



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.0.1, Avaya Aura® Session Manager R6.1 and Avaya Session Border Controller for Enterprise R6.3 to support Telenet SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Telenet SIP Trunking Service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server.

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.

Telenet 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 Telenet SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R6.0.1; Avaya Aura® Session Manager R6.1; Avaya Session Border Controller for Enterprise R6.3; 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 Telenet SIP Trunking service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

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

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using Telenet SIP Trunking, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via Telenet SIP Trunking 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 Law and G.729A codecs.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38 and G.711.
- DTMF transmission using RFC 2833 and in-band 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 Telenet SIP Trunking requiring Avaya response and sent by Avaya requiring Telenet response.

2.2. Test Results

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

- DTMF sent using telephone events as described in RFC2833 did not work where media attributes had been changed by the Telenet network. When the network sent a re-INVITE, the media attributes for telephone events were not present. Telenet prefer to send DTMF in-band and this was used during testing.
- Communication Manager rejected the Proxy-Require header in the INVITE for inbound calls with CLI Restricted. This was resolved by removing the header in the Avaya SBCE (See **Section 7.8**).
- Although PSTN Hold and Resume worked as expected, there were no messages received from the network to indicate that the call was on hold.
- Call Forwarding Off-net did not work until the CLI presented to the network matched the DDI range allocated to Communication Manager. Initial tests used the Avaya preferred E.164 format but the range configured in the network was in national format with no leading zero. Once the format was changed to national, call forwarding off-net was successful.
- The method of Fax transmission preferred by Telenet is G.711. Fax transmission using T.38 was tested but was not successful. Fax transmission between the Telenet network and Communication Manager is only successful when G.711 is the negotiated codec.
- Calls using one-X Communicator softphones connected via SIP transferring or conferencing to a PSTN phone experienced two ring tones. This did not occur with one-X Communicator connected via H.323. Also, calls using one-X Communicator softphones connected via SIP did not function at all in “Other Phone” mode. It is recommended to use H.323 for one-X Communicator at this build of Communication Manager.

Items not tested include the following:

- There is no native support on Communication Manager Release 6.0.1 for 96x1 phones so these weren't used during testing.
- No Inbound Toll-Free access was available for testing
- 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 Telenet products please contact the following website: <https://www2.telenet.be/en/>

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Telenet SIP Trunking service. Located at the Enterprise site is an Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series IP telephones (with SIP and 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.

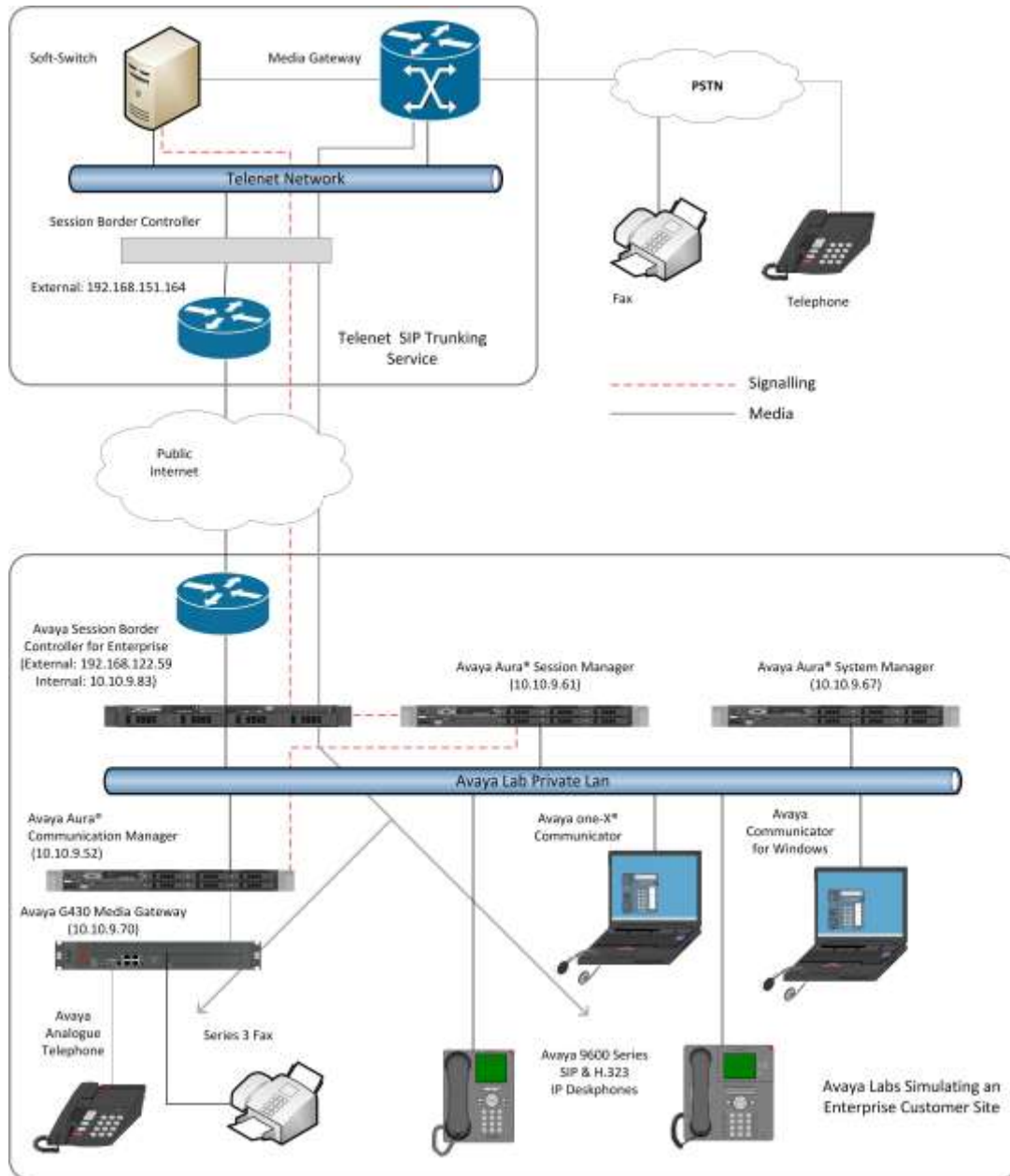


Figure 1: Test Setup Telenet SIP Trunking Service to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Session Manager	6.1.7.0.617012
Avaya Aura® System Manager	6.1.7 1860
Avaya Aura® Communication Manager	6.0.1 21061
Avaya Session Border Controller for Enterprise	6.3.5-03-7142
Avaya G430 Media Gateway	31.26
Avaya 9600 series Handsets: SIP 96x0 H.323 96x0	2.6.10-132005 3.2.3-071814
Avaya One-X Communicator	6.2.10.03-FP10
Avaya Communicator for Windows	2.1.3.80
Analogue Handset	N/A
Analogue Fax	N/A
Telenet	
Sonus GSX9000 SBC	v09.00.08 R000
Genband CS2K	CVM17

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 Telenet SIP Trunking service. For incoming calls, Session Manager receives SIP messages from the Avaya SBCE and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Telenet 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 Telenet SIP Trunking service 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	0
Maximum Concurrently Registered IP Stations:		18000	1
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		18000	0
Maximum Video Capable IP Softphones:		18000	0
Maximum Administered SIP Trunks:		24000	20
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:		300	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? n
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? n	
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 using the **change node-names ip** command. In this case, **Session_Manager** and **10.10.9.61** 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.

change node-names ip		IP NODE NAMES
Name	IP Address	
Session_Manager	10.10.9.61	
default	0.0.0.0	
procr	10.10.9.52	
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
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.

