



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to support SFR SIP Trunk (Collecte SIP) - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the SFR Collecte SIP 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. SFR 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 SFR Collecte SIP service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with SFR SIP Trunk 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 use the SIP Trunking service provided by SFR.

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using the SIP Trunk provided by SFR, calls made to SIP and H.323 telephones at the enterprise
- Outgoing calls from the enterprise site completed via SFR SIP Trunk to PSTN destinations, calls made from SIP and H.323 telephones
- Calls using the G.729A and G.711 A Law codecs
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Direct IP-to-IP media (also known as “shuffling”) with 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 SFR SIP Trunk requiring Avaya response and sent by Avaya requiring SFR response

2.2. Test Results

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

- Inbound Toll Free calls were not tested as no Toll Free access was available
- There is no signalling from the network when the PSTN places the call on hold. Though this is an acceptable method of placing the call on hold, it is not a particularly informative test.
- On some of the Supplementary Features tests, there was no ringback or there was one way media. This was thought to be a network issue and Early Media was enabled to work around it. Early Media is enabled by setting Initial IP-IP Direct Media to “n”.
- When a call was transferred or forwarded to the PSTN such that both parties were on the PSTN, there was a media delay in excess of half a second. This was thought to be due to multiple VoIP hops and is a characteristic of the test network.
- Incoming fax calls failed when made from a PSTN line in the Avaya Lab in Galway. Calls succeeded when made from SFR premises in Paris. There was also a fault where the network detected the fax before the call was answered and sent an UPDATE message to Communication Manager to change the media to T.38. Communication Manager was rejecting this with “488 Fax request rejected”. A workaround for this is to use a separate SIP line for fax and to disable early media by setting Initial IP-IP Direct Media to “y” in the Signaling Group. Refer to **Section 5.5** for details.
- Tests using SIP one-X Communicator in Other Phone mode were not completely reliable. The application shut down during the first test of consultative transfer to the PSTN and the first conference with a PSTN endpoint filed.
- The outgoing long duration call failed on the first attempt but was successful on a subsequent attempt.

2.3. Support

Le Service Technique SFR Business Team est joignable 24H/24, 7J/7 par un numéro gratuit pour signalisation des incidents techniques sur le service Collecte SIP.

CENTRE SERVICE CLIENT SFR Business Team

0 800 950 920

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to SFR Collecte SIP. Located at the Enterprise site is an Avaya Session Border Controller for Enterprise, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya A175 Desktop Video Device running Flare® Experience (audio only), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Flare® for Windows running on a laptop PC. Within the enterprise, RTP was used for transport of media.

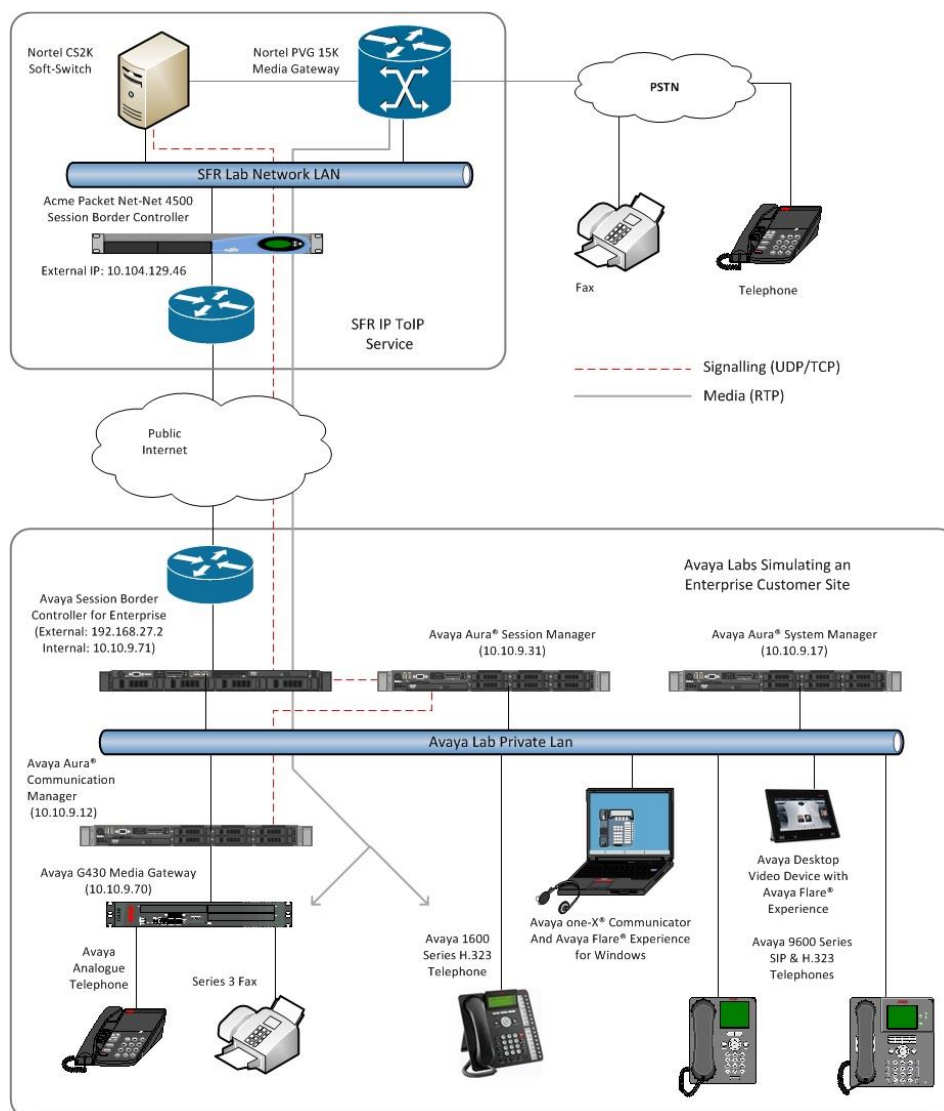


Figure 1: Test Setup SFR Collecte SIP to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Dell PowerEdge R620 running Session Manager on VM Version 8	6.3.10.0.631008 VMware Tools: 9.0.0.15210 (782409)
Dell PowerEdge R620 running System Manager on VM Version 8	6.3.10 Build No. 6.3.0.8.5682 Patch 6.3.8.4514 Build No. 6.3.10.7.2656
Dell PowerEdge R620 running Communication Manager on VM Version 8	R016x.03.0.124.0 patch 21754
Avaya Session Border Controller Advanced for Enterprise Server	6.3.0.Q19
G430 Media Gateway	FW Version/HW Vintage: 36.9
Avaya 1616 Phone (H.323)	1.3 Maintenance Release 6
Avaya 96x0 Phone (H.323)	3.2.3
Avaya 96x1 Phone (H.323)	6.4
Avaya A175 Desktop Video Device (SIP)	Flare® Experience Release 1.1.2
Avaya 96x0 Phone (SIP)	R2.6.12
Avaya 96x1 Phone (SIP)	R6.4.1
Avaya one-X® Communicator (H.323) on Lenovo T510 Laptop PC	6.2 FP4
Avaya Flare® experience for Windows on Lenovo T510 Laptop PC	Release 1.1.4.23
Analogue Handset	NA
Analogue Fax	NA
SFR	
Nortel Media Server	Communication Server 2000 (CS2K) CVM16
Nortel PSTN gateway	PVG 15k PCR 8.2
Acme Packet Net-Net 4500 SBC	SCX6.2.0 MR-6 GA

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 SFR SIP Trunk. For incoming calls, the Session Manager receives SIP messages from the Avaya SBC for Enterprise (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 the 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 SFR 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 SFR network, and any other SIP trunks used.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks:	12000	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:	41000	0
Maximum Video Capable IP Softphones:	18000	0
Maximum Administered SIP Trunks:	24000	30
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? y	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y		Multifrequency Signaling? y
Global Call Classification? y		Multimedia Call Handling (Basic)? y
Hospitality (Basic)? y		Multimedia Call Handling (Enhanced)? y
Hospitality (G3V3 Enhancements)? y		Multimedia IP SIP Trunking? y
IP Trunks? y		
IP Attendant Consoles? y		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 the Session Manager. In this case, **SMVM1** and **10.10.9.31** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** address as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SMVM1	10.10.9.31	
default	0.0.0.0	
procr	10.10.9.12	
procr6	::	

