



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R7.0 as an Evolution Server, Avaya Aura® Session Manager R7.0 and Avaya Session Border Controller for Enterprise R7.1 to support Virgin Media SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Virgin Media SIP Trunk Service and an Avaya SIP enabled enterprise solution.

The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server. Virgin Media 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 Virgin Media's SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Customers using this Avaya SIP-enabled enterprise solution with Virgin Media SIP Trunk are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

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

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 PSTN calls to various phone types including H.323, SIP, digital and analogue telephones at the enterprise. Calls were routed to the enterprise across the SIP trunk from Virgin Media Business.
- Outgoing PSTN calls from various phone types including H.323, SIP and analogue telephones at the enterprise. Calls were routed from the enterprise across the SIP trunk to Virgin Media Business.
- Direct IP-to-IP media with SIP and H.323 telephones
- Calls using the G.711A and G.711MU codecs
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38 and G.711 pass-through fax transmissions.
- Outgoing calls from the enterprise site completed via Virgin Media's SIP Trunk to UK Emergency Call handling 999, 112 and 18000 Text Direct
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, call mute, transfer, and conference.
- Off-net call forwarding and mobile twinning.

- Transmission and response of SIP OPTIONS messages sent by Virgin Media's SIP Trunk requiring Avaya response and sent by Avaya requiring Virgin Media response

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for Virgin Media's SIP Trunk Service with the following observations:

- The Virgin Media SIP Trunk was unable to handle outbound SIP Invites/messages with an Avaya proprietary parameter in the Contact header. The parameter "+avaya-cm-keep-mpro" is present with a value of "no" when Initial IP-IP Direct Media is enabled on Communication Manager SIP Trunk. A SigMa script on the Avaya SBCE was required to remove the parameter "+avaya-cm-keep-mpro". The details of the SigMa script and how to configure the script on the Avaya SBCE are outlined in **Section 7.2.7**.
- At the time of testing, the Virgin Media Business SIP trunk was not configured to support the G.729 codec.
- Inbound and outbound fax was tested successfully using T.38 and G.711 pass-through protocols however T.38 is the preferred fax protocol supported by Avaya.
- Network quality issues were encountered when testing outbound T.38 fax and the fax transmission was unreliable; however, further retesting of fax proved reliable quality of T.38 transmissions.
- The conferencing of outbound calls from Avaya Communicator for Windows was not tested. The softphone requires the use of a conferencing server that was not available at the time of testing.
- Inbound Toll-Free calls were not tested as no Toll-Free access was available for test.

2.3. Support

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

For technical support on Virgin Media Business products please contact the following website: <http://www.virginmediabusiness.co.uk/help/s/>

3. Reference Configuration

The following equipment in **Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to Virgin Media's SIP Trunk Service. Located at the Enterprise site is an Avaya Session Border Controller for Enterprise, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration were Avaya One-X® Communicator and Avaya Communicator for Windows soft phones running on a laptop PC.

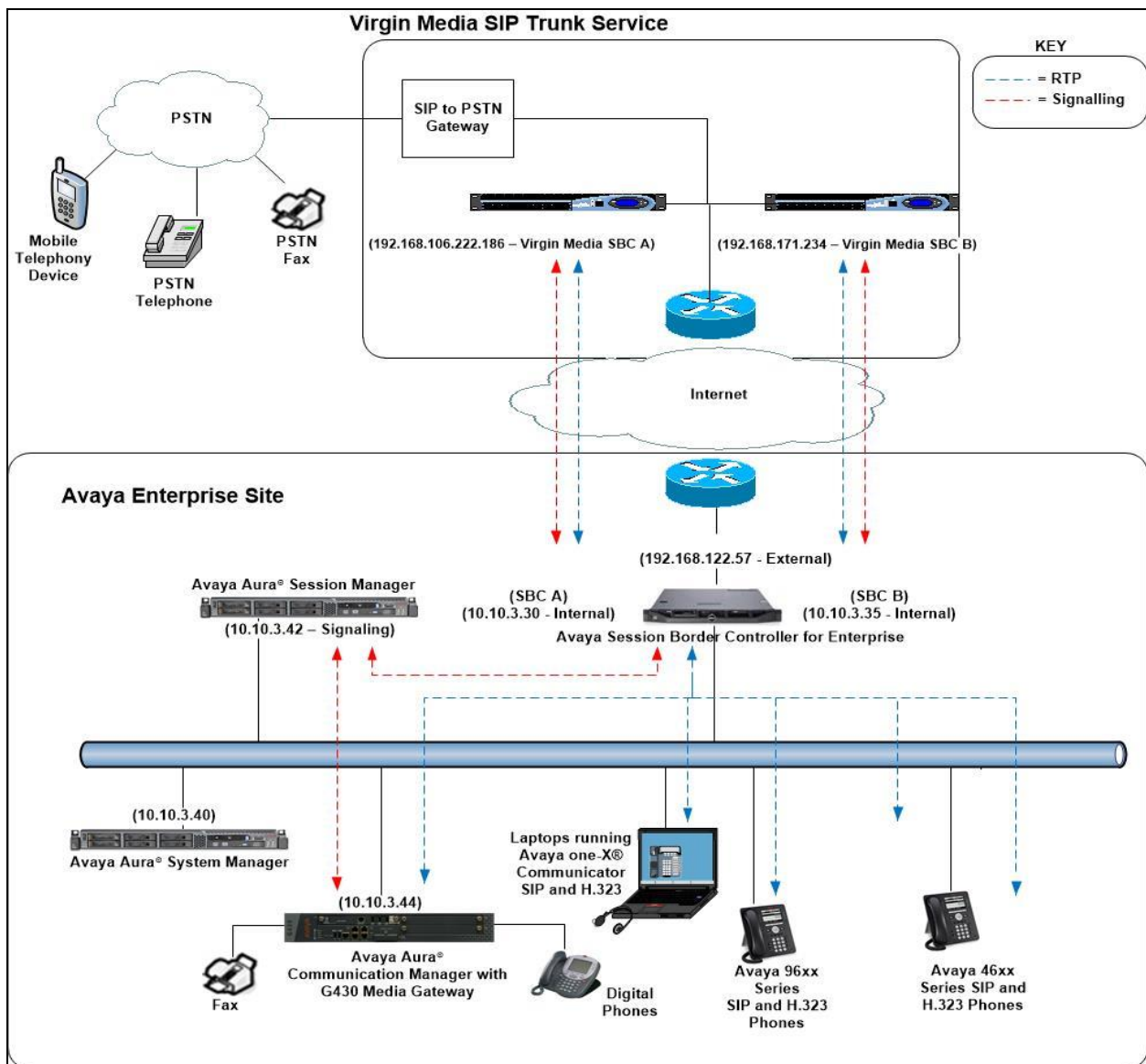


Figure 1: Test Setup Virgin Media SIP Trunk to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Dell PowerEdge R620 running System Manager on VM Version 8	7.0.1.2 - Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.2.086007 Service Pack 2
Dell PowerEdge R620 running Session Manager on VM Version 8	7.0.1.2.701230
Avaya S8300D Server running Avaya Aura® Communication Manager	R017x.00.0.441.0 (23523)
Avaya G430 Media Gateway	7.0.1.0 (g430_sw_37_41_0)
Avaya Aura® Media Server	7.7.0.375
Avaya Session Border Controller for Enterprise	7.1.0.2-01-13249
Avaya 1600 IP Deskphone (H.323)	1.3.10
Avaya 9670 IP DeskPhone (H.323)	6.6
Avaya 96x0 IP DeskPhone (H.323)	6.6
Avaya 9611 IP DeskPhone (SIP)	7.0
Avaya 9608 IP DeskPhone (SIP)	7.0
Avaya 9621 IP DeskPhone (SIP)	7.0
Avaya 9608 IP DeskPhone (SIP)	7.0
Avaya one-X® Communicator (H.323 & SIP)	6.2.12.04-FP12
Avaya Communicator for Windows	2.1.3.0
Analogue Handset	N/A
Analogue Fax	N/A
Virgin Media	
Soft Switch C20	CVM18 Q20 8.3.19
Genband Q20	V8.3.8