5.4. Administer IP Codec Set

Use the **change ip-codec set n** command where **n** is 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 codecs supported by Telenet were configured, namely **G.711A** and **G.729A**.

change ip-codec-set 2

Page 1 of 2

IP Codec Set

Codec Set: 2

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

Telenet prefers G.711 for transmission of fax. Navigate to **Page 2** and define G.711 fax by setting the **FAX Mode** to **pass-through**.

change ip-codec-set 2				Page	2 of	2
IP Codec Set						
Allow Direct-IP Multimedia? n						
	Mode	Redundancy				
FAX	pass-through	0				
Modem	off	0				
TDD/TTY	US	3				
Clear-channel	n	0				

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Telenet SIP Trunking service. During test, this was configured to use TCP and port 5060.

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

- Set **Group Type** to **sip**.
- Set **Transport Method** to required protocol. Although TLS is recommended for security, **tcp** was used during testing.
- 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, during testing, **5060** was used. These must correspond to those used on the Session Manager Entity Links (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 Media Gateway resources
- Leave **Initial IP-IP Direct Media** to default **n** to facilitate the use of Early Media.
- Set **DTMF over IP** to **in-band** which is Telenet's preference for transmission of DTMF.

If Telenet have agreed to use RFC2833, set this to **rtp-payload**

The default values for the other fields may be used.

change signaling-group 2		Page 1 of 1
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: Session_Manager	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
Far-end Network Region: 2		
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: in-band	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-netwrk** 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-netwrk	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 Telenet to prevent unnecessary SIP messages during call setup. During testing, a value of **900** was used that sets the SIP Min-SE header to 1800.

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

On **Page 3**, set the **Numbering Format** field to **private** if national numbering is to be used as was the case during testing. If E.164 with preceding + is to be used, select public.

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

On **Page 4** of this form:

- Set **Mark Users as Phone** to **y** as required by Telenet
- Set **Network Call Redirection** to **n** as redirection using “302 Moved Temporarily” or REFER are not supported.
- 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**.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Telenet (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.

change trunk-group 2	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? y	
Prepend '+' to Calling 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? n	
Identity for Calling Party Display: From	
Enable Q-SIP? n	

5.7. Administer Calling Party Number Information

Use the **change private-numbering** command to configure Communication Manager to send the calling party number in national format with no leading zero. These calling party numbers are sent in the SIP From, Contact and PAI headers. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	2	1		4	Total Administered: 7
4	2000	2	329nnnn0	8	Maximum Entries: 540
4	2290	2	329nnnn2	8	
4	2316	2	329nnnn3	8	
4	2396	2	329nnnn1	8	
4	2400	2	329nnnn4	8	

Use the **change public-unknown-numbering** command if it has been agreed with Telenet to use E.164 numbering. Communication Manager automatically prefixes a “+” to the numbers when this table is used.

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	32329nnnn0	10	Maximum Entries: 9999
4	2290	2	32329nnnn2	10	Note: If an entry applies to a SIP connection to Avaya Aura(tm) Session Manager, the resulting number must be a complete E.164 number.
4	2316	2	32329nnnn3	10	
4	2396	2	32329nnnn1	10	
4	2400	2	32329nnnn4	10	
4	2401	2	32329nnnn5	10	

Note: During testing the extension numbers were reformatted to national 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 Telenet 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. 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 with leading **0**. Note that exact maximum number lengths should be used where possible to reduce post-dial delay, the example shows international numbers with country code **353** for Ireland and area code **91** for Galway. 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	Total		Route	Call	Node	ANI	
String	Min	Max	Pattern	Type	Num	Reqd	
0	8	17	2	pubu		n	
0035391	13	13	2	pubu		n	
03	9	9	2	pubu		n	
1	4	4	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 Trunk													
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:	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			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 Communication Manager extensions. The incoming digits sent in the INVITE message from Telenet 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, 8 digits are received with no preceding zero. 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	30
INCOMING CALL HANDLING TREATMENT							
Service/ Feature	Number Len	Number Digits	Del	Insert			
public-ntwrk	8	329nnnn0	8	2000			
public-ntwrk	8	329nnnn1	8	2396			
public-ntwrk	8	329nnnn2	8	2290			
public-ntwrk	8	329nnnn3	8	2316			
public-ntwrk	8	329nnnn4	8	2400			
public-ntwrk	8	329nnnn5	8	2401			
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 2396. 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 2396							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
2396	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.

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

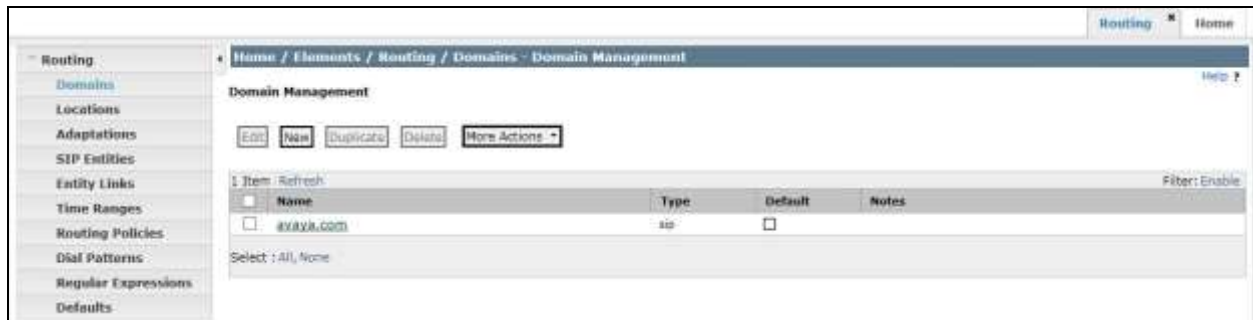
6.1. Log in to Avaya Aura® System Manager

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** screen 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 **Elements, Home** screen 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 Telenet; 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.



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.

Home / Elements / Routing / Locations - Location Details

Location Details Help ? Commit Cancel

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): Kbit/Sec

Minimum Multimedia Bandwidth: Kbit/Sec

* Default Audio Bandwidth:

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	*10.10.*	

Select : All, None

* Input Required Commit Cancel

6.4. Administer Adaptations

Session Manager Adaptations can be used to alter parameters in the SIP message headers. During compliance testing, an Adaptation was used to change the calling party number of incoming calls to a diallable format for display on Communication Manager extensions. Calling Party Numbers were received from the network with no leading zeros, so the Adaption was used to analyse the numbers and prefix national numbers with a single zero and international numbers with two zeros.

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. During testing **Diallable** was used.
- In the **Module Name** field, type **DigitConversionAdapter**. This is used for simple digit conversion adaptations.
- In the **Module Parameter** field, type **fromto=true**.
- 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.

Home / Elements / Routing / Adaptations - Adaptation Details

Adaptation Details

Help ↑

Commit Cancel

General

* Adaptation name: Diallable

Module name: DigitConversionAdapter

Module parameter: fromto=true

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

18 Items Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*1	*10	*15		*0	00	origination	
<input type="checkbox"/>	*1	*8	*9		*0	0	origination	
<input type="checkbox"/>	*2	*10	*15		*0	00	origination	
<input type="checkbox"/>	*2	*8	*9		*0	0	origination	
<input type="checkbox"/>	*3	*10	*15		*0	00	origination	
<input type="checkbox"/>	*3	*8	*9		*0	0	origination	
<input type="checkbox"/>	*4	*10	*15		*0	00	origination	
<input type="checkbox"/>	*4	*8	*9		*0	0	origination	
<input type="checkbox"/>	*5	*10	*15		*0	00	origination	
<input type="checkbox"/>	*5	*8	*9		*0	0	origination	
<input type="checkbox"/>	*6	*10	*15		*0	00	origination	
<input type="checkbox"/>	*6	*8	*9		*0	0	origination	
<input type="checkbox"/>	*7	*10	*15		*0	00	origination	
<input type="checkbox"/>	*7	*8	*9		*0	0	origination	
<input type="checkbox"/>	*8	*10	*15		*0	00	origination	

Select: All, None

< Previous Page 1 of 2 Next >

The screenshot shows how the calling party numbers were analysed for testing. The first digit was analysed and national and international numbers were identified by number length. A “0” or “00” was prefixed accordingly.