5.3. Administer IP Network Region

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

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

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
    Region: 1
    Location: 1          Authoritative Domain: avaya.com
        Name: default      Stub Network Region: n
MEDIA PARAMETERS          Intra-region IP-IP Direct Audio: yes
    Codec Set: 1          Inter-region IP-IP Direct Audio: yes
        UDP Port Min: 2048      IP Audio Hairpinning? n
        UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
    Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      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
```


5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form in **Section 5.3**. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codecs supported by SFR were configured, namely **G.729A** and **G.711A**.

change ip-codec-set 1 Page 1 of 2

IP CODEC SET

Codec Set: 1

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1:	G.729A	n	2	20
2:	G.711A	n	2	20
3:				
4:				
5:				
6:				
7:				

Media Encryption

1: none

2:

3:

SFR Collecte SIP supports T.38 for transmission of fax. To allow transmission using T.38, Navigate to **Page 2** and define as follows:

- Set the **FAX - Mode** to **t.38-G711-fallback**

change ip-codec-set 1 Page 2 of 2

IP Codec Set

Allow Direct-IP Multimedia? n

	Mode	Redundancy	
FAX	t.38-G711-fallback	0	ECM: y
Modem	off	0	
TDD/TTY	US	3	
Clear-channel	n	0	

Note: The fax **Mode** can be set to **t.38-standard** where fallback is not required. SFR also supports transmission of fax over G.711, though this did not work during testing. Refer to **Section 2.2** for details.

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to SFR Collecte SIP. During test, this was configured to use TCP and port 5060 to facilitate tracing and fault analysis. It is recommended however, to use TLS (Transport Layer Security) and the default TLS port of 5061 for security. Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tcp**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SMVM1** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region 1)
- Leave **Far-end Domain** blank (allows Communication Manager to accept calls from any SIP domain on the associated trunk)
- Set **Direct IP-IP Audio Connections** to **y**
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.

add signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Near-end Node Name: procr	Far-end Node Name: SMVM1	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

Note: Setting **Initial IP-IP Direct Media** to **y** allows the establishment of the media directly between the Avaya SBCE and the endpoint without establishment via the Media Gateway first. This makes efficient use of Media Gateway resources as they are not required for initial set-up of the call. The disadvantage is that Early Media is not used and this was having a detrimental effect during testing with occasional one way transmission and no ringback in some call scenarios. To work around this, **Initial IP-IP Direct Media** was set to **n** for testing of voice calls.

The issues with T.38 fax testing described in **Section 2.2** were resolved by setting **Initial IP-IP Direct Media** to **y**. To have it set differently for voice and fax, two trunks are required. The two trunks would be used by splitting the voice and fax traffic at the Session Manager and differentiating by port, for example 5060 for voice and 5062 for fax.

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 x** command, where **x** is an available trunk group. On **Page 1** of this form:

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

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: OUTSIDE CALL	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 1	
		Number of Members: 10	

On **Page 2** of the trunk-group form, the Preferred **Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with SFR to prevent unnecessary SIP messages during call setup.

add trunk-group 1	Page 2 of 21
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
	Redirect On OPTIM Failure: 10000
SCCAN? n	Digital Loss Group: 18
	Preferred Minimum Session Refresh Interval(sec): 900
Disconnect Supervision - In? y Out? y	

On **Page 3**, set the **Numbering Format** field to **private**. This allows delivery of CLI in formats other than E.164 with leading “+”. In test, CLI was sent as the national number with leading zeros. This format was successfully verified in the network.

add trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	
	UII Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n

On **Page 4** of this form:

- Set **Send Diversion Header** to **n**
- Set **Support Request History** to **y**
- Set the **Telephone Event Payload Type** to **101**
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on the Communication Manager extension

add trunk-group 1		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? n		
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n		
Send Transferring Party Information? n		
Network Call Redirection? n		
Send Diversion Header? n		
Support Request History? y		
Telephone Event Payload Type: 101		
Convert 180 to 183 for Early Media? n		
Always Use re-INVITE for Display Updates? n		
Identity for Calling Party Display: From		
Block Sending Calling Party Location in INVITE? n		
Accept Redirect to Blank User Destination? n		
Enable Q-SIP? n		

Note: The Payload Type is a dynamic value and the meaning is agreed during codec negotiation which was tested successfully. The value used is therefore not critical, 101 is shown as that is the value used during testing. The Payload Type defined on Communication Manager is not applied to calls from SIP end-points. Some Avaya SIP endpoints have a default value of 120.

5.7. Administer Calling Party Number Information

Use the **change private-unknown-numbering** command to configure Communication Manager to send the calling party number in the format required. In test, calling party number was sent unmodified as the extension number; this was adapted in the Session Manager to the national number format required by SFR Collecte SIP. See **Section 6.4** for details of the adaptation. This calling party number is sent in the SIP From, Contact and PAI headers as well as the History-Info header for forwarded calls.

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

5.8. Administer Route Selection for Outbound Calls

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

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

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning with 0. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

change ars analysis 0						Page 1 of 2	
ARS DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 0	
Dialed	Total		Route	Call	Node	ANI	
String	Min	Max	Pattern	Type	Num	Reqd	
0	10	10	1	pubu		n	
00	13	15	1	pubu		n	
0035391	13	13	1	pubu		n	
030	10	10	1	pubu		n	
0800	8	14	1	pubu		n	
0900	8	8	1	pubu		n	
1	4	4	1	pubu		n	
112	3	3	1	pubu		n	
118	3	6	1	pubu		n	
3	4	4	1	pubu		n	
7000	4	4	1	pubu		n	

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**. **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 1												Page	1 of	3					
Pattern Number: 1												Pattern Name:							
SCCAN? n												Secure SIP? n							
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC						
No			Mrk	Lmt	List	Del	Digits					QSIG							
Dgts												Intw							
1:	1	0										n	user						
2:											n	user							
3:											n	user							
4:											n	user							
5:											n	user							
6:											n	user							
BCC VALUE												TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No. Numbering	LAR
0	1	2	M	4	W	Request						Dgts	Format						
												Subaddress							
1:	y	y	y	y	y	n	n	rest				unk-unk	none						
2:	y	y	y	y	y	n	n	rest					none						
3:	y	y	y	y	y	n	n	rest					none						
4:	y	y	y	y	y	n	n	rest					none						
5:	y	y	y	y	y	n	n	rest					none						
6:	v	v	v	v	v	n	n	rest					none						

5.9. Administer Incoming Digit Translation