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 Virgin Media SIP Trunk. For incoming calls, the Session Manager receives SIP messages from the Avaya SBC for Enterprise (Avaya SBCE) and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to the Session Manager. The Session

Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Virgin Media 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 Virgin Media SIP Trunk network, 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	2	
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	10	
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 the Session Manager. In this case, **SM100** and **10.10.3.42** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

display node-names ip		IP NODE NAMES
Name	IP Address	
SM100	10.10.3.42	
default	0.0.0.0	
procr	10.10.3.44	
procr6	::	

5.3. Administer IP Network Region

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

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

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


5.4. Administer IP Codec Set

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

change ip-codec-set 1 Page 1 of 2

IP Codec Set

Codec Set: 1

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

Virgin Media's SIP Trunk supports T.38 for transmission of fax. Navigate to **Page 2** and define T.38 fax as follows:

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

change ip-codec-set 1 Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? n

	Mode	Redundancy	ECM: y	Packet Size (ms)
FAX	t.38-standard	0		
Modem	off	0		
TDD/TTY	US	3		
H.323 Clear-channel	n	0		
SIP 64K Data	n	0		20

5.5. Administer SIP Signaling Groups

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

- Set **Group Type** to **sip**.
- Set **Transport Method** to **tcp**.
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Far-end Node Name** to the Session Manager (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value).
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region 1).
- Leave **Far-end Domain** blank (allows the CM to accept calls from any SIP domain on the associated trunk).
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager).
- Set **Direct IP-IP Audio Connections** to **y**.
- Set **Initial IP-IP Direct Media** to **y**.
- Set **H.323 Station Outgoing Direct Media** to **y**.

The default values for the other fields may be used.

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

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

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

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

add trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
		Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 1800			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	

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

TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: public	UI Treatment: service-provider
	Replace Restricted Numbers? n	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? y	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y		

On **Page 4** of this form:

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

add trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	Mark Users as Phone? y
	Send Transferring Party Information? n
	Network Call Redirection? n
	Send Diversion Header? y
	Support Request History? n
	Telephone Event Payload Type: 101
	Convert 180 to 183 for Early Media? n
	Always Use re-INVITE for Display Updates? y
	Identity for Calling Party Display: P-Asserted-Identity
	Block Sending Calling Party Location in INVITE? n
	Accept Redirect to Blank User Destination? n
	Enable Q-SIP? n
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number in the format required. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones.

change private-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	6102	1	441xxxxxxx40	12	Total Administered: 4
4	6020	1	441xxxxxxx41	12	Maximum Entries: 240
4	6104	1	441xxxxxxx42	12	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
4	6010	1	441xxxxxxx43	12	
					Communication Manager automatically inserts a '+' digit in this case.

Note: The above configuration accepts all 4 digit numbers starting with 6, which includes all SIP and H.323 extension numbers.

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 Virgin Media's SIP Trunk. The single digit 9 was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

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

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

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
	0	11	14	1	pubu		n
	00	13	15	1	pubu		n
	0035391	13	13	1	pubu		n
	030	10	10	1	pubu		n
	0800	8	10	1	pubu		n
	0900	8	8	1	pubu		n
	118	3	6	1	pubu		n

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**. **Numbering Format** is applied to CLI and is used to set TDM signalling parameters such as type of number and numbering plan indicator. This doesn't have the same significance in SIP calls and during testing it was set to **unk-unk**.

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

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Virgin Media can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DID numbers provided by Virgin Media correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers to a 4 digit extension by deleting all of the incoming digits and inserting an extension. Public DID numbers have been masked for security purposes.

change inc-call-handling-trmt trunk-group 1					Page	1	of	3
INCOMING CALL HANDLING TREATMENT								
Service/ Feature	Number Len	Number Digits	Del	Insert				
public-ntwrk	13	+441xxxxxxx40	all	6102				
public-ntwrk	13	+441xxxxxxx41	all	6020				
public-ntwrk	13	+441xxxxxxx42	all	6104				
public-ntwrk	13	+441xxxxxxx43	all	6010				

5.10. EC500 Configuration

When EC500 is enabled on the Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 6102. Use the command **change off-pbx-telephone station-mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration.
- For the **Phone Number** enter the phone that will also be called (e.g. **0035391xxxxxx**).
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing.
- Set the **Config Set** to **1**.

change off-pbx-telephone station-mapping 6102							Page	1	of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION										
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode			
6102	EC500	-		0035391xxxxxx	1	1				
-										

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

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

6. Configuring Avaya Aura® Session Manager

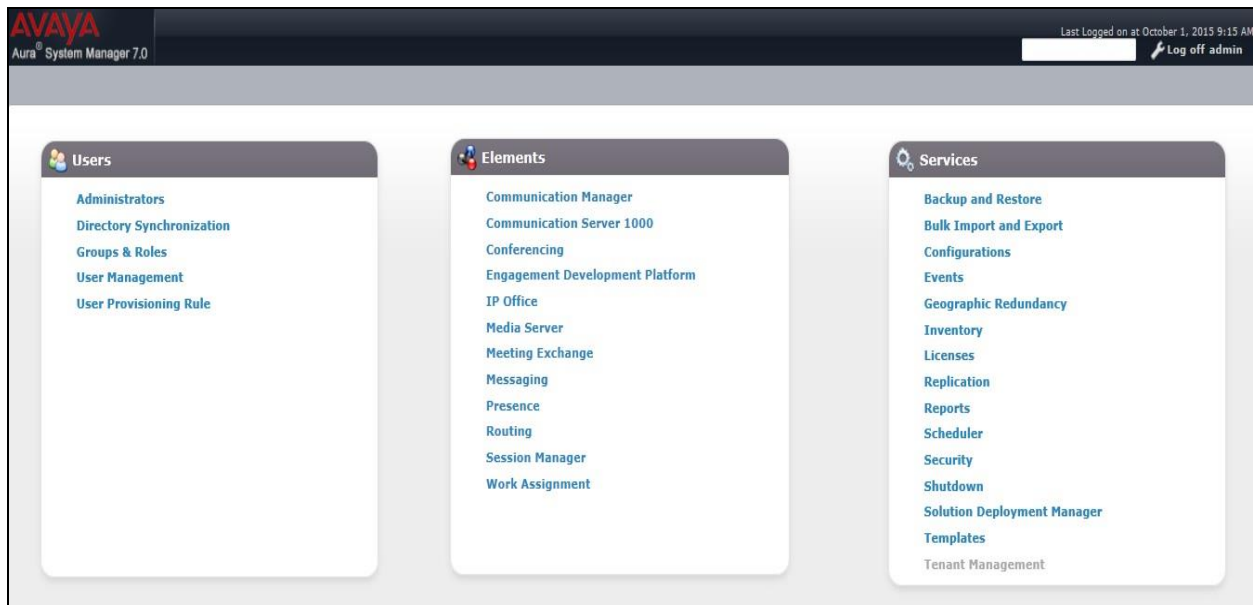
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager.
- Administer SIP Domain.
- Administer SIP Location.
- Administer Adaptations.
- Administer SIP Entities.
- Administer Entity Links.
- Administer Routing Policies.
- Administer Dial Patterns.

