



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 BT Ireland SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between BT Ireland 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. BT Ireland 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 BT Ireland'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 BT Ireland SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

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

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 BT Ireland, calls made to SIP, H.323, Digital and Analogue telephones at the enterprise.
- All inbound PSTN calls were routed to the enterprise across the SIP trunk to BT Ireland.
- Outgoing calls from the enterprise site completed via BT Ireland's SIP Trunk to PSTN destinations, calls made from SIP, H.323, Digital and Analogue telephones.
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to BT Ireland.
- Inbound and outbound PSTN calls to/from Avaya One-X® Communicator and Avaya Flare® Experience for Windows softphones.
- Calls using the G.729 and G.711A codecs.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using T.38.
- Caller ID Presentation and Caller ID Restriction.
- DTMF transmission using RFC 2833.
- Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer and conference.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Off-net call forwarding and twinning.
- Transmission and response of SIP OPTIONS messages sent by BT Ireland's SIP Trunk requiring Avaya response and sent by Avaya requiring BT Ireland response.

2.2. Test Results

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

- When there were no matching codecs in the SDP offer of an outbound call, "408 Service Unavailable" response was returned from the BT Ireland network. The more commonly used response is "488 Not Acceptable Here".
- No inbound toll free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Access to Emergency Services was not tested as no test call had been booked with the Emergency Services Operator.

2.3. Support

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

For technical support on BT Ireland products described in these Application Notes, please contact BT Ireland Customer Support at:

- Telephone: 1800924924
- Telephone: +353 1 4328846

3. Reference Configuration

The following equipment in **Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to BT Ireland'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 16xx series IP telephones (with H.323 firmware), Avaya A175 Desktop Video Device running Avaya 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 Avaya Flare® Experience for Windows running on a laptop PC.