This step configures the settings to map incoming Direct Dial-In (DDI) calls to the Communication Manager extensions if not already mapped using a Session Manager adaptation. The incoming digits sent in the INVITE message from the Service Provider can be manipulated as necessary to route calls to the desired extension. During test, the incoming DDI numbers were adapted in Session Manager to the Communication Manager extension numbers; this process is described in **Section 6.4**. When done this way, there is no requirement for any incoming digit translation in Communication Manager. If incoming digit translation is required, use the **change inc-call-handling-trmt trunk-group x** command where **x** is the Trunk Group defined in **Section 5.6**.

change inc-call-handling-trmt trunk-group 1										Page	1 of	30
INCOMING CALL HANDLING TREATMENT												
Service/	Number	Number	Del Insert									
Feature	Len	Digits										

Note: One reason for configuring the enterprise in this way is to ensure correct routing and handling of CLI in a solution with Avaya Aura® Messaging.

5.10. EC500 Configuration

When EC500 is enabled on the Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2291. Use the command **change off-pbx-telephone station-mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** enter the phone that will also be called (e.g., **0035389434nnnn**)
- Set the **Trunk Selection** to **1** so that Trunk Group 1 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
2291	OPS	-		2291	aar	1	
2291	EC500	-		0035389434nnnn	ars	1	-

Note: The phone number shown is for a mobile phone used for testing at Avaya Labs and is in international format with international dialling prefix 00. To use facilities for calls coming in from EC500 mobile phones, the number received in Communication Manager must exactly match the number specified in the above table.

In the above screenshot the Mobile phone number is partially obscured.

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

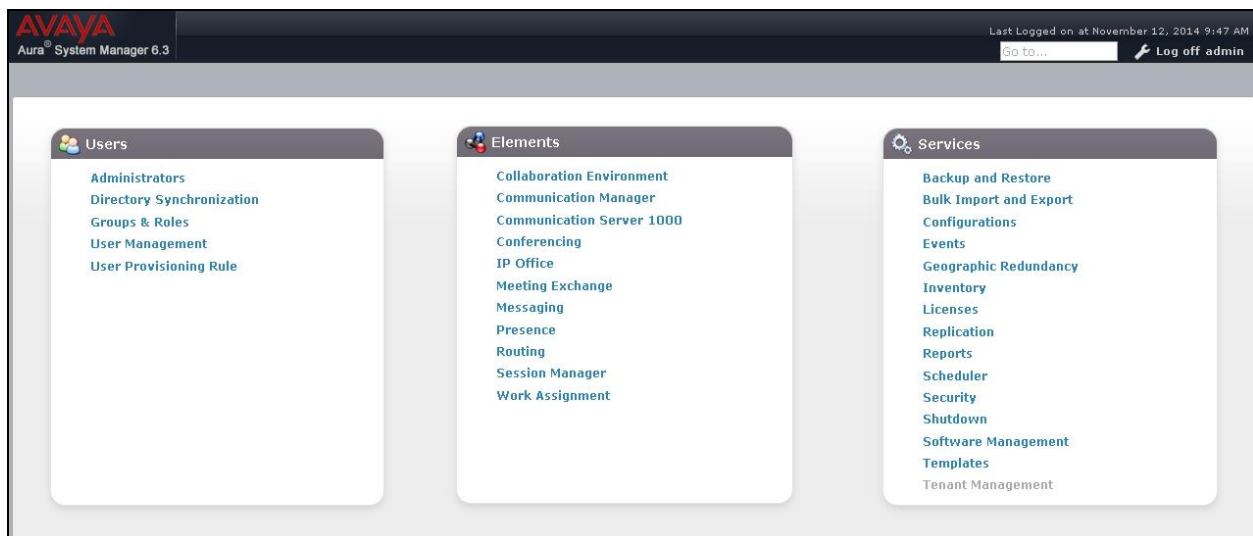
6. Configuring Avaya Aura® Session Manager

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

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- 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 by entering **http://<FQDN >/SMGR**, where <FQDN> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** tab will be presented with menu options shown below.



6.2. Administer SIP Domain

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

The screenshot shows the 'Domain Management' interface. On the left is a navigation menu with 'Routing' selected and 'Domains' highlighted. The main area has a breadcrumb 'Home / Elements / Routing / Domains' and a 'Help ?' link. Below the breadcrumb are buttons: 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A table shows '1 Item' with columns 'Name', 'Type', and 'Notes'. The table contains one row with 'avaya.com' in the Name column and 'sip' in the Type column. Below the table is a 'Select : All, None' option.

Name	Type	Notes
avaya.com	sip	

Note: If the existing domain name used in the enterprise equipment does not match that used in the network, a Session Manager adaptation can be used to change it.

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. Under **General**, in the **Name** field, enter an informative name for the location.

The screenshot shows the 'Location Details' form. At the top is a breadcrumb 'Home / Elements / Routing / Locations'. Below it are 'Commit' and 'Cancel' buttons. The 'General' section is highlighted. It contains a required field 'Name' with the value 'Galway' and a 'Notes' field which is empty.

Name: Galway

Notes:

Scroll down for bandwidth configuration. During testing, these were left at default values.

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

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: Kbit/sec

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.

Alarm Threshold

Overall Alarm Threshold: %

Multimedia Alarm Threshold: %

* Latency before Overall Alarm Trigger: Minutes

* Latency before Multimedia Alarm Trigger: Minutes

Location Pattern

Add Remove

1 Item Filter: Enable

IP Address Pattern	Notes
* 10.10.*	Galway Labs

Select : All, None

Commit Cancel

6.4. Administer Adaptations

Calls from SFR are received at the enterprise in national format with leading “0” on the Request URI. An Adaptation specific to SFR is used to convert the called number to an extension number as defined in the Communication Manager before onward routing to Communication Manager SIP Entity and removes the requirement for incoming digit manipulation on Communication Manager. It is also applied to messages coming from Communication Manager so that the SIP PUBLISH message for message waiting indicator on SIP end-points is handled correctly.

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

- In the **Adaptation name** field, enter a descriptive title for the adaptation.
- In the **Module name** enter **DigitConversionAdapter**. This is used for simple digit conversion adaptations.
- In the **Module parameter** field, select **Name-Value Parameter** in the **Module Parameter Type** drop down menu and enter **fromto** with a value of **true** in the resultant dialogue box. This will apply the adaptation to the From and To headers as well as the Request URI.

Home / Elements / Routing / Adaptations

Adaptation Details Commit Cancel Help ?

General

* Adaptation Name:

Module Name:

Module Parameter Type:

Add Remove

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	fromto	true

Select : All, None

Egress URI Parameters:

Notes:

Scroll down and in the section **Digit Conversion for Incoming Calls to SM**, click on **Add**. An additional row will appear. This allows information to be entered for the manipulation of numbers coming from the network. This is where the called party number is translated from national format to the extension number for termination of calls on Communication Manager.

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

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

Digit Conversion for Incoming Calls to SM									
Add Remove									
9 Items		Filter: Enable							
<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*04274nnnn0	*10	*10		*10	2000	destination ▼		
<input type="checkbox"/>	*04274nnnn1	*10	*10		*10	2390	destination ▼		
<input type="checkbox"/>	*04274nnnn2	*10	*10		*10	2391	destination ▼		
<input type="checkbox"/>	*04274nnnn3	*10	*10		*10	2290	destination ▼		
<input type="checkbox"/>	*04274nnnn4	*10	*10		*10	2291	destination ▼		
<input type="checkbox"/>	*04274nnnn5	*10	*10		*10	2316	destination ▼		
<input type="checkbox"/>	*04274nnnn6	*10	*10		*10	2412	destination ▼		
<input type="checkbox"/>	*04274nnnn7	*10	*10		*10	6101	destination ▼		
<input type="checkbox"/>	*04274nnnn9	*10	*10		*10	2801	destination ▼		
Select : All, None									

Note: In the above screenshot the DDI numbers are partially obscured

The screenshot below shows a translation for each calling party number. Again, this is not normally necessary where the extension number forms part of the national number.

- Under **Matching Pattern** enter the extension number as received from the CM.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the extension number, during testing this was **4**.
- Under **Delete Digits** enter the number of digits to delete to remove all digits that don't form part of the national number, during testing this was all of them..
- Under **Insert Digits** enter digits to be inserted. During test, this was the full national number. If the extension number forms part of the DDI number, only the most significant digits are entered here.
- Under **Address to Modify** choose **origination** from the drop down box to apply this rule to the From and P-Asserted-Identity headers only.

Digit Conversion for Outgoing Calls from SM

Add Remove

7 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify ▼	Adaptation Data	Notes
<input type="checkbox"/>	* 2000	* 4	* 4		* 4	04274nnnn0	origination ▼		
<input type="checkbox"/>	* 2290	* 4	* 4		* 4	04274nnnn3	origination ▼		
<input type="checkbox"/>	* 2291	* 4	* 4		* 4	04274nnnn4	origination ▼		