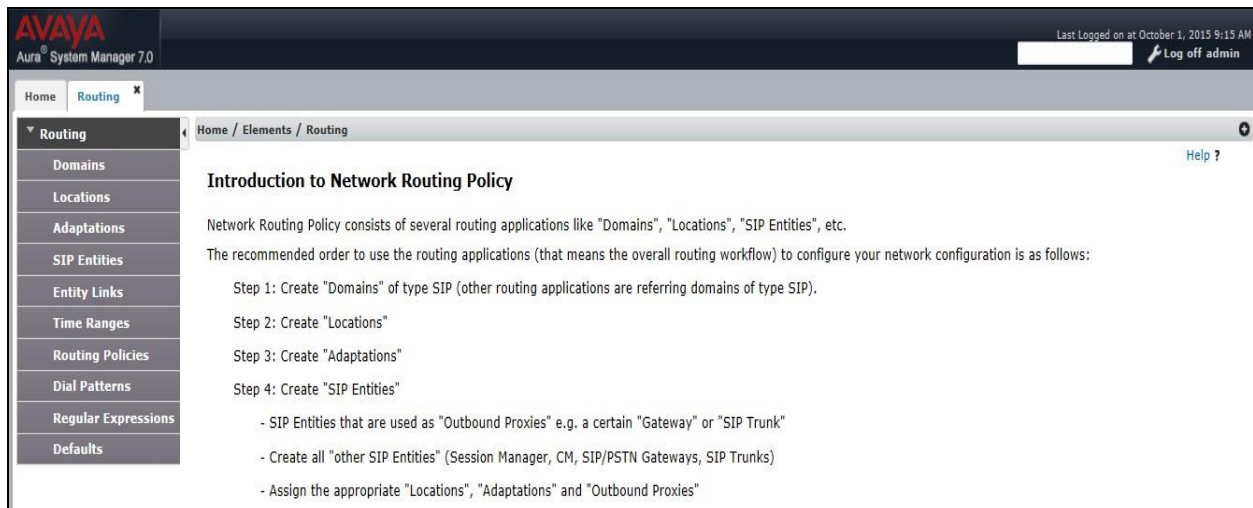
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. Log in to Avaya Aura® System Manager

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



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



AVAYA
Aura® System Manager 7.0

Last Logged on at: October 1, 2015 9:15 AM
Log off admin

Home Routing

Routing

- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

Home / Elements / Routing

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"

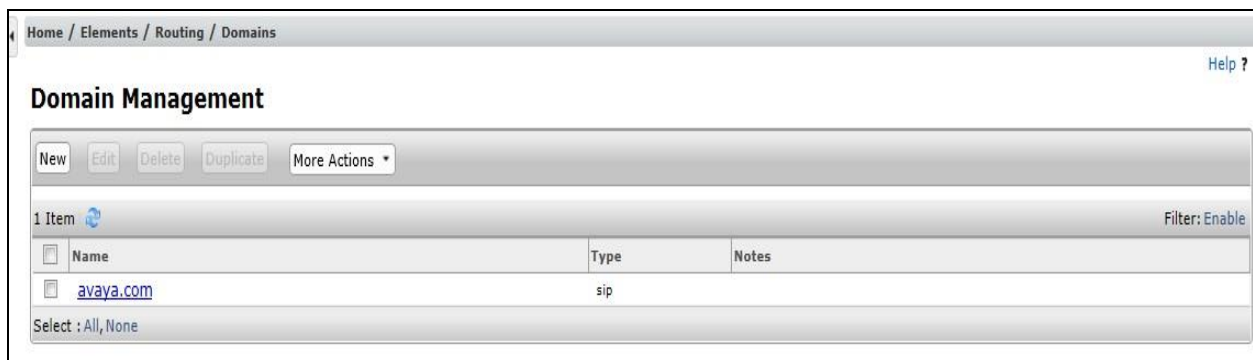
- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

6.2. Administer SIP Domain

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

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

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.



Home / Elements / Routing / Domains

Help ?

Domain Management

New Edit Delete Duplicate More Actions

1 Item Filter: Enable

Name	Type	Notes
avaya.com	sip	

Select : All, None

6.3. Administer Locations

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

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

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

In the **Location Pattern** section, click **Add** and enter the following values.

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

Click **Commit** to save. The screenshot below shows the Location **SM_7** defined for the compliance testing.

The screenshot displays the 'Location Details' and 'Location Pattern' configuration interface. The top section, 'Location Details', includes a 'General' tab with fields for 'Name' (set to 'SM_7') and 'Notes'. Below this is the 'Dial Plan Transparency in Survivable Mode' section with an 'Enabled' checkbox and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'. The 'Overall Managed Bandwidth' section includes a 'Managed Bandwidth Units' dropdown (set to 'Kbit/sec') and fields for 'Total Bandwidth' and 'Multimedia Bandwidth'. A checkbox for 'Audio Calls Can Take Multimedia Bandwidth' is checked. The bottom section, 'Location Pattern', features an 'Add' button and a table with 3 items. The table has columns for 'IP Address Pattern' and 'Notes'. The patterns listed are '*10.10.3.*', '*10.10.5.*', and '*10.10.8.*'. The 'Select' dropdown is set to 'All, None'. Buttons for 'Commit' and 'Cancel' are present at the bottom of both sections.

IP Address Pattern	Notes
10.10.3.	
10.10.5.	
10.10.8.	

6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. In order to improve interoperability with third party elements, Session Manager 7.0 incorporates the ability to use Adaptation modules to remove specific SIP headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements.

For the compliance test, an Adaptation named “**VMB**” was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

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

- **Adaption Name:** Enter an appropriate name such as **VMB**.
- **Module Name:** Select **DigitConversionAdapter**.
- **Modular Parameter Type:** Select **Name-Value Parameter**.

Click **Add** to add the name and value parameters.

- **Name:** Enter **eRHdrs**. This parameter will remove the specific headers from messages in the egress direction.
- **Value:** Enter “**AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, P-Location**”.
- **Name:** Enter **fromto**. Modifies From and To header of a message.
- **Value:** Enter **true**.
- **Name:** Enter **MIME**. Remove MIME message bodies from Session Manager.
- **Value:** Enter **no**.

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel Help ?

General

* Adaptation Name: VMB

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
eRHdrs	Alert-Info, x-nt-e164-clid, P-Charging-Vector, AV-Global-Session-ID, P-Location, P-AV-Message-ID
fromto	true
MIME	no

Select : All, None

Egress URI Parameters:

Notes:

6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **General**:

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP Entity, **CM** for a Communication Manager SIP Entity and **SIP Trunk** for the Avaya SBCE SIP Entity.
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity.

In this configuration there are four SIP Entities.

- Session Manager SIP Entity.
- Communication Manager SIP Entity.
- Avaya SBCE SIP Entity x 2.

6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface and **Type** is **Session Manager**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb trail is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is active. Fields include: 'Name' (Session Manager), 'FQDN or IP Address' (10.10.3.42), 'Type' (Session Manager), 'Notes' (empty), 'Location' (SM_7), 'Outbound Proxy' (empty), 'Time Zone' (Europe/Dublin), and 'Credential name' (empty). The 'SIP Link Monitoring' section shows 'SIP Link Monitoring' set to 'Use Session Manager Configuration'.

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

- In the **Port** field enter the port number on which the system listens for SIP requests.
- In the **Protocol** field 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.

The screenshot shows the 'Listen Ports' configuration section. It includes input fields for 'TCP Failover port' and 'TLS Failover port'. Below these are 'Add' and 'Remove' buttons. A table lists 3 items with columns: Listen Ports, Protocol, Default Domain, and Notes. The table contains three rows: (5060, TCP, avaya.com), (5060, UDP, avaya.com), and (5061, TLS, avaya.com). A 'Filter: Enable' link is at the top right. At the bottom, it says 'Select : All, None'.

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

6.5.2. Avaya Aura® Communication Manager SIP Entity

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

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The configuration fields are as follows:

- Name:** Communication_Manager
- * FQDN or IP Address:** 10.10.3.44
- Type:** CM (dropdown)
- Notes:** (empty text area)
- Adaptation:** (dropdown)
- Location:** SM_7 (dropdown)
- Time Zone:** Europe/Dublin (dropdown)
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text area)
- Securable:** ☐
- Call Detail Recording:** none (dropdown)

The 'Loop Detection' tab is also visible, showing:

- Loop Detection Mode:** Off (dropdown)

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

The screenshot shows the 'SIP Link Monitoring' configuration page. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Link Monitoring'. The configuration fields are as follows:

- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows one of the SIP Entities for the Avaya SBCE. Two SIP Entities were used for the two interfaces established so that routing could take place to both the Virgin Media SBCs. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interfaces (see **Figure 1**). Set **Type** to **SIP Trunk** and **Adaptation** to that defined in **Section 6.4**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Name: Virgin_SBC_A

*** FQDN or IP Address:** 10.10.3.30

Type: SIP Trunk

Notes:

Adaptation: VMB

Location: SM_7

Time Zone: Europe/Dublin

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

Credential name:

Securable: ☐

Call Detail Recording: none

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Commit **Cancel**

The following screenshot shows the SIP Entity for Virgin SBC B.

