



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to support 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.

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 calls to the enterprise site from PSTN phones using the SIP Trunk provided by Virgin Media, calls made to SIP and H.323 telephones at the enterprise
- Outgoing calls from the enterprise site completed via Virgin Media's SIP Trunk to PSTN destinations, calls made from SIP and H.323 telephones
- Calls using the G.711A and G.729 codecs
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
- 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
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Direct IP-to-IP media with SIP and H.323 telephones
- Call coverage and call forwarding for endpoints at the enterprise site
- Transmission and response of SIP OPTIONS messages sent by 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:

- During testing, an issue was found in the use of the UPDATE message between Virgin Media SIP Trunk service and the enterprise that could not be resolved by other methods such as Server Interworking and Signaling Rules. The issue occurred when the UPDATE message was sent from the Virgin Media network to change the codec to T.38 for fax calls. The enterprise was not successfully changing the codec and the fax calls were failing. The solution was to remove UPDATE from the Supported header in messages going from the enterprise to the network. This prompts the network to use re-INVITE instead of UPDATE.
- Inbound and outbound T.38 fax calls using dedicated fax machines terminated successfully. However inbound T.38 fax calls sent from a fax client failed thus fax clients are not supported for T.38 fax transmissions.
- Inbound and Outbound fax was tested successfully using G.711 pass-through however G.711 pass-through is not supported by Avaya.
- 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 the Virgin Media Business products described in these Application Notes, please contact your Account or Service Manager, your Provisioning contact or the Helpdesk on 0800 052 0800.

3. Reference Configuration

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

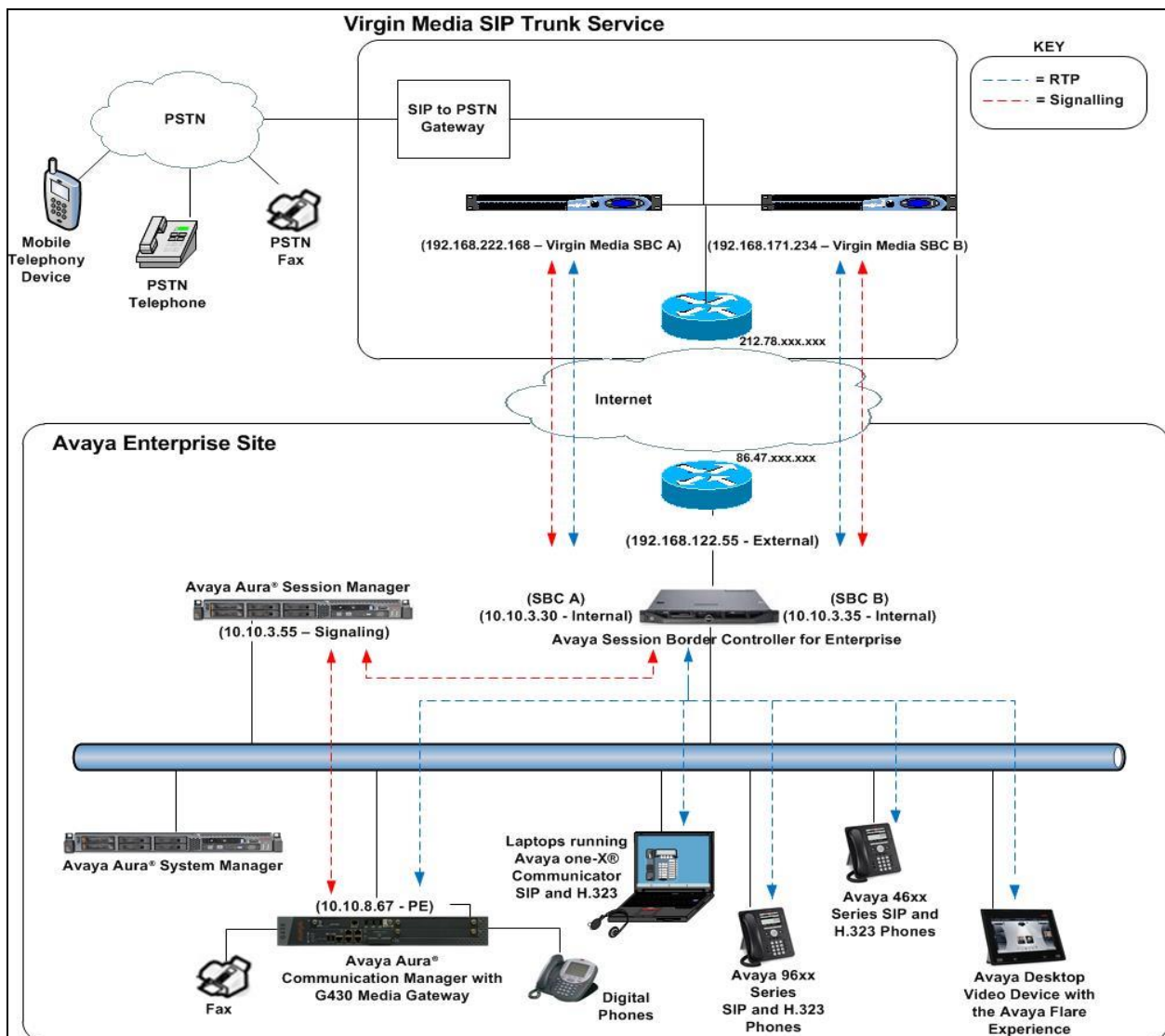


Figure 1: Test Setup of Virgin Media SIP Trunk to Avaya Enterprise

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 Session Manager on VM Version 8	R6.3.6 - 6.3.6.0.636005
Dell PowerEdge R620 running System Manager on VM Version 8	R6.3.6 - Build No. - 6.3.0.8.5682-6.3.8.3007 Software Update Revision No: 6.3.6.6.2103
Avaya S8800 Server running Communication Manager	R016x.03.0.124.0 -21291
Avaya Session Border Controller for Enterprise	6.2.1.Q07
Avaya 9670 IP Deskphone (H.323)	6.3
Avaya 96x0 IP Deskphone (H.323)	6.3
Avaya 9611 IP Deskphone (SIP)	6.2.2
Avaya 9608 IP Deskphone (SIP)	6.2.2
Avaya 9621 IP Deskphone (SIP)	6.2.2
Avaya 9608 IP Deskphone (SIP)	R6.2 SP1
Avaya one-X® Communicator (H.323) on Lenovo T510 Laptop PC	6.1.8.06-SP8-40314
Avaya Flare Experience for Windows	1.1.3.14
Avaya 2420 Digital Handset	R6
Analogue Handset	N/A
Analogue Fax	N/A
Virgin Media	
Genband Softswitch with Q20 Network SBC	Version 8.1

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 11
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks:	12000	0
Maximum Concurrently Registered IP Stations:	18000	3
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	41000	0
Maximum Video Capable IP Softphones:	18000	0
Maximum Administered SIP Trunks:	24000	10
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	0
Maximum Media Gateway VAL Sources:	250	1
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0

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

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

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 **10.10.73.5** 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	10.10.73.5	
default	0.0.0.0	
procr	10.10.8.67	
procr6	::	

5.3. Administer IP Network Region

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

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the Avaya SBCE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** is used.
- 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 codecs supported by Virgin Media were configured, namely **G.711A** and **G.729**.