<input type="checkbox"/>	* 2316	* 4	* 4		* 4	04274nnnn5	origination ▼		
<input type="checkbox"/>	* 2390	* 4	* 4		* 4	04274nnnn1	origination ▼		
<input type="checkbox"/>	* 2391	* 4	* 4		* 4	04274nnnn2	origination ▼		
<input type="checkbox"/>	* 2412	* 4	* 4		* 4	04274nnnn6	origination ▼		

Select : All, None

Commit Cancel

Note: In the above screenshot the DDI numbers are partially obscured.

6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the 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 the 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 three SIP Entities:

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

6.5.1. Avaya Aura® Session Manager SIP Entity

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

The screenshot shows a web-based configuration interface for SIP Entities. The breadcrumb trail at the top is "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details" with "Commit" and "Cancel" buttons. A "Help ?" link is in the top right. The "General" tab is selected. The form contains the following fields:

- Name:** SM1
- FQDN or IP Address:** 10.10.9.31
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text area)
- Location:** (empty dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (empty text area)

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

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

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

Port

TCP Failover port:

TLS Failover port:

3 Items Filter: Enable

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

Select : All, None

6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities Help ?

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

Note: No adaptation is required for Communication Manager as all required number modifications are performed by the adaptation applied to the Avaya SBCE.

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

The screenshot shows two configuration sections. The first section, 'Loop Detection', has a 'Loop Detection Mode' dropdown menu set to 'Off'. The second section, 'SIP Link Monitoring', has a 'SIP Link Monitoring' dropdown menu set to 'Use Session Manager Configuration'.

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

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

The screenshot shows the 'SIP Entity Details' configuration page. The 'General' tab is selected. The 'Name' field is set to 'ASBCE'. The 'FQDN or IP Address' field is set to '10.10.9.71'. The 'Type' dropdown is set to 'SIP Trunk'. The 'Notes' field is empty. The 'Adaptation' dropdown is set to 'SFR_DDI_2_Ext'. The 'Location' dropdown is set to 'Galway'. The 'Time Zone' dropdown is set to 'Europe/Dublin'. The 'SIP Timer B/F (in seconds)' field is set to '4'. The 'Credential name' field is empty. The 'Call Detail Recording' dropdown is set to 'egress'. The 'Commit' and 'Cancel' buttons are visible at the top right.

6.6. Administer Entity Links

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

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

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

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	ASBCE_Link	SM1	TCP	5060	ASBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM1_Link	SM1	TCP	5060	CM1	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Messaging_Link	SM1	TCP	5060	Messaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

Select : All, None

Note: The **Messaging_Link** Entity Link is used for the Avaya Aura ® Messaging system and is not described in this document.

6.7. Administer Routing Policies

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

Under **General**:

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

The following screen shows the routing policy for Communication Manager.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name: Incoming

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM1	10.10.9.12	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

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

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name: Outgoing

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE	10.10.9.71	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

6.8. Administer Dial Patterns

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

Under **General**:

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

Under **Originating Locations and Routing Policies**:

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

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

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

Help ?

General

* Pattern: 0

* Min: 10

* Max: 15

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

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

Select : All, None

The following screen shows the test dial pattern configured for Communication Manager which identifies the extension number. All extension numbers used during testing were four digit numbers starting with 2.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		Incoming	0	<input type="checkbox"/>	CM1	

Select : All, None

Note: The above configuration is used where the called party number has been converted to an extension number on Session Manager using an adaptation. If an adaptation is not used, a dial pattern will be required for the incoming DDI number.

6.9. Administer Application for Avaya Aura® Communication Manager

From the **Home** tab select **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration** → **Applications** and click **New**.

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

Home / Elements / Session Manager / Application Configuration / Applications

Application Editor Commit Cancel

Application

*Name

*SIP Entity

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

Description

Application Attributes (optional)

Name	Value
Application Handle	<input type="text"/>
URI Parameters	<input type="text"/>

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**.

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

Home / Elements / Session Manager / Application Configuration / Application Sequences Help ?

Application Sequence Editor

Commit Cancel

Application Sequence

*Name

Description

Applications in this Sequence

Move First Move Last Remove

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		BG_CM_App	CM1	<input checked="" type="checkbox"/>	

Select : All, None

Available Applications

1 Item Filter: Enable

	Name	SIP Entity	Description
+	BG_CM_App	CM1	

*Required Commit Cancel

6.11. Administer SIP Extensions

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

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of user@domain e.g. **2292@avaya.com** which is used to create the user's primary handle
- The **Authentication Type** should be **Basic**
- In the **Password/Confirm Password** fields enter an alphanumeric password
- Set the **Language Preference** and **Time Zone** as required

Home / Users / User Management / Manage Users

Help ?

New User Profile

Commit & Continue Commit Cancel

Identity * Communication Profile Membership Contacts

User Provisioning Rule

User Provisioning Rule: [v]

Identity

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

* First Name: [9608]
First Name (Latin Translation): [9608]
Middle Name: []
Description: []

* Login Name: [2292@avaya.com]

* Authentication Type: [Basic v]
Password: [*****]
Confirm Password: [*****]
Localized Display Name: []
Endpoint Display Name: []
Title: []

Language Preference: [French (France) v]
Time Zone: [(+1:0)Amsterdam, Berlin, Rom v]
Employee ID: []
Department: []
Company: []

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

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 displays the 'Communication Profile' configuration window. At the top, there are tabs for 'Identity', 'Communication Profile' (selected), 'Membership', and 'Contacts'. Below the tabs, the 'Communication Profile' section contains two password fields: 'Communication Profile Password' and 'Confirm Password', both masked with dots. Below these is a table for 'Communication Address' with columns 'Name', 'Handle', and 'Domain'. The table currently shows 'Primary' as the only entry. Below the table, there is a 'New' button and a form for adding a new address. The form includes a 'Type' dropdown menu set to 'Avaya SIP', a 'Fully Qualified Address' field with the extension '2292', and a domain dropdown menu set to 'avaya.com'. There are 'Add' and 'Cancel' buttons at the bottom right of the form.