If E.164 numbering is used, a similar Adaptation could be used to analyse Belgian numbers and replace the preceding “+32” with “0”. It could also be used to analyse international numbers and replace the preceding “+” with “00”.

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.

There is also a SIP Entity for Avaya Aura® Messaging but that is not described in this document.

6.5.1. Avaya Aura® Session Manager SIP Entity

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

The screenshot shows the 'SIP Entity Details' configuration page for a Session Manager. The breadcrumb trail is 'Home / Elements / Routing / SIP Entities - SIP Entity Details'. The page has 'Commit' and 'Cancel' buttons in the top right. The 'General' tab is selected. The form contains the following fields:

- Name:** Session_Manager
- FQDN or IP Address:** 10.10.9.61
- Type:** Session Manager
- Notes:** (empty text area)
- Location:** Galway (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (empty text field)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)

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.
- Click on **Commit**.

The screenshot shows the 'Port' configuration section. It has 'Add' and 'Remove' buttons. Below the buttons 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 of data:

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

Below the table, there is a 'Select' dropdown menu set to 'All, None'. At the bottom right, there are 'Commit' and 'Cancel' buttons. A note '* Input Required' is visible at the bottom left.

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**.

The screenshot shows the 'SIP Entity Details' configuration page for 'CM_Trunk'. The page has a breadcrumb trail: Home / Elements / Routing / SIP Entities - SIP Entity Details. In the top right corner, there are 'Commit' and 'Cancel' buttons, and a 'Help' link. The 'General' tab is selected. The configuration fields are as follows:

- Name:** CM_Trunk
- FQDN or IP Address:** 10.10.9.52
- Type:** CM
- Notes:** (empty text box)
- Adaptation:** (dropdown menu)
- Location:** Galway (dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text box)
- Call Detail Recording:** none (dropdown menu)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)

Note: A second SIP Entity for Communication Manager is required for SIP Endpoints. In the test environment this is named “CM_SIP_Endpoints”. The parameters are the same, and the two are assigned to different Entity Links, as described in **Section 6.6**, so that different ports can be used. It is these different ports that distinguish between traffic for SIP Endpoints and traffic for the SIP Trunk.

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The screenshot over the page 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.

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details Help ? Commit Cancel

General

* Name: ASBCE

* FQDN or IP Address: 10.10.9.83

Type: SIP Trunk

Notes:

Adaptation: Dialable

Location: Galway

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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. Fill in the following fields in the new row that is displayed (not shown).

- 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.

Home / Elements / Routing / Entity Links - Entity Links Help ?

Entity Links

Edit New Duplicate Delete More Actions

4 Items Refresh Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
<input type="checkbox"/>	ASBCE Link	Session_Manager	TCP	5060	ASBCE	5060	Trusted	
<input type="checkbox"/>	CM_Endpoint_Link	Session_Manager	TLS	5061	CM_Endpoints	5061	Trusted	
<input type="checkbox"/>	CM_Trunk_Link	Session_Manager	TCP	5060	CM_Trunk	5060	Trusted	
<input type="checkbox"/>	Messaging_Link	Session_Manager	TCP	5060	Messaging	5060	Trusted	

Select : All, None

Click **Commit** (not shown) 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, defined in **Section 6.5**, to which this routing policy applies (not shown).
- Under **Time of Day**, click **Add**, and then select the time range. **24/7** is provided as a default

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

The screenshot displays the 'Routing Policy Details' page in a web browser. The breadcrumb trail at the top reads 'Home / Elements / Routing / Routing Policies - Routing Policy Details'. In the top right corner, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

The 'General' section contains the following fields:

- Name:** CM_Trunk
- Disabled:** ☐
- Notes:** (empty text area)

The 'SIP Entity as Destination' section features a 'Select' button. Below it is a table with the following data:

Name	FQDN or IP Address	Type	Notes
CM_Trunk	10.10.9.52	CM	

The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. Below these is a table with one item:

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
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

At the bottom of the table, there is a 'Select : All, None' option. A 'Filter: Enable' link is located in the top right corner of the table area.

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

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details Commit Cancel Help ?

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE	10.10.9.83	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

Ranking	1 = Name	2 =	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 all calls starting with zero to the PSTN via Telenet SIP Trunking.

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details Help ↑ Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh 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	0	<input checked="" type="checkbox"/>	ASBCE	

Select : All, None

Note: Additional dial patterns (not shown) will be required for PSTN numbers that do not start with zero, for example directory enquiries. This was tested with a dial pattern for 4 digit numbers starting with 1.

The next screenshot shows the test dial pattern configured for Communication Manager. This 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.

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details Help ↑ Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh 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		CM_Trunk	0	<input checked="" type="checkbox"/>	CM_Trunk	

Select : All, None

6.9. Administer Application for Avaya Aura® Communication Manager

From the **Home** screen select **Session Manager** from the Elements 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.

The screenshot shows the Avaya Aura® System Manager 6.1 web interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, Applications, Application Sequences, Implicit Users, NRS Proxy Users, System Status, and System Tools. The main content area is titled 'Application Editor' and shows the configuration for an application named 'SIP_Endpoints'. The 'SIP Entity' is set to 'CM_Endpoints' and the 'CM System for SIP Entity' is set to 'Communication_Manager'. There are buttons for 'View/Add CM Systems' and 'Refresh'. Below the main configuration fields is a section for 'Application Attributes (optional)' with a table for Name and Value. The table has two rows: 'Application Handle' and 'URI Parameters'. At the bottom right, there are 'Commit' and 'Cancel' buttons.

Name	Value
Application Handle	
URI Parameters	

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 is 'Home / Elements / Session Manager / Application Configuration / Application Sequences - Application Sequences'. The title bar says 'Application Sequence Editor' with 'Commit' and 'Cancel' buttons. Below the title, there's a section 'Application Sequence' with a '*Name' field containing 'SIP_Endpoints_Seq' and an empty 'Description' field. Underneath is a section 'Applications in this Sequence' with 'Move First', 'Move Last', and 'Remove' buttons. Below that is a table with 0 items, showing columns: Sequence Order (first to last), Name, SIP Entity, Mandatory, and Description. The text 'No Applications Have Been Added' is displayed. Below the table is a section 'Available Applications' with a '1 Item / Refresh' header and a 'Filter: Enable' option. The table has columns: Name, SIP Entity, and Description. One item is listed: '+ SIP_Endpoints' with SIP Entity 'CM_Endpoints'. At the bottom, there's a '*Required' label and 'Commit' and 'Cancel' buttons.

