



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

Abstract

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

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

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

1. Introduction

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

2. General Test Approach and Test Results

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

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

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

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Vodafone NL SIP Trunking Service with the following observations:

- Inbound Toll-Free calls were not testing as there was no Inbound Toll-Free access available
- Emergency calls were not tested as no test call was booked with the Emergency Services Operator.
- Hold from the PSTN was handled in the PSTN with no notification to Communication manager that the call was on hold. This is an issue with the PSTN test phones used and is not an interworking issue between Communication manager and the Vodafone NL SIP Trunking Service
- Calls were failing when making a call from the PSTN to an extension with EC500 and answering at the host station. This was resolved by using PRACK handling on the Avaya SBCE so that 183 Session Progress was sent to the network when the host station was ringing as opposed to 180 Ringing with SDP. PRACK handling is defined in the Avaya SBCE Server Interworking described in **Section 7.4**.
- Outbound calls from one-X Communicator were failing initially. This was resolved by configuring the Avaya SBCE to remove P-Conference from outbound SIP messages.
- There was no ringback heard when making calls to one-X Communicator in Other Phone mode when the “Other Phone” was a Communication Manager H.323 extension. This is not a typical use of this feature as the phone used when outside the office would normally be a PSTN phone. Ringback was heard when the “Other Phone” was a PSTN phone, but this issue is noted for information purposes.

2.3. Support

For technical support on Vodafone Netherlands SIP trunking services, contact Vodafone Netherlands support at <http://www.vodafone.nl/midden-groot-bedrijf/oplossingen/>.

3. Reference Configuration

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

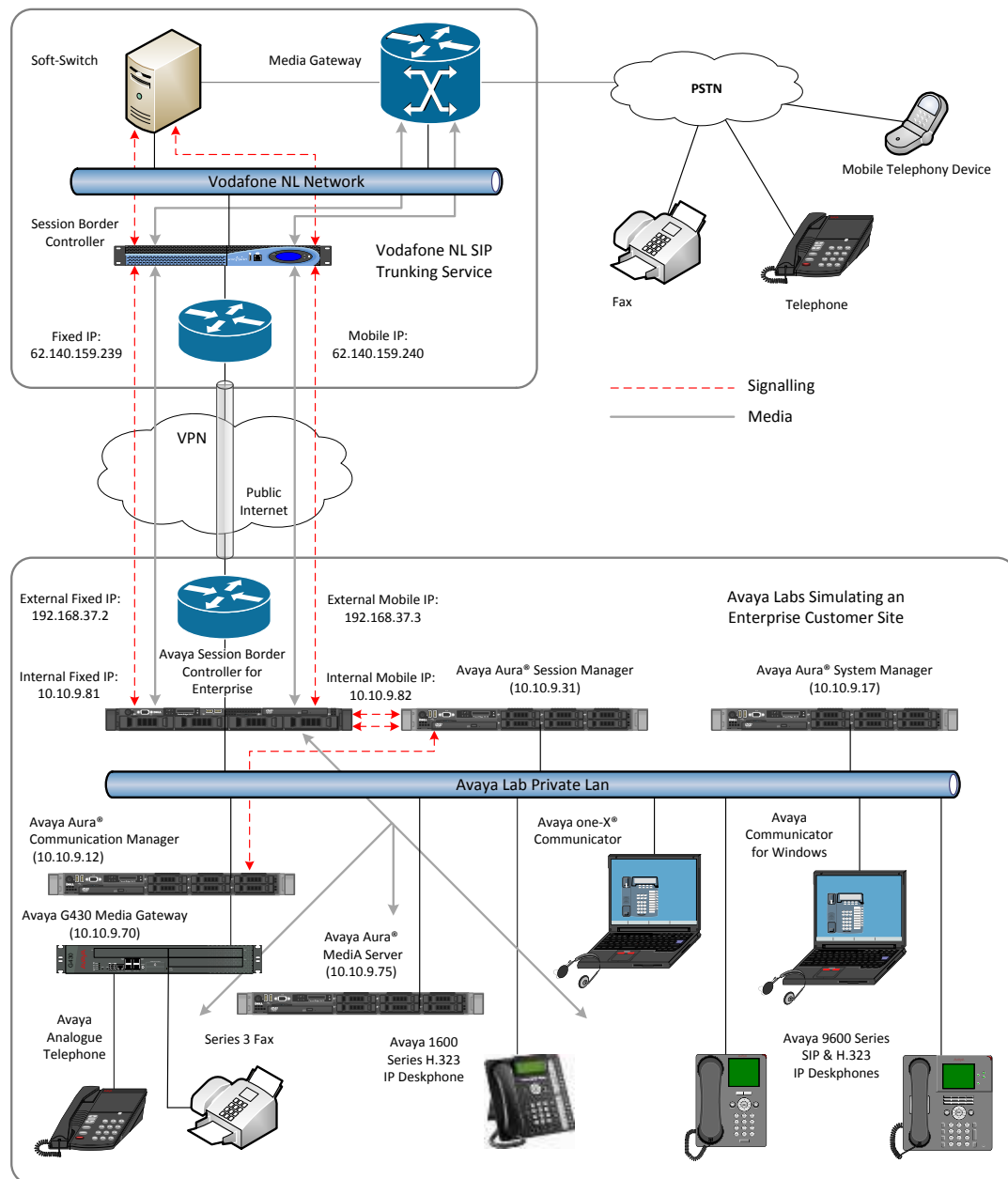


Figure 1: Test Setup Vodafone NL SIP Trunking Service to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Aura® System Manager	7.0.0.0.16266
Avaya Aura® Communication Manager	7.0-441 Build 0.22477
Avaya Session Border Controller for Enterprise	7.0.0-21-6602 Patch sbc700-p001-20151005-7.0.0-21.x86_64.rpm
Avaya Aura® Media Server	7.7.0.236_2015.07.24
Avaya G430 Media Gateway	37.19.0
Avaya 96x0 Phone (SIP)	2_6_14_5
Avaya 9608 Phone (SIP)	7.0.0 R39
Avaya 96x0 Phone (H.323)	3.230A
Avaya 9608 Phone (H.323)	6.3116
Avaya 1616 Phone (H.323)	1.380B
Avaya One-X Communicator	6.2.7.03-SP7
Avaya Communicator for Windows	2.1.2.75
Avaya 2400 Series Digital Handsets	N/A
Analogue Handset	N/A
Analogue Fax	N/A
Vodafone Netherlands	
Acme Packet Net-Net 4500	SCX620m11p4
OneAccess One700	ONEOS11-VOIP_SIP_11N-V4.3R7C11
SIP GW CPE Cisco 2901	VF-CUBE 1.1 (15.3(3)M4)

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 Vodafone NL SIP Trunking Service. For incoming calls, Session Manager receives SIP messages from the Avaya SBCE and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Vodafone NL 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 Vodafone NL SIP Trunking Service and any other SIP trunks used.