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: Virgin_SBC_B

* FQDN or IP Address: 10.10.3.35

Type: SIP Trunk

Notes:

Adaptation: VMB

Location: SM_7

Time Zone: Europe/Dublin

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

Credential name:

Securable: ☐

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

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 **Protocol** field enter the transport protocol to be used to send SIP requests.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field 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.

Click **Commit** to save changes. The following screen shows the Entity Links **Communication Manager, Virgin_SBC_A** and **Virgin_SBC_B** used in this configuration.

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	Aura_Messaging	Session Manager	TCP	5060	Aura_Messaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Communication_Manager	Session Manager	TCP	5060	Communication_Manager	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CS1K	Session Manager	TCP	5060	CS1K_7.6	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Virgin_SBC_A	Session Manager	TCP	5060	Virgin_SBC_A	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Virgin_SBC_B	Session Manager	TCP	5060	Virgin_SBC_B	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

Select : All, None

6.7. Administer Routing Policies

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

Under **General**:

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

The following screen shows the routing policy for Communication Manager.

The screenshot shows the 'Routing Policy Details' configuration page. The breadcrumb trail is 'Home / Elements / Routing / Routing Policies'. The page has a 'Commit' and 'Cancel' button in the top right. The 'General' tab is active, showing fields for 'Name' (to_Communication Manager), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. The 'SIP Entity as Destination' section has a 'Select' button and a table with one entry: 'Communication_Manager' with FQDN or IP Address '10.10.3.44' and Type 'CM'. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows '1 Item' with a table of days and times. The table has columns for Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The entry shows '24/7' with checkboxes for all days and a time range of '00:00' to '23:59'.

Name	FQDN or IP Address	Type	Notes
Communication_Manager	10.10.3.44	CM	

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

In the Virgin Media network, two network SBCs are provided as the interface to the enterprise equipment. These are Sandbox SBCs and for the purposes of this document have been designated as A and B. The routing and fallback for these two SBCs is configured on the Session Manager, with two server flows configured on the Avaya SBCE for routing to each network SBC. There is an interface configured on the Avaya SBCE for each of these server flows, and a corresponding SIP Entity, Entity Link and Routing Policy is required on the Session Manager for each of these interfaces.

A full description of the configuration of the interfaces and server flows on the Avaya SBCE is provided in **Section 7**.

The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed on to Virgin Media via SBC A.

The screenshot shows the 'Routing Policy Details' page for the policy named 'to_Virgin_SBC_A'. The 'General' tab is active, showing fields for Name, Disabled, Retries, and Notes. The 'SIP Entity as Destination' section shows a table with one entry: 'Virgin_SBC_A' with FQDN or IP Address '10.10.3.30' and Type 'SIP Trunk'. The 'Time of Day' section shows a table with one item: '24/7' with a ranking of 1, and a time range from 00:00 to 23:59.

Routing Policy Details [Commit] [Cancel] Help ?

Administering Routing Policies
Page Fields

General

* Name: to_Virgin_SBC_A x

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Virgin_SBC_A	10.10.3.30	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
1	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 on to Virgin Media via SBC B.

The screenshot shows the 'Routing Policy Details' page for the policy named 'to_Virgin_SBC_B'. The 'General' tab is active, showing fields for Name, Disabled, Retries, and Notes. The 'SIP Entity as Destination' section shows a table with one entry: 'Virgin_SBC_B' with FQDN or IP Address '10.10.3.35' and Type 'SIP Trunk'. The 'Time of Day' section shows a table with one item: '24/7' with a ranking of 2, and a time range from 00:00 to 23:59.

Routing Policy Details [Commit] [Cancel] Help ?

Administering Routing Policies
Page Fields

General

* Name: to_Virgin_SBC_B x

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Virgin_SBC_B	10.10.3.35	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
2	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

Note: Ranking value has been set to **1** for Virgin SBC A and set to **2** for Virgin SBC B. Lower ranking values indicate higher priority for call routing so all calls will route to Virgin SBC A. Should Virgin SBC A encounter routing difficulties, then all call routing will automatically failover to Virgin SBC B.

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 out to the Virgin Media network via network SBC A with fallback via network SBC B.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 00353

* Min: 5

* Max: 15

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.com

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"/>	SM_7		to_Virgin_SBC_A	1	<input type="checkbox"/>	Virgin_SBC_A	
<input type="checkbox"/>	SM_7		to_Virgin_SBC_B	2	<input type="checkbox"/>	Virgin_SBC_B	

Select : All, None

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

Home / Elements / Routing / Dial Patterns

Help ?

Dial Pattern Details

CommitCancel

General

* Pattern: +44

* Min: 3

* Max: 15

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

AddRemove

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"/>	SM_7		to_Communication Manager	0	<input type="checkbox"/>	Communication_Manager	

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

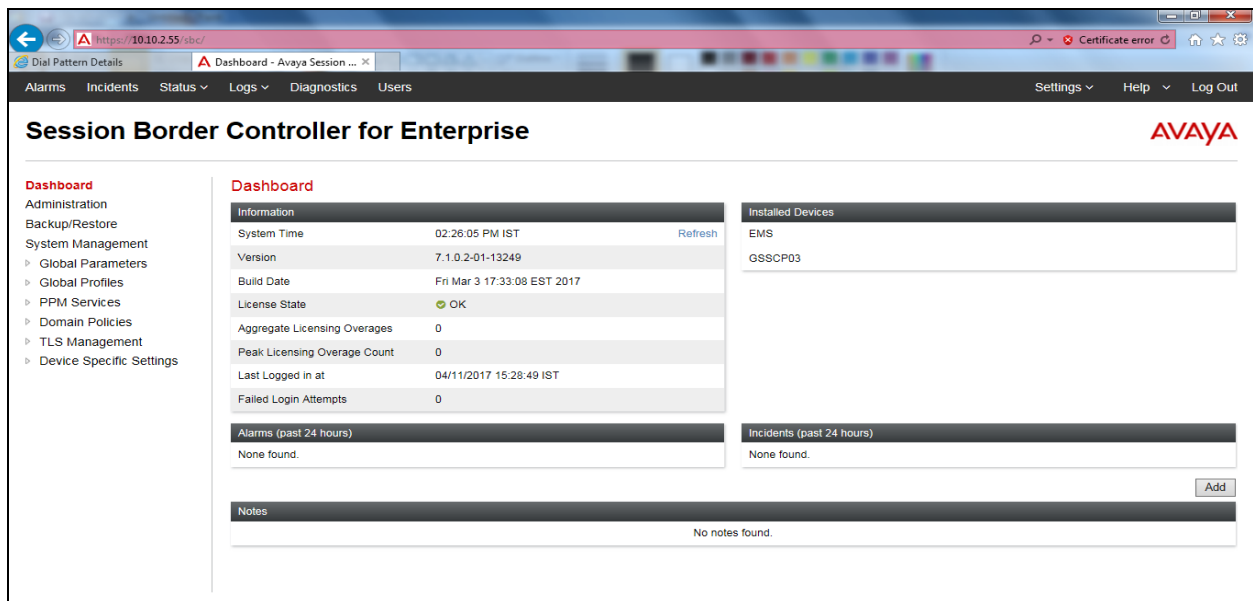
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP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

