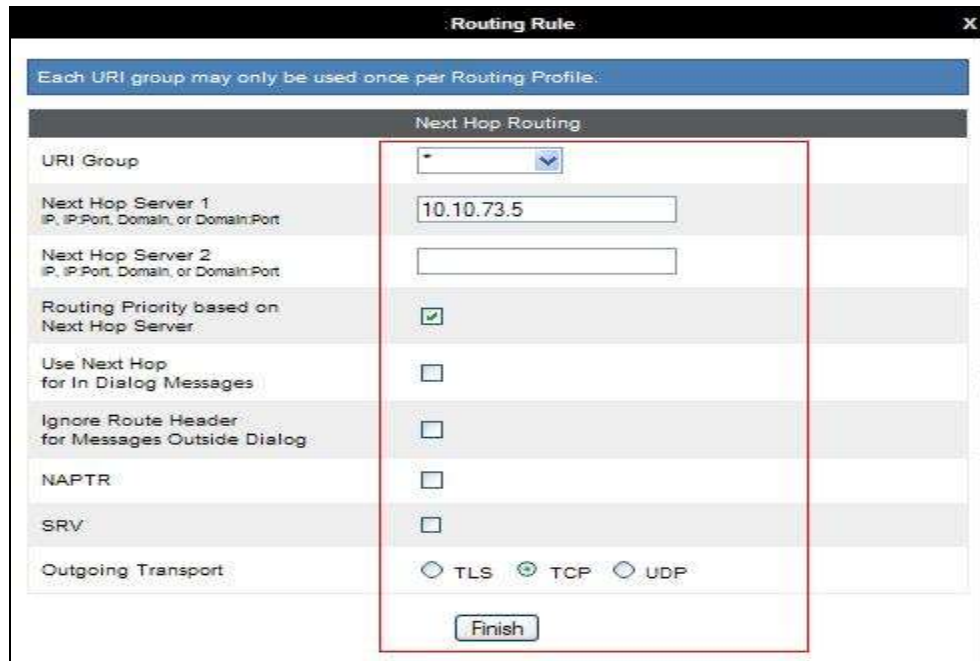
Create a routing profile for both Session Manager and Telenor SIP trunk. To add a routing profile, navigate to **Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **URI Group:** Select “*” from the drop down box.
- **Next Hop Server 1:** Enter the domain name or IP address of the primary Next Hop server, e.g. Session Manager.
- **Next Hop Server 2:** (Optional) Enter the domain name or IP address of the secondary Next Hop server.
- **Routing Priority based on Next Hop Server:** Checked.
- **Use Next Hop for In Dialog Messages:** Select only if there is no secondary Next Hopserver
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signalling packets.

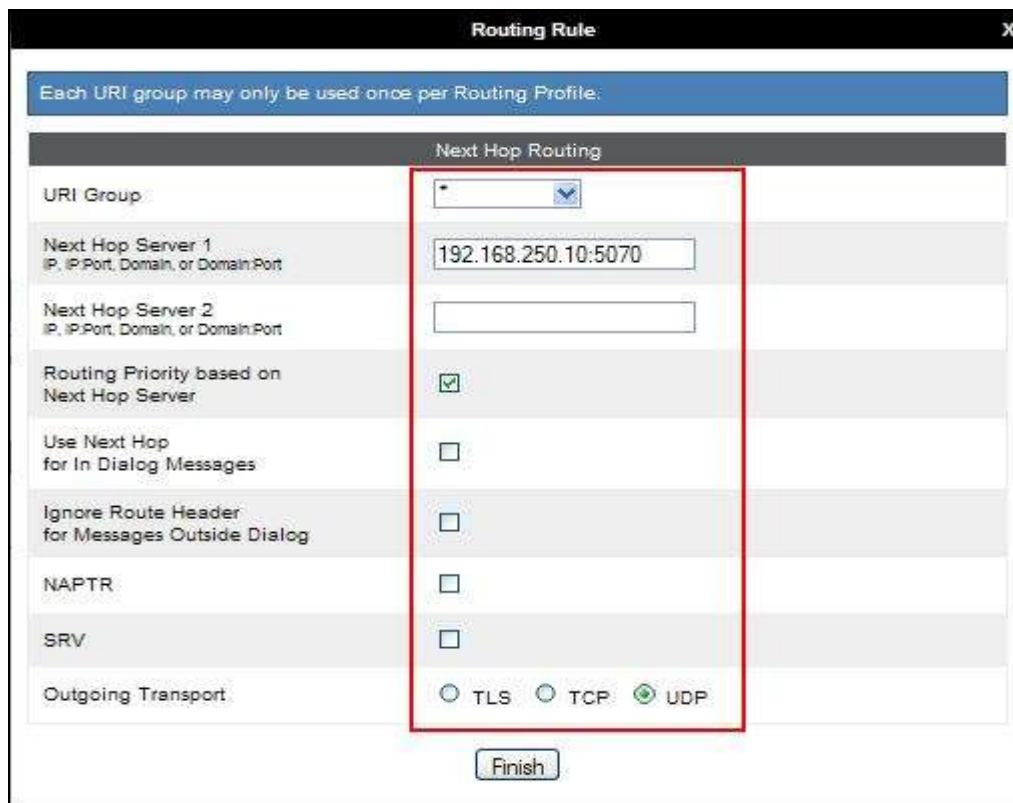
Click **Finish**.