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

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

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

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

IP Attendant Consoles? y
```

5.2. Administer IP Node Names

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

```
display node-names ip
                                IP NODE NAMES

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

5.3. Administer IP Network Region

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

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

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

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

5.4. Administer IP Codec Set

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

change ip-codec-set 2		Page 1 of 2	
IP CODEC SET			
Codec Set: 2			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711A	n	2	20
2: G.729A	n	2	20
3:			
4:			

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

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

change ip-codec-set 2		Page 2 of 2	
IP CODEC SET			
Allow Direct-IP Multimedia? n			
	Mode	Redundancy	Packet Size (ms)
FAX	t.38-standard	0	ECM: y
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

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

5.5. Administer SIP Signaling Groups

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

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

- Set **Group Type** to **sip**.
- Set **Transport Method** to **tcp**.
- Set **Peer Detection Enabled** to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Far-end Node Name** to Session Manager interface (node name **Session_Manager** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** as required. The standard value for TCP is **5060**, though **5062** was used in test to separate the SIP Trunk from the SIP endpoints on Session Manager (See **Section 6.5**).
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3** (logically establishes the far-end for calls using this signalling group as region **2**).
- Leave **Far-end Domain** blank (allows Communication Manager to accept calls from any SIP domain on the associated trunk).
- Set **Direct IP-IP Audio Connections** to **y**.
- Set both **H.323 Station Outgoing Direct Media** and **Initial IP-IP Direct Media** to **y** to establish direct media immediately and avoid shuffling during call set-up.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).

The default values for the other fields may be used.

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

5.6. Administer SIP Trunk Group

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

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

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

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

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

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

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

On **Page 4** of this form:

- Set **Send Diversion Headet** to **y**.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Vodafone NL (this Payload Type is not applied to calls from SIP end-points).
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on Communication Manager extension.

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

Note: - The above screenshot shows **Network Call Redirection** set to **y**. Though this was set during testing, it had no effect as “302 Moved Temporarily” and REFER messages are not currently used in the Vodafone NL SIP trunking Service. Note also that during testing **Send Transferring Party Information** was set to **y**. Again, this was not used in the Vodafone NL SIP Trunking call flows.

5.7. Administer Calling Party Number Information

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

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

5.8. Administer Route Selection for Outbound Calls

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

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

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

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

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

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

5.9. Administer Incoming Digit Translation

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

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

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

5.10. EC500 Configuration

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

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** if required by the routing configuration, none was required during testing.
- For the **Phone Number** enter the phone that will also be called (e.g. **0035389434nnnn**).
- Set the **Trunk Selection** to **ars** so that the ARS table will be used for routing.
- Set the **Config Set** to **1**.

change off-pbx-telephone station-mapping 2391								Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION										
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual			
Extension		Prefix			Selection	Set	Mode			
2391	EC500	-		0035389434nnnn	ars	1				

Note: The phone number shown is for a mobile phone in the Avaya Lab. To use facilities for calls coming in from EC500 mobile phones, the calling party number received in Communication Manager must exactly match the number specified in the above table.

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

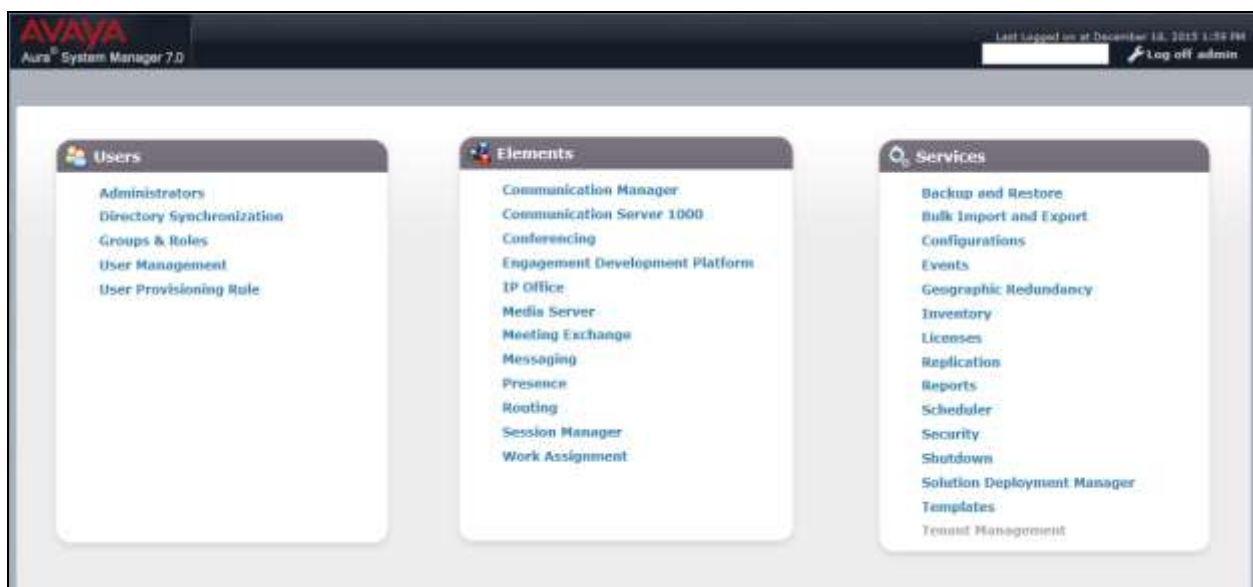
6. Configuring Avaya Aura® Session Manager

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

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

6.1. Log in to Avaya Aura® System Manager

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



6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name of the enterprise site or a name agreed with Vodafone NL; 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' page in a web application. The left sidebar has a 'Routing' menu with sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, and Dial Patterns. The 'Domains' item is selected. The main content area has a breadcrumb 'Home / Elements / Routing / Domains' and a title 'Domain Management'. Below the title are buttons: 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A table below shows '1 Item' with a refresh icon. The table has columns: Name, Type, and Notes. One row is visible with 'avaya.com' in the Name column and 'sip' in the Type column. At the bottom, there is a 'Select' dropdown with options 'All' and 'None'.

Name	Type	Notes
avaya.com	sip	

Note: If the existing domain name used in the enterprise equipment does not match that used in the network, a Session Manager Adaptation can be used to change it (see **Section 6.4**).

6.3. Administer Locations

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

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

Home / Elements / Routing / Locations

Help ?

Location Details

Commit Cancel

General

* Name: Galway

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☐

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

1 Item Filter: Enable

IP Address Pattern	Notes
*10.10.9.x	

Select : All, None

6.4. Administer Adaptations

Calls from Vodafone NL are received at the enterprise in national format with leading “0” on the Request URI. An Adaptation specific to Communication Manager is used to convert the called party number to a pre-defined extension number before onward routing to the Communication Manager SIP Entity and removes the requirement for incoming digit manipulation on Communication Manager.

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

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

Home / Elements / Routing / Adaptations

Adaptation Details

General

* **Adaptation Name:**

* **Module Name:**

Module Parameter Type:

Module Parameter :

Egress URI Parameters:

Notes:

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

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

- Under **Matching Pattern** enter the DDI number as received from the network.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the incoming DDI number.
- Under **Delete Digits** enter the number of digits to delete to leave only the extension number remaining, for testing 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 the testing, 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.

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*+	12	15		1	00	origination		
<input type="checkbox"/>	*+31	12	13		4	0	origination		
<input type="checkbox"/>	*03870nnnn0	10	10		10	2000	destination		
<input type="checkbox"/>	*03870nnnn1	10	10		10	2391	destination		
<input type="checkbox"/>	*03870nnnn2	10	10		10	2291	destination		
<input type="checkbox"/>	*03870nnnn3	10	10		10	2396	destination		
<input type="checkbox"/>	*03870nnnn4	10	10		10	2316	destination		
<input type="checkbox"/>	*03870nnnn5	10	10		10	2400	destination		
<input type="checkbox"/>	*03870nnnn6	10	10		10	2401	destination		
<input type="checkbox"/>	*03870nnnn7	10	10		10	7000	destination		
<input type="checkbox"/>	*03870nnnn8	10	10		10	6099	destination		
<input type="checkbox"/>	*03870nnnn9	10	10		10	6002	destination		

Select : All, None

Commit Cancel

Note: In the above screenshot the DDI numbers are partially obscured. If the number is to be changed to diallable format for display on Communication Manager extensions, additional rows may be required. These would replace a leading “+” with “00” for international calling party numbers and “+31” would be replaced by “0” for national calling party numbers.