Home / Elements / Session Manager / Application Configuration / Application Sequences - Application Sequences

Application Sequence Editor

Application Sequence

*Name: SIP_Endpoints_Seq

Description:

Applications in this Sequence

Move First Move Last Remove

0 Items

Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
No Applications Have Been Added				

Available Applications

1 Item / Refresh Filter: Enable

Name	SIP Entity	Description
+ SIP_Endpoints	CM_Endpoints	

*Required

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** screen select **User Management** from the **Users** 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. **2290@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.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

User Management * Home

Home / Users / User Management / Manage Users - New User Profile

New User Profile

Commit Cancel

Identity * Communication Profile * Membership Contacts

Identity *

* Last Name: SIP

* First Name: 9630G

Middle Name:

Description:

* Login Name: 2290@avaya.com

* Authentication Type: Basic

* Password: *****

* Confirm Password: *****

Localized Display Name:

Endpoint Display Name:

Honorific:

Language Preference: English

Time Zone: (+1:0)GMT : Dublin, Edinburgh, Lisbon, London, Casablanca

Address *

*Required

Commit Cancel

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

The screenshot shows the 'New User Profile' form with the 'Communication Profile' tab selected. The form includes fields for 'Communication Profile Password' and 'Confirm Password', both masked with dots. Below these are buttons for 'New', 'Delete', 'Done', and 'Cancel'. A table with the header 'Name' shows a single entry 'Primary' selected. Below the table, the 'Name' field is set to 'Primary' and the 'Default' checkbox is checked. The 'Communication Address' section is expanded, showing buttons for 'New', 'Edit', and 'Delete'. Below these is a table with headers 'Type', 'Handle', and 'Domain', which is currently empty with the text 'No Records found'.

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' form with the 'New' button clicked. The form includes buttons for 'New', 'Edit', and 'Delete'. Below these is a table with headers 'Type', 'Handle', and 'Domain', which is currently empty with the text 'No Records found'. The 'Type' field is a drop-down menu set to 'Avaya SIP'. The 'Fully Qualified Address' field is a text input containing '2290', followed by an '@' symbol and a domain drop-down menu set to 'avaya.com'. At the bottom right are 'Add' and 'Cancel' buttons.

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.

The screenshot shows the 'Session Manager Profile' configuration form. It includes the following fields and values:

- Primary Session Manager:** Session_Manager
- Secondary Session Manager:** (None)
- Origination Application Sequence:** SIP_Endpoints_Seq
- Termination Application Sequence:** SIP_Endpoints_Seq
- Survivability Server:** (None)
- Home Location:** Galway

There are two summary tables on the right side of the form:

Primary	Secondary	Maximum
1	0	1

Primary	Secondary	Maximum

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.

The screenshot shows the 'Endpoint Profile' configuration form. It includes the following fields and values:

- System:** Communication_Manager
- Profile Type:** Endpoint
- Use Existing Endpoints:** ☐
- Extension:** 2290
- Template:** DEFAULT_9630SIP_CM_6_0
- Set Type:** 9630SIP
- Security Code:** (empty)
- Port:** IP
- Voice Mail Number:** (empty)
- Delete Endpoint on Unassign of Endpoint from User or on Delete User:** ☒

Select **Commit** (Not Shown) to save changes and the System Manager will add Communication Manager user configuration automatically.

7. Configure Avaya Session Border Controller for Enterprise

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

7.1. Access Avaya Session Border Controller for Enterprise

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



The login screen features the Avaya logo in red on the left. To the right, under the heading "Log In", is a "Username:" label followed by a text input field and a "Continue" button. Below the input field, there is a block of text stating that the system is restricted to authorized users and that unauthorized access is prohibited. Further down, another block of text states that the use of the system may be monitored and recorded for administrative and security reasons. At the bottom, a copyright notice reads "© 2011 - 2013 Avaya Inc. All rights reserved."

AVAYA

Log In

Username:

Continue

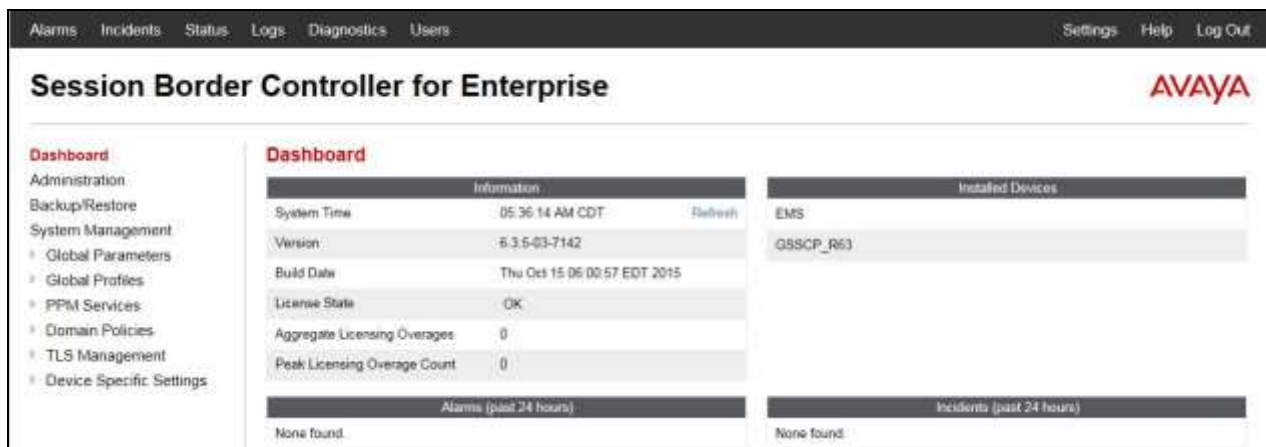
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under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

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

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

© 2011 - 2013 Avaya Inc. All rights reserved.

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



The dashboard has a top navigation bar with links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left is a sidebar menu with categories like 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 system details like time, version, build date, license state, and licensing overages; "Installed Devices" showing a list of devices (EMS, GSSCP_R63); "Alarms (past 24 hours)" and "Incidents (past 24 hours)", both currently showing "None found".

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise **AVAYA**

Dashboard

Information

System Time	05:36:14 AM CDT	Refresh
Version	6.3.5-03-7142	
Build Date	Thu Oct 15 06:00:57 EDT 2015	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	

Installed Devices

EMS
GSSCP_R63

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found.

7.2. Define Network Management

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

The screenshot shows the 'Network Management: GSSCP_R63' page. On the left is a sidebar menu with options: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management), and Device Specific Settings (with sub-items: Network Management, Media Interface, Signaling Interface). The 'Network Management' sub-item is highlighted. The main content area has tabs for 'Devices', 'Interfaces', and 'Networks'. The 'Networks' tab is active, showing a table with columns: Name, Gateway, Subnet Mask, Interface, and IP Address. An 'Add' button is in the top right corner of the table area.

Enter details for the external interfaces in the dialogue box:

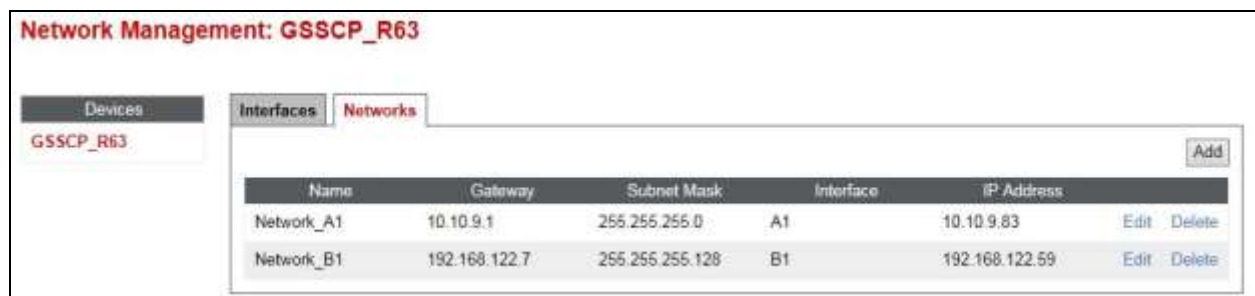
- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the 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 has a sidebar menu on the left with the same options as the previous screenshot, with 'Network Management' highlighted. The dialog box has a title bar 'Add Network' with a close button 'X'. The main area contains input fields for 'Name' (Network_B1), 'Default Gateway' (192.168.122.7), 'Subnet Mask' (255.255.255.128), and 'Interface' (B1). An 'Add' button is in the bottom right. Below these fields is a table with columns: IP Address, Public IP, and Gateway Override. The 'IP Address' column has a value of 192.168.122.59. A 'Delete' button is in the bottom right of the table. A 'Finish' button is at the bottom center of the dialog box.