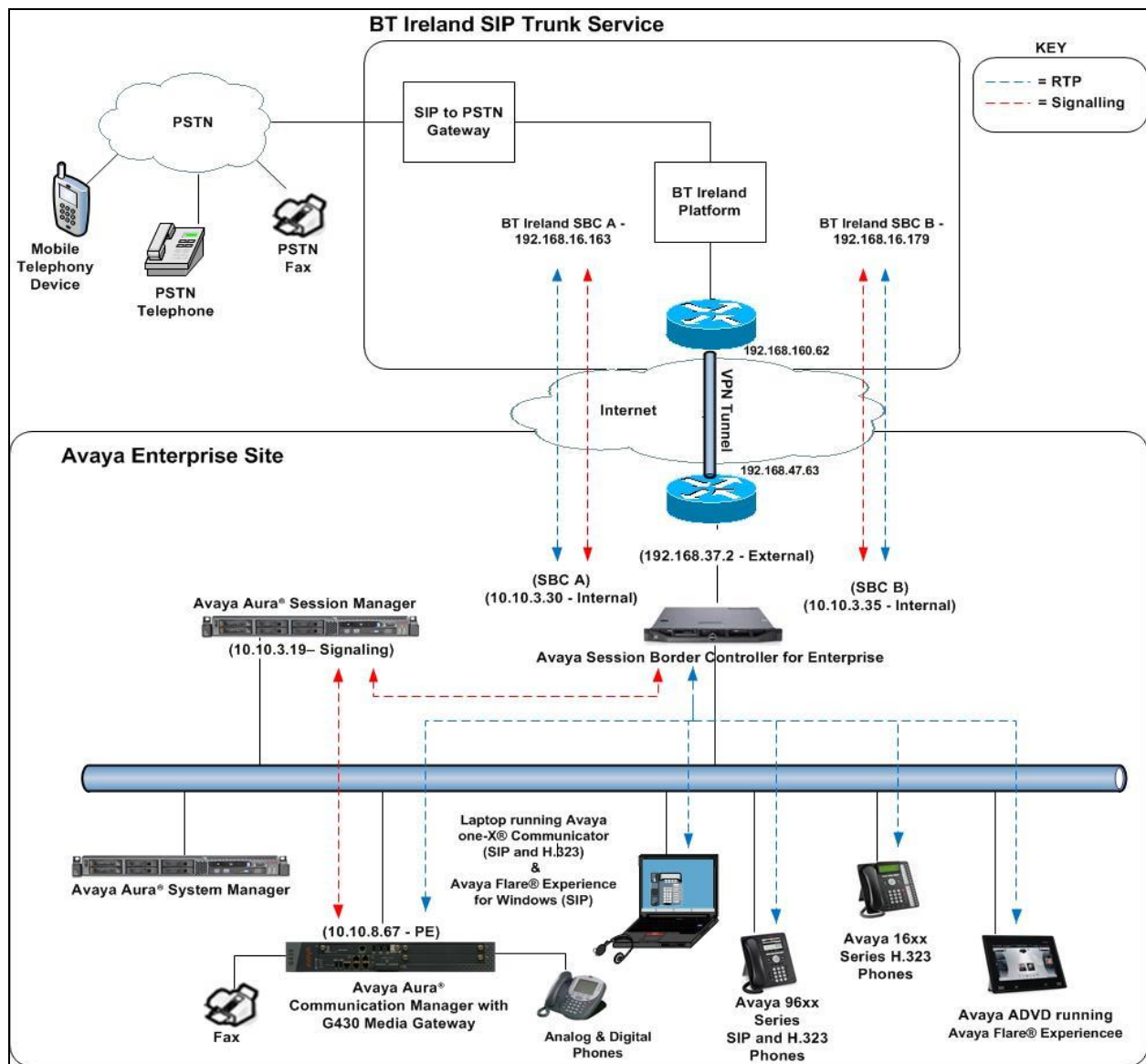


Figure 1: Test Setup BT Ireland SIP Trunk to Avaya Enterprise

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	6.3.10 - 6.3.10.0.631008
Dell PowerEdge R620 running System Manager on VM Version 8	6.3.10 - Build No. - 6.3.0.8.5682-6.3.8.4514 Software Update Revision No: 6.3.10.7.2656
Avaya S8300D Server running Avaya Aura® Communication Manager	R016x.03.0.124.0 -21754
Avaya Session Border Controller for Enterprise	Version 6.2.1.Q18
Avaya 1600 IP Deskphone (H.323)	1.3.6
Avaya 9670 IP DeskPhone (H.323)	6.4
Avaya 96x0 IP DeskPhone (H.323)	6.4
Avaya 9611 IP DeskPhone (SIP)	6.4.1
Avaya 9608 IP DeskPhone (SIP)	6.4.1
Avaya 9621 IP DeskPhone (SIP)	6.4.1
Avaya 9608 IP DeskPhone (SIP)	6.4.1
Avaya A175 Desktop Video Device with Avaya Flare® Experience	1.1.3
Avaya one-X® Communicator (H.323 & SIP) on Lenovo T510 Laptop PC	6.2.4.07-FP4
Avaya Flare® Experience for Windows	1.1.3.14
Avaya Digital Handset	N/A
Analogue Handset	N/A
Analogue Fax	N/A
BT Ireland	
BT Ireland SIP Trunk	Genband Q20 SBC R.8.3.2.0 Genband Experius Call Server R.17.0.2.15

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 BT Ireland 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 BT Ireland 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 BT Ireland 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 Session Manager. In this case, **SM100** and **10.10.3.19** 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	10.10.3.19	
default	0.0.0.0	
procr	10.10.8.67	
procr6	::	

5.3. Administer IP Network Region

Use the **change ip-network-region x** command where x is the desired network-region to set the following values:

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

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


5.4. Administer IP Codec Set

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

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

BT Ireland SIP Trunk supports T.38 for transmission of fax. Navigate to **Page 2** and define fax properties 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 Signalling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the BT Ireland 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 Communication Manager to automatically detect if the peer server is a Session Manager.
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Far-end Node Name** to Session Manager (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 Communication Manager 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 **n**.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).

The default values for the other fields may be used.

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? n	
	Alternate Route Timer(sec): 6	

5.6. Administer SIP Trunk Group

A trunk group is associated with the signalling 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 BT Ireland 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 national formats.

add trunk-group 1		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
UUI 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 **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 BT Ireland.
- 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? 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		

5.7. Administer Calling Party Number Information

Use the **change private-numbering x** 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	14xxxxx0	10	Total Administered: 2
4	61	1	14xxxxx0	10	Maximum Entries: 540.

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to BT Ireland'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							
ARS DIGIT ANALYSIS TABLE							
Location: all				Percent Full: 0			
	Dialed String	Total Min 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	

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 BT Ireland 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 BT Ireland correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers **014xxxxxx0**, **014xxxxxx1**, and **014xxxxxx2** 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	10	014xxxxxx0	all	6010		
public-ntwrk	10	014xxxxxx1	all	6012		
public-ntwrk	10	014xxxxxx2	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.**089434xxxx**).
- 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	Application	Dial	CC	Phone Number	Trunk	Config	Dual		
Extension		Prefix			Selection	Set	Mode		
6102	EC500	-		089434xxxx	1	1			
-									

Note: The phone number shown is for a mobile phone used for testing at Avaya Labs and is in national format with national dialling prefix 0. 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