The following screen shows the routing profile to Session Manager



The screenshot shows a 'Routing Rule' window with a blue header bar containing the text 'Each URI group may only be used once per Routing Profile:'. Below this is a 'Next Hop Routing' section. A red rectangular box highlights the following fields: 'URI Group' (a dropdown menu with a '*' icon), 'Next Hop Server 1' (a text field containing '10.10.73.5'), 'Next Hop Server 2' (an empty text field), 'Routing Priority based on Next Hop Server' (a checked checkbox), 'Use Next Hop for In Dialog Messages' (an unchecked checkbox), 'Ignore Route Header for Messages Outside Dialog' (an unchecked checkbox), 'NAPTR' (an unchecked checkbox), 'SRV' (an unchecked checkbox), and 'Outgoing Transport' (radio buttons for TLS, TCP, and UDP, with TCP selected). A 'Finish' button is located at the bottom of the highlighted area.

The following screen shows the routing profile to Telenor. Note: IP Port **5070** was used in the Telenor configuration for this compliance test.



The screenshot shows a 'Routing Rule' window with a blue header bar containing the text 'Each URI group may only be used once per Routing Profile:'. Below this is a 'Next Hop Routing' section. A red rectangular box highlights the following fields: 'URI Group' (a dropdown menu with a '*' icon), 'Next Hop Server 1' (a text field containing '192.168.250.10:5070'), 'Next Hop Server 2' (an empty text field), 'Routing Priority based on Next Hop Server' (a checked checkbox), 'Use Next Hop for In Dialog Messages' (an unchecked checkbox), 'Ignore Route Header for Messages Outside Dialog' (an unchecked checkbox), 'NAPTR' (an unchecked checkbox), 'SRV' (an unchecked checkbox), and 'Outgoing Transport' (radio buttons for TLS, TCP, and UDP, with UDP selected). A 'Finish' button is located at the bottom of the highlighted area.

7.2.4. Server Configuration – Avaya Aura® Session Manager

Servers are defined for each server connected to the Avaya SBCE. In this case, Telenor is connected as the Trunk Server and Session Manager is connected as the Call Server.

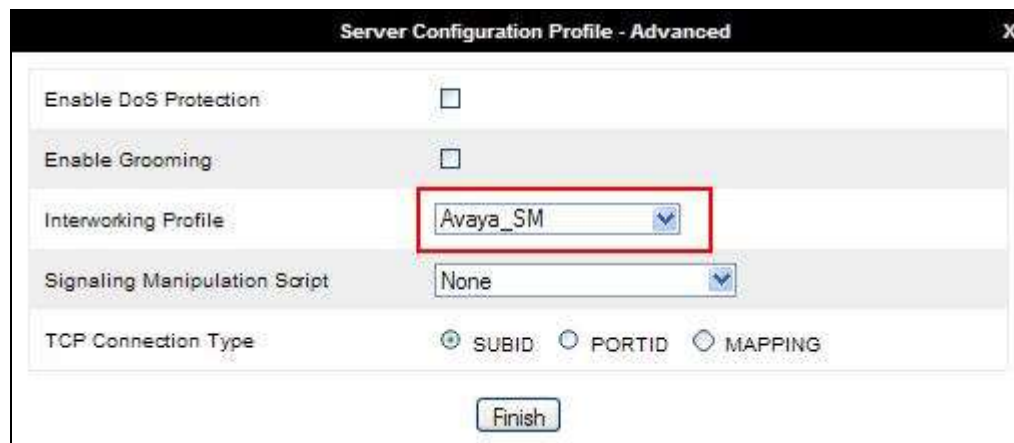
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow the configuration and management of various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signalling parameters and some advanced options. From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add Profile** and enter a descriptive name (not shown). On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**.
- Enter **IP Addresses / Supported FQDNs** to **10.10.73.5** (Session Manager IP Address).
- For **Supported Transports**, check **TCP**.
- Set **TCP Port** to **5060**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