An additional Adaptation is required to convert extension numbers to national format. Calls from Communication Manager are received at Session Manager with the extension number in the From header. An Adaptation specific to Vodafone NL is used to convert the calling party number to national format with leading “0” before onward routing to the Vodafone NL SIP Trunking Service.

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

- In the **Adaptation Name** field, enter a descriptive title for the adaptation.
- In the **Module Name** drop down menu, select **DigitConversionAdapter**. This is used for simple digit conversion adaptations.
- In the **Module Parameter Type** drop down menu, select **Single Parameter**.
- In the Module Parameter box, type **fromto=true**. This will apply the adaptation to the From and To headers as well as the Request URI.

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

* **Adaptation Name:** Extn_to_E164

* **Module Name:** DigitConversionAdapter

Module Parameter Type: Single Parameter

Module Parameter : fromto=true x

Egress URI Parameters:

Notes:

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

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

- Under **Matching Pattern** enter the extension number as received from Communication Manager.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the originating extension number.
- Under **Delete Digits** enter the number of digits to delete to remove any digits that will not form part of the national number, during testing 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 testing, this was the full national number with leading “0”. If the extension number forms part of the DDI number, only the necessary prefix digits will be required.
- Under **Address to Modify** choose **origination** from the drop down box to apply this rule to the From and P-Asserted-Identity headers only.

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*2000	*4	*4		*4	03870nnnn0	origination		
<input type="checkbox"/>	*2291	*4	*4		*4	03870nnnn2	origination		
<input type="checkbox"/>	*2316	*4	*4		*4	03870nnnn4	origination		
<input type="checkbox"/>	*2391	*4	*4		*4	03870nnnn1	origination		
<input type="checkbox"/>	*2396	*4	*4		*4	03870nnnn3	origination		
<input type="checkbox"/>	*2400	*4	*4		*4	03870nnnn5	origination		
<input type="checkbox"/>	*2401	*4	*4		*4	03870nnnn6	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 Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu, and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **General**:

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

In this configuration there are five SIP Entities:

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

6.5.1. Avaya Aura® Session Manager SIP Entity

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

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

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

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

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

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

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

6.5.2. Avaya Aura® Communication Manager SIP Entities

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

SIP Entity Details

General

* Name: CM Trunk

* FQDN or IP Address: 10.10.9.12

Type: CM

Notes:

Adaptation: E.164_to_Extn

Location: Galway

Time Zone: Europe/Dublin

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

Credential name:

Securable: ☐

Call Detail Recording: none

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

Loop Detection

Loop Detection Mode: On ▼

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration ▼

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association: ▼

Backup Session Manager Bandwidth Association: ▼

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

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

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

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel Help ?

General

* Name: ASBCE_Fixed

* FQDN or IP Address: 10.10.9.81

Type: SIP Trunk ▼

Notes:

Adaptation: Extn_to_E164 ▼

Location: Galway ▼

Time Zone: Europe/Dublin ▼

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

Credential name:

Securable: ☐

Call Detail Recording: egress ▼

The next screen shows the SIP Entity for the Avaya SBCE used for mobile destinations. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface

used for mobile destinations (see **Figure 1**). Set the **Adaptation**, **Location** and **Time Zone** as for the Avaya SBCE SIP Entity used for PSTN fixed destinations.

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: ASBCE_Mobile

* FQDN or IP Address: 10.10.9.82

Type: SIP Trunk

Notes:

Adaptation: Extn_to_E164

Location: Galway

Time Zone: Europe/Dublin

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

Credential name:

Securable: ☐

Call Detail Recording: egress

6.6. Administer Entity Links

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

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

Home / Elements / Routing / Entity Links

Entity Links

New Edit Delete More Actions

5 Items Filter: Enable

<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 Fixed Link	Session_Manager	TCP	5060	ASBCE_Fixed	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	ASBCE Mobile Link	Session_Manager	TCP	5060	ASBCE_Mobile	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM Entity Link	Session_Manager	TCP	5060	CM_SIP_Endpoints	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM Trunk Link	Session_Manager	TCP	5062	CM Trunk	<input type="checkbox"/>	5062	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Messaging Link	Session_Manager	TCP	5060	Messaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

Select : All, None

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

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

6.7. Administer Routing Policies

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

Under **General**:

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

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

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: CM_Inbound

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM Trunk	10.10.9.12	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item

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

Select: All, None

The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed off-net to PSTN fixed destinations via the Vodafone NL SIP Trunking Service.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE_Fixed	10.10.9.81	SIP Trunk	

Time of Day

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 next screen shows the Routing Policy for the Avaya SBCE interface that will be routed on-net to mobile destinations via the Vodafone NL SIP Trunking Service.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE_Mobile	10.10.9.82	SIP Trunk	

Time of Day

1 Item Filter: Enable

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

Select : All, None

6.8. Administer Dial Patterns

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

Under **General**:

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

Under **Originating Locations and Routing Policies**:

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

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls off-net to PSTN destinations via the Vodafone NL SIP Trunking Service.

The screenshot displays the 'Dial Pattern Details' configuration window. The 'General' tab is active, showing fields for Pattern (0), Min (8), Max (17), Emergency Call (unchecked), Emergency Priority (1), Emergency Type, SIP Domain (set to -ALL-), and Notes. Below this, the 'Originating Locations and Routing Policies' section contains an 'Add' button and a table with one item. The table has columns for Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The single entry shows '-ALL-' as the location, 'Fixed_Outbound' as the policy, rank 0, and 'ASBCE_Fixed' as the destination. A 'Filter: Enable' button is at the top right of the table, and a 'Select : All, None' button is at the bottom left.

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

The next screen shows an example dial pattern configured for the Avaya SBCE which will route the calls on-net to mobile destinations via the Vodafone NL SIP Trunking Service.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Commit] [Cancel] Help ?

General

* Pattern: 78

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

[Add] [Remove]

2 Items Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Galway		Mobile_Outbound	0	<input checked="" type="checkbox"/>	ASBCE_Mobile	

Select : All, None

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

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Commit] [Cancel] Help ?

General

* Pattern: 03870nnnn

* Min: 9

* Max: 10

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-		CM_Inbound	0	<input checked="" type="checkbox"/>	CM Trunk	

Select : All, None

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

6.9. Administer Application for Avaya Aura® Communication Manager

From the **Home** tab select **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration** → **Applications** and click **New** (not shown).

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

The screenshot shows the 'Application Editor' window in the Avaya Aura Communication Manager interface. The left sidebar contains a navigation menu with the following items: Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, and Applications. The 'Applications' item is selected. The main content area displays the 'Application Editor' form. At the top right of the form are 'Commit' and 'Cancel' buttons. The form fields are as follows: 'Name' is a text field containing 'CM_App'; 'SIP Entity' is a dropdown menu showing 'CM_SIP_Endpoints'; 'CM System for SIP Entity' is a dropdown menu showing 'CM1_Element' with a 'Refresh' button next to it; and 'Description' is a text field. There are also links for 'View/Add CM Systems'.

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

6.10. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Session Manager** → **Application Configuration** → **Application Sequences** and click on **New** (not shown).