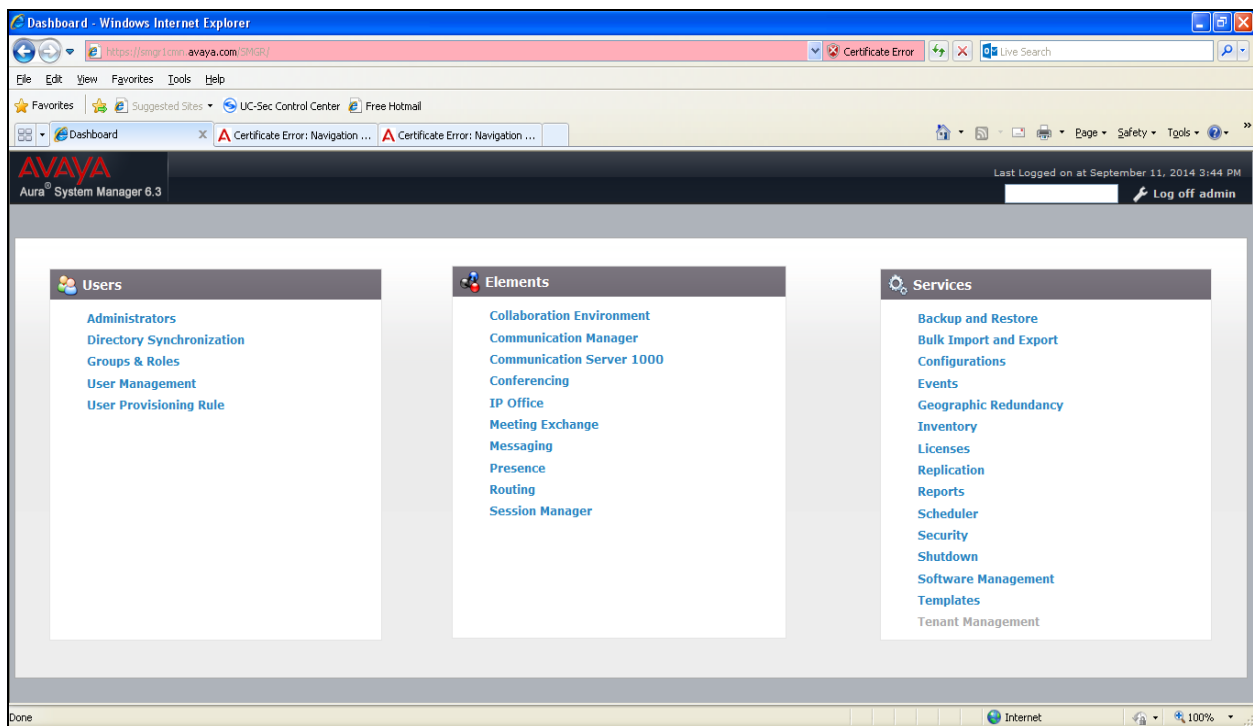
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- 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.

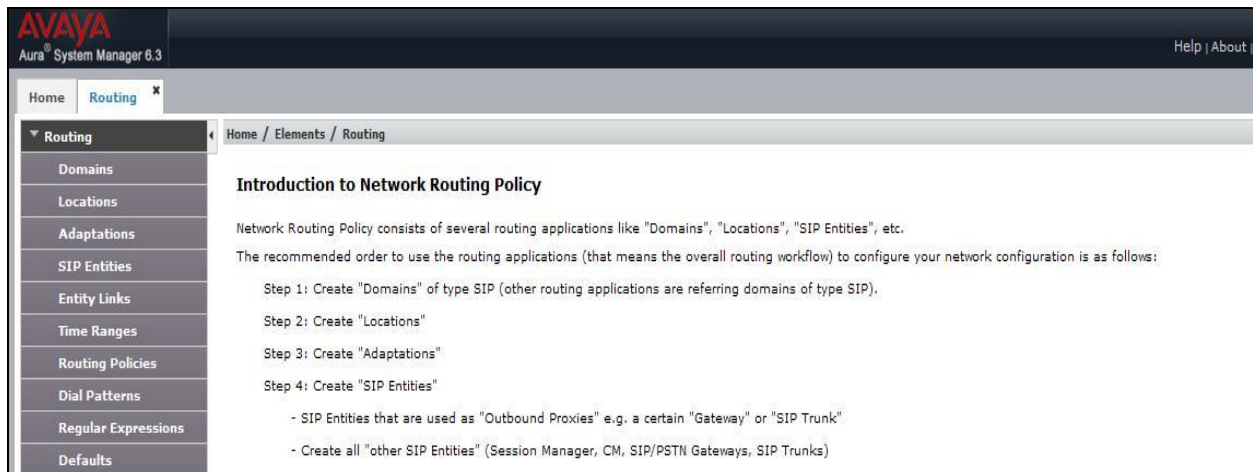
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. Log in to Avaya Aura® System Manager

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



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.