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.729A	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				
FAX	Mode	Redundancy	ECM: y	
Modem	t.38-standard	0		
TDD/TTY	off	0		
Clear-channel	US	3		
	n	0		

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the 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)
- Set **Direct IP-IP Audio Connections** to **y**
- Set **Initial IP-IP Direct Media** to **y**
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.

add signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y Peer Server: SM		
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Near-end Node Name: procr		Far-end Node Name: SM100
Near-end Listen Port: 5060		Far-end Listen Port: 5060
		Far-end Network Region: 1
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? 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: 10000			
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 900			
Disconnect Supervision - In? y Out? Y			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	

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

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

On **Page 4** of this form:

- Set **Mark Users as Phone** to **y**
- Set **Send Transferring Party Information** to **n**
- Set **Network Call Direction** to **y** as this enables use of the SIP REFER message for call transfer supported by Virgin Media
- Set **Send Diversion Header** to **n**
- 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		
Mark Users as Phone? y		
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n		
Send Transferring Party Information? n		
Network Call Redirection? Y		
Send Diversion Header? n		
Support Request History? n		
Telephone Event Payload Type: 101		
Convert 180 to 183 for Early Media? n		
Always Use re-INVITE for Display Updates? y		
Identity for Calling Party Display: P-Asserted-Identity		
Block Sending Calling Party Location in INVITE? n		
Accept Redirect to Blank User Destination? n		
Enable Q-SIP? n		

5.7. Administer Calling Party Number Information

Use the **change private-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 - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
4	60	1	0118xxxxxx00	10	Total Administered: 5
4	61	1	0118xxxxxx00	10	Maximum Entries: 540

Note: The above configuration accepts all 4 digit numbers starting with 6, which includes all SIP and H.323 extension numbers, and passes them on with no prefix.

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 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 Reqd	
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 **change inc-call-handling-trmt trunk-group x** command is used to translate numbers **011xxxxxx40** to **011xxxxxx42** to the 4 digit extension by deleting all (**11**) of the incoming digits and inserting the extension number. 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	11	011xxxxxx40		all 6010		
public-ntwrk	11	011xxxxxx41		all 6012		
public-ntwrk	11	011xxxxxx42		all 6102		

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. **0035386781nnnn**)
- 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	-		0035386781nnnn	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. The number has been masked for security purposes. To use facilities for calls coming in from EC500 mobile phones, the number received in Communication Manager must exactly match the number specified in the above table.

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

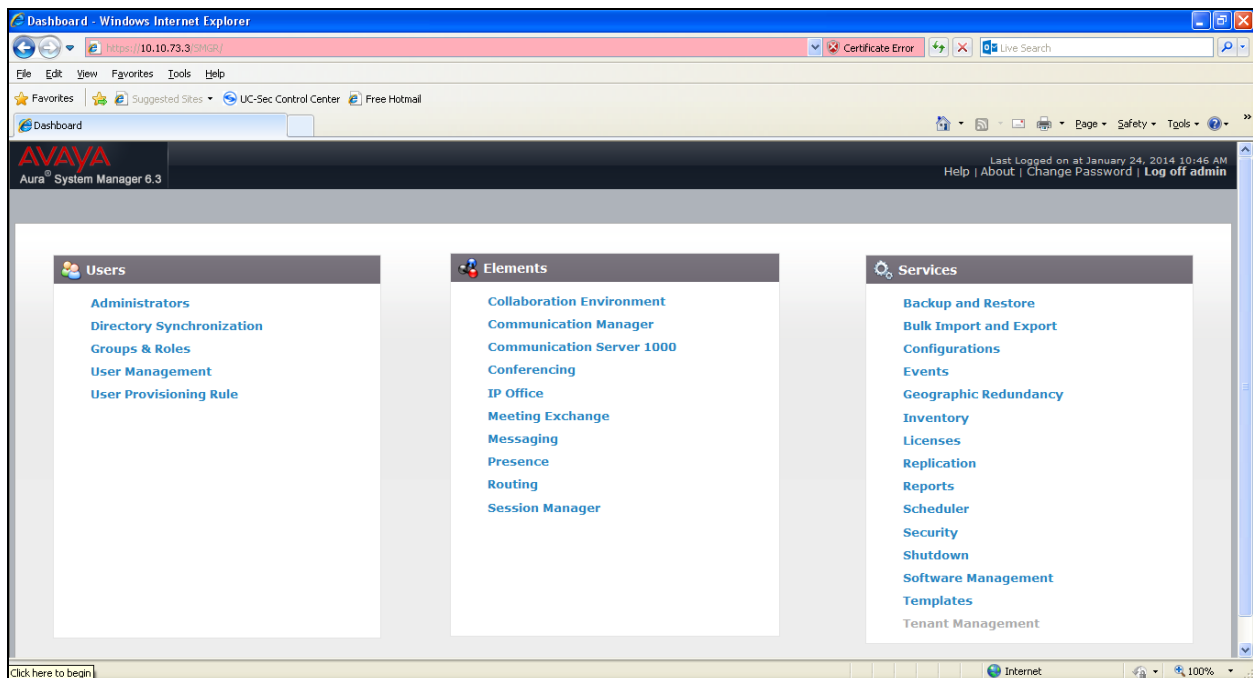
6. Configuring Avaya Aura® Session Manager

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

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

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.