Name	Handle	Domain
Primary		

Type	Handle	Domain
No Records found		

Type: Avaya SIP

* Fully Qualified Address: 2292 @ avaya.com

Add Cancel

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

Communication Address ▼

New Edit Delete

Type	Handle	Domain
Avaya SIP	2292	avaya.com

Select : All, None

☒ **Session Manager Profile** ▼

SIP Registration

* Primary Session ManagerSM1 ▼

Secondary Session Manager(None) ▼

Survivability Server(None) ▼

Max. Simultaneous Devices1 ▼

Block New Registration When Maximum Registrations Active?☐

Application Sequences

Origination SequenceBG_CM_App_Seq ▼

Termination SequenceBG_CM_App_Seq ▼

Call Routing Settings

* Home LocationGalway ▼

Conference Factory Set(None) ▼

Call History Settings

Enable Centralized Call History?☐

Primary	Secondary	Maximum
6	0	6

BG; Reviewed:
SPOC 02/04/2015

Solution & Interoperability Test Lab Application Notes
©2015 Avaya Inc. All Rights Reserved.

33 of 58
SFR_CM63_SM

Expand the **Endpoint Profile** section.

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

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

- System:** Communication_Manager_1 (dropdown)
- Profile Type:** Endpoint (dropdown)
- Use Existing Endpoints:** ☐
- Extension:** 2292 (text field) with an 'Endpoint Editor' button
- Template:** 9608SIP_DEFAULT_CM_6_3 (dropdown)
- Set Type:** 9608SIP (text field)
- Security Code:** (empty text field)
- Port:** IP (text field)
- Voice Mail Number:** (empty text field)
- Preferred Handle:** (None) (dropdown)
- Enhanced Callr-Info display for 1-line phones:** ☐
- Delete Endpoint on Unassign of Endpoint from User or on Delete User:** ☒
- Override Endpoint Name and Localized Name:** ☒

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the 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.

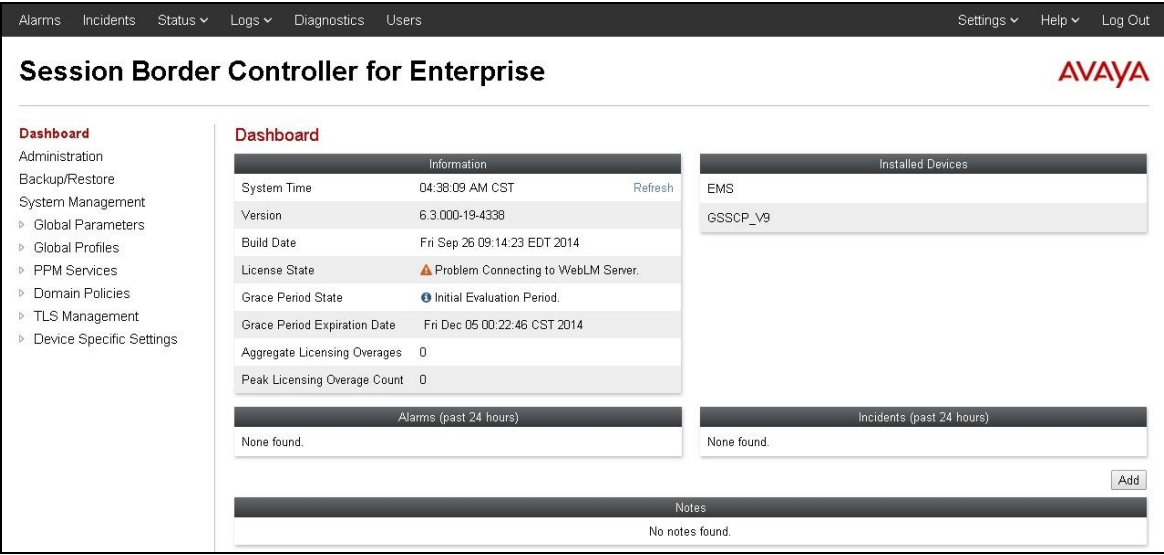
7.1. Access Avaya Session Border Controller for Enterprise

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 username ucsec and the appropriate 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. Below the input field is a "Continue" button. Further down, there is a block of text stating: "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." This is followed by another block of text: "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." Below that is a third block of text: "All users must comply with all corporate instructions regarding the protection of information assets." At the bottom, it says "© 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: Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. On the left is a sidebar menu with "Dashboard" selected, and sub-items: Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is divided into several sections: "Information" (System Time: 04:38:09 AM CST, Version: 6.3.000-19-4338, Build Date: Fri Sep 26 09:14:23 EDT 2014, License State: Problem Connecting to WebLM Server, Grace Period State: Initial Evaluation Period, Grace Period Expiration Date: Fri Dec 05 00:22:46 CST 2014, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0), "Installed Devices" (listing EMS and GSSCP_V9), "Alarms (past 24 hours)" (None found), "Incidents (past 24 hours)" (None found), and "Notes" (No notes found). There is an "Add" button next to the Incidents section.

7.2. Define Network Information

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

To define the network information, navigate to **Device Specific Settings → Network Management** in the main menu on the left hand side. The **Interface** tab appears first, click on the status of the required interfaces to change the state.

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

Select the **Networks** tab and click on **Add**. Enter details in the blank box that appears at the end of the list.

- Define the internal IP address with screening mask and assign to interface **A1**
- Select **Save** to save the information
- Click on **Add**
- Define the external IP address with screening mask and assign to interface **B1**
- Select **Save** to save the information
- Click on **System Management** in the main menu
- Select **Restart Application** indicated by an icon in the status bar (not shown)

Name	Gateway	Subnet Mask	Interface	IP Address	
Network_A1	10.10.9.1	255.255.255.0	A1	10.10.9.71	Edit Delete
Network_B1	192.168.27.1	255.255.255.224	B1	192.168.27.2	Edit Delete

7.3. Define Interfaces

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

7.3.1. Signalling Interfaces

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

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the internal signalling interface
- For **Signaling IP**, select an **internal** signalling interface IP address defined in **Section 7.2**
- Select **TCP** port number, **5060** is used for the Session Manager
- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the external signalling interface
- For **Signaling IP**, select an **external** signalling interface IP address defined in **Section 7.2**
- Select **UDP** port number, **5060** is used for the SFR Collecte SIP

Signaling Interface: GSSCP_V9

Devices

GSSCP_V9

Signaling Interface

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

Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Int_Sig	10.10.9.71	5060	---	---	None	Edit	Delete
Ext_Sig	192.168.27.2	---	5060	---	None	Edit	Delete

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 and SRTP 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 internal media interface in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface
- For **Media IP**, select an **internal** media interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the enterprise end-points
- 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
- For **Media IP**, select an **external** media interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the media path with SFR Collecte SIP

Media Interface: GSSCP_V9

Devices
GSSCP_V9

Media Interface

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

Add

Name	Media IP	Port Range	Edit	Delete
Int_Med	10.10.9.71	2048 - 3329	Edit	Delete
Ext_Med	192.168.27.2	2048 - 3329	Edit	Delete

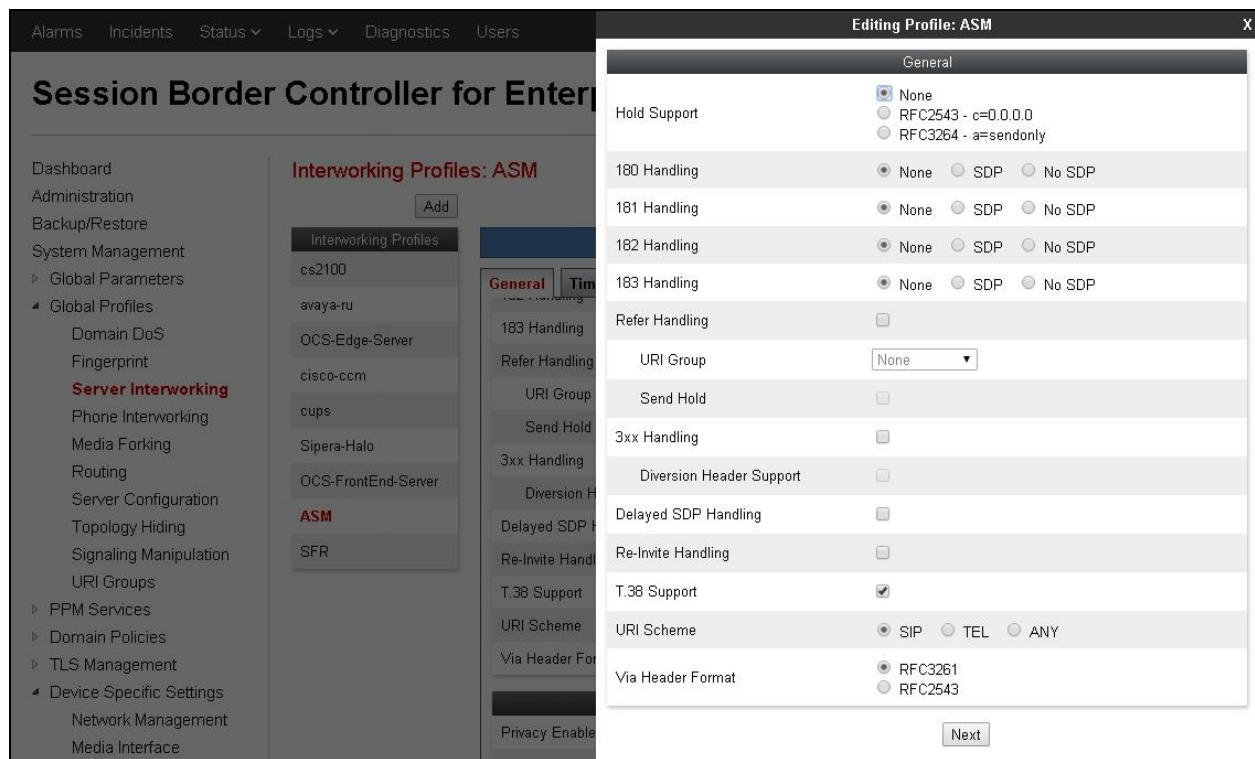
Note: During test, the port ranges for the internal and external media interfaces were set to the default values used on Communication Manager.

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, SFR Collecte SIP 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 Session Manager, highlight the **avaya-ru** profile which is a factory setting appropriate for Avaya equipment and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown).

- In the **Clone Name** field enter a descriptive name for the Session Manager and click **Finish** – in test **ASM** was used
- In the **General** tab (not shown) Select **Edit** and enter details in the pop-up menu
- Check the **T.38 Support** box then click **Next** and **Finish** (not shown)



- In the **Advanced** tab (not shown) Select **Edit** and enter details in the pop-up menu
- Uncheck the **AVAYA Extensions** box

Editing Profile: ASM [X]

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

Finish

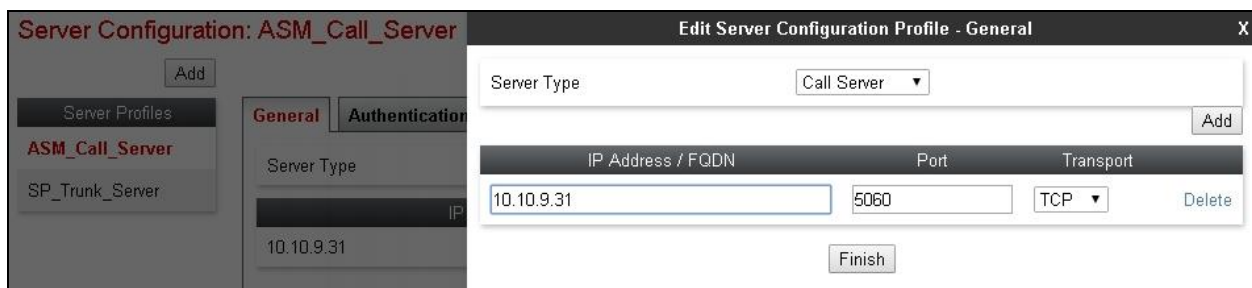
To define Server Interworking for SFR Collecte SIP, highlight the previously defined profile for the Session Manager and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown).

- In the **Clone Name** field enter a descriptive name for server interworking profile for SFR Collecte SIP and click **Finish** – in test **SFR** was used
- Select **Edit** and enter details in the pop-up menu
- Ensure the **T.38 Support** box is checked
- Select **Next** three times and **Finish**

7.5. Define Servers

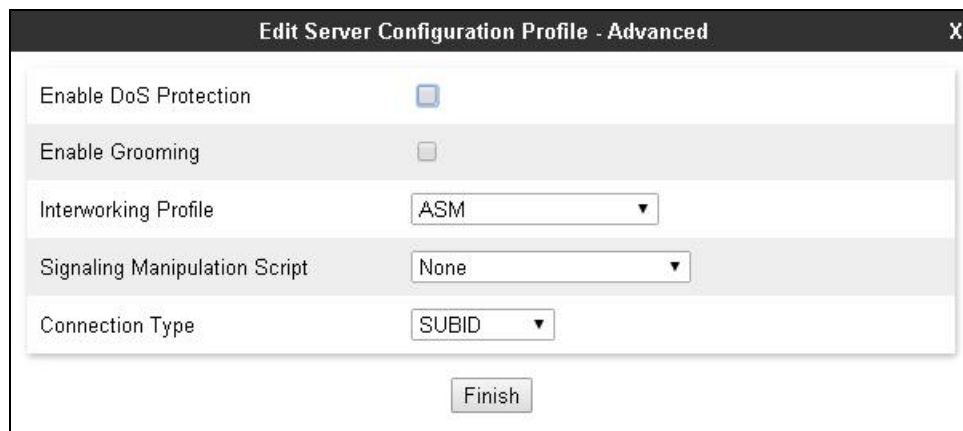