The screenshot shows the 'Server Configuration Profile - General' window. The 'Server Type' dropdown is set to 'Call Server'. The 'IP Addresses / Supported FQDNs' text box contains '10.10.73.5'. Under 'Supported Transports', the 'TCP' checkbox is checked, while 'UDP' and 'TLS' are unchecked. The 'TCP Port' text box contains '5060'. The 'UDP Port' and 'TLS Port' text boxes are empty. A 'Finish' button is at the bottom.

On the **Advanced** tab:

- Select **Avaya_SM** for **Interworking Profile**.
- Click **Finish**.



Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile **Avaya_SM**

Signaling Manipulation Script **None**

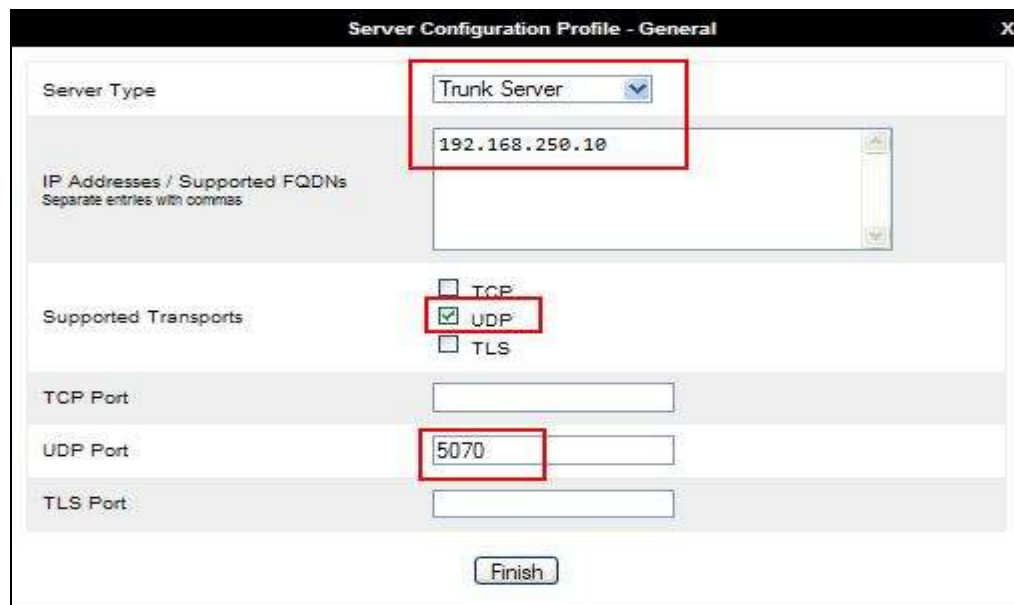
TCP Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

Finish

7.2.5. Server Configuration – Telenor

To define the Telenor Trunk Server, navigate to select **Global Profiles → Server Configuration** and click on **Add Profile** and enter a descriptive name (not shown). On the **Add Server Configuration Profile** tab, click on **Edit** and set the following:

- Select **Server Type** as **Trunk Server**.
- Set **IP Address** to **192.168.250.10** (Telenor SIP Trunks).
- **Supported Transports**: Check **UDP**.
- Set **UDP Port** to **5070**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



Server Configuration Profile - General

Server Type **Trunk Server**

IP Addresses / Supported FQDNs
Separate entries with commas
192.168.250.10

Supported Transports ☐ TCP ☒ **UDP** ☐ TLS

TCP Port

UDP Port **5070**

TLS Port

Finish

On the **Advanced** tab:

- Select **Telenor** for **Interworking Profile**.
- Click **Finish**.