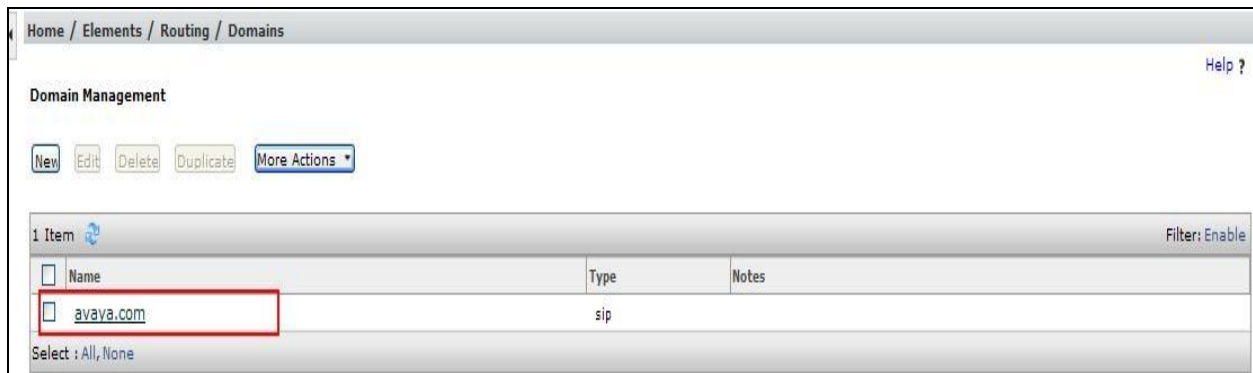


6.2. Administer SIP Domain

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.



6.3. Administer Locations

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

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

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

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

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

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

Home / Elements / Routing / Locations

Location Details

CommitCancel

General

* Name:

VM_SMGR

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

2000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

2000

Kbit/Sec

Location Pattern

AddRemove

7 Items

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.2.*	
<input type="checkbox"/>	* 10.10.3.*	
<input type="checkbox"/>	* 10.10.5.*	
<input type="checkbox"/>	* 10.10.73.*	
<input type="checkbox"/>	* 10.10.8.*	
<input type="checkbox"/>	* 10.10.9.*	
<input type="checkbox"/>	*	

Select : All, None

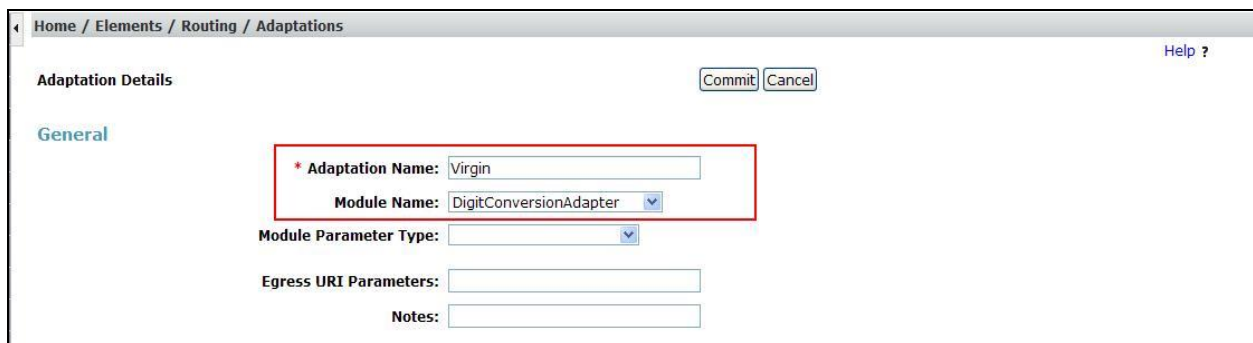
CommitCancel

6.4. Administer Adaptations

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

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

- In the **Adaptation name** field enter an informative name.
- In the **Module name** field click on the down arrow and then select the **<click to add module>** entry from the drop down list and type **DigitConversionAdapter** in the resulting New Module Name field.



Home / Elements / Routing / Adaptations

Adaptation Details Commit Cancel Help ?

General

* Adaptation Name:

Module Name:

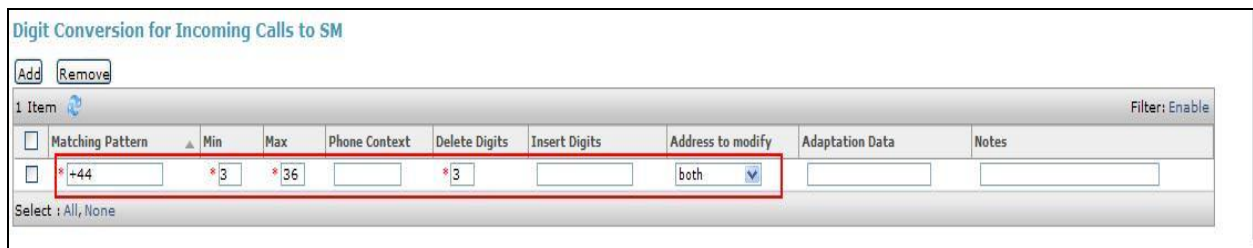
Module Parameter Type:

Egress URI Parameters:

Notes:

Scroll down the page and under **Digit Conversion for Incoming Calls to SM**, click the **Add** button and specify the digit manipulation to be performed as follows:

- Enter the leading digits that will be matched in the Matching Pattern field.
- In the **Min** and **Max** fields set the minimum and maximum digits allowed in the digit string to be matched.
- In the **Delete Digits** field enter the number of leading digits to be removed.
- In the **Insert Digits** field specify the digits to be prefixed to the digit string.
- In the **Address to modify** field specify the digits to manipulate by the adaptation. In this configuration, **both** was selected..



Digit Conversion for Incoming Calls to SM

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*+44	*3	*36		*3		both		

Select : All, None

This will ensure any incoming numbers will have the + symbol and international dialing code removed before being presented to Communication Manager.

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 'General' tab is selected. The 'Name' field is 'Session Manager'. The 'FQDN or IP Address' field is '10.10.73.5'. The 'Type' dropdown is set to 'Session Manager'. The 'Location' dropdown is set to 'VM_SMGR'. The 'Outbound Proxy' dropdown is empty. The 'Time Zone' dropdown is set to 'Europe/Dublin'. The 'Credential name' field is empty. The 'SIP Link Monitoring' dropdown is set to 'Use Session Manager Configuration'. There are 'Commit' and 'Cancel' buttons at the top right.

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 'Port' configuration section. It includes fields for 'TCP Failover port' and 'TLS Failover port', and 'Add' and 'Remove' buttons. Below is a table with 3 items. The table has columns: Port, Protocol, Default Domain, and Notes. The first three rows are highlighted with a red box.

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

Select : All, None

6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signaling 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 for 'Communication Manager'. The 'General' tab is active. A red box highlights the 'Name' (Communication Manager), 'FQDN or IP Address' (10.10.8.67), 'Type' (CM), and 'Notes' fields. Below this, the 'Adaptation' is set to 'None', 'Location' is 'VM_SMGR' (highlighted with a red box), and 'Time Zone' is 'Europe/Dublin'. Other fields include 'SIP Timer B/F (in seconds)' set to 4, 'Credential name' (empty), 'Call Detail Recording' set to 'none', and 'Loop Detection Mode' set to 'Off'. Buttons for 'Commit', 'Cancel', and 'Help ?' are at the top right.