7.1. Access Avaya Session Border Controller for Enterprise

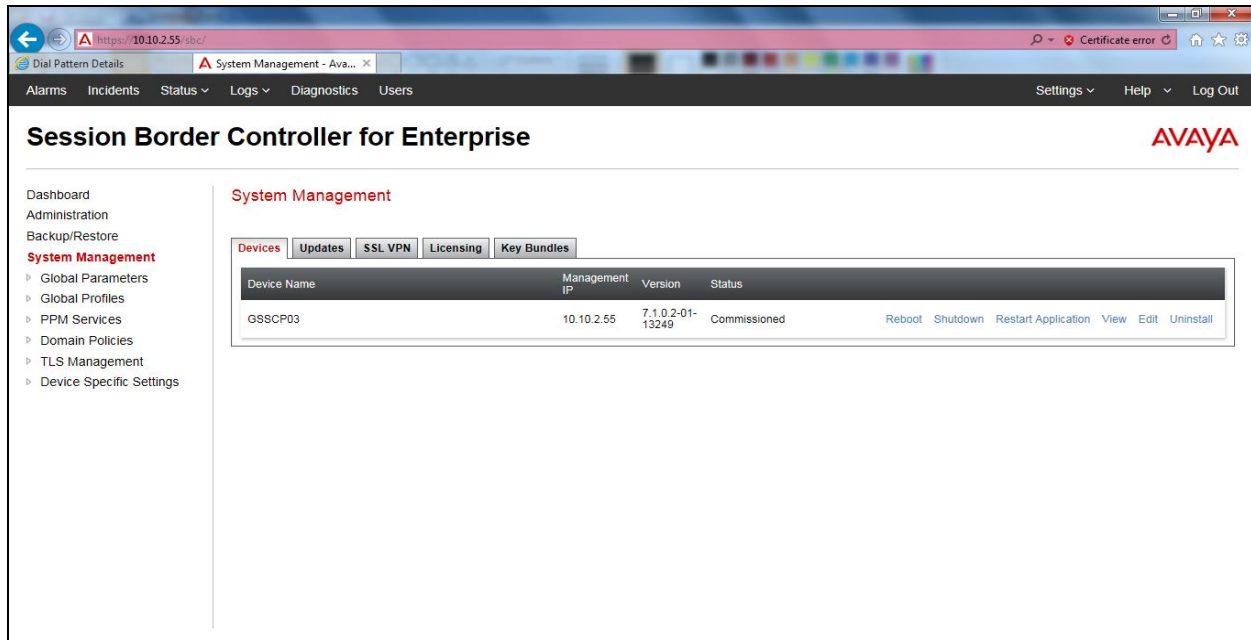
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



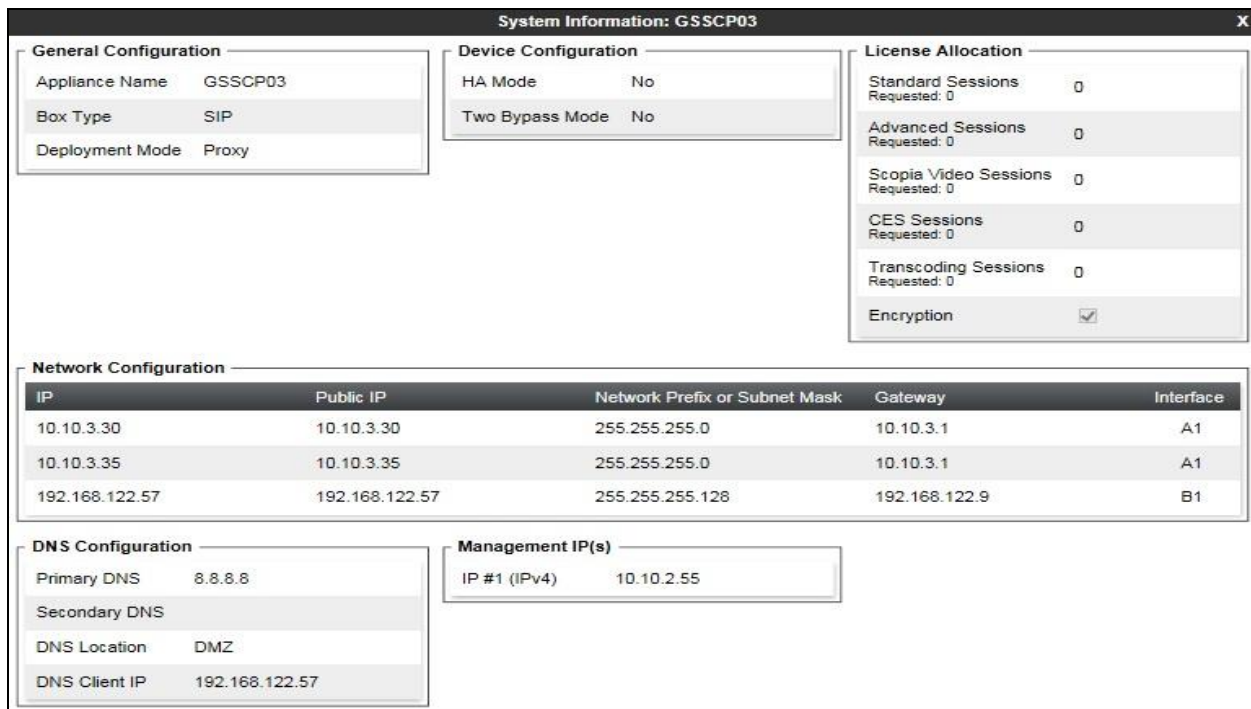
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



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



The System Information screen shows the **Appliance Name**, **Device Settings** and **DNS Configuration** information.



7.2. Global Profiles

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

7.2.1. Server Internetworking - Avaya

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

- Enter profile name such as **Avaya** and click **Next** (Not Shown).
- **Check Hold Support=None.**
- **Check T.38 Support.**
- All other options on the **General** Tab can be left at default.

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 type="checkbox"/>
Delayed Offer	<input 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 type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = Avaya**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides <input type="radio"/> Dialog-Initiate Only (Single Side) <input type="radio"/> Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	<input checked="" type="checkbox"/>
Extensions	Avaya ▼
Diversion Manipulation	<input type="checkbox"/>
Diversion Condition	None ▼
Diversion Header URI	
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Relay INVITE Replace for SIPREC	<input type="checkbox"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP Notify <input type="radio"/> SIP Info <input type="radio"/> Inband
<input type="button" value="Finish"/>	

7.2.2. Server Internetworking – Virgin Media

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

- Enter profile name such as **VMB** and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- Check **Delayed SDP handling**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

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

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 type="checkbox"/>
Delayed Offer	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input checked="" type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

On the **Advanced** Tab:

- Check **Record Routes = Both Sides**.
- Ensure **Extensions = None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.

Record Routes

☐ None

☐ Single Side

☒ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup ☒

Extensions None ▾

Diversion Manipulation ☐

Diversion Condition None ▾

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

Relay INVITE Replace for SIPREC ☐

DTMF

DTMF Support

☒ None

☐ SIP Notify

☐ SIP Info

☐ Inband

Finish

7.2.3. Server Configuration – Avaya

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

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow the configuration and management of various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signalling parameters and some advanced options.

From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name such as **Avaya**. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**.
- Enter **IP Address / FQDN** to **10.10.3.42** (Session Manager IP Address).
- For **Port**, enter **5060**.
- For **Transport**, select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

Server Configuration Profile - General		
Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.		
Server Type	Call Server	
TLS Client Profile	None	
Add		
IP Address / FQDN	Port	Transport
10.10.3.42	5060	TCP
		Delete
Finish		

On the **Advanced** tab:

- Select **Avaya** for **Interworking Profile** (Section 7.2.1).
- Click **Finish**.

The screenshot shows the 'Server Configuration Profile - Advanced' dialog box. It contains several configuration options: 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (dropdown menu set to 'Avaya'), 'Signaling Manipulation Script' (dropdown menu set to 'None'), 'Securable' (checkbox), 'Enable FGDN' (checkbox), 'TCP Failover Port' (text input field), and 'TLS Failover Port' (text input field). A 'Finish' button is located at the bottom right of the dialog.

7.2.4. Server Configuration – Virgin Media

To define Virgin Media SBC A as a Trunk Server, navigate to **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. **VMB_SBC_A** and **VMB_SBC_B** naming was used in this compliance test for the respective Virgin Media SBC's.

On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **192.168.222.186** (Virgin SBC A address).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Click on **Next** (not shown).

The screenshot shows the 'Server Configuration Profile - General' dialog box. At the top, there is a blue warning banner that reads: 'Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.' Below this, the 'Server Type' dropdown is set to 'Trunk Server'. The 'SIP Domain' field is empty. The 'TLS Client Profile' dropdown is set to 'None'. An 'Add' button is located to the right of these fields. At the bottom, there is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'. The first row contains the values '192.168.222.186', '5060', and 'UDP' (selected from a dropdown). A 'Delete' button is located to the right of the table.