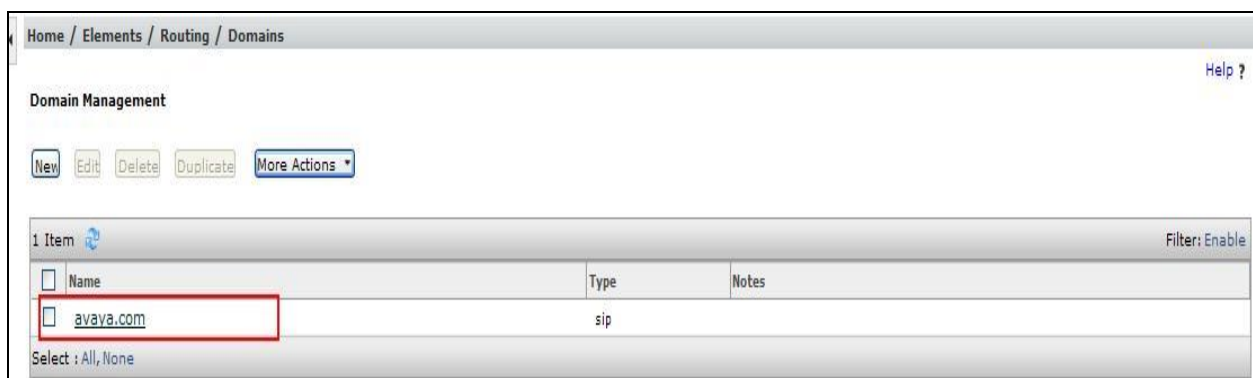


6.2. Administer SIP Domain

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.

The screenshot displays the Avaya Session Manager Administration console. The breadcrumb navigation at the top reads 'Home / Elements / Routing / Locations'. The 'Location Details' section is active, showing the 'General' tab. The 'Name' field is populated with 'VM_SMGR'. Below it, the 'Notes' field is empty. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox that is unchecked. The 'Listed Directory Number' and 'Associated CM SIP Entity' fields are empty. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' set to 'Kbit/sec', with empty fields for 'Total Bandwidth' and 'Multimedia Bandwidth'. The 'Audio Calls Can Take Multimedia Bandwidth' checkbox is checked. Below the 'Location Details' section is the 'Location Pattern' section. It has 'Add' and 'Remove' buttons. A table lists 7 items, each with a checkbox, an 'IP Address Pattern' (e.g., '10.10.2.*'), and a 'Notes' column. At the bottom of the 'Location Pattern' section, there is a 'Select : All, None' dropdown and 'Commit' and 'Cancel' buttons.

IP Address Pattern	Notes
10.10.2.*	
10.10.3.*	
10.10.5.*	
10.10.73.*	
10.10.8.*	
10.10.9.*	

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 during testing 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.
- **Module parameter** **MIME =no** Strips MIME message bodies on egress from Session Manager.
fromto=true Modifies from and to headers of a message.

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

Help ?

General

* Adaptation Name:

Module Name:

Module Parameter Type:

Add Remove

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	fromto	<input type="text" value="true"/>
<input type="checkbox"/>	MIME	<input type="text" value="no"/>

Select : All, None

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 the dialed number is the target so **both** have been selected.

Digit Conversion for Incoming Calls to SM

Add
Remove

1 Item
Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*+353	*4	*16		*4	0	both		

Select : All, None

This will ensure any incoming numbers will have the **+353** E.164 international dialing code removed and replaced with **0** 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 signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP Entity, **CM** for a Communication Manager SIP Entity and **SIP Trunk** for the Avaya SBCE SIP Entity
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities.

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Avaya SBCE SIP Entity

6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface 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. A red box highlights the main configuration fields: Name (Session_Manager), FQDN or IP Address (10.10.3.19), Type (Session Manager), Notes, Location (VM_SMGR), Outbound Proxy, Time Zone (Europe/Dublin), and Credential name. Below the red box, the 'SIP Link Monitoring' section shows 'Use Session Manager Configuration' selected. Buttons for 'Commit' and 'Cancel' are at the top right, and a 'Help ?' link is in the top right corner.

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. A red box highlights the first three rows of the table, which are: Port 5060, Protocol TCP, Default Domain avaya.com; Port 5060, Protocol UDP, Default Domain avaya.com; and Port 5061, Protocol TLS, Default Domain avaya.com. The table has columns for Port, Protocol, Default Domain, and Notes. At the bottom, there is a 'Select : All, None' option.

Port	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.

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: Communication_Manager

* FQDN or IP Address: 10.10.8.67

Type: CM

Notes:

Adaptation:

Location: VM_SMGR

Time Zone: Europe/Dublin

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

Credential name:

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set **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.