The screenshot shows a window titled "Server Configuration Profile - Advanced". It contains several configuration options:

- Enable DoS Protection**: A checkbox that is currently unchecked.
- Enable Grooming**: A checkbox that is currently unchecked.
- Interworking Profile**: A dropdown menu with "Telenor" selected. This dropdown is highlighted with a red rectangular box.
- Signaling Manipulation Script**: A dropdown menu with "None" selected.
- UDP Connection Type**: Three radio buttons labeled "SUBID", "PORTID", and "MAPPING". The "SUBID" radio button is selected.

At the bottom of the window is a button labeled "Finish".

7.2.6. 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. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from the Session Manager. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define topology hiding for the Session Manager, navigate to **Global Profiles → Topology Hiding** in the menu on the left-hand side (not shown). Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive profile name such as **Avaya_SM**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For **Overwrite Value**, insert **avaya.com**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Avaya_SM

Buttons: Add, Rename, Done, Delete

Topology Hiding Profile list: default, cisco_th_profile, **Avaya_SM**, Telecor

Click here to add a description.

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

Edit

To define topology hiding for Telenor, navigate to **Global Profiles → Topology Hiding** in the menu on the left hand side (not shown). Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive profile name such as **Telenor**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For **Overwrite Value**, insert **ipt.telenor.com**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Telenor

Add

Topology Hiding Profiles

default

cisco_th_profile

Avaya_SMI

Telenor

Rename Done Delete

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	ipt.telenor.com
From	IP/Domain	Overwrite	ipt.telenor.com
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	ipt.telenor.com
SIP	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---

Edit

7.3. Domain Policies

Domain policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain policies include rules for application, media, signalling, security, etc.

In the reference configuration, only a new signalling rule was defined. All other rules under domain policies, linked together on end point policy groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule.

7.3.1. Signalling Rules

Signalling rules are a mechanism on the Avaya SBCE to manipulate the signalling beyond simple header manipulation. Signalling rules allow action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signalling request and response message. In the case of Telenor, the SIP messages are manipulated to avoid the overhead of re-assembling fragmented UDP packets, reduce packet size and removed unnecessary Headers. This is achieved by removing Avaya proprietary and unnecessary headers to reduce the SIP messages packet size to below the Maximum Transmission Unit (MTU) so that fragmentation does not occur.

To define the signalling rule, navigate to **Domain Policies → Signaling Rules** in the main menu on the left hand side. Click on **Add** and enter details in the **Signaling Rule** pop-up box.

- In the **Rule Name** field enter a descriptive name such as **Telenor** for the signalling rule to remove Avaya proprietary and unnecessary headers and click **Next** and **Next** again, then **Finish** (not shown).

The screenshot shows the 'Signaling Rules: Telenor' configuration window. On the left is a sidebar with a list of signaling rules: 'default', 'No-Content-Type-Checks', 'Phonact', 'Belgacom', 'Swisscom', 'CS1K', and 'Telenor' (which is highlighted in red). The main area has a top bar with 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete' buttons. Below this is a tabbed interface with tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling Go\$', and 'UCID'. The 'General' tab is active, showing a description field with the placeholder 'Click here to add a description.' Below the tabs are three sections: 'Requests' with a table of actions (Requests, Non-2XX Final Responses, Optional Request Headers, Optional Response Headers) all set to 'Allow'; 'Outbound' with a similar table of actions also set to 'Allow'; and 'Content-Type Policy' with a table containing 'Enable Content-Type Checks' (checked), 'Action' (Allow), 'Multipart Action' (Allow), and an 'Exception List'.

Select the **Request Headers** tab (not shown) and define the rules to remove Avaya proprietary headers as follows:

- Click on **Add In Header Control** (not shown).
- Check the **Proprietary Request Header** box.
- Enter the name of the header to be removed in the **Header Name** field.
- Select **ALL** in the **Method Name** field.
- Check **Forbidden** in the **Header Criteria** options.
- In the **Presence Action** drop down menu, select **Remove header**.
- Click **Finish**.

The following example shows configuration for removal of **P-Location** headers from request messages.