In the new window that appears, enter the following values as Virgin Media require authentication to connect to their network:

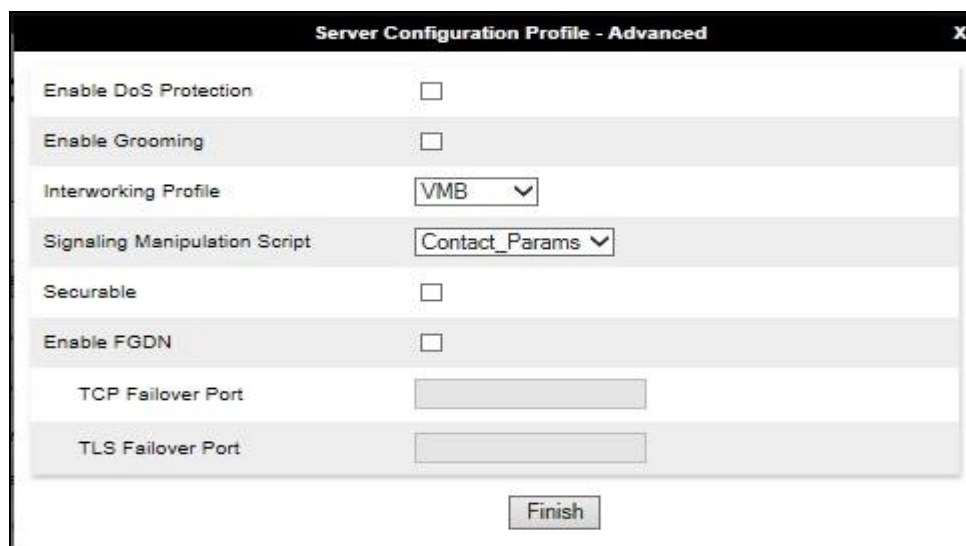
- **Enabled Authentication:** Checked.
- **User Name:** Enter username provided by the Service Provider.
- **Realm:** Enter realm details provided by the Service Provider.
- **Password** Enter password provided by the Service Provider.
- **Confirm Password** Re-enter password provided by the Service Provider.



Click on **Next** (not shown) to use default entries on the **Heartbeat** tab as registration to the Virgin Media SIP trunk was not required during testing.

On the Advanced tab:

- Select **VMB** for **Interworking Profile** (Section 7.2.2).
- Select **Contact_Params** for **Signaling Manipulation Script** (Section 7.2.7).
- Click **Finish**.



Repeat the process to define a Server Configuration for Virgin SBC B.

7.2.5. Routing

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

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

7.2.5.1 Routing – Avaya

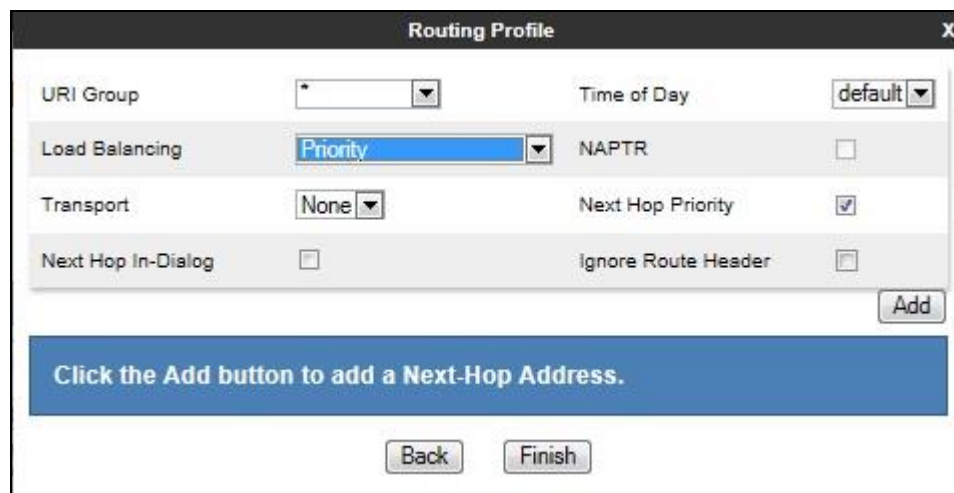
Create a Routing Profile for Session Manager.

- Navigate to **Global Profiles → Routing** and select **Add**.
- Enter a **Profile Name** and click **Next**.



The screenshot shows a 'Routing Profile' window. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a text input field labeled 'Profile Name' containing the text 'Avaya'. Below the input field is a 'Next' button.

The Routing Profile window will open. Use the default values displayed and click **Add**.



The screenshot shows the 'Routing Profile' window with various settings. The title bar has 'Routing Profile' and a close button 'X'. The settings are as follows:

URI Group	Time of Day
*	default
Load Balancing	NAPTR
Priority	<input type="checkbox"/>
Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>
Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

At the bottom right is an 'Add' button. Below the settings is a blue banner with the text 'Click the Add button to add a Next-Hop Address.' At the very bottom are 'Back' and 'Finish' buttons.

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = Avaya** (Section 7.2.3) from drop down menu.
- **Next Hop Address = Select 10.10.3.42:5060 (TCP)** from drop down menu.
- Click **Finish**.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Avaya	10.10.3.42:5060 (TCP)	None

7.2.5.2 Routing – Virgin Media

Create a Routing Profile for Virgin SBC A.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

Profile Name: VMB_SBC_A

Next

The Routing Profile window will open. Use the default values displayed and click **Add**.

The 'Routing Profile' window displays the following settings:

- URI Group: *
- Time of Day: default
- Load Balancing: Priority
- NAPTR: ☐
- Transport: None
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐

An 'Add' button is located at the bottom right. Below the settings is a blue banner that reads: 'Click the Add button to add a Next-Hop Address.' At the very bottom are 'Back' and 'Finish' buttons.

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = VMB_SBC_A** (Section 7.2.4) from drop down menu.
- **Next Hop Address = Select 192.168.222.186:5060 (UDP)** from drop down menu.
- Click **Finish**.

The 'Profile : VMB_SBC_A' window displays the following settings:

- URI Group: *
- Time of Day: default
- Load Balancing: Priority
- NAPTR: ☐
- Transport: None
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐
- ENUM: ☐
- ENUM Suffix:

An 'Add' button is located at the bottom right. Below the settings is a table with the following data:

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	VMB_SBC_A	192.168.222.186:5060 (UDP)	None	Delete

A 'Finish' button is located at the bottom center.

Repeat the process to define a Routing Profile for Virgin SBC B.

7.2.6. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**. This replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single **Via** and **Record-Route** headers externally where multiple headers may be received from the enterprise. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

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

- Enter a descriptive Profile Name such as **Avaya**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **avaya.com**.
- Click **Finish** (not shown).

The screenshot shows the 'Topology Hiding Profiles: Avaya' configuration window. On the left, a sidebar lists 'Topology Hiding Profiles' with options: 'default', 'cisco_th_profile', 'Avaya' (selected), and 'VMB'. An 'Add' button is at the top of the sidebar. The main area has a blue header bar with 'Click here to add a description.' and buttons for 'Rename', 'Clone', and 'Delete'. Below this is a 'Topology Hiding' tab and a table with the following data:

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

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

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

- In the **Profile Name** field enter a descriptive name for Virgin Media such as (**VMB**) and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Auto** under **Replace Action**.
- Click **Finish** (not shown).

Topology Hiding Profiles: VMB

Add

RenameCloneDelete

Topology Hiding Profiles

default

cisco_th_profile

Avaya

VMB

Click here to add a description.