The screenshot displays the 'SIP Entity Details' configuration page for an Avaya SBCE. The page is titled 'Home / Elements / Routing / SIP Entities' and includes a 'Help ?' link. The 'SIP Entity Details' section has a 'Commit' button and a 'Cancel' button. The 'General' tab is selected, showing the following fields:

- Name:** AvayaSBCE
- FQDN or IP Address:** loadbalance.avaya.com
- Type:** SIP Trunk
- Notes:** (empty text area)
- Adaptation:** BT_Ireland
- Location:** VM_SMGR
- Time Zone:** Europe/Dublin
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text area)
- Call Detail Recording:** egress

The 'Loop Detection' section shows:

- Loop Detection Mode:** Off

The 'SIP Link Monitoring' section shows:

- 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 **Trusted** from the drop-down menu to make the other system trusted.

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

Home / Elements / Routing / Entity Links

Entity Links

New Edit Delete Duplicate More Actions

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"/>	Avaya_SBCE	Session_Manager	TCP	5060	Avaya_SBCE	<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"/>	

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' form in a web application. The breadcrumb trail at the top is 'Home / Elements / Routing / Routing Policies'. The form has three main sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. In the 'General' section, the 'Name' field is set to 'to_Communication_Manager', 'Disabled' is unchecked, 'Retries' is 0, and 'Notes' is empty. In the 'SIP Entity as Destination' section, a 'Select' button is present, and a table below it lists the selected entity 'Communication_Manager' with FQDN/IP '10.10.8.67' and Type 'CM'. In the 'Time of Day' section, there are 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. A table below shows one item with a ranking of 0, a name of '24/7', and a time range from 00:00 to 23:59. The table has columns for days of the week (Mon-Sun) and checkboxes for each day, all of which are checked. The 'Notes' column for this item contains 'Time Range 24/7'. At the bottom, there is a 'Select : All, None' option.

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel Help ?

General

* Name: to_Communication_Manager

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Communication_Manager	10.10.8.67	CM	

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
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.

The screenshot shows the 'Routing Policy Details' configuration page. The 'General' tab is active, showing the policy name 'to_AvayaSBCE', a 'Disabled' checkbox, 'Retries' set to 0, and a 'Notes' field. Below this, the 'SIP Entity as Destination' section has a 'Select' button and a table listing destinations. The table has columns for Name, FQDN or IP Address, Type, and Notes. One entry is visible: 'AvayaSBCE' with FQDN 'loadbalance.avaya.com' and Type 'SIP Trunk'. The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons, and a table showing a single time range item for 24/7, from 00:00 to 23:59.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name: to_AvayaSBCE

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AvayaSBCE	loadbalance.avaya.com	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
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

6.8. Administer Dial Patterns

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

Under **General**:

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

Under **Originating Locations and Routing Policies**:

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

The following screen shows an example dial pattern configured for the Avaya SBCE.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	VM_SMGR		to_AvayaSBCE	0	<input type="checkbox"/>	AvayaSBCE	

Select : All, None

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

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	VM_SMGR		to_Communication_Manager	0	<input type="checkbox"/>	Communication_Manager	

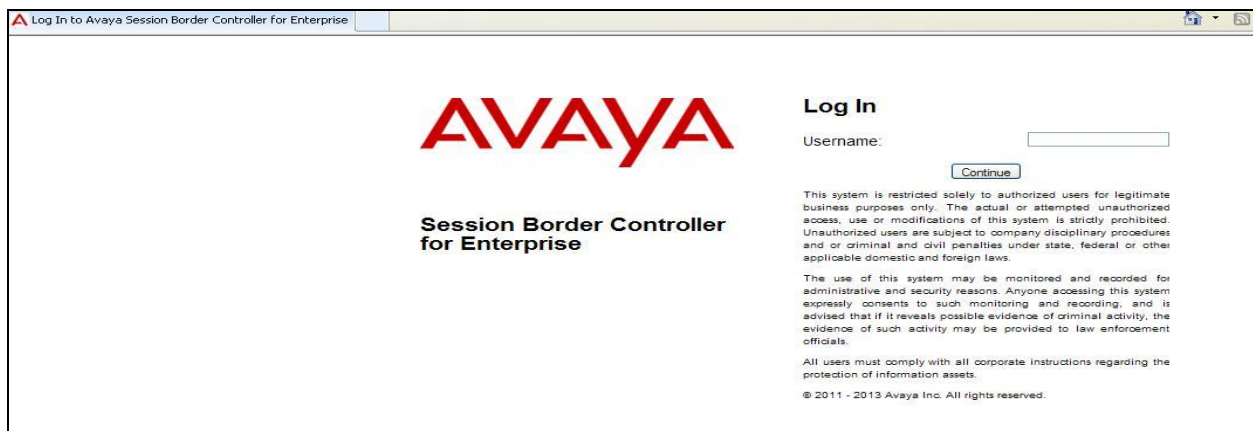
Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