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

This screenshot shows the 'Loop Detection' and 'SIP Link Monitoring' sections. 'Loop Detection Mode' is set to 'Off'. 'SIP Link Monitoring' is set to 'Use Session Manager Configuration'.

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 interface (see **Figure 1**). Set **Type** to **SIP Trunk** and **Adaptation** to that defined in **Section 6.4**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* **Name:** AvayaSBCE_Virgin_A

* **FQDN or IP Address:** 10.10.3.30

Type: SIP Trunk

Notes:

Adaptation: Virgin

Location: VM_SMGR

Time Zone: Europe/Dublin

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

Credential name:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screenshot shows the SIP Entity for Avaya SBCE Virgin B.

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

*** Name:** AvayaSBCE_Virgin_B

*** FQDN or IP Address:** 10.10.3.35

Type: SIP Trunk

Notes:

Adaptation: Virgin

Location: VM_SMGR

Time Zone: Europe/Dublin

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

Credential name:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (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 used in this configuration.

Home / Elements / Routing / Entity Links Help ?

Entity Links

3 Items Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	AvayaSBCE_Virgin_A_Link	Session Manager	TCP	5060	AvayaSBCE_Virgin_A	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	AvayaSBCE_Virgin_B_Link	Session Manager	TCP	5060	AvayaSBCE_Virgin_B	<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"/>	

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 'Commit' and 'Cancel' buttons at the top right. The 'General' section contains 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 '10.10.8.67' and Type 'CM'. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. Below is a table with 1 item, showing a time range of 00:00 to 23:59 for 24/7. The table has columns for Ranking, Name, days of the week, Start Time, End Time, and Notes.

Name	FQDN or IP Address	Type	Notes
Communication Manager	10.10.8.67	CM	

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	✓	✓	✓	✓	✓	✓	✓	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.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
AvayaSBCE_Virgin_A	10.10.3.30	SIP Trunk	

Time of Day

1 Item Filter: Enable

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

Select : All, None

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

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
AvayaSBCE_Virgin_B	10.10.3.35	SIP Trunk	

Time of Day

1 Item Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	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

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: 00

* Min: 2

* Max: 16

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	VM_SMGR		to_Virgin_SBC_A	0	<input type="checkbox"/>	AvayaSBCE_Virgin_A	
<input type="checkbox"/>	VM_SMGR		to_Virgin_SBC_B	2	<input type="checkbox"/>	AvayaSBCE_Virgin_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

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

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"/>	VM_SMGR		to_Communication Manager	0	<input type="checkbox"/>	Communication Manager	

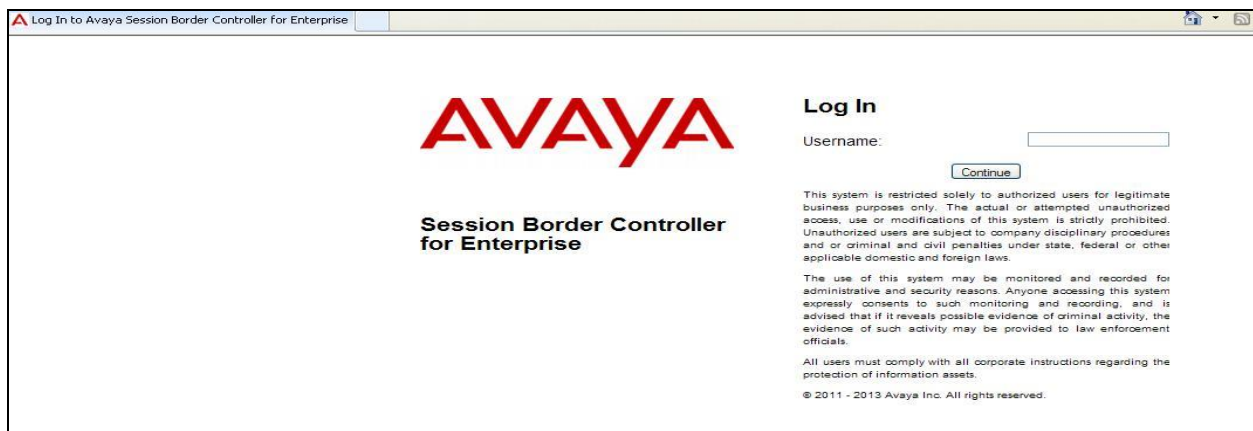
Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

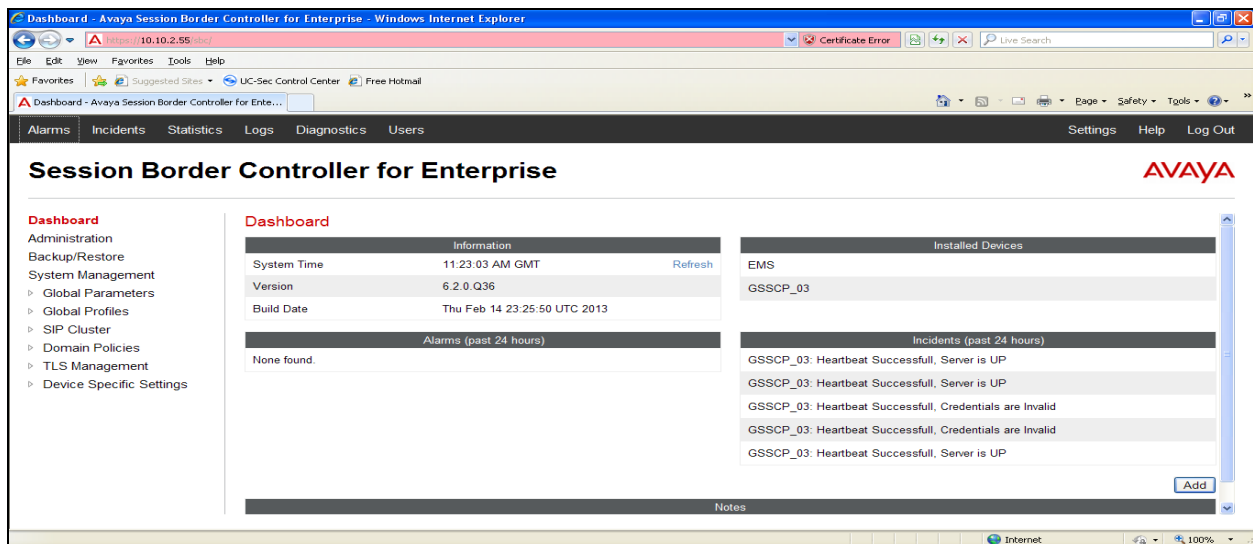
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP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