Topology Hiding

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

Edit

7.2.7. Signalling Manipulation

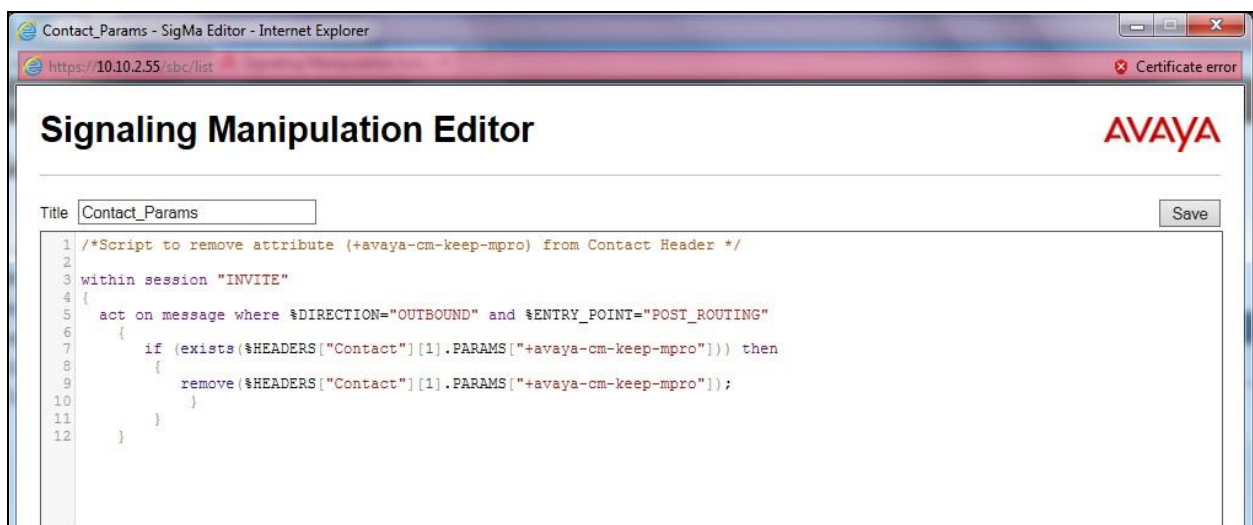
The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa. The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE.

During compliance testing, an issue was found with the handling of an Avaya specific parameter in the Contact Header. The Avaya proprietary parameter “+avaya-cm-keep-mpro=no” is present when Initial IP-IP Direct Media is enabled on the Communication Manager SIP Trunk. A script was required to remove the proprietary parameter “+avaya-cm-keep-mpro” from the Contact Header.

To define the signalling manipulation to delete the Avaya proprietary parameter from the Contact Header, navigate to **Dashboard → Global Profiles → Signaling Manipulation** and click on **Add** and enter a title. A new blank SigMa Editor window will pop up. The script text is as follows:

```
/*Script to remove attribute (+avaya-cm-keep-mpro) from Contact Header */  
within session "INVITE"  
{  
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"  
  {  
    if (exists(%HEADERS["Contact"][1].PARAMS["+avaya-cm-keep-mpro"])) then  
    {  
      remove(%HEADERS["Contact"][1].PARAMS["+avaya-cm-keep-mpro"]);  
    }  
  }  
}
```

Once entered and saved, the script appears as shown in the following screenshot:



7.3. Define Network Information

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

In the test configuration, two IP addresses were used on the internal interface so that different server flows could be assigned depending on which interface address the SIP messages were received on. These server flows were used to direct traffic to the two Virgin Media SBCs separately.

To define the network information, navigate to **Device Specific Settings → Network Management** from the menu on the left-hand side and click on **Add**. Enter details in the blank box that appears at the end of the list.

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

Network Management: GSSCP03

Devices	Interfaces	Networks
GSSCP03		

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
Internal_A1	10.10.3.1	255.255.255.0	A1	10.10.3.30, 10.10.3.35	Edit	Delete
External_B1	192.168.122.9	255.255.255.128	B1	192.168.122.57	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: GSSCP03

Devices	Interfaces	Networks
GSSCP03		

Add VLAN

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

7.4. Define Interfaces

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

7.4.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** from the menu on the left hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

To enter details of transport protocol and ports for the SIP signalling on the internal interface to be used in the server flow for Virgin SBC A:

- Select **Add** and enter details of the first internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **Signaling IP**, select one of the **internal** signalling interface IP addresses defined in **Section 7.3**.
- Select **TCP** port number, **5060** is used for the Session Manager.

To enter details of transport protocol and ports for the SIP signalling on internal interface to be used in the server flow for Virgin SBC B:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for interface.
- For **Signaling IP**, select the other **internal** signalling interface IP address defined in **Section 7.3**.
- Select **TCP** port number, **5060** is used for the Session Manager.

To enter details of transport protocol and ports for the SIP signalling on the external interface:

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field, enter a descriptive name for the external signalling interface.
- For **Signaling IP**, select an **external** signalling interface IP address defined in **Section 7.3**.
- Select **UDP** port number, **5060** is used for the Virgin Media SIP Trunk.

Signaling Interface: GSSCP03

Devices

GSSCP03

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	
Ext_Sig	192.168.122.57 External_B1 (B1, VLAN 0)	---	5060	---	None	Edit Delete
Int_Sig_B	10.10.3.35 Internal_A1 (A1, VLAN 0)	5060	5060	---	None	Edit Delete
Int_Sig_A	10.10.3.30 Internal_A1 (A1, VLAN 0)	5060	---	---	None	Edit Delete

7.4.2. Media Interfaces

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

To enter details of the media IP and RTP port range on the internal interface to be used in the server flow for Virgin SBC A:

- Select **Add** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select the **internal** media interface IP address defined in **Section 7.3**.
- Select **RTP port** ranges for the media path with the enterprise end-points.

To enter details of the media IP and RTP port range on the internal interface to be used in the server flow for Virgin SBC B:

- Select **Add** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select the **internal** media interface IP address defined in **Section 7.3**.
- Select **RTP port** ranges for the media path with the enterprise end-points.

To enter details of the media IP and RTP port range on the external interface to be used in the server flow.

- Select **Add** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select the **external** media interface IP address defined in **Section 7.3**.
- Select **RTP port** ranges for the external media path.

The following screen shows the Media Interfaces created in the sample configuration for the inside and outside IP interfaces.

Media Interface: GSSCP03

Devices

GSSCP03

Media Interface

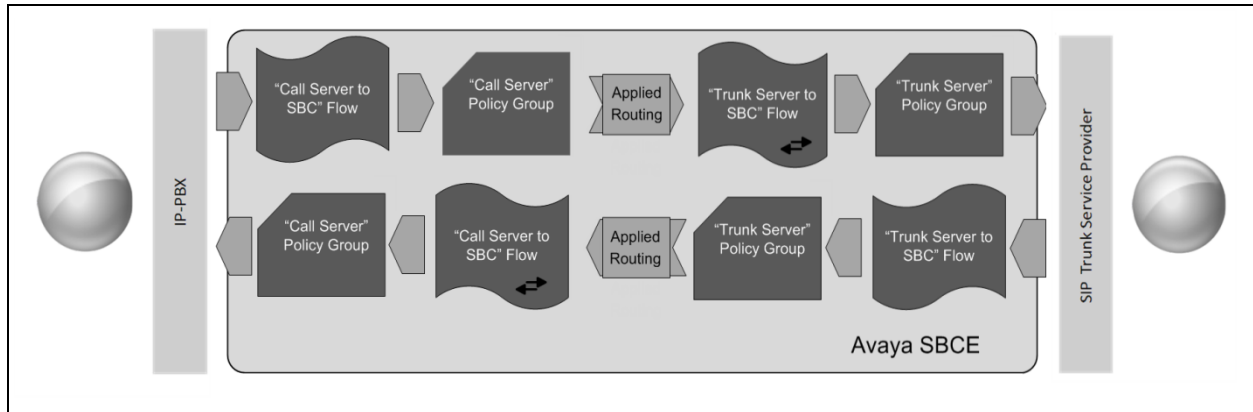
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP Network	Port Range	Edit	Delete
Ext_Media	192.168.122.57 External_B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete
Int_Media_A	10.10.3.30 Internal_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Int_Media_B	10.10.3.35 Internal_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete

7.5. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to Virgin Media's SIP Trunk and incoming flows from Virgin Media's SIP Trunk to Session Manager. This configuration ties all the previously entered information together so that signalling can be routed from the Session Manager to the PSTN via the Virgin Media network and vice versa. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



Two server flows are required for outgoing traffic and two are required for incoming. This is so that traffic can be routed to both the network SBCs and can also be received from both network SBCs. As mentioned previously, the network SBCs have been designated as Virgin SBC A and Virgin SBC B for the purposes of the testing and documentation.

Subscriber Flows

Server Flows

Click here to add a row description.