A server definition is required for each server connected to the Avaya SBCE. In this case, SFR Collecte SIP is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the Session Manager, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** and enter details in the pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next** (not shown)
- In the **Server Type** drop down menu, select **Call Server**
- In the **IP Addresses / Supported FQDNs** box, type the Session Manager SIP interface address which is the same as that defined on the Communication Manager in **Section 5.2**
- Check **TCP** in **Supported Transports**
- Define the **TCP** port for SIP signalling, **5060** is used for the Session Manager and click **Finish**



The screenshot shows the 'Edit Server Configuration Profile - General' window. On the left, a sidebar lists 'Server Profiles' with 'ASM_Call_Server' and 'SP_Trunk_Server'. The main area has tabs for 'General' and 'Authentication'. The 'General' tab is active, showing 'Server Type' as 'Call Server' and a table with one entry: IP Address / FQDN: 10.10.9.31, Port: 5060, Transport: TCP. There are 'Add' and 'Delete' buttons for the table, and a 'Finish' button at the bottom.

- Select the **Advanced** tab (not shown)
- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for the Session Manager defined in **Section 7.4**
- Click **Finish**



The screenshot shows the 'Edit Server Configuration Profile - Advanced' window. It contains several settings: 'Enable DoS Protection' (checkbox unchecked), 'Enable Grooming' (checkbox unchecked), 'Interworking Profile' (dropdown set to 'ASM'), 'Signaling Manipulation Script' (dropdown set to 'None'), and 'Connection Type' (dropdown set to 'SUBID'). A 'Finish' button is located at the bottom.

To define SFR Collecte SIP as a Trunk Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** and enter details in the pop-up menu.

- In the **Profile Name** field enter a descriptive name for SFR Collecte SIP and click **Next** (not shown)
- In the **Server Type** drop down menu, select **Trunk Server**
- In the **IP Addresses / Supported FQDNs** box, type the IP address of SFR Collecte SIP
- Check **UDP** in **Supported Transports**
- Define the **UDP** port for SIP signaling, **5060** is used for SFR
- Click **Finish**

IP Address / FQDN	Port	Transport
10.104.129.46	5060	UDP

- Select the **Advanced** tab (not shown)
- Select the **Interworking Profile** for the SFR Collecte SIP defined in **Section 7.4** from the drop down menu

7.6. Define Routing

Routing information is required for routing to the Session Manager on the internal side and SFR Collecte SIP on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop Address**, default 5060 is used for TCP and UDP, and 5061 for TLS.

To define routing to the Session Manager, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field (not shown) enter a descriptive name for the Session Manager, in this case **Call Server**, and click **Next**
- Select the Session Manager Server Configuration in the **Server Configuration** field
- Select the Session Manager SIP interface address and port in the **Next Hop Address** field
- Select **TCP** for the **Transport**
- Click **Finish**

The screenshot shows the 'Session Border Controller for Enterprise' interface. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and Routing. The 'Routing' option is selected. In the center, there's a 'Routing Profiles: Call Server' section with an 'Add' button. A pop-up window titled 'Profile : Call Server - Edit Rule' is open. It contains fields for URI Group (set to '*'), Time of Day (set to 'default'), Load Balancing (set to 'Priority'), Transport (set to 'None'), Next Hop In-Dialog (unchecked), and Ignore Route Header (unchecked). Below these is a table with columns: Priority / Weight, Server Configuration, Next Hop Address, and Transport. The table has one row with values: 1, ASM_Call_Server, 10.10.9.31:5060 (TCP), and None. There are 'Add', 'Delete', and 'Finish' buttons.

To define routing to SFR Collecte SIP, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field (not shown) enter a descriptive name for SFR Collecte SIP, in this case a generic name of **Trunk Server** was used, and click **Next**
- Select the SFR Collecte SIP Server Configuration in the **Server Configuration** field
- Select the SFR Collecte SIP IP address and port in the **Next Hop Address** field
- Select **UDP** for the **Transport**
- Click **Finish**

The screenshot shows the 'Profile : Trunk Server - Edit Rule' dialog box. It contains fields for URI Group (set to '*'), Time of Day (set to 'default'), Load Balancing (set to 'Priority'), Transport (set to 'None'), Next Hop In-Dialog (unchecked), and Ignore Route Header (unchecked). Below these is a table with columns: Priority / Weight, Server Configuration, Next Hop Address, and Transport. The table has one row with values: 1, SP_Trunk_Server, 10.104.129.46:5060 (UDP), and None. There are 'Add', 'Delete', and 'Finish' buttons.

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

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

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- If the **Request-Line**, **Via**, **Refer-To**, **To** and **Record-Route** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **Referred-By**, **From** and **SDP** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten)
- For each of the headers leave the **Replace Action** at the default value of **Auto**

Topology Hiding Profiles: ASM

Add

Topology Hiding Profiles

default

cisco_th_profile

ASM

SFR

Rename

Clone

Delete

Click here to add a description.

Topology Hiding

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

Edit

Note: The use of **Auto** results in an IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used where appropriate, and the required domain names entered in the **Overwrite Value** field. Different domain names can be used for the enterprise and SFR Collecte SIP.

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

- In the **Profile Name** field enter a descriptive name for SFR Collecte SIP and click **Next**
- If the **Request-Line**, **Via**, **Refer-To**, **To** and **Record-Route** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **Referred-By**, **From** and **SDP** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten)
- For each of the headers leave the **Replace Action** at the default value of **Auto**

Topology Hiding Profiles: SFR

Add

Topology Hiding Profiles

default

cisco_th_profile

ASM

SFR

Rename

Clone

Delete

Click here to add a description.

Topology Hiding

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

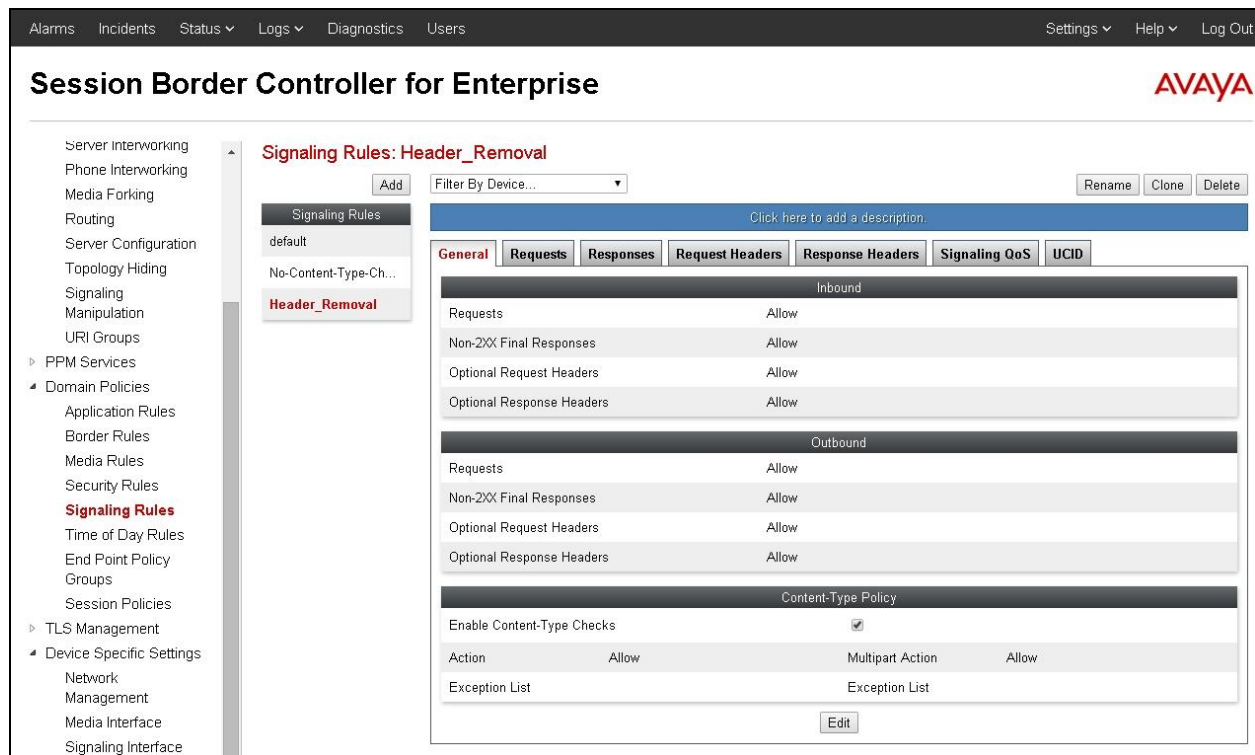
Edit

7.8. Signalling Rules

Signalling rules are a mechanism on the Avaya SBCE to manipulate the signalling beyond simple header manipulation. In the case of SFR, the SIP messages are manipulated to avoid the overhead of re-assembling fragmented UDP packets. This is achieved by removing Avaya proprietary and unnecessary headers to reduce the SIP messages to below the Maximum Transmission Unit (MTU) so that fragmentation does not occur.

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

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



Select the **Request Headers** tab and define the rules to remove Avaya proprietary headers as follows:

- Click on **Add In Header Control** (not shown)
- Check the **Proprietary Request Header** box
- Enter the name of the header to be removed in the **Header Name** field

Rules to remove unnecessary headers are slightly different

- Click on **Add In Header Control** (not shown)
- Select the name of the header to be removed in the **Header Name** field

In both cases, the following steps are required:

- Select **ALL** in the Method Name field
- Check **Forbidden** in the Header Criteria options
- In the **Presence Action** drop down menu, select **Remove Header**
- Click **Finish**

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

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

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

Signaling Rules: Header_Removal

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

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