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 Telenet 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** 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** (not shown) 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 **192.168.122.59** for the Avaya SBCE interface on the SIP Trunk.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for the Telenet SIP Trunking.
- Click on **Finish**

The screenshot shows the 'Add Signaling Interface' configuration window. 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 in red), End Point Flows, Session Flows, DMZ Services, and TURN/STUN Service. The main window has a title bar 'Add Signaling Interface' with a close button 'X'. The form contains the following fields:

- Name:** External
- IP Address:** Network_B1 (B1, VLAN 0) (dropdown menu), 192.168.122.59 (dropdown menu)
- TCP Port:** (text field), Leave blank to disable
- UDP Port:** 5060 (text field), Leave blank to disable
- TLS Port:** (text field), Leave blank to disable
- TLS Profile:** None (dropdown menu)
- Enable Shared Control:** ☐
- Shared Control Port:** (text field)
- Finish:** (button)

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:

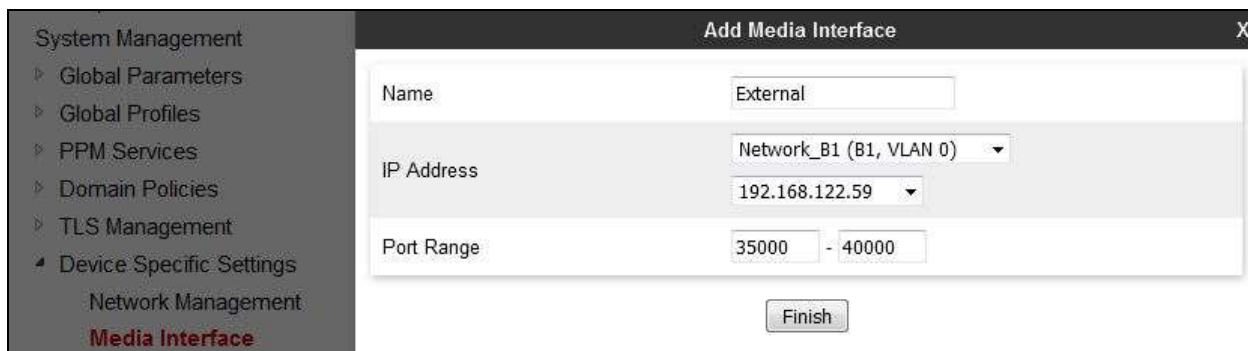


Note: In the test environment, the internal IP address was **10.10.9.83**.

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 **192.168.122.59**.
- Define the **RTP Port Range** for the media path with the Telenet SIP Trunking, during testing this was left at default values of **35000 - 40000**.



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



Check the **T.38 Support** box and click on **Next**.

The screenshot shows the 'Interworking Profile' dialog box with the 'General' tab selected. The 'T.38 Support' checkbox is checked. Other options include 'Hold Support' (None), '180 Handling' (None), '181 Handling' (None), '182 Handling' (None), '183 Handling' (None), 'Refer Handling' (unchecked), 'URI Group' (None), 'Send Hold' (checked), '3xx Handling' (checked), 'Diversion Header Support' (unchecked), 'Delayed SDP Handling' (checked), 'Re-Invite Handling' (checked), 'Prack Handling' (checked), 'Allow 18X SDP' (unchecked), 'URI Scheme' (SIP), and 'Via Header Format' (RFC3261). The 'Back' and 'Next' buttons are at the bottom.

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

The left screenshot shows the 'Privacy' tab of the 'Interworking Profile' dialog box. It includes fields for 'User Name', 'P-Asserted-Identity', 'P-Preferred-Identity', and 'Privacy Header'. The 'DTMF Support' section has radio buttons for 'None', 'SIP NOTIFY', and 'SIP INFO'. The right screenshot shows the 'SIP Timers' tab, which includes input fields for 'Min-SE', 'Init Timer', 'Max Timer', 'Trans Expire', 'Invite Expire', and 'TCP Connection Inactive Timer', each with a range in brackets. The 'Back' and 'Next' buttons are at the bottom of each dialog.

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' configuration window. It contains several settings:

- Record Routes:** Radio buttons for None (selected), Single Side, Dialog-Initiate Only (Single Side), and Both Sides.
- Topology Hiding: Change Call-ID:** Checked checkbox.
- Call-Info NAT:** Unchecked checkbox.
- Change Max Forwards:** Checked checkbox.
- Include End Point IP for Context Lookup:** Unchecked checkbox.
- OCS Extensions:** Unchecked checkbox.
- AVAYA Extensions:** Unchecked checkbox.
- NORTEL Extensions:** Unchecked checkbox.
- Diversion Manipulation:** Unchecked checkbox.
- Diversion Condition:** Dropdown menu set to 'None'.
- Diversion Header URI:** Empty text field.
- Metaswitch Extensions:** Unchecked checkbox.
- Reset on Talk Spurt:** Unchecked checkbox.
- Reset SRTP Context on Session Refresh:** Unchecked checkbox.
- Has Remote SBC:** Checked checkbox.
- Route Response on Via Port:** Unchecked checkbox.
- Cisco Extensions:** Unchecked checkbox.
- Lync Extensions:** Unchecked checkbox.
- SBC FQDN:** Empty text field.

At the bottom are 'Back' and 'Finish' buttons.

Repeat the process to define Server Interworking for Session Manager using the same parameter settings apart from **Record Routes** which is set to **Both Sides** as the Session Manager uses the Record-Route header.

The screenshot over the page shows the **Advance** tab.

Interworking Profiles: ASM

Buttons: Add, Rename, Clone, Delete

Interworking Profiles List:

- cs2100
- avaya-ru
- OCS-Edge-Server
- cisco-ccm
- cups
- Sipera-Halo
- OCS-FrontEnd-Server
- ASM**
- Telenet

Click here to add a description

Tabs: General, Timers, URI Manipulation, Header Manipulation, **Advanced**

Record Routes	Both Sides
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	Yes
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No
Lync Extensions	No

Edit

7.5. Define Servers

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

To define the Telenet SIP Trunking Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** (not shown) and enter an appropriate name in the pop-up menu.

Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration

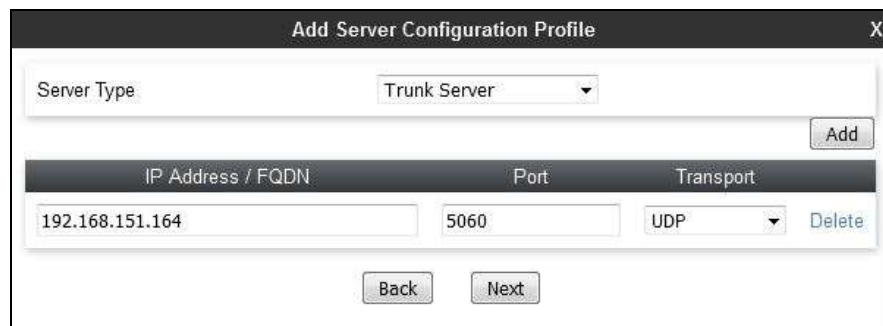
Add Server Configuration Profile X

Profile Name: Telenet

Next

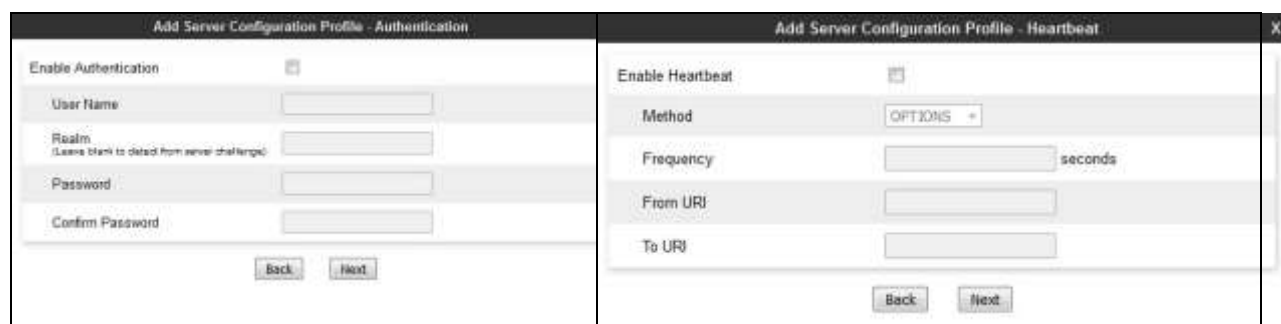
Click on **Next** and enter details in the dialogue box.