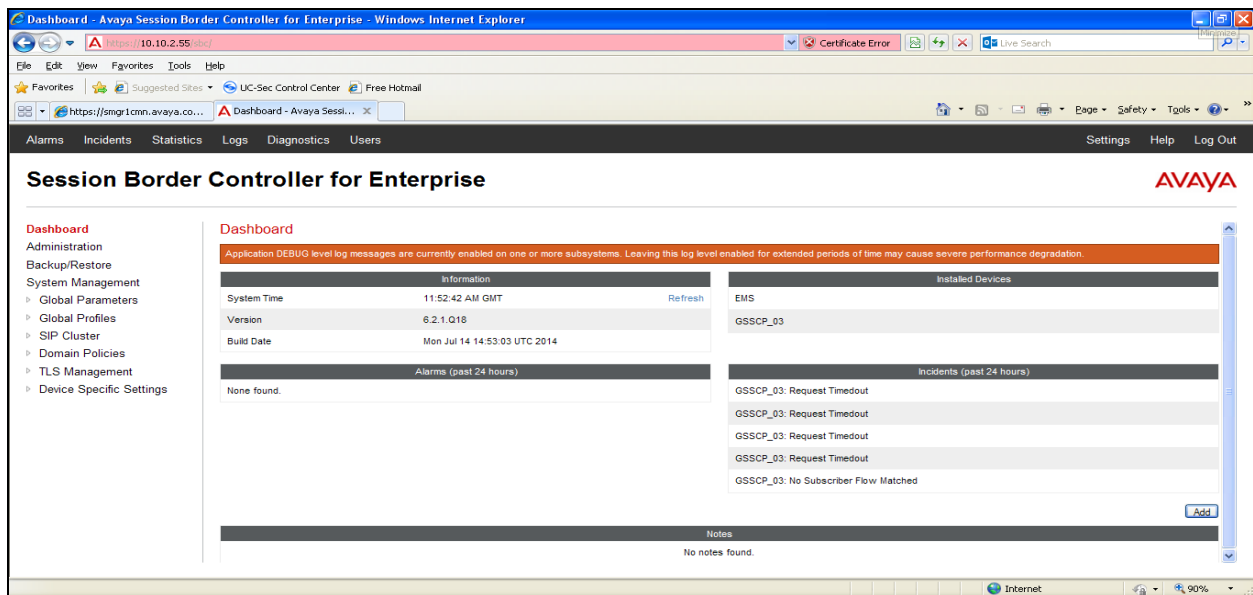
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP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

7.1. Access Avaya Session Border Controller for Enterprise

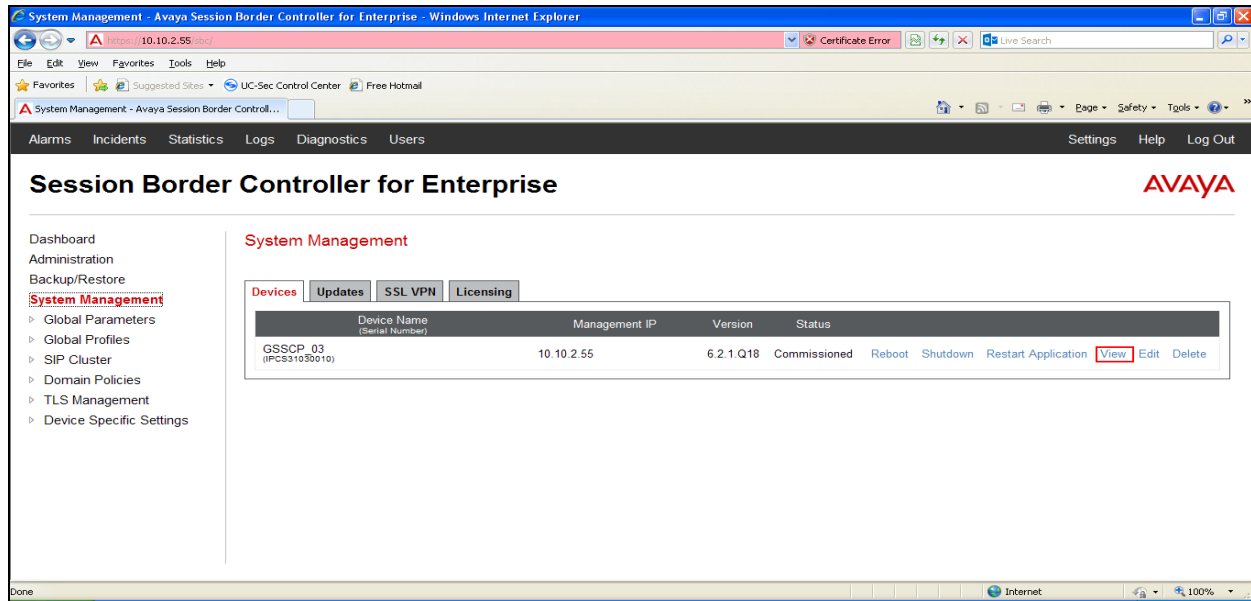
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



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 Configuration**, **Network Configuration**, and **DNS Configuration** information.