7.1. Access Avaya Session Border Controller for Enterprise

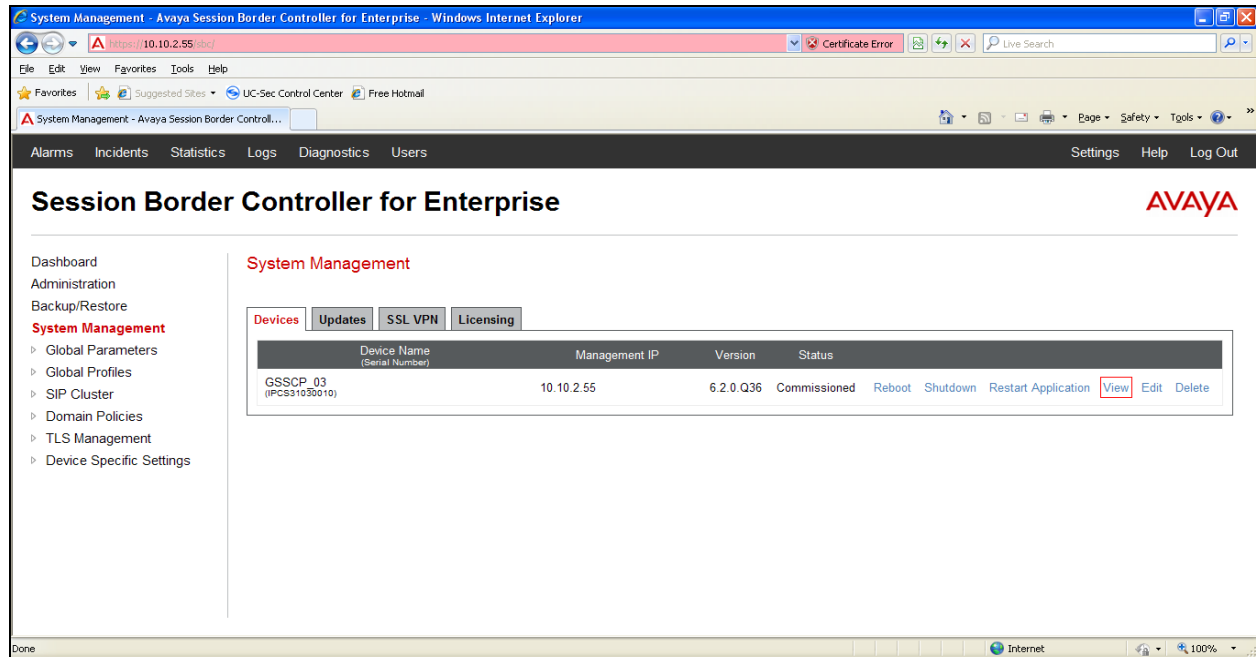
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



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.

System Information: GSSCP_03

General Configuration

Appliance NameGSSCP_03

Box TypeSIP

Deployment ModeProxy

Device Configuration

HA ModeNo

Two Bypass ModeNo

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.10.3.30	10.10.3.30	255.255.255.0	10.10.3.1	A1
192.168.122.55	192.168.122.55	255.255.255.128	192.168.122.7	B1

DNS Configuration

Primary DNS10.10.7.100

Secondary DNS10.10.101.115

DNS LocationDMZ

DNS Client IP10.10.3.30

Management IP(s)

IP10.10.2.55

7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all UC-Sec 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_SM** 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

Click on **Next** and then on **Finish** (not shown).

Profile: Avaya_SM

General

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

Next

Default values can be used for the **Advanced Settings** window. Click **Finish**

Profile: Avaya_SM X

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

Finish

7.2.2. Server 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 **Virgin** 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

Click on **Next** and then on **Finish** (not shown).

Profile: Virgin

General

Hold Support: ☒ None ☐ RFC2543 - c=0.0.0.0 ☐ RFC3264 - a=sendonly

180 Handling: ☒ None ☐ SDP ☐ No SDP

181 Handling: ☒ None ☐ SDP ☐ No SDP

182 Handling: ☒ None ☐ SDP ☐ No SDP

183 Handling: ☒ None ☐ SDP ☐ No SDP

Refer Handling: ☐

URI Group:

3xx Handling: ☐

Diversion Header Support: ☐

Delayed SDP Handling: ☐

Re-Invite Handling: ☐

T.38 Support: ☒

URI Scheme: ☒ SIP ☐ TEL ☐ ANY

Via Header Format: ☒ RFC3261 ☐ RFC2543

Next

Default values can be used for the **Advanced Settings** window. Click **Finish**.

Profile: Virgin X

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

Finish

7.2.3. Routing

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

Routing information is required for routing to Session Manager on the internal side and 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.

Create a Routing Profile for both Session Manager and Virgin Media SIP trunk. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.

In the new window that appears (not shown), enter the following values. Use default values for all remaining fields:

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

Click **Finish**.

The following screen shows the Routing Profile to Session Manager

The screenshot shows the 'Routing Profiles: Avaya_SM' configuration window. On the left, a sidebar lists 'Routing Profiles' with options: 'default', 'Avaya_SM' (highlighted), 'Virgin_SBC_A', and 'Virgin_SBC_B'. The main area has a blue header bar with the text 'Click here to add a description.' Below this, a 'Routing Profile' section contains a table with the following data:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	10.10.73.5	---

Below the table, there are 'View' and 'Edit' links. The entire table and links are enclosed in a red rectangular box. At the top right of the main area, there are buttons for 'Rename', 'Clone', and 'Delete'. An 'Add' button is located at the bottom right of the 'Routing Profile' section.

The following screen shows the Routing Profile to Virgin Media SBC A.

Routing Profiles: Virgin_SBC_A

Buttons: Add, Rename, Clone, Delete

Routing Profiles List:

- default
- Avaya_SM
- Virgin_SBC_A
- Virgin_SBC_B

Click here to add a description.

Routing Profile

Buttons: Add, View, Edit

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	192.168.222.186:5060	---

The following screen shows the Routing Profile to Virgin Media SBC B.

Routing Profiles: Virgin_SBC_B

Buttons: Add, Rename, Clone, Delete

Routing Profiles List:

- default
- Avaya_SM
- Virgin_SBC_A
- Virgin_SBC_B

Click here to add a description.