- 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 Telenet SIP Trunking IP address.
- In the **Port** box, enter the port to be used for the SIP Trunk.
- In the **Transport** drop down menu, select **UDP**.
- Click on **Next**.



The dialog box titled "Add Server Configuration Profile" contains a "Server Type" dropdown menu set to "Trunk Server". Below this is an "Add" button. A table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row contains the values "192.168.151.164", "5060", and "UDP". A "Delete" button is to the right of the table. At the bottom are "Back" and "Next" buttons.

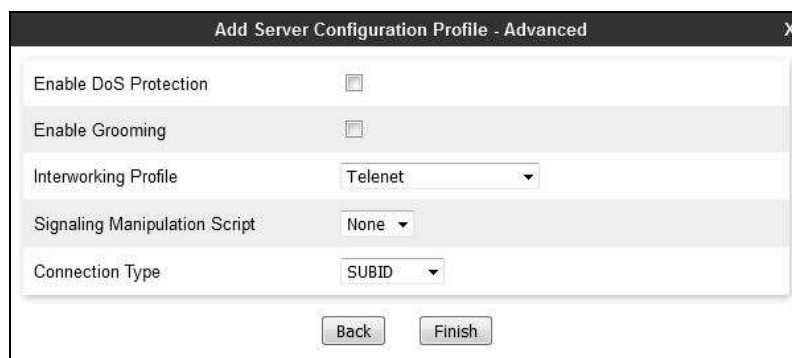
Click on **Next** and **Next** again. Leave the fields in the dialogue boxes at default values.



Two side-by-side dialog boxes. The left one is titled "Add Server Configuration Profile - Authentication" and contains fields for "User Name", "Realm", "Password", and "Confirm Password", with "Enable Authentication" checked. The right one is titled "Add Server Configuration Profile - Heartbeat" and contains fields for "Method" (set to "OPTIONS"), "Frequency" (with a "seconds" unit), "From URI", and "To URI", with "Enable Heartbeat" checked. Both have "Back" and "Next" buttons.

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 Telenet SIP Trunking defined in **Section 7.4**.
- Leave the other fields at default settings.
- Click **Finish**.



The dialog box titled "Add Server Configuration Profile - Advanced" contains checkboxes for "Enable DoS Protection" and "Enable Grooming", both unchecked. It has dropdown menus for "Interworking Profile" (set to "Telenet"), "Signaling Manipulation Script" (set to "None"), and "Connection Type" (set to "SUBID"). At the bottom are "Back" and "Finish" buttons.

Use the process described 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 (not shown).
- 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 (not shown).

The following screenshots show the **General** and **Advanced** tabs of the completed Server Configuration:

Server Configuration: Session_Manager

Buttons: Add, Rename, Clone, Delete

Server Profiles: Session_Manager, Telenet

Tabs: General, Authentication, Heartbeat, Advanced

Server Type: Call Server

IP Address / FQDN	Port	Transport
10.10.9.61	5060	TCP

Edit

Server Configuration: Session_Manager

Buttons: Add, Rename, Clone, Delete

Server Profiles: Session_Manager, Telenet

Tabs: General, Authentication, Heartbeat, Advanced

Enable DoS Protection: ☐

Enable Grooming: ☐

Interworking Profile: ASM

Signaling Manipulation Script: None

Connection Type: SUBID

Edit

7.6. Define Routing

Routing information is required for routing to the Telenet SIP Trunking 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 Telenet SIP Trunking, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** (not shown) and enter an appropriate name in the dialogue box.

Routing Profile

Profile Name: WAN

Next

Global Profiles: Fingerprint, Server Interworking, Phone Interworking, Media Forking, **Routing**

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 Telenet SIP Trunking, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side. Click on **Add** (not shown) 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 a dialog box titled "Topology Hiding Profile". On the left is a sidebar menu with options: Phone Interworking, Media Forking, Routing, Server Configuration, and **Topology Hiding**. The main area contains a "Profile Name" text box with the value "Telenet" 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.

This screenshot shows the configuration step within the "Topology Hiding Profile" dialog. It features a table with columns: Header, Criteria, Replace Action, and Overwrite Value. The first row shows "Request-Line" as the header, "IP/Domain" as the criteria, and "Auto" as the replace action. An "Add Header" button is at the top right, and "Back" and "Finish" buttons are 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 Telenet SIP Trunk.

This screenshot displays the "Topology Hiding Profiles: Telenet" configuration page. On the left, a sidebar lists profiles: default, cisco_th_profile, ASM, and **Telenet**. The main area shows a table of configured headers. At the top right are "Rename", "Clone", and "Delete" buttons. Below the table is an "Edit" button.

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

To define Topology hiding for Session Manager, follow the same process. This can be simplified by cloning the profile defined for Telenet SIP Trunking. Do this by highlighting the profile defined for Telenet 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

Buttons: Add, Rename, Clone, Delete

Click here to add a description

Topology Hiding

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

Buttons: Edit

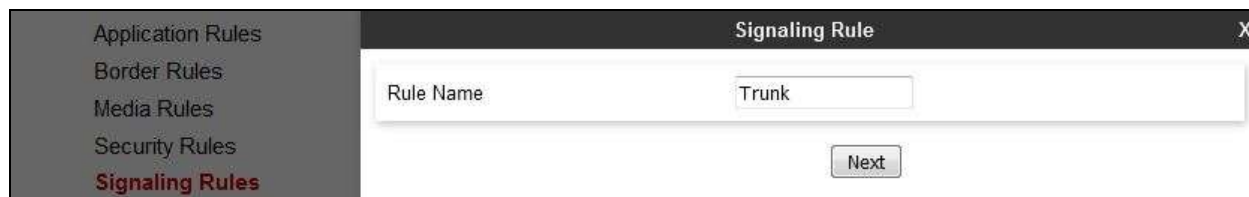
7.8. End Point Policy Groups

End Point Policy Groups are used to bring together a number of different rules for use in a server flow described in **Section 7.9**. During testing of Telenet SIP Trunking, a Signalling Rule was used so an End Point Policy Group was also required to apply it to the Server Flow