System Information: GSSCP_03

General Configuration

Appliance Name	GSSCP_03
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

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
192.168.37.2	192.168.37.2	255.255.255.128	192.168.37.1	B1
10.10.3.35	10.10.3.35	255.255.255.0	10.10.3.1	A1

DNS Configuration

Primary DNS	8.8.8.8
Secondary DNS	10.10.7.100
DNS Location	DMZ
DNS Client IP	192.168.37.2

Management IP(s)

IP	10.10.2.55
----	------------

7.2. Global Profiles

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

7.2.1. Server Interworking - Avaya

Server Interworking allows the configuration and management of 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**.

- 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

The screenshot shows a configuration window titled "Profile: Avaya" with a close button (X) in the top right corner. The window contains a "General" tab with various configuration options. The options and their current settings are as follows:

Option	Current Setting
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 (dropdown menu)
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

At the bottom of the window, there is a "Next" button.

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

Profile: Avaya 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 Interworking – BT Ireland

Server Interworking allows the configuration and management of 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**.

- Enter profile name such as **BT** 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** on the following screens and then **Finish**.

The screenshot shows a configuration window titled "Profile: BT" with a close button (X) in the top right corner. The window contains a "General" tab with various configuration options. The options and their current states are as follows:

Option	Value / State
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 (dropdown menu)
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

At the bottom right of the window is a "Next" button.

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

Profile: BT

X

Record Routes	<div><div><input type="radio"/> None</div><div><input type="radio"/> Single Side</div><div><input checked="" type="radio"/> Both Sides</div></div>
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 BT Ireland 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 BT Ireland SIP trunk. To add a routing profile, navigate to **Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.

In the new window that appears, 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 Hop server.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signalling packets.

Click **Finish**.

The following screen shows the Routing Profile to Session Manager.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	10.10.3.19	---	View Edit

The following screen shows the Routing Profile to BT Ireland SBC A.

Routing Profiles: BT_SBC_A

Add

Routing Profiles

default

Avaya

BT_SBC_A

BT_SBC_B

Rename

Clone

Delete

Click here to add a description.

Routing Profile

Add

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	192.168.16.163	---	<div>View</div> <div>Edit</div>

The following screen shows the Routing Profile to BT Ireland SBC B.

Routing Profiles: BT_SBC_B

Add

Routing Profiles

default

Avaya

BT_SBC_A

BT_SBC_B

Rename

Clone

Delete

Click here to add a description.

Routing Profile

Add

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	62.172.16.179	---	<div>View</div> <div>Edit</div>

7.2.4. Server Configuration– Avaya Aura® Session Manager

Servers are defined for each server connected to the Avaya SBCE. In this case, BT Ireland 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 administrator to configure and manage 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 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** to **10.10.3.19** (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. A red rectangular box highlights the following fields:

- Server Type:** A dropdown menu with 'Call Server' selected.
- IP Addresses / Supported FQDNs:** A text box containing '10.10.3.19'.
- Supported Transports:** A section with three checkboxes: 'TCP' (checked), 'UDP' (unchecked), and 'TLS' (unchecked).
- TCP Port:** A text box containing '5060'.

Below the highlighted fields, there are empty text boxes for 'UDP Port' and 'TLS Port'. At the bottom of the window is a 'Finish' button.

On the **Advanced** tab:

- Select **Avaya** for **Interworking Profile** defined in **Section 7.2.1**.
- 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 with "Avaya" selected. This dropdown is highlighted with a red rectangular box.
- Signaling Manipulation Script**: A dropdown menu with "None" selected.
- TCP Connection Type**: Three radio buttons labeled "SUBID", "PORTID", and "MAPPING". The "SUBID" radio button is selected.

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

7.2.5. Server Configuration – BT Ireland

To define the BT Ireland SBC as a Trunk Servers, navigate to select **Global Profiles → Server Configuration** and click on **Add** 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 **192.168.16.163** (BT Ireland SBC A)
- **Supported Transports**: Check **UDP**
- **UDP Port**: **5060**
- Hit **Next** (not shown)

Server Configuration Profile - General

Server Type: Trunk Server

IP Addresses / Supported FQDNs
Separate entries with commas: 192.168.16.163

Supported Transports:
☐ TCP
☒ UDP
☐ TLS

TCP Port:

UDP Port: 5060

TLS Port:

Finish

In the new window that appears, enter the following values as BT Ireland 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 **Next** to continue (not shown).