Server Configuration: Avaya

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
<input type="text" value="1"/>	Call_Server_A	*	Ext_Sig	Int_Sig_A	default-low	VMB_SBC_A	View	Clone	Edit	Delete
<input type="text" value="2"/>	Call_Server_B	*	Ext_Sig	Int_Sig_B	default-low	VMB_SBC_B	View	Clone	Edit	Delete

Server Configuration: VMB_SBC_A

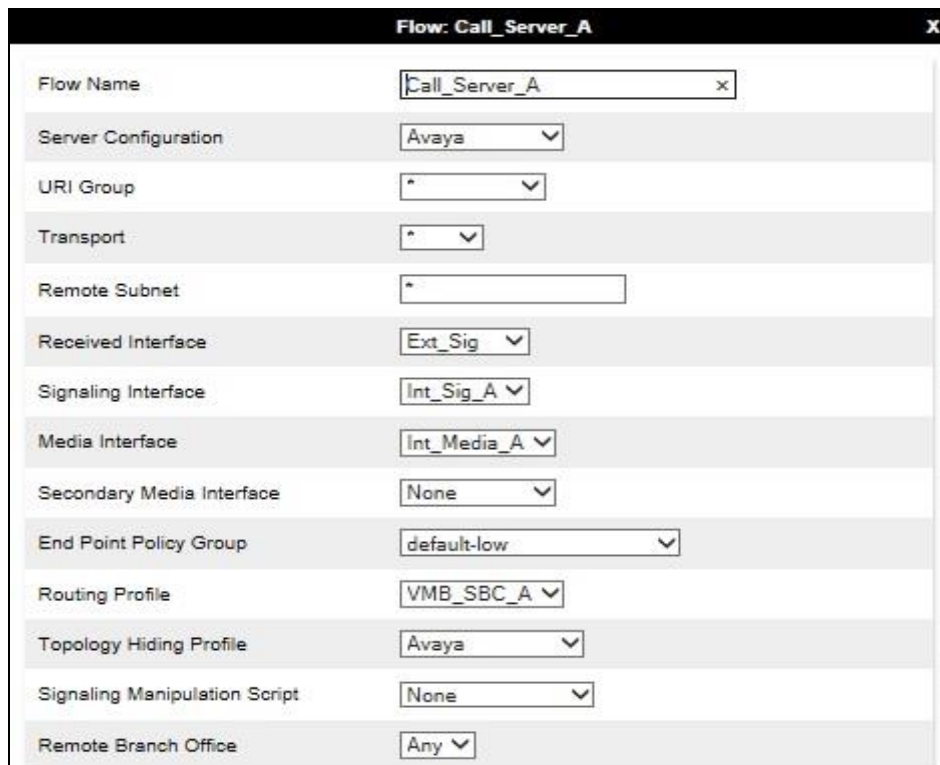
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
<input type="text" value="1"/>	Trunk_Server_A	*	Int_Sig_A	Ext_Sig	default-low	Avaya	View	Clone	Edit	Delete

Server Configuration: VMB_SBC_B

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
<input type="text" value="1"/>	Trunk_Server_B	*	Int_Sig_B	Ext_Sig	default-low	Avaya	View	Clone	Edit	Delete

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

- Click on the **Server Flows** tab (shown above).
- Select **Add** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the server flow for the Session Manager, in this case **Call_Server_A** was used.
- In the **Server Configuration** drop-down menu, select the Session Manager server configuration defined in **Section 7.2.3**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Virgin_SBC_A defined in **Section 7.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.2.6** and click **Finish**.



Flow: Call_Server_A	
Flow Name	Call_Server_A
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig_A
Media Interface	Int_Media_A
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	VMB_SBC_A
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any

Repeat the above process for Call Server B, selecting the specific Call Server B entries for server flow configuration.

To define Server Flows for the Virgin Media network SBCs (Virgin SBC A and Virgin SBC B), navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab (shown above).
- Select **Add** and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for Virgin SBC A SIP Trunk, in the test environment **Trunk_Server_A** was used.
- In the **Server Configuration** drop-down menu, select the Virgin SBC A server configuration defined in **Section 7.2.4**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Virgin SBC A SIP Trunk is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**. This is the interface that signalling bound for Virgin SBC A SIP Trunk is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**. This is the interface that media bound for Virgin SBC A SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Virgin SBC A SIP Trunk defined in **Section 7.2.6** and click **Finish**.

Flow: Trunk_Server_A	
Flow Name	Trunk_Server_A
Server Configuration	VMB_SBC_A
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig_A
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	VMB
Signaling Manipulation Script	None
Remote Branch Office	Any

Repeat the above process for Virgin SBC B, selecting the specific Virgin SBC B entries for server flow configuration.

8. Configure Virgin Media SIP Trunk Equipment

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

9. Verification Steps

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

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

Home / Elements / Session Manager / System Status / SIP Entity Monitoring								
Session Manager Entity Link Connection Status								
This page displays detailed connection status for all entity links from a Session Manager.								
All Entity Links for Session Manager: Session Manager								
Summary View								
Status Details for the selected Session Manager:								
5 Items Refresh Filter: Enable								
	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	Virgin_SBC_A	10.10.3.30	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Communication_Manager	10.10.3.44	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Aura_Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	CS1K_7.6	10.10.9.21	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Virgin_SBC_B	10.10.3.35	5060	TCP	FALSE	UP	200 OK	UP

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

status trunk 1			
TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports
			Busy
0001/001	T00001	in-service/idle	no
0001/002	T00002	in-service/idle	no
0001/003	T00003	in-service/idle	no
0001/004	T00004	in-service/idle	no
0001/005	T00005	in-service/idle	no
0001/006	T00006	in-service/idle	no
0001/007	T00007	in-service/idle	no
0001/008	T00008	in-service/idle	no
0001/009	T00009	in-service/idle	no
0001/010	T00010	in-service/idle	no

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

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

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

Trace: GSSCP03

Devices

GSSCP03

Packet Capture

Captures

Packet Capture Configuration

Status

Ready

Interface

B1

Local Address
IP[:Port]

192.168.122.57

Remote Address
*, *-Port, IP, IP-Port

*

Protocol

All

Maximum Number of Packets to Capture

1000

Capture Filename
Using the name of an existing capture will overwrite it.

TEST.pcap

Start Capture

Clear

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



The screenshot shows a web interface for a trace named 'GSSCP03'. On the left, there is a 'Devices' sidebar with 'GSSCP03' selected. The main area has two tabs: 'Packet Capture' and 'Captures', with 'Captures' being the active tab. A 'Refresh' button is located in the top right corner of the main area. Below the tabs is a table with three columns: 'File Name', 'File Size (bytes)', and 'Last Modified'. The table contains one entry: 'TEST_20170413141915.pcap' with a file size of '0' and a last modified date of 'April 13, 2017 2:19:52 PM IST'. A 'Delete' button is located to the right of the table entry.

File Name	File Size (bytes)	Last Modified
TEST_20170413141915.pcap	0	April 13, 2017 2:19:52 PM IST

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R7.0 as an Evolution Server, Avaya Aura® Session Manager R7.0 and Avaya Session Border Controller for Enterprise R7.1 to Virgin Media's SIP Trunk Service. Virgin Media's SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

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

- [1] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, Oct 2016
- [2] *Avaya Aura® Communication Manager 7.0 Documentation library*, Oct 2016
- [3] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide Release 7.0* Oct 2016
- [4] *Implementing Avaya Aura® System Manager Release 7.0*, Aug 2016
- [5] *Upgrading Avaya Aura® System Manager to Release 7.0*, Aug 2016
- [6] *Administering Avaya Aura® System Manager Release 7.0*, Aug 2016
- [7] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide Release 7.0*, 2016
- [8] *Implementing Avaya Aura® Session Manager Release 7.0*, Nov 2016
- [9] *Upgrading Avaya Aura® Session Manager Release 7.0*, Nov 2016
- [10] *Administering Avaya Aura® Session Manager Release 7.0*, Nov 2016
- [11] *Deploying Avaya Session Border Controller for Enterprise Release 7.1*, Nov 2016
- [12] *Upgrading Avaya Session Border Controller for Enterprise Release 7.1*, Jul 2016
- [13] *Administering Avaya Session Border Controller for Enterprise Release 7.1*, Jun 2016
- [14] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2017 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.