The same is required for Response headers. Select the **Response Headers** tab and define the rules to remove proprietary headers as follows:

- Click on **Add In Header Control** (not shown)
- Check the **Proprietary Request Header** box
- Enter the name of the header to be removed in the **Header Name** field

As described for request headers, the process to remove unnecessary headers is slightly different:

- Click on **Add In Header Control** (not shown)
- Select the name of the header to be removed from the **Header Name** drop down menu

The following steps are required in both cases:

- Select **1XX** in the **Response Code** drop down menu, this will remove the header from 183 Session Progress and 180 Ringing messages.
- Select **ALL** in the Method Name field
- Check **Forbidden** in the Header Criteria options
- In the **Presence Action** drop down menu, select **Remove Header**
- Click **Finish**

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

The following example shows configuration for removal of **Accept** headers from 1XX responses.

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

- Proprietary Response Header:** A checkbox that is currently unchecked.
- Header Name:** A dropdown menu with "Accept" selected.
- Response Code:** A dropdown menu with "1XX" selected.
- Method Name:** A dropdown menu with "ALL" selected.
- Header Criteria:** Three radio button options: "Forbidden" (selected), "Mandatory", and "Optional".
- Presence Action:** A dropdown menu with "Remove header" selected.
- 486:** A text input field containing "486".
- Busy Here:** A text input field containing "Busy Here".
- Finish:** A button at the bottom of the dialog.

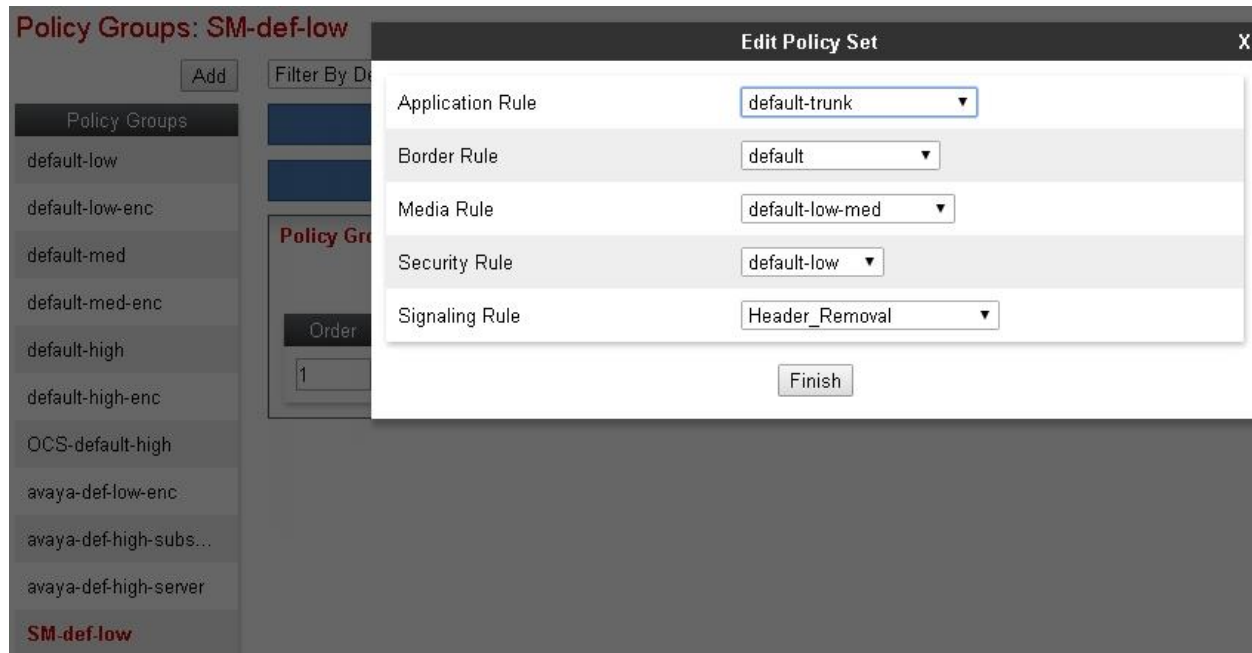
Note: The previous screenshot shows an example of an unnecessary header. During test, the same was done for Alert-Info, AV-Global-Session-ID, Endpoint-View, P-AV-Message-ID, P-Charging-Vector and P-Location.

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

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID				
							Add In Header Control		Add Out Header Control	
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction			
1	Accept-Language	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete	
2	Accept-Language	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete	
3	Alert-Info	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete	
4	Alert-Info	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete	
5	Aw-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete	
6	Aw-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete	
7	Endpoint-View	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete	
8	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete	
9	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete	
10	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete	
11	P-Charging-Vector	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete	
12	P-Charging-Vector	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete	
13	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete	
14	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete	

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

- In the **Group Name** field enter a descriptive name for the Session Manager Policy Group, in this case **SM-def-low**, and click **Next**
- Leave the **Application Rule**, **Border Rule**, **Media Rule** and **Security Rule** fields at their default values
- In the **Signaling** drop down menu, select the recently added signalling rule for the Session Manager (**Header_Removal**)



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 SFR Collecte SIP. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to SFR Collecte SIP and vice versa.

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

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for the Session Manager; in this case **ASM_Call_Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the 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 the 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 the 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 the Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the SFR SIP Trunk defined in **Section 7.6**.
- In the **End Point Policy Group** drop down menu, select the End Point Policy Group that contains the Signalling Rules for the Session Manager defined in **Section 7.8**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.7** and click **Finish**.

Edit Flow: ASM_Call_Server	
Flow Name	ASM_Call_Server
Server Configuration	ASM_Call_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Med
End Point Policy Group	SM-def-low
Routing Profile	Trunk Server
Topology Hiding Profile	ASM
File Transfer Profile	None
Signaling Manipulation Script	None

Finish

To define a Server Flow for SFR Collecte SIP, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for SFR Collecte SIP, in this case a generic name of **Trunk Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the Trunk Server 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 SFR Collecte SIP 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 SFR Collecte SIP 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 SFR Collecte SIP is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the SFR Collecte SIP defined in **Section 7.7** and click **Finish**.

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

Field	Value
Flow Name	Trunk Server
Server Configuration	SP_Trunk_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Med
End Point Policy Group	default-low
Routing Profile	Call Server
Topology Hiding Profile	SFR
File Transfer Profile	None
Signaling Manipulation Script	None

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

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

The screenshot displays the Avaya SBCE web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand navigation menu lists various configuration categories: Routing, Server Configuration, Topology Hiding, Signaling Manipulation, URI Groups, PPM Services, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, Time of Day Rules, End Point Policy Groups, Session Policies, TLS Management, and Device Specific Settings. The "End Point Flows" option is highlighted in red. The main content area is titled "End Point Flows: GSSCP_V9". It features two tabs: "Subscriber Flows" and "Server Flows", with "Server Flows" being the active tab. Below the tabs, there is a section for "Server Configuration: ASM_Call_Server" and another for "Server Configuration: SP_Trunk_Server". Each section contains a table with columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. The "ASM_Call_Server" table has one row with Priority 1, Flow Name "ASM_Call_Server", URI Group "*", Received Interface "Ext_Sig", Signaling Interface "Int_Sig", End Point Policy Group "SM-def-low", and Routing Profile "Trunk Server". The "SP_Trunk_Server" table has one row with Priority 1, Flow Name "Trunk Server", URI Group "*", Received Interface "Int_Sig", Signaling Interface "Ext_Sig", End Point Policy Group "default-low", and Routing Profile "Call Server". Both tables include "View", "Clone", "Edit", and "Delete" action links for each row.

8. Configure SFR Collecte SIP Equipment

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

9. Verification Steps

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

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

Home	Routing	Session Manager	User Management
Session Manager	Dashboard	Session Manager Administration	Communication Profile Editor
Network Configuration	Device and Location Configuration	Application Configuration	System Status
SIP Entity Monitoring	Managed Bandwidth Usage		

Home / Elements / Session Manager / System Status / SIP Entity Monitoring	Help ?
---	--------

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: SM1

Summary View

Status Details for the selected Session Manager:

3 Items Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	CM1	10.10.9.12	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	ASBCE	10.10.9.71	5060	TCP	FALSE	UP	200 OK	UP

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