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

The screenshot shows the 'Application Sequence Editor' window. At the top, there is a breadcrumb trail: 'Home / Elements / Session Manager / Application Configuration / Application Sequences'. The window title is 'Application Sequence Editor' with 'Commit' and 'Cancel' buttons. Below the title, there is a section for 'Application Sequence' with a required 'Name' field containing 'CM_App_Seq' and an empty 'Description' field. Below this is a section titled 'Applications in this Sequence' with 'Move First', 'Move Last', and 'Remove' buttons. It shows '1 Item' in a table with columns: Sequence Order (first to last), Name, SIP Entity, Mandatory, and Description. The table contains one row for 'CM_App' with SIP Entity 'CM_SIP_Endpoints' and 'Mandatory' checked. Below the table is a 'Select : All, None' option. At the bottom is a section titled 'Available Applications' with '1 Item' in a table with columns: Name, SIP Entity, and Description. It contains one row for 'CM_App' with SIP Entity 'CM_SIP_Endpoints'. A '+ CM_App' link is visible to the left of the row. A 'Filter: Enable' link is at the top right of this section. At the bottom left, there is a '*Required' label, and at the bottom right, there are 'Commit' and 'Cancel' buttons.

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

Name	SIP Entity	Description
CM_App	CM_SIP_Endpoints	

6.11. Administer SIP Extensions

The SIP extensions are likely to have been defined during installation. The configuration shown in this section is for reference. SIP extensions are registered with Session Manager and use Communication Manager for their feature and configuration settings. From the **Home** tab select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

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

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

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

The screenshot shows the 'Communication Profile' tab in a configuration window. At the top, there are tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' section has two password fields: 'Communication Profile Password' and 'Confirm Password', both masked with dots. Below these is a 'Name' section with a 'New' button, a 'Delete' button, a 'Done' button, and a 'Cancel' button. The 'Name' list shows 'Primary' selected. Below the list, there is a 'Name' field with 'Primary' entered and a 'Default' checkbox which is checked. At the bottom, there is a 'Communication Address' section with a 'New' button, an 'Edit' button, and a 'Delete' button. Below these buttons is a table with columns 'Type', 'Handle', and 'Domain'. The table is empty, showing 'No Records found'.

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

The screenshot shows the 'Communication Address' section expanded. It has buttons for 'New', 'Edit', and 'Delete'. Below these is a table with columns 'Type', 'Handle', and 'Domain'. The table is empty, showing 'No Records found'. Below the table, there is a 'Type' field with a dropdown menu showing 'Avaya SIP'. Below that is a 'Fully Qualified Address' field with a text input containing '2291' and a domain dropdown menu showing 'avaya.com'. At the bottom right, there are 'Add' and 'Cancel' buttons.

Expand the **Session Manager Profile** section.

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

☒ **Session Manager Profile**

SIP Registration

- * Primary Session Manager

Primary	Secondary	Maximum
4	0	4
- Secondary Session Manager
- Survivability Server
- Max. Simultaneous Devices
- Block New Registration When Maximum Registrations Active? ☐

Application Sequences

- Origination Sequence
- Termination Sequence

Call Routing Settings

- * Home Location
- Conference Factory Set

Call History Settings

- Enable Centralized Call History? ☐

Expand the **Endpoint Profile** section.

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

☒ **CM Endpoint Profile** ▼

* System

CM1_Element ▼

* Profile Type

Endpoint ▼

Use Existing Endpoints ☐

* Extension

Q 2291

Endpoint Editor

* Template

9608SIP_DEFAULT_CM_7_0 ▼

Set Type

9608SIP

Security Code

Port

IP

Voice Mail Number

Preferred Handle

(None) ▼

Calculate Route Pattern ☐

Sip Trunk

aar

Enhanced Callr-Info display for 1-line phones ☐

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

Override Endpoint Name and Localized Name ☒

Allow H.323 and SIP Endpoint Dual Registration ☐

7. Configure Avaya Session Border Controller for Enterprise

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

7.1. Access Avaya Session Border Controller for Enterprise

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



The login screen features the Avaya logo in red on the left. To the right, under the heading "Log In", is a "Username:" label followed by a text input field and a "Continue" button. Below the input field, there is a block of text stating that the system is restricted to authorized users and that unauthorized access is prohibited. Further down, another block of text mentions that system use may be monitored for administrative and security reasons. At the bottom, a copyright notice for 2011-2015 Avaya Inc. is displayed.

AVAYA

Session Border Controller for Enterprise

Log In

Username:

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

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

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

© 2011 - 2015 Avaya Inc. All rights reserved.

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



The dashboard has a dark header bar with navigation links: Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is titled "Session Border Controller for Enterprise" and features the Avaya logo. On the left is a sidebar menu with "Dashboard" selected, listing options like Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main area contains several panels: "Information" with system details (Time, Version, Build Date, License State, etc.), "Installed Devices" showing EMS and GSSCP_V9, and "Alarms (past 24 hours)" and "Incidents (past 24 hours)" both showing "None found".

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise **AVAYA**

Dashboard

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

Dashboard

Information

System Time	09:14:50 AM GMT	Refresh
Version	7.0.0-21-6002	
Build Date	Sun Aug 9 21:08:40 EDT 2015	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	12/01/2015 11:31:58 GMT	
Failed Login Attempts	0	

Installed Devices

EMS
GSSCP_V9

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

7.2. Define Network Management

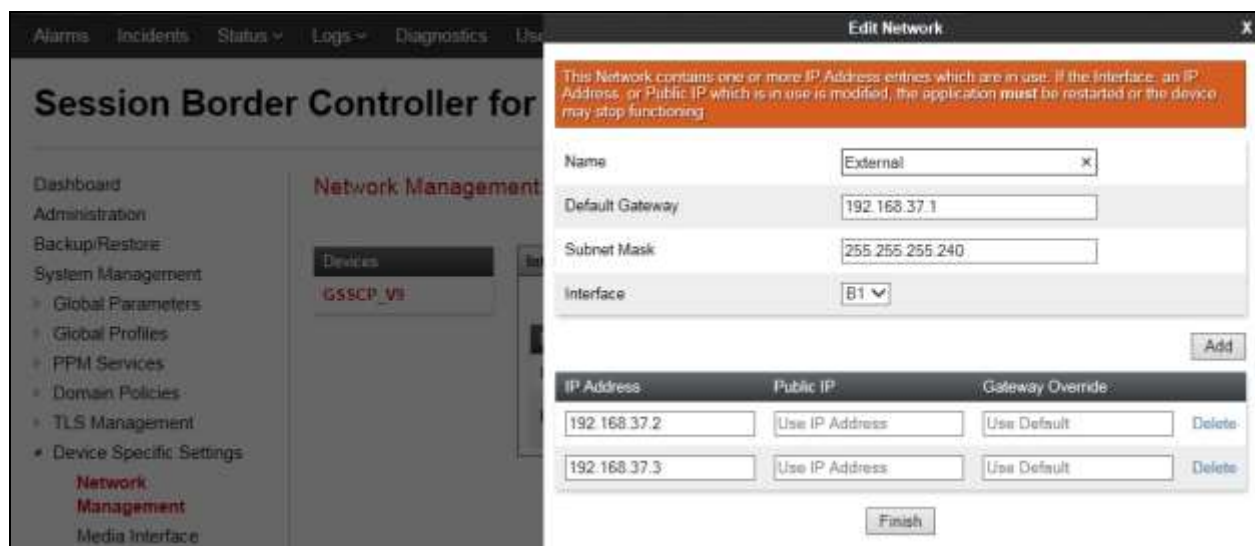
Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one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

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



Enter details for the external interfaces in the dialogue box:

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



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

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

The following screenshot shows the completed Network Management configuration:

Network Management: GSSCP_V9

Devices: GSSCP_V9

Interfaces Networks

Add

Name	Gateway	Subnet Mask	Interface	IP Address	Edit	Delete
Internal	10.10.9.1	255.255.255.0	A1	10.10.9.81, 10.10.9.82	Edit	Delete
External	192.168.37.1	255.255.255.240	B1	192.168.37.2, 192.168.37.3	Edit	Delete

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

Network Management: GSSCP_V9

Devices: GSSCP_V9

Interfaces Networks

Add VLAN

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

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

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

A status box will appear that will indicate when the restart is complete.