7.8.1. Signalling Rules

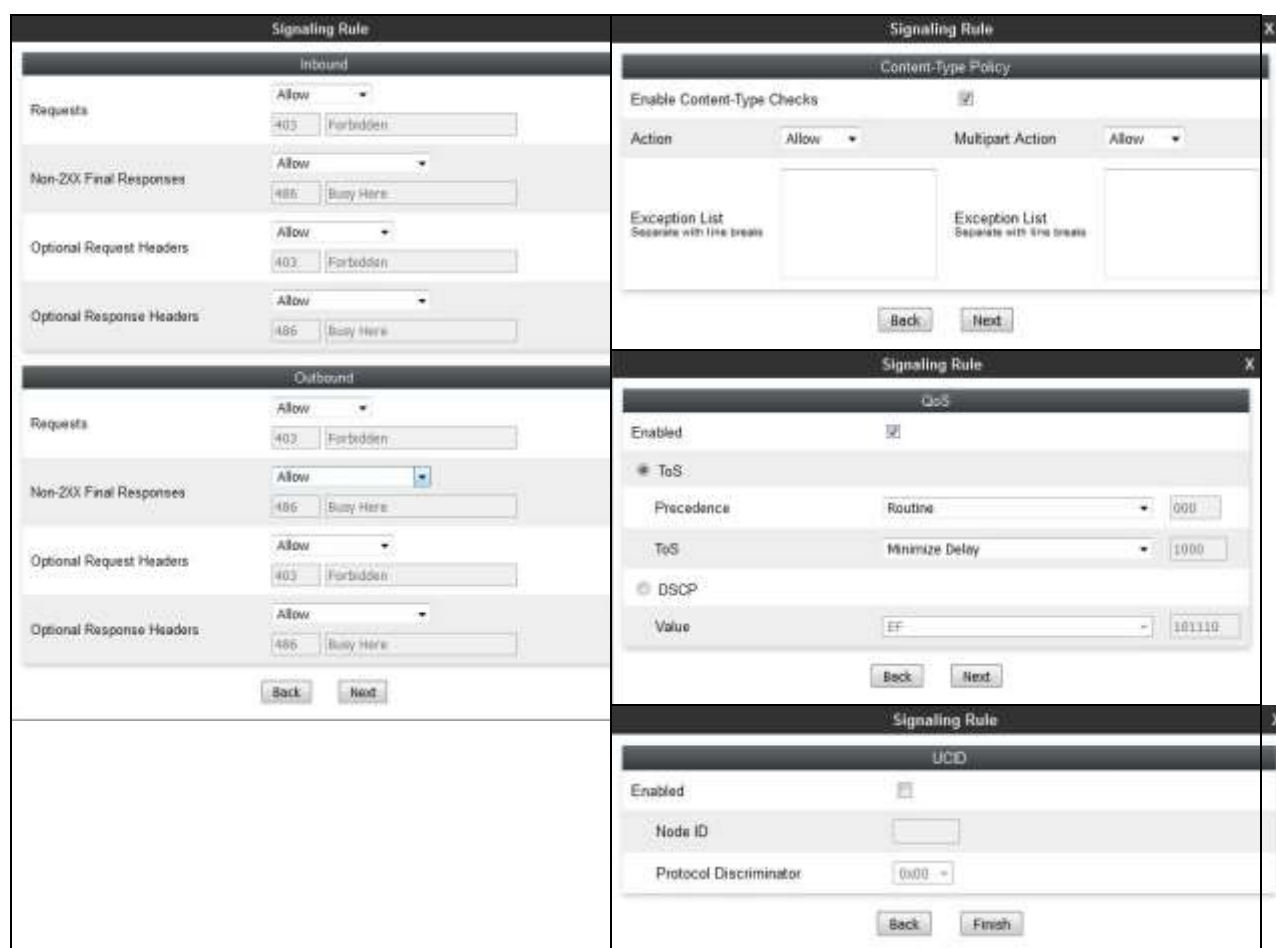
Signalling rules are a mechanism on the Avaya SBCE to handle any incompatible signalling that may be encountered on the SIP Trunk of a particular Service Provider. In the case of the Telenet SIP Trunk, it was found that Communication Manager rejected the Proxy-Require header in the INVITE message of incoming calls with CLI Restricted (See **Section 2.2**). A signalling Rule was used to remove the Proxy-Require header along with some other headers that were not used or Avaya proprietary.

To define a signalling rule to remove the Proxy-Require header, navigate to **Domain Policies** → **Signaling Rules** in the main menu on the left hand side. Click on **Add** (not shown) and enter details in the Signaling Rule pop-up box. In the **Rule Name** field enter a descriptive name for the signalling rule, in this case **Trunk**.



The screenshot shows a 'Signaling Rule' configuration window. On the left is a sidebar with menu items: Application Rules, Border Rules, Media Rules, Security Rules, and Signaling Rules (highlighted in red). The main area has a 'Rule Name' field containing the text 'Trunk' and a 'Next' button below it.

Click on **Next** 3 times leaving the settings at default values then click on **Finish**.



This block contains four sequential screenshots of the 'Signaling Rule' configuration interface, showing the progression from the initial rule name to the final 'Finish' button.

- First Screenshot:** Shows the 'Inbound' and 'Outbound' sections. Both sections have 'Requests' and 'Non-2XX Final Responses' set to 'Allow' with a default value of 403. 'Optional Request Headers' and 'Optional Response Headers' are also set to 'Allow' with a default value of 403. 'Back' and 'Next' buttons are at the bottom.
- Second Screenshot:** Shows the 'Content-Type Policy' section. 'Enable Content-Type Checks' is checked. 'Action' and 'Multipart Action' are both set to 'Allow'. There are empty 'Exception List' boxes. 'Back' and 'Next' buttons are at the bottom.
- Third Screenshot:** Shows the 'QoS' section. 'Enabled' is checked. Under 'ToS', 'Precedence' is set to 'Routine' (000) and 'ToS' is set to 'Minimize Delay' (1000). Under 'DSCP', 'Value' is set to 'EF' (101110). 'Back' and 'Next' buttons are at the bottom.
- Fourth Screenshot:** Shows the 'UCD' section. 'Enabled' is unchecked. 'Node ID' is an empty field. 'Protocol Discriminator' is set to '0x00'. 'Back' and 'Finish' buttons are at the bottom.

Once the rule is created, it is edited to provide the required functionality. To edit the rule, navigate to **Domain Policies → Signaling Rules** in the main menu on the left hand side and highlight the rule.

- Click on the **Request Headers** tab and then click on **Add In Header Control** for Headers to be deleted from SIP INVITE messages coming from Communication Manager or **Add Out Header Control** for messages going from the Avaya SBCE out to Communication Manager (not shown).
- Select a standard header from the **Header Name** drop down menu or check the **Proprietary Request Header** box and enter the name manually. The example shows **Proxy-Require**.
- Select **ALL** from the **Method Name** drop down menu.
- Check the **Forbidden** button in the **Header Criteria** menu.
- Select **Remove Header** from the **Presence Action** drop down menu.

Add Header Control

Proprietary Request Header ☐

Header Name: Proxy-Require

Method Name: ALL

Header Criteria: ☒ Forbidden, ☐ Mandatory, ☐ Optional

Presence Action: Remove header

486 Busy Here

Finish

During testing, the **Proxy-Require** header was removed from INVITE messages going **OUT** to Communication Manager. The **P-Location**, **P-Charging-Vector** and **Alert-Info** headers were removed from INVITE messages coming **IN** from Communication Manager:

Signaling Rules: Trunk

Filter By Device...