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

- Proprietary Request Header:** A checkbox that is checked.
- Header Name:** A text field containing "P-Location".
- Method Name:** A dropdown menu set to "ALL".
- Header Criteria:** Three radio button options: "Forbidden" (selected), "Mandatory", and "Optional".
- Presence Action:** A dropdown menu set to "Remove header".
- Below the Presence Action dropdown, there are two small text fields: "486" and "Busy Here".
- Finish:** A button at the bottom of the dialog.

Note: The above is an example of the proprietary headers. During test, the same was done for Alert-Info, Av-Global-Session-ID, Endpoint-View, P-AV-Message-Id, P-Charging-Vector and P-Location headers.

When finished, all the Request Headers defined will be shown under the **Request Headers** tab as shown in the screenshot.

Signaling Rules: Telenor

Buttons: Add, Filter By Device, Rename, Clone, Delete

Left sidebar: Signaling Rules, default, No-Content-Type-Checks, Phonect, Belgacom, Swisscom, CSTK, **Telenor**

Top tabs: General, Requests, Responses, **Request Headers**, Response Headers, Signaling QoS, UCID

Buttons: Add In Header Control, Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
2	Av-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

The same is required for Response headers. Select the **Response Headers** tab (not shown) and define the rules to remove Avaya proprietary headers as follows:

- Click on **Add In Header Control** (not shown).
- Check the **Proprietary Response Header** box.
- Enter the name of the header to be removed in the **Header Name** field.
- Select **1XX** in the **Response Code** drop down menu, this will remove the header from 183 Session Progress and 180 Ringing messages.
- Select **ALL** in the **Method Name** field.
- Check **Forbidden** in the **Header Criteria** options.
- In the **Presence Action** drop down menu, select **Remove header**.
- Click **Finish**.

Repeat above process and select **2XX** in the **Response Code** so that the header is removed from 200 OK messages.

The following example shows configuration for removal of **Av-Global-Session-ID** headers from **1XX** responses.

Header Control

Proprietary Response Header: ☒

Header Name: Av-Global-Session-ID

Response Code: 1XX

Method Name: ALL

Header Criteria:

☒ Forbidden

☐ Mandatory

☐ Optional

Presence Action: Remove header

486 Busy Here

Finish

Note: The previous screenshot shows an example of an unnecessary header. During test, the same was done for Alert-Info, Av-Global-Session-ID, Endpoint-View, P-AV-Message-Id and P-Location headers.

When finished, all the Response Headers defined will be shown under the **Response Headers** tab as shown in the screenshot.

Signaling Rules: Telenor

Filter By Device: [v]

Click here to add a description.

General Requests Responses Request Headers **Response Headers** Signaling QoS UCID

Add In Header Control Add Out Header Control

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	Alert-Info	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
2	Alert-Info	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
3	Av-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Av-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	Endpoint-View	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
10	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

End point policy groups are required to implement the signalling rules. To define one for the Session Manager, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

- In the **Group Name** field enter a descriptive name for Telenor network, in this case **Telenor**, and click **Next** (not shown).
- Leave the **Application Rule**, **Border Rule**, **Media Rule**, **Security Rule** and **Time of Day Rule** fields at their default values.
- In the **Signaling Rule** drop down menu, select the recently added signalling rule for **Telenor**.

Click **Finish**.

Policy Set [X]

Application Rule: default [v]

Border Rule: default [v]

Media Rule: default-low-med [v]

Security Rule: default-low [v]

Signaling Rule: Telenor [v]

Time of Day Rule: default [v]

Finish

7.4. Define Network Information

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 interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** in the menu on the left hand side and click on **Add** (not shown). Enter details in the blank box that appears at the end of the list.

- Click on **Add**.
- Define **A1 Netmask**, **IP Address** and **Gateway** and assign to **Interface A1**.
- Click **Save** to save the information.
- Click on **Add**.
- Define **B1 Netmask**, **IP Address** and **Gateway** and assign to **Interface B1**.
- Click **Save** to save the information.
- Click on **System Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

Network Management: GSSCP_03

Devices: GSSCP_03

Network Configuration | Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

Changes will not take effect until the interface is updated.

A1 Netmask: 255.255.255.0 A2 Netmask: B1 Netmask: 255.255.255.128 B2 Netmask:

Add Save Clear

IP Address	Public IP	Gateway	Interface	
10.10.3.30		10.10.3.1	A1	Delete
192.168.122.57		192.168.122.7	B1	Delete

Select the **Interface Configuration** tab and click on **Toggle** to enable the interfaces.