7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces. Testing was carried out with TCP used for transport of signalling between Session Manager and the Avaya SBCE, and UDP for transport of signalling between the Avaya SBCE and the Vodafone NL SIP Trunking Service. Two signalling and two media interfaces were required on both the internal and external sides of the Avaya SBCE to handle on-net and off-net traffic. This document shows the configuration for TCP and UDP, if additional security is required, it's recommended to use TLS and port 5061.

7.3.1. Signalling Interfaces

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

- Select **Add** and enter details of the external signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP addresses **192.168.37.2** for off-net PSTN signalling and **192.168.37.3** for on-net mobile signalling.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for the Vodafone NL SIP Trunking Service.

The screenshot shows the 'Session Border Controller for VoIP' configuration interface. On the left is a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. Under 'Device Specific Settings', 'Signaling Interface' is highlighted. The main area shows 'Signaling Interface: Global Parameters' with a 'Devices' dropdown set to 'GSSCP_V9'. A modal dialog box titled 'Edit Signaling Interface' is open, showing the following fields: Name (External_Foxed), IP Address (External (B1, VLAN 0) with a dropdown showing 192.168.37.2), TCP Port (Leave blank to disable), UDP Port (5060), TLS Port (Leave blank to disable), TLS Profile (None), Enable Shared Control (checkbox), and Shared Control Port. A 'Finish' button is at the bottom right of the dialog.

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

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

The following screenshot shows details of the signalling interfaces:

Signaling Interface: GSSCP_V9

Devices
GSSCP_V9

Signaling Interface

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

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Internal_Fixed	10.10.9.81 Internal (A1, VLAN 0)	5060	---	---	None	Edit Delete
External_Fixed	192.168.37.2 External (B1, VLAN 0)	---	5060	---	None	Edit Delete
Internal_Mobile	10.10.9.82 Internal (A1, VLAN 0)	5060	---	---	None	Edit Delete
External_Mobile	192.168.37.3 External (B1, VLAN 0)	---	5060	---	None	Edit Delete

Note: In the test environment, the internal IP addresses were **10.10.9.81** for off-net PSTN signalling and **10.10.9.82** for on-net mobile signalling.

7.3.2. Media Interfaces

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

- Select **Add** and enter details of the external media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP addresses **192.168.37.2** for off-net PSTN media and **192.168.37.3** for on-net mobile media.
- Define the RTP **Port Range** for the media path with the Vodafone NL SIP Trunking Service, during testing this was left at the default values.

Media Interface: GSSCP_V9

Dashboard
Administration
Backup/Restore
System Management
▶ Global Parameters
▶ Global Profiles
▶ PPM Services
▶ Domain Policies
▶ TLS Management
▶ Device Specific Settings
 Network Management
 Media Interface

Devices
GSSCP_V9

Edit Media Interface X

Name: External_Fixed x

IP Address: External (B1, VLAN 0) v
192.168.37.2 v

Port Range: 35000 - 40000

Finish

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

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

The following screenshot shows details of the media interfaces:

Media Interface: GSSCP_V9

Devices

GSSCP_V9

Media Interface

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

Add

Name	Media IP Network	Port Range	Edit	Delete
Internal_Fixed	10.10.9.81 Internal (A1, VLAN 0)	35000 - 40000	Edit	Delete
External_Fixed	192.168.37.2 External (B1, VLAN 0)	35000 - 40000	Edit	Delete
Internal_Mobile	10.10.9.82 Internal (A1, VLAN 0)	35000 - 40000	Edit	Delete
External_Mobile	192.168.37.3 External (B1, VLAN 0)	35000 - 40000	Edit	Delete

Note: In the test environment, the internal IP addresses were **10.10.9.81** for off-net PSTN media and **10.10.9.82** for on-net mobile media.

7.4. Define Server Interworking

Server interworking is defined for servers connected to the Avaya SBCE. The Vodafone NL SIP Trunking Service has two separate interfaces, one for off-net PSTN traffic and the other for on-net mobile traffic. Each of these is defined as a separate server. The server interworking, however, is the same so only one server interworking profile needs to be defined. Session Manager has a single signalling interface and requires its own server interworking profile.

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

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

Domain DoS

Server Interworking

Interworking Profiles: VFNL

Add

Interworking Profile

Profile Name

VFNL

Next

Configuration of interworking includes Hold support, T.38 fax support and SIP extensions. In the General dialogue box shown in the screenshot, define the interworking as follows:

- Check the **Prack Handling** and **Allow 18X SDP** boxes to convert 180 Ringing with SDP to 183 Session Progress with SDP. This works around an issue with EC500 calls described in **Section 2.2**.
- Check the **T.38 Support** box.
- During testing, the rest of the parameters were left at default values.

Interworking Profile X

General

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

Back Next

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

In the final dialogue box, ensure that **Both Sides** is selected for **Record Routes** and that the **Has Remote SBC** box is checked. Note that Avaya extensions are not supported for the SIP Trunk. Click on **Finish**

Repeat the process to define Server Interworking for Session Manager. The configuration is the same apart from **Prack Handling** which is not required for Session manager. The following screenshot shows the **General** tab.

The screenshot shows the 'Interworking Profiles: ASM' configuration page. On the left is a sidebar with a list of profiles: cs2100, avaya-nu, OCS-Edge-Server, cisco-ccm, cups, Sipera-Halo, OCS-FrontEnd-Server, **ASM** (highlighted in red), and VFNL. The main area has a title bar with 'Add', 'Rename', 'Clone', and 'Delete' buttons. Below the title bar is a blue bar with the text 'Click here to add a description'. The 'General' tab is selected, showing a table of configuration options.

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

An 'Edit' button is located at the bottom right of the configuration area.

The next screenshot is the **Advanced** tab. This was left at default values.

The screenshot shows the 'Interworking Profiles: ASM' configuration page with the 'Advanced' tab selected. The sidebar and title bar are the same as in the previous screenshot. The 'Advanced' tab shows a table of configuration options.

Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
DTMF	
DTMF Support	None

An 'Edit' button is located at the bottom right of the configuration area.

7.5. Define Servers

A server definition is required for each server connected to the Avaya SBCE. The Vodafone NL SIP Trunking service has two separate interfaces for off-net PSTN traffic and on-net mobile traffic. Each of these is connected as a separate Trunk Server. Session Manager has a single signalling interface and is connected as a Call Server.

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

The screenshot shows the 'Add Server Configuration Profile' dialog box. The 'Profile Name' field contains 'VFNL_Fixed'. Below the field is a 'Next' button. The background shows the 'Server Configuration' menu with 'VFNL_Fixed' selected.

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

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

The screenshot shows the 'Edit Server Configuration Profile - General' dialog box. The 'Server Type' dropdown is set to 'Trunk Server'. Below it is an 'Add' button. The 'IP Address / FQDN' field contains '62.140.159.239', the 'Port' field contains '5060', and the 'Transport' dropdown is set to 'UDP'. There is a 'Delete' button next to the 'Transport' dropdown. At the bottom are 'Back' and 'Next' buttons.