Routing Profile

Buttons: Add, View, Edit

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	192.168.171.234:5060	---

7.2.4. Server Configuration– Avaya Aura® Session Manager

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 you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles** → **Server Configuration** and click on **Add Profile** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

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

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

Field	Value
Server Type	Call Server
IP Addresses / Supported FQDNs	10.10.73.5
Supported Transports	<input checked="" type="checkbox"/> TCP, <input type="checkbox"/> UDP, <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	
TLS Port	

On the **Advanced** tab:

- Select **Avaya_SM** for **Interworking Profile** defined in **Section 7.2.1**
 - Select **Virgin_Media** for **Signaling Manipulation Script**
- Note:** Signaling Manipulation Scripting is discussed in **Section 7.2.7**
- Click **Finish**

The screenshot shows a window titled "Server Configuration Profile - Advanced" with a close button (X) in the top right corner. The window contains several configuration options:

- Enable DoS Protection**: A checkbox that is currently unchecked.
- Enable Grooming**: A checkbox that is currently unchecked.
- Interworking Profile**: A dropdown menu showing "Avaya_SM". This dropdown is highlighted with a red rectangle.
- Signaling Manipulation Script**: A dropdown menu showing "Virgin_Media". This dropdown is also highlighted with a red rectangle.
- TCP Connection Type**: Three radio buttons labeled "SUBID", "PORTID", and "MAPPING". The "SUBID" radio button is selected.
- Finish**: A button located at the bottom center of the window.

7.2.5. Server Configuration – Virgin Media

To define the first Virgin Media SBC A as a Trunk Server, navigate to select **Global Profiles** → **Server Configuration** and click on **Add Profile** and enter a descriptive name. On the **Add Server Configuration Profile** tab, click on **Edit** and set the following:

- Select **Server Type** as **Trunk Server**
- Set **IP Address** to **192.168.222.186** (Virgin Media SBC A)
- **Supported Transports**: Check **UDP**
- **UDP Port**: **5060**
- Hit **Next**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs

Server Configuration Profile - General

Server Type: Trunk Server

IP Addresses / Supported FQDNs
Separate entries with commas: 192.168.222.186

Supported Transports:
☐ TCP
☒ UDP
☐ TLS

TCP Port:

UDP Port: 5060

TLS Port:

Finish

On the **Advanced** tab:

- Select **Virgin** for **Interworking Profile** as defined in **Section 7.2.2**.
- Click **Finish**

Server Configuration Profile - Advanced

Enable DoS Protection: ☐

Enable Grooming: ☐

Interworking Profile: Virgin

Signaling Manipulation Script: None

UDP Connection Type: ☒ SUBID ☐ PORTID ☐ MAPPING

Finish

To define the second Virgin Media SBC B as a Trunk Server, navigate to select **Global Profiles** → **Server Configuration** and click on **Add Profile** and enter a descriptive name. On the **Add Server Configuration Profile** tab, click on **Edit** and set the following:

- Select **Server Type** as **Trunk Server**
- Set **IP Address** to **192.168.171.234** (Virgin Media SBC B)
- **Supported Transports**: Check **UDP**
- **UDP Port**: **5060**
- Hit **Next**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs

Server Configuration Profile - General

Server Type: Trunk Server

IP Addresses / Supported FQDNs: 192.168.171.234

Supported Transports: ☐ TCP, ☒ UDP, ☐ TLS

TCP Port:

UDP Port: 5060

TLS Port:

Finish

On the **Advanced** tab:

- Select **Virgin** for **Interworking Profile** as defined in **Section 7.2.2**.
- Click **Finish**

Server Configuration Profile - Advanced

Enable DoS Protection: ☐

Enable Grooming: ☐

Interworking Profile: Virgin

Signaling Manipulation Script: None

UDP Connection Type: ☒ SUBID, ☐ PORTID, ☐ MAPPING

Finish

7.2.6. Topology Hiding

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

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

- In the **Profile Name** field enter a descriptive name for Session Manager and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **Request-Line**, **To** and **From** as the required headers from the **Header** drop down menu
- Select the required action from the **Required Action** drop down menu, **Auto** was used for test

The screenshot shows the 'Topology Hiding Profiles: Avaya_SM' configuration page. On the left, a sidebar lists 'Topology Hiding Profiles' with options: 'default', 'cisco_th_profile', 'Avaya_SM' (highlighted in red), and 'Virgin'. An 'Add' button is above this list. 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
To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---

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** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** 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 and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **Request-Line, To** and **From** as the required headers from the **Header** drop down menu
- Select the required action from the **Required Action** drop down menu, **Auto** was used for test

Topology Hiding Profiles: Virgin

Add

Topology Hiding Profiles

default
cisco_th_profile
Avaya_SM
Virgin

Click here to add a description.

Topology Hiding

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

Edit

CMN; Reviewed:
SPOC 5/29/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

43 of 55
Virgin_CM63_SM

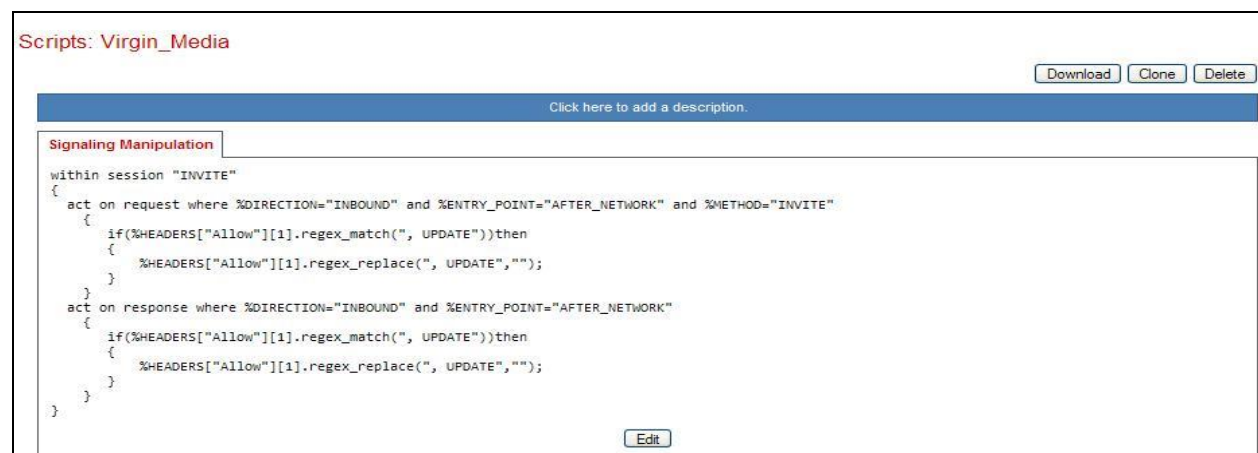
7.2.7. Signalling Manipulation

Signalling manipulation is required in some cases to ensure effective interworking. During test, an issue was found in the use of the UPDATE message between Virgin Media SIP Trunk service and the Avaya enterprise that could not be resolved by other methods such as Server Interworking and Signaling Rules. The issue occurred when the UPDATE message was sent from the Virgin Media network to change the codec to T.38 for fax calls. The enterprise was not successfully changing the codec and the fax calls were failing. The solution was to remove UPDATE from the Supported header in messages going from the enterprise to the network. This prompts the network to use re-INVITE instead of UPDATE.