Network Management: GSSCP_03

Devices: GSSCP_03

Network Configuration | Interface Configuration

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

7.5. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

7.5.1. Signalling Interfaces

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

- Select **Add Signaling Interface** and enter details in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the internal signalling interface.
- For **Signaling IP**, select an **internal** signalling interface IP address defined in **Section 7.4**.
- Select **UDP** and **TCP** port numbers, **5060** is used for the Session Manager.

Repeat the procedures to add details of transport protocol and ports for the external SIP signalling.

- Select **Add Signaling Interface** and enter details in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **Signaling IP**, select an **external** signalling interface IP address defined in **Section 7.4**.
- Select **UDP** and **TCP** port numbers, **5060** is used for Telenor.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.3.30	5060	5060	—	None	Edit Delete
Ext_Sig	192.168.122.57	5060	5060	—	None	Edit Delete

7.5.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** in the menu on the left hand side (not shown). Details of the RTP and SRTP port ranges for the internal media streams are entered here. The IP addresses for media can be the same as those used for signalling.

- Select **Add Media Interface** and enter details in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select an **internal** media interface IP address defined in **Section 7.4**.
- Select RTP port ranges for the media path with the enterprise end-points.

Repeat the procedures to add details of the RTP and SRTP port ranges for the external media streams.

- Select **Add Media Interface** and enter details in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select an **external** media interface IP address defined in **Section 7.4**.
- Select RTP port ranges for the media path with Telenor SIP Trunk service.



Media Interface: GSSCP_03

Devices

GSSCP_03

Media Interface

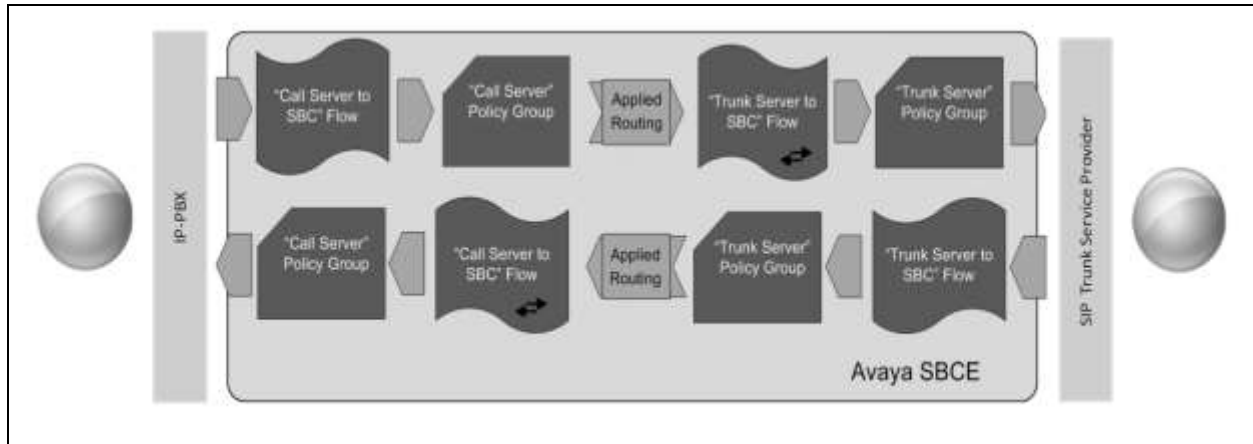
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Add

Name	Media IP	Port Range	
Int_Media	10.10.3.30	35000 - 51000	Edit Delete
Ext_Media	192.168.122.57	35000 - 51000	Edit Delete

7.6. Server Flows

When a packet is received by the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



To create a server flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** (not shown).

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a server configuration created in **Section 7.2.4** and **7.2.5** and assign to the flow.
- **Received Interface:** Select the signalling interface the server configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the signalling interface used to communicate with the server configuration.
- **Media Interface:** Select the media interface used to communicate with the server configuration.
- **End Point Policy Group:** Select the policy assigned to the server configuration.
- **Routing Profile:** Select the profile the server configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the profile to apply toward the server configuration.

Click **Finish** to save and exit.

The following screen shows the server flow for Session Manager.