Signaling Rules: default, No-Content-Type-Ch..., **Trunk**

Click here to add a description

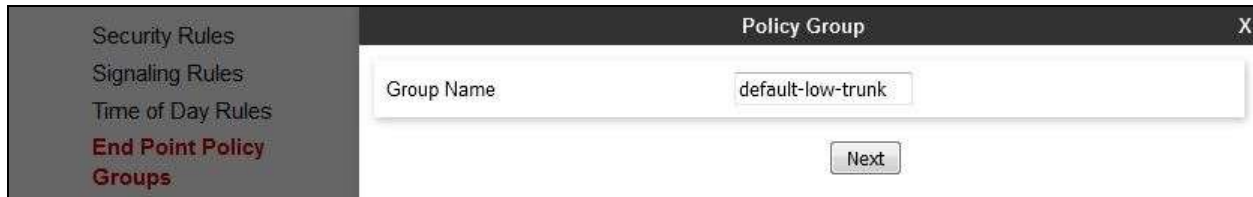
General | Requests | Responses | **Request Headers** | Response Headers | Signaling QoS | UCID

Add In Header Control | Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
2	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Proxy-Require	ALL	Forbidden	Remove Header	No	OUT	Edit	Delete

7.8.2. End Point Policy Groups

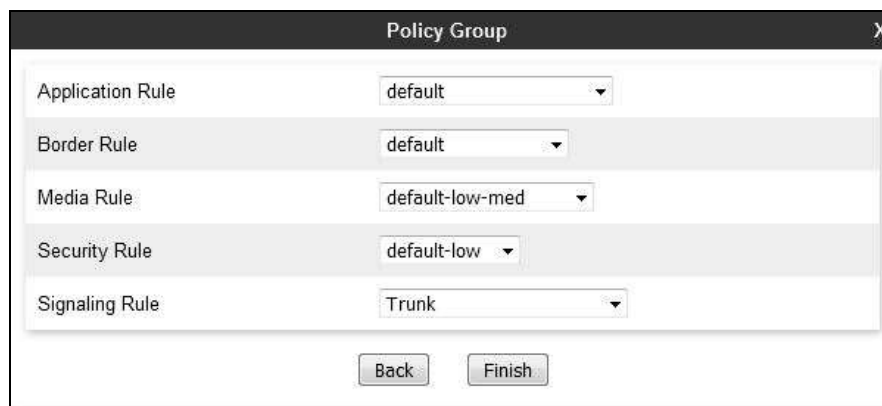
End Point Policy Groups are required to implement the signalling rules. To define one for use in the SIP Trunk server flow to remove Telenet proprietary headers, navigate to **Domain Policies** → **End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up box.



The screenshot shows a 'Policy Group' dialog box. On the left, a sidebar lists 'Security Rules', 'Signaling Rules', 'Time of Day Rules', and 'End Point Policy Groups' (which is highlighted in red). The main area of the dialog has a 'Group Name' text field containing 'default-low-trunk' and a 'Next' button.

Click on **Next** to configure the Policy Set. Enter details as follows:.

- Leave the **Application Rule**, **Border Rule**, **Media Rule** and **Security Rule** at their default values.
- Select the **Signaling Rule** created in the previous section in the drop down menu, in this case **Trunk**.
- Click on **Finish**.



The screenshot shows the 'Policy Group' dialog box with the following configurations:

Rule Type	Value
Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	Trunk

At the bottom, there are 'Back' and 'Finish' buttons.

7.9. Server Flows

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

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

- Click on the **Server Flows** tab (not shown).
- Select **Add Flow** (not shown) and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for the Telenet SIP Trunk, in the test environment **Telenet** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the Telenet 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 Telenet 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	Telenet
Server Configuration	Telenet
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	Telenet
File Transfer Profile	None
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 (not shown).
- Select **Add Flow** (not shown) 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 **Session_Manager** 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 Telenet SIP Trunking 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 a list of configuration fields, each with a label and a value field (text input or dropdown menu). The fields are: Flow Name (text input with "Session_Manager"), Server Configuration (dropdown with "Session_Manager"), URI Group (dropdown with "*"), Transport (dropdown with "*"), Remote Subnet (text input with "*"), Received Interface (dropdown with "External"), Signaling Interface (dropdown with "Internal"), Media Interface (dropdown with "Internal"), End Point Policy Group (dropdown with "default-low-trunk"), Routing Profile (dropdown with "WAN"), Topology Hiding Profile (dropdown with "ASM"), File Transfer Profile (dropdown with "None"), Signaling Manipulation Script (dropdown with "None"), and Remote Branch Office (dropdown with "Any"). At the bottom of the dialog is a "Finish" button.

Field	Value
Flow Name	Session_Manager
Server Configuration	Session_Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	External
Signaling Interface	Internal
Media Interface	Internal
End Point Policy Group	default-low-trunk
Routing Profile	WAN
Topology Hiding Profile	ASM
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

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

End Point Flows: GSSCP_R63

Devices
GSSCP_R63

Subscriber Flows Server Flows

Add

Hover over a row to see its description.

Server Configuration: Session_Manager

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

Server Configuration: Telenet

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

8. Configure the Telenet SIP Trunking Equipment

The configuration of the Telenet 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 Telenet equipment and system configuration please contact an authorized Telenet 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** screen click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with categories like Session Manager, Dashboard, Session Manager, Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, Managed Bandwidth Usage, Security Module Status, Registration Summary, User Registrations, SIP Performance, and System Performance. The main content area is titled 'SIP Entity Link Monitoring Status Summary' and includes a 'Run Monitor' button. Below this is a table with columns: Session Manager Name, Entity Links Down/Total, Entity Links Partially Down, SIP Entities - Monitoring Not Started, and SIP Entities - Not Monitored. The table shows one entry for 'Session Manager' with 0/4 links down and 0 links partially down. Below the table is a section for 'All Monitored SIP Entities' with a 'Run Monitor' button and a list of entities: ASBCE, CM Endpoints, CM Trunk, and Messaging. A 'Select: All, None' dropdown is also present.

Select the relevant SIP Entities from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.

The screenshot shows the Avaya Aura System Manager 6.1 interface, specifically the 'SIP Entity, Entity Link Connection Status' page. The page title is 'SIP Entity, Entity Link Connection Status' and it includes a 'Summary View' button. Below this is a table with columns: Details, Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. The table shows one entry for 'Session Manager' with a resolved IP of 10.10.9.83, port 5060, protocol TCP, connection status 'Up', reason code '200 OK', and link status 'Up'.

- 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
0002/008	T00018	in-service/idle	no
0002/009	T00019	in-service/idle	no
0002/010	T00020	in-service/idle	no

- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.
- 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 a trace on the Avaya SBCE, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main menu on the left hand side and select the **Packet Capture** tab.

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

Trace: GSSCP_R63

Devices
GSSCP_R63

Packet Capture **Captures**

Packet Capture Configuration

Status	Ready
Interface	BT
Local Address (IP Port)	192.168.122.58
Remote Address (*, *Port, IP, IP Port)	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename (Using the name of an existing capture will overwrite it)	SIP_Trunk_Test.pcap

Start Capture **Clear**

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

Trace: GSSCP_R63

Devices
GSSCP_R63

Packet Capture **Captures**

File Name	File Size (bytes)	Last Modified	
SIP_Trunk_Test_20160622054516.pcap	8,192	June 22, 2016 7:06:11 AM CDT	Delete

Refresh

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 Telenet network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.0.1, Avaya Aura® Session Manager R6.1 and Avaya Session Border Controller for Enterprise R6.3 to Telenet SIP Trunking. The Telenet SIP Trunking service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

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

- [1] *Installing and Configuring Avaya Aura System Platform Release 6.0.3*, 15th March 2012.
- [2] *Avaya Aura® Release 6.0 Documentation Library*, 26th August 2013
- [3] *Installing and Upgrading Avaya Aura® System Manager Release 6.1*, 29th November 2010.
- [4] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, 8th April 2011
- [5] *Upgrading Avaya Aura® Session Manager*, Release 6.1, 22nd June 2011
- [6] *Installing Service Packs for Avaya Aura® Session Manager*, Release 6.1, 11th January 2012.
- [7] *Deploying Avaya Session Border Controller*, Release 6.3, 27th August 2015
- [8] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.3, 27th October 2014
- [9] *Administering Avaya Session Border Controller*, Release 6.3, 12th February 2016
- [10] *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.