To define the signalling manipulation to remove UPDATE from the Supported header in outgoing messages, navigate to **Global Profiles → Signaling Manipulation** in the main menu on the left hand side. Click on **Add Script** and enter a title and the script in the script editor. The title in the example is *Virgin_Media*. The script text is as follows:

```
within session "INVITE"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and %METHOD="INVITE"
  {
    if(%HEADERS["Allow"][1].regex_match(", UPDATE"))then
    {
      %HEADERS["Allow"][1].regex_replace(", UPDATE","");
    }
  }
  act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    if(%HEADERS["Allow"][1].regex_match(", UPDATE"))then
    {
      %HEADERS["Allow"][1].regex_replace(", UPDATE","");
    }
  }
}
```

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** in the **UC-Sec Control Center** menu on the left hand side and click on **Add IP**. Enter details in the blank box that appears at the end of the list.

- Define the two internal IP address with screening mask and assign to interface **A1**
- Select **Save** to save the information
- 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: GSSCP_03

Devices: GSSCP_03

Network Configuration | Interface Configuration

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

A1 Netmask: 255.255.255.0 | A2 Netmask: | B1 Netmask: 255.255.255.128 | B2 Netmask: | Add | Save | Clear

IP Address	Public IP	Gateway	Interface	
10.10.3.30		10.10.3.1	A1	Delete
192.168.122.55		192.168.122.7	B1	Delete
10.10.3.35		10.10.3.1	A1	Delete

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

Network Management: GSSCP_03

Devices: GSSCP_03

Network Configuration | Interface Configuration

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

7.4. 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** in the **UC-Sec Control Center** 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 Media 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 Media 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 the external SIP signalling:

- 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 the **external** signalling interface IP address defined in **Section 7.3**
- Select **UDP** port number, **5060** is used for the SIP Trunk

Signaling Interface: GSSCP_03

Devices

GSSCP_03

Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.3.30	5060	---	---	None	Edit Delete
Ext_Sig	192.168.122.55	5060	5060	---	None	Edit Delete
Int_Sig_2	10.10.3.35	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** in the **UC-Sec Control Center** menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

- Select **Add Media Interface** 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 an **internal** media interface IP address defined in **Section 7.3**
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select **Add Media Interface** 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 (Virgin Media SIP Trunk service)

Media Interface: GSSCP_03

Devices

GSSCP_03

Media Interface

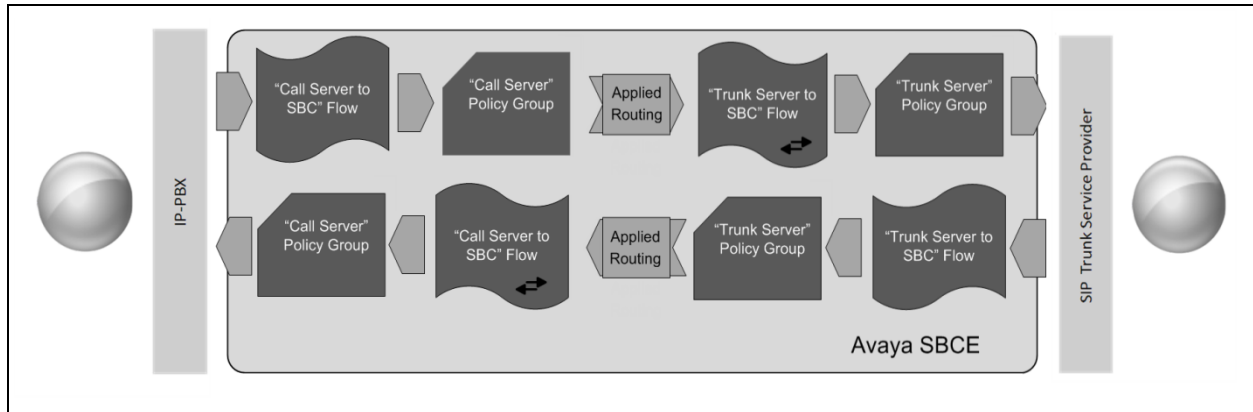
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP	Port Range	
Int_Media	10.10.3.30	35000 - 51000	Edit Delete
Ext_Media	192.168.122.55	35000 - 51000	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 Media SBC A and Virgin Media SBC B for the purposes of the testing and documentation.

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

Subscriber Flows

Server Flows

hover over a row to see its description.

Server Configuration: Avaya_SM

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	default-low	Virgin_SBC_A	View Clone Edit Delete
<input type="text" value="2"/>	Call_Server_B	*	Ext_Sig	Int_Sig_2	default-low	Virgin_SBC_B	View Clone Edit Delete

Server Configuration: Virgin_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	Ext_Sig	default-low	Avaya_SM	View Clone Edit Delete

Server Configuration: Virgin_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_2	Ext_Sig	default-low	Avaya_SM	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.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for the Session Manager, in this case **Call_Server_A** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.2.4** for Session manager.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**.
- In the **Signaling Interface** drop-down menu, select the first internal SIP signalling interface defined in **Section 7.4.1**.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.4.2**.
- In the **Routing Profile** drop-down menu, select the routing profile of Virgin SBC A defined in **Section 7.2.3**.
- 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_SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Media
End Point Policy Group	default-low
Routing Profile	Virgin_SBC_A
Topology Hiding Profile	Avaya_SM
File Transfer Profile	None

Finish

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 Media SBC A and Virgin Media SBC B), navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Virgin Media SBC A, in this case **Trunk_Server_A** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.2.5** for Virgin Media SBC A
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.3**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Virgin Media defined in **Section 7.2.6** and click **Finish**.