The screenshot shows a configuration window titled "Flow: Call_Server". It contains the following fields and values:

Field	Value
Flow Name	Call_Server
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Media
End Point Policy Group	default-low
Routing Profile	Telenor
Topology Hiding Profile	Avaya
File Transfer Profile	None

A "Finish" button is located at the bottom right of the form.

The following screen shows the server flow for Telenor.

The screenshot shows a configuration window titled "Flow: Trunk_Server". It contains the following fields and values:

Field	Value
Flow Name	Trunk_Server
Server Configuration	Telenor
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	Telenor
File Transfer Profile	None

A "Finish" button is located at the bottom right of the form.

This configuration ties all the previously entered information together so that calls can be routed from Session Manager to Telenor SIP Trunk service and vice versa. The following screenshot shows all configured flows.

Subscriber Flows

Server Flows

Add

Hover over a row to see its description.

Server Configuration: Avaya

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Call_Server	*	Ext_Sig	Int_Sig	default-low	Telenor	View Clone Edit Delete

Server Configuration: Telenor

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Trunk_Server	*	Int_Sig	Ext_Sig	default-low	Avaya	View Clone Edit Delete

8. Telenor Configuration

The configuration of the Telenor equipment used to support the Telenor SIP Trunk service is outside of 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**.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	Session Manager	10.10.3.30	5060	TCP	Up	200 OK	Up

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

```
status trunk 1
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0001/001	T00001	in-service/idle	no
0001/002	T00002	in-service/idle	no
0001/003	T00003	in-service/idle	no
0001/004	T00004	in-service/idle	no
0001/005	T00005	in-service/idle	no
0001/006	T00006	in-service/idle	no
0001/007	T00007	in-service/idle	no
0001/008	T00008	in-service/idle	no
0001/009	T00009	in-service/idle	no
0001/010	T00010	in-service/idle	no

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.

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

To define the trace, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main menu on the left hand side and select the **Packet Capture** tab. Select the SIP Trunk interface from the **Interface** drop down menu.

- Select the signalling interface IP address from the **Local Address** drop down menu.
- Enter the IP address of the Service Provider's 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 shows the Avaya SBCE web interface. The left sidebar contains a navigation menu with options like Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is titled 'Session Border Controller for Enterprise' and 'AVAYA'. Under the 'Trace' section, there are three tabs: 'Devices', 'Call Trace', 'Packet Capture', and 'Captures'. The 'Packet Capture' tab is selected, showing a 'Packet Capture Configuration' form. The form includes fields for 'Interface' (set to 'S1'), 'Local Address' (set to 'All'), 'Remote Address' (set to '*'), 'Protocol' (set to 'All'), 'Maximum Number of Packets to Capture' (set to '10000'), and 'Capture Filename' (set to 'SIP_Trunk_Test.pcap'). There are 'Start Capture' and 'Clear' buttons at the bottom of the form.

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

The screenshot shows the 'Captures' tab selected in the 'Trace' section. It displays a table of captured files. The table has three columns: 'File Name', 'File Size (bytes)', and 'Last Modified'. There is a 'Refresh' button in the top right corner and a 'Delete' button next to the file name.

File Name	File Size (bytes)	Last Modified
SIP_Trunk_Test_20130802123856.pcap	4,096	August 2, 2013 12:39:31 PM GMT

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to R6.2 Telenor SIP Trunk service. 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. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3, May 2014
- [2] *Administering Avaya Aura® System Platform*, Release 6.3, May 2014
- [3] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, April 2014
- [4] *Avaya Aura® Communication Manager 6.3 Documentation library*, August 2014
- [5] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 April 2014
- [6] *Implementing Avaya Aura® System Manager* Release 6.3, May 2014
- [7] *Upgrading Avaya Aura® System Manager to 6.3* May 2014
- [8] *Administering Avaya Aura® System Manager* Release 6.3, May 2014
- [9] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 August 2014
- [10] *Implementing Avaya Aura® Session Manager* Release 6.3, May 2014
- [11] *Upgrading Avaya Aura® Session Manager* Release 6.3, May 2014
- [12] *Administering Avaya Aura® Session Manager* Release 6.3, June 2014
- [13] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2 June 2014
- [14] *Upgrading Avaya Session Border Controller for Enterprise* Release 6.2 July 2014
- [15] *Administering Avaya Session Border Controller for Enterprise* Release 6.2 March 2014
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2015 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.