```
status trunk 1
```

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

- 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 the Session Manager via the Avaya SBCE to the network SBCs are receiving a response.

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

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 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, a sidebar menu lists various configuration categories, with "Trace" highlighted under "Troubleshooting". The main content area is titled "Trace: GSSCP_V9" and features three tabs: "Call Trace", "Packet Capture" (which is active), and "Captures". The "Packet Capture Configuration" form includes the following fields:

Packet Capture Configuration	
Status	Ready
Interface	B1
Local Address <small>IP[Port]</small>	All :
Remote Address <small>*, *Port, IP, IP:Port</small>	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	SP_Trunk_Test1.pcap

At the bottom of the configuration form are two buttons: "Start Capture" and "Clear".

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

Trace: GSSCP_V9

Devices

GSSCP_V9

Call Trace

Packet Capture

Captures

Refresh

File Name	File Size (bytes)	Last Modified	
SP_Trunk_Test1_20141113050837.pcap	0	November 13, 2014 5:08:37 AM CST	Delete

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

10. Conclusion

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

11. Additional References

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

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3, May 2013.
- [2] *Administering Avaya Aura® System Platform*, Release 6.3, May 2013.
- [3] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, May 2013
- [4] *Avaya Aura® Communication Manager 6.3 Documentation library*, August 2013.
- [5] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013
- [6] *Implementing Avaya Aura® System Manager* Release 6.3, May 2013
- [7] *Upgrading Avaya Aura® System Manager to 6.3.2*, May 2013.
- [8] *Administering Avaya Aura® System Manager* Release 6.3, May 2013
- [9] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013
- [10] *Implementing Avaya Aura® Session Manager* Release 6.3, May 2013
- [11] *Upgrading Avaya Aura® Session Manager* Release 6.3, May 2013
- [12] *Administering Avaya Aura® Session Manager* Release 6.3, June 2013,
- [13] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2 June 2013
- [14] *Upgrading Avaya Session Border Controller for Enterprise* Release 6.2 July 2013
- [15] *Administering Avaya Session Border Controller for Enterprise* Release 6.2 March 2013
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2015 Avaya Inc. All Rights Reserved.

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

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