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

The image shows two side-by-side configuration dialog boxes. The left box is titled 'Add Server Configuration Profile - Authentication' and contains fields for 'Enable Authentication' (checkbox), 'User Name', 'Realm' (with a note '(Leave blank to detect from server challenge)'), 'Password', and 'Confirm Password'. The right box is titled 'Add Server Configuration Profile - Heartbeat' and contains fields for 'Enable Heartbeat' (checkbox), 'Method' (dropdown menu), 'Frequency' (text input with 'seconds' unit), 'From URI', and 'To URI'. Both boxes have 'Back' and 'Next' buttons at the bottom.

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

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

The image shows the 'Add Server Configuration Profile - Advanced' dialog box. It contains the following fields: 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (dropdown menu showing 'VFNL'), 'Signaling Manipulation Script' (dropdown menu showing 'None'), 'Connection Type' (dropdown menu showing 'SUBID'), and 'Securable' (checkbox). At the bottom are 'Back' and 'Finish' buttons.

Repeat the above process to define the trunk server for the on-net mobile traffic. The screenshot below shows the **General** tab for the completed configuration. Ensure that the **Interworking Profile** defined for Vodafone NL in **Section 7.4** is selected in the **Advanced** tab.

The image shows the 'Server Configuration: VFNL_Mobile' dialog box with the 'General' tab selected. The 'Server Type' is set to 'Trunk Server'. Below this is a table with the following data:

IP Address / FQDN	Port	Transport
62.140.159.240	5060	UDP

There are 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' buttons visible in the interface.

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

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

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

The screenshot shows the 'General' tab of the 'Server Configuration: CPE' dialog. On the left, a sidebar lists 'Server Profiles' with 'CPE', 'VFNL_Fixed', and 'VFNL_Mobile'. The main area has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing 'Server Type' as 'Call Server'. Below this is a table with columns 'IP Address / FQDN', 'Port', and 'Transport'. The table contains one row with values '10.10.9.31', '5060', and 'TCP'. An 'Edit' button is at the bottom right of the table. At the top right of the dialog are 'Rename', 'Clone', and 'Delete' buttons.

IP Address / FQDN	Port	Transport
10.10.9.31	5060	TCP

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

The screenshot shows the 'Advanced' tab of the 'Server Configuration: CPE' dialog. The sidebar and 'General' tab are the same as in the previous screenshot. The 'Advanced' tab is active, showing several configuration options: 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (dropdown set to 'ASM'), 'Signaling Manipulation Script' (dropdown set to 'None'), 'Connection Type' (dropdown set to 'SUBID'), and 'Securable' (checkbox). An 'Edit' button is at the bottom right of the main area. 'Rename', 'Clone', and 'Delete' buttons are at the top right of the dialog.

7.6. Define Routing

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

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

The screenshot shows a web interface for configuring routing profiles. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Server Interworking, Media Forking, and Routing. The main area is titled 'Routing Profiles: VFNL_Fixed'. It contains an 'Add' button, a 'Routing Profiles' dropdown menu showing 'default', and a 'Routing Profile' button. A modal dialog box titled 'Routing Profile' is open, showing a 'Profile Name' field with the value 'VFNL_Fixed' and a 'Next' button.

Click on **Next** and enter details for the Routing Profile for the off-net PSTN trunk:

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

The screenshot shows the 'Routing Profile' dialog box with various configuration options. The 'URI Group' is set to '*'. The 'Time of Day' is set to 'default'. The 'Load Balancing' is set to 'Priority'. The 'NAPTR' checkbox is unchecked. The 'Transport' is set to 'None'. The 'Next Hop Priority' checkbox is checked. The 'Next Hop In-Dialog' checkbox is unchecked. The 'Ignore Route Header' checkbox is unchecked. The 'Add' button is visible. Below these options is a table with columns: Priority / Weight, Server Configuration, Next Hop Address, Transport, and a Delete button. The table contains one row with the following values: 1, VFNL_Fixed, 62.140.159.239:5060 (UDP), None, and a Delete button. At the bottom are 'Back' and 'Finish' buttons.

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	VFNL_Fixed	62.140.159.239:5060 (UDP)	None	Delete

Repeat the above process for the Routing Profile for the on-net mobile trunk. The screenshot over the page shows the completed configuration.

Routing Profiles: VFNL_Mobile

Buttons: Add, Rename, Clone, Delete

Click here to add a description

Routing Profile

Buttons: Update Priority, Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	62.140.159.240	UDP

Buttons: Edit, Delete

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

Routing Profiles: LAN

Buttons: Add, Rename, Clone, Delete

Click here to add a description

Routing Profile

Buttons: Update Priority, Add

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

Buttons: Edit, Delete

7.7. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop or external interfaces.

To define Topology Hiding for the Vodafone NL SIP Trunking Service, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side. Click on **Add** to bring up a dialogue box, assign an appropriate name and click on **Next** to configure Topology Hiding for each header as required:

Topology Hiding Profiles: VFNL

Buttons: Add

Click here to add a description

Topology Hiding

Header	Criteria	Replace Action
--------	----------	----------------

Topology Hiding Profile X

Profile Name: VFNL

Buttons: Next

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

- Click on **Add Header** and select from the **Header** drop down menu.
- Select **IP** or **IP/Domain** from the **Criteria** drop down menu depending on requirements. During testing **IP** was used for the From header so that the domain name of “anonymous.invalid” for CLI restricted calls was not overwritten.
- Leave the **Replace Action** at the default value of **Auto** unless a specific domain name is required. In this case, select **Overwrite** and define a domain name in the **Overwrite Value** field.
- Topology hiding was defined for all headers where the function is available.

The screenshot shows a window titled "Topology Hiding Profile" with a close button (X) in the top right corner. Inside the window, there is a table with four columns: "Header", "Criteria", "Replace Action", and "Overwrite Value". The "Header" column has a dropdown menu with "Request-Line" selected. The "Criteria" column has a dropdown menu with "IP/Domain" selected. The "Replace Action" column has a dropdown menu with "Auto" selected. The "Overwrite Value" column is empty. To the right of the table is a "Delete" button. Above the table is an "Add Header" button. Below the table are "Back" and "Finish" buttons.

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

The following screenshot shows the completed **Topology** Hiding configuration for the Vodafone NL SIP Trunking Service.

The screenshot shows a web interface titled "Topology Hiding Profiles: VFNL". On the left, there is a sidebar with a list of profiles: "default", "cisco_th_profile", "ASM", and "VFNL" (highlighted in red). Above the sidebar is an "Add" button. To the right of the sidebar, there is a table with the following columns: "Header", "Criteria", "Replace Action", and "Overwrite Value". The table contains the following rows:

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

Below the table is an "Edit" button. Above the table, there is a "Click here to add a description." link. To the right of the table, there are "Rename", "Clone", and "Delete" buttons.

To define Topology hiding for Session Manager, follow the same process. This can be simplified by cloning the profile defined for the Vodafone NL SIP Trunking Service. Do this by highlighting the profile defined for the Vodafone NL and clicking on **Clone**. Enter an appropriate name for Session Manager and click on Next. Make any changes where required, in the test environment the settings were left at the same values.

Topology Hiding Profiles: ASM

Buttons: Add, Rename, Clone, Delete

Left sidebar: Topology Hiding Profiles, default, cisco_th_profile, **ASM**, VFNL

Click here to add a description.

Topology Hiding

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

Edit

7.8. End Point Policy Groups

End Point Policy Groups are used to bring together a number of different rules for use in a server flow described in **Section 7.10**. The Vodafone NL SIP Trunking Service was tested with a signalling rule to remove unnecessary and Avaya proprietary SIP headers. This was not necessary for the effective functioning of the SIP Trunk but was used to reduce the SIP message size.