Flow: Trunk_Server_A

Flow Name	Trunk_Server_A
Server Configuration	Virgin_SBC_A
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
End Point Policy Group	default-low
Routing Profile	Avaya_SM
Topology Hiding Profile	Virgin
File Transfer Profile	None

Finish

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

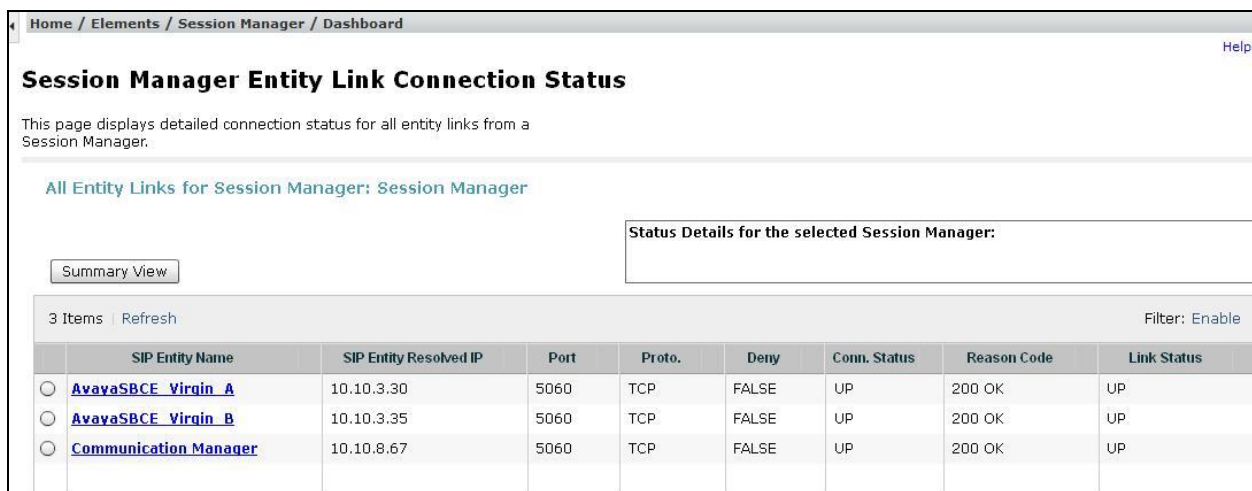
8. Configure Virgin Media SIP Trunk Equipment

The configuration of the Virgin Media equipment used to support VirginMedia'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

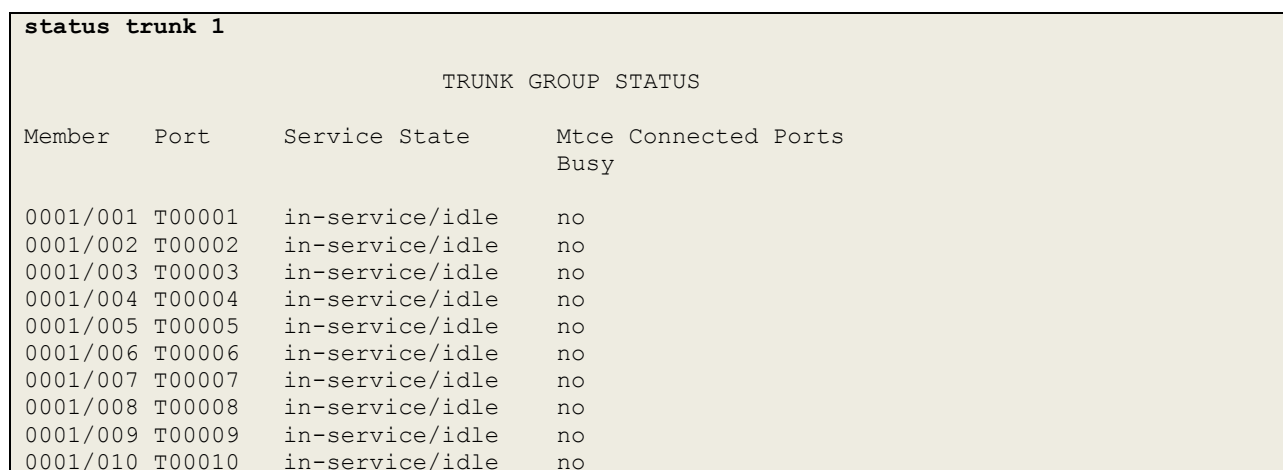
This section provides steps that may be performed to verify that the solution is configured correctly.

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 / Dashboard								Help
Session Manager Entity Link Connection Status								
This page displays detailed connection status for all entity links from a Session Manager.								
All Entity Links for Session Manager: Session Manager								
Summary View								
Status Details for the selected Session Manager:								
3 Items Refresh								Filter: Enable
	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	AvayaSBCE_Virgin_A	10.10.3.30	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	AvayaSBCE_Virgin_B	10.10.3.35	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Communication Manager	10.10.8.67	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: GSSCP_R3S3

Devices	Call Trace	Packet Capture	Captures
GSSCP_R3S3	<div> <div>Packet Capture Configuration</div> <div> <div>Status</div> <div>Ready</div> </div> <div> <div>Interface</div> <div>B1</div> </div> <div> <div>Local Address IP[:Port]</div> <div>192.168122.59</div> </div> <div> <div>Remote Address *, *:Port, IP, IP:Port</div> <div>*</div> </div> <div> <div>Protocol</div> <div>UDP</div> </div> <div> <div>Maximum Number of Packets to Capture</div> <div>1000</div> </div> <div> <div>Capture Filename Using the name of an existing capture will overwrite it.</div> <div>SIP_Trunk_Test.pcap</div> </div> <div> <div>Start Capture</div> <div>Clear</div> </div> </div>		

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

Trace: GSSCP_R3S3

Devices
GSSCP_R3S3

Call Trace

Packet Capture

Captures

Refresh

File Name	File Size (bytes)	Last Modified	
SIP_Trunk_Test_20130927113029.pcap	4,096	September 27, 2013 11:33:45 AM IST	Delete

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to 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] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3, May 2013.
- [2] *Administering Avaya Aura® System Platform*, Release 6.3, May 2013.
- [3] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, May 2013
- [4] *Avaya Aura® Communication Manager 6.3 Documentation library*, August 2013.
- [5] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013
- [6] *Implementing Avaya Aura® System Manager* Release 6.3, May 2013
- [7] *Upgrading Avaya Aura® System Manager to 6.3.2*, May 2013.
- [8] *Administering Avaya Aura® System Manager* Release 6.3, May 2013
- [9] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013
- [10] *Implementing Avaya Aura® Session Manager* Release 6.3, May 2013
- [11] *Upgrading Avaya Aura® Session Manager* Release 6.3, May 2013
- [12] *Administering Avaya Aura® Session Manager* Release 6.3, June 2013,
- [13] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2 June 2013
- [14] *Upgrading Avaya Session Border Controller for Enterprise* Release 6.2 July 2013
- [15] *Administering Avaya Session Border Controller for Enterprise* Release 6.2 March 2013
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2014 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.