7.8.1. Signalling Rules

Signalling rules are used to handle any non-standard signalling that may be encountered on a SIP Trunk, in this case the transmission of Avaya proprietary and unnecessary SIP message headers from the Avaya equipment.

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

Signaling Rules: Header_Removal_ASM

Buttons: Add, Filter By Device...

Left sidebar: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, **Signaling Rules**

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

Click here to add a description.

General, Requests, Responses, Request Headers, Resp...

Inbound

Requests Allow

Signaling Rule X

Rule Name: Removal_ASM x

Next

Click **Next** three times to scroll through the set-up dialogue boxes leaving the fields at their default values, then click on **Finish**. Highlight the resultant Signalling rule and click on **Edit**.

The image shows three overlapping 'Signaling Rule' configuration windows. The leftmost window displays the 'Inbound' and 'Outbound' sections with dropdown menus for 'Requests', 'Non-2XX Final Responses', 'Optional Request Headers', and 'Optional Response Headers'. The middle window shows the 'Content-Type Policy' section with 'Enable Content-Type Checks' checked and 'Action' set to 'Allow'. The rightmost window shows the 'QoS' section with 'Enabled' checked, 'ToS' selected, and 'Precedence' set to 'Routine'. The bottom window shows the 'UCID' section with 'Enabled' unchecked, 'Node ID' empty, and 'Protocol Discriminator' set to '0x00'. Each window has 'Back' and 'Next' or 'Finish' buttons.

Click on the **Request Headers** tab and then click on **Add Out Header Control** (not shown).

The 'Add Header Control' dialog box is shown with the following configuration: 'Proprietary Request Header' is checked; 'Header Name' is 'P-Location'; 'Method Name' is 'ALL'; 'Header Criteria' has 'Forbidden' selected; 'Presence Action' is 'Remove header'; and the status is '486 Busy Here'. A 'Finish' button is at the bottom.

The example on the previous page shows the configuration to remove the P-Location header. This is proprietary so the Proprietary Request Header box must be checked.

- Type the header name as it appears in the signalling
- Select the **Method Name** from the drop down menu, the example shows **ALL**.
- Check the **Forbidden** button in the **Header Criteria** menu.
- Select **Remove Header** from the **Presence Action** drop down menu.

The following screenshot shows the applied Request Header removal:

Signaling Rules: Header_Removal_ASM

Add Filter By Device Rename Clone Delete

Click here to add a description

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

Add In Header Control Add Out Header Control

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

Response headers are defined in the same way as request headers. The screenshot shows the additional drop down menu for **Response Code**. During testing this was applied to **1XX**, **2XX** and **4XX** response codes as required. The removal of the P-Location header from **4XX** messages is shown as an example:

Add Header Control

Proprietary Response Header ☒

Header Name P-Location

Response Code 4XX

Method Name ALL

Header Criteria ☒ Forbidden ☐ Mandatory ☐ Optional

Presence Action Remove header

486 Busy Here

Finish

The screenshot below shows the applied Response Header removal:

Signaling Rules: Header_Removal_ASM

Add Filter By Device

Rename Clone Delete

Click here to add a description.

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

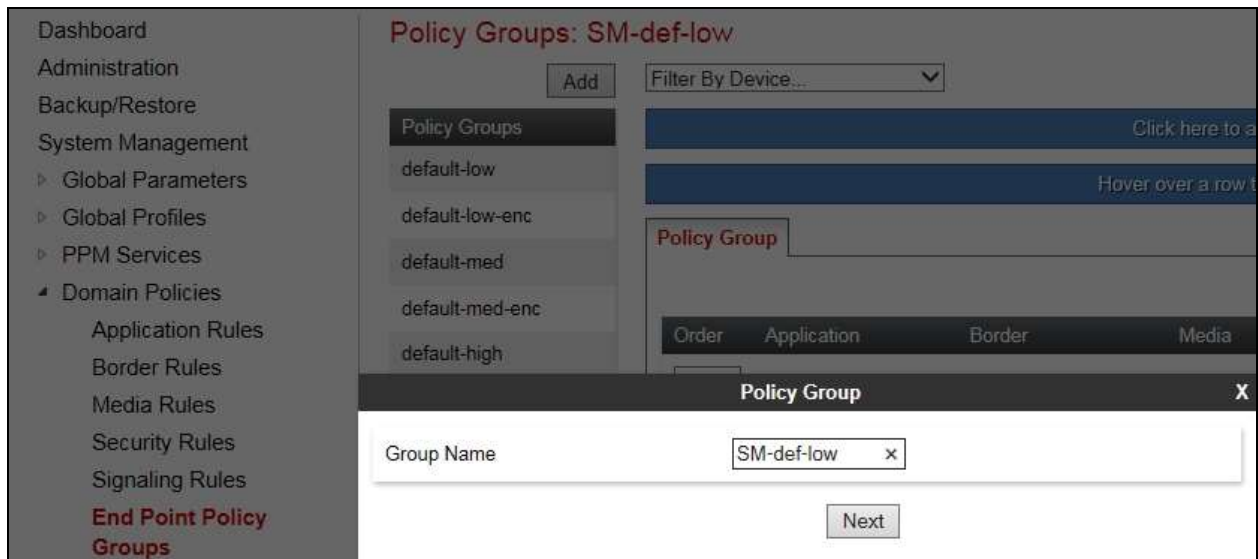
Add In Header Control Add Out Header Control

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

Note: The header removal signalling rule shown was applied to headers seen in the signalling during testing. As mentioned previously, this is not necessary for the functioning of the SIP Trunk, but can be used as a tool to reduce message size.

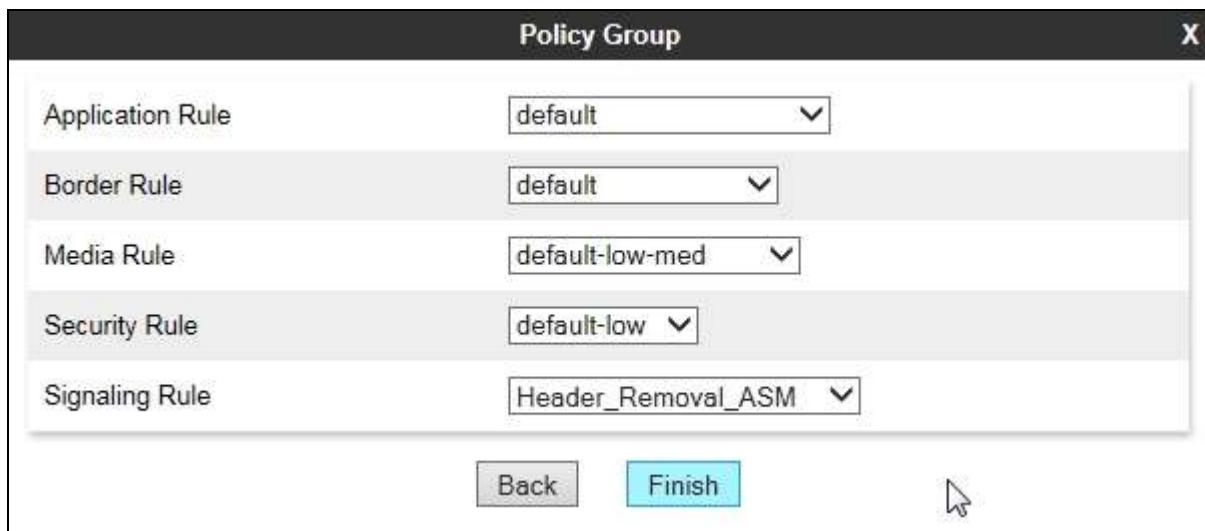
7.8.2. End Point Policy Group

An End Point Policy Group is required to implement the signalling rule. To define one for use in the Session Manager server flow, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up box.



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

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



7.9. Server Flows

Server Flows combine the previously defined profiles into three End Point Server Flows, two for the Vodafone NL SIP Trunking Service and one for Session Manager. The Vodafone NL SIP Trunking Service requires one End Point Server Flow for the off-net PSTN traffic and another for the on-net mobile traffic. These End Point Server Flows allow calls to be routed from Session Manager to the Vodafone NL SIP Trunks and vice versa.

To define a Server Flow for the Vodafone NL off-net PSTN trunk, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for the Vodafone NL off-net PSTN trunk, in the test environment **VFNL_Fixed** was used.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the off-net PSTN trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the off-net PSTN trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for the off-net PSTN trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Vodafone NL SIP Trunking Service defined in **Section 7.7** and click **Finish**.

The screenshot shows a dialog box titled "Add Flow" with a close button (X) in the top right corner. The dialog contains several configuration fields, each with a label and a value or dropdown menu:

Field	Value
Flow Name	VFNL_Fixed
Server Configuration	VFNL_Fixed
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal_Fixed
Signaling Interface	External_Fixed
Media Interface	External_Fixed
End Point Policy Group	default-low
Routing Profile	LAN
Topology Hiding Profile	VFNL
Signaling Manipulation Script	None
Remote Branch Office	Any

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

To define a Server Flow for the Vodafone NL on-net mobile trunk, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for the Vodafone NL on-net mobile trunk, in the test environment **VFNL_Mobile** was used.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the on-net mobile trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the on-net mobile trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for the on-net mobile trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Vodafone NL SIP Trunking Service defined in **Section 7.7** and click **Finish**.

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

Field	Value
Flow Name	VFNL_Mobile
Server Configuration	VFNL_Mobile
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal_Mobile
Signaling Interface	External_Mobile
Media Interface	External_Mobile
End Point Policy Group	default-low
Routing Profile	LAN
Topology Hiding Profile	VFNL
Signaling Manipulation Script	None
Remote Branch Office	Any

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

To define a Server Flow for Session Manager for the off-net PSTN traffic, 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 off-net PSTN server flow for Session Manager, in the test environment **CPE_Fixed** was used.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that off-net PSTN signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that off-net PSTN signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that off-net PSTN media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Vodafone NL SIP Trunking Service defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.7** and click **Finish**.

The screenshot shows a window titled "Add Flow" with a close button (X) in the top right corner. The window contains a list of configuration fields, each with a label and a corresponding input field or dropdown menu. The fields are as follows:

Field Label	Value
Flow Name	CPE_Fixed
Server Configuration	CPE
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	External_Fixed
Signaling Interface	Internal_Fixed
Media Interface	Internal_Fixed
End Point Policy Group	SM-def-low
Routing Profile	VFNL_Fixed
Topology Hiding Profile	ASM
Signaling Manipulation Script	None
Remote Branch Office	Any

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

To define a Server Flow for Session Manager for the on-net mobile traffic, 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 on-net mobile server flow for Session Manager, in the test environment **CPE_Mobile** was used.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that on-net mobile signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that on-net mobile signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that on-net mobile media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Vodafone NL SIP Trunking Service defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.7** and click **Finish**.

Add Flow	
Flow Name	CPE_Mobile
Server Configuration	CPE
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	External_Mobile
Signaling Interface	Internal_Mobile
Media Interface	Internal_Mobile
End Point Policy Group	SM-def-low
Routing Profile	VFNL_Mobile
Topology Hiding Profile	ASM
Signaling Manipulation Script	None
Remote Branch Office	Any
Finish	

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

End Point Flows: GSSCP_V9

Devices
GSSCP_V9

Subscriber Flows
Server Flows

Add

Hover over a row to see its description.

Server Configuration: CPE

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	CPE_Fixed	*	External_Fixed	Internal_Fixed	SM-def-low	VFNL_Fixed	View Clone Edit Delete
2	CPE_Mobile	*	External_Mobile	Internal_Mobile	SM-def-low	VFNL_Mobile	View Clone Edit Delete

Server Configuration: VFNL_Fixed

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	VFNL_Fixed	*	Internal_Fixed	External_Fixed	default-low	LAN	View Clone Edit Delete

Server Configuration: VFNL_Mobile

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	VFNL_Mobile	*	Internal_Mobile	External_Mobile	default-low	LAN	View Clone Edit Delete

8. Configure the Vodafone NL SIP Trunking Service Equipment

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

9. Verification Steps

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

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

SIP Entity Name	SIP Entity Received IP	Port	Proto	Deny	Conn. Status	Reason Code	Link Status
CM_SIP_Endpoints	10.10.9.12	5060	TCP	FALSE	UP	200 OK	UP
ASBCE_Fixed	10.10.9.81	5060	TCP	FALSE	UP	200 OK	UP
CM_Trunk	10.10.9.12	5062	TCP	FALSE	UP	200 OK	UP
ASBCE_Mobile	10.10.9.82	5060	TCP	FALSE	UP	200 OK	UP
Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP

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

```
status trunk 2
```

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

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

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

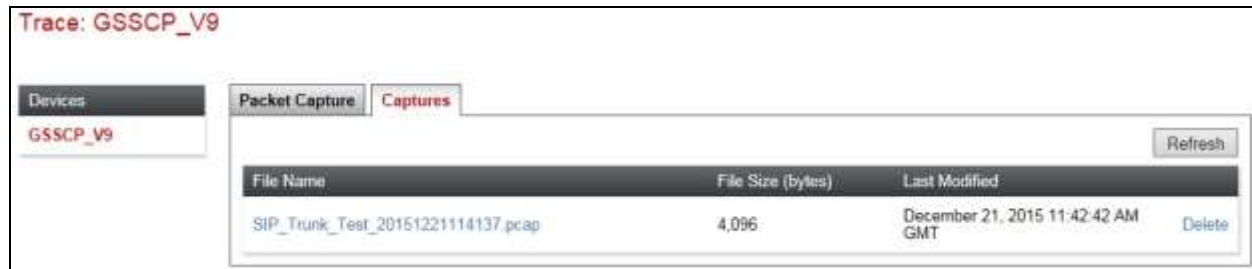
- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select the signalling interface IP address or **All** from the **Local Address** drop down menu.
- Enter the IP address of the network SBC in the **Remote Address** field or enter a * to capture all traffic.
- Specify the **Maximum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

The screenshot displays the 'Packet Capture Configuration' window in the Avaya SBCE interface. The left-hand navigation pane lists various system management options, with 'Trace' highlighted under the 'Troubleshooting' section. The main window title is 'Trace: GSSCP_V9'. Below this, there are two tabs: 'Packet Capture' (active) and 'Captures'. The configuration form contains the following fields and values:

- Status:** Ready
- Interface:** B1 (selected from a dropdown)
- Local Address (IP Port):** All (selected from a dropdown)
- Remote Address:** * (entered in the text field)
- Protocol:** All (selected from a dropdown)
- Maximum Number of Packets to Capture:** 10000 (entered in the text field)
- Capture Filename:** SIP_Trunk_Test.pcap (entered in the text field, with a note: 'Using the name of an existing capture will overwrite it')

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

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



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

10. Conclusion

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

11. Additional References

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

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

©2016 Avaya Inc. All Rights Reserved.

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

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