Server Configuration Profile - Authentication X

Enable Authentication ☒

User Name

Realm
(Leave blank to detect from server challenge)

Password
(Leave blank to keep existing password)

Confirm Password

Finish

On the Advanced tab:

- Select **BT** for Interworking Profile
- Click Finish

Server Configuration Profile - Advanced X

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile

Signaling Manipulation Script

UDP Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

Finish

To define the second BT Ireland SBC B as a Trunk Servers, 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 **192.168.16.179** (BT Ireland SBC B)
- **Supported Transports**: Check **UDP**
- **UDP Port**: **5060**
- Hit **Next** (not shown)

Server Configuration Profile - General

Server Type: Trunk Server

IP Addresses / Supported FQDNs
Separate entries with commas
192.168.16.179

Supported Transports:
☐ TCP
☒ UDP
☐ TLS

TCP Port:

UDP Port: 5060

TLS Port:

Finish

In the new window that appears, enter the following values as BT Ireland 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 **Next** to continue (not shown).

Server Configuration Profile - Authentication

Enable Authentication ☒

User Name

Realm
(Leave blank to detect from server challenge)

Password
(Leave blank to keep existing password)

Confirm Password

Finish

On the Advanced tab:

- Select **BT** for Interworking Profile
- Click Finish

Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile

Signaling Manipulation Script

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 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 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 page. On the left, a sidebar lists 'Topology Hiding Profiles' with options: 'default', 'cisco_th_profile', 'Avaya' (selected), and 'BT'. 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
From	IP/Domain	Overwrite	avaya.com
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	avaya.com
To	IP/Domain	Overwrite	avaya.com
Record-Route	IP/Domain	Auto	---

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

To define Topology Hiding for BT Ireland, 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 BT Ireland such as **BT** 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: BT

Add

Topology Hiding Profiles

default

cisco_th_profile

Avaya

BT

Click here to add a description.

Topology Hiding

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

Edit

CMN; Reviewed:
SPOC 2/2/2015

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

44 of 56
BTIRE_CMSM63SBC

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 BT Ireland 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 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
- Click on **Add IP**
- 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
192.168.37.2		192.168.37.1	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** 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 BT Ireland 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 BT Ireland 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 an **external** signalling interface IP address defined in **Section 7.3**
- Select **UDP** port number, **5060** is used for the SIP Trunk

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig_A	10.10.3.30	5060	5060	---	None	Edit Delete
Ext_Sig	192.168.37.2	5060	5060	---	None	Edit Delete
Int_Sig_B	10.10.3.35	5060	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 BT Ireland SBC A.

- 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 6.3**
- 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 BT Ireland SBC B.

- 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 6.3**
- 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 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 an **external** media interface IP address defined in **Section 6.3**
- 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: GSSCP_03

Devices

GSSCP_03

Media Interface

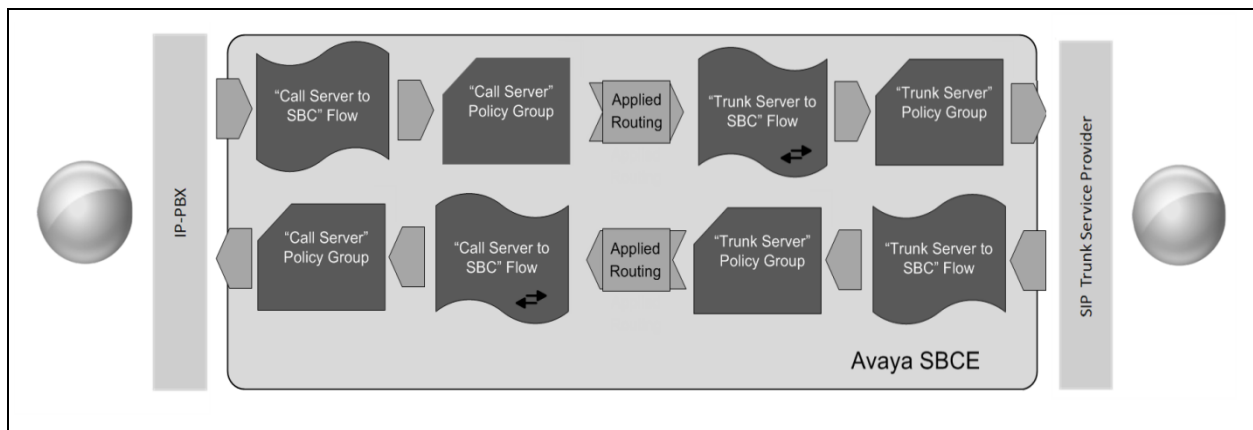
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP	Port Range	
Int_Media_A	10.10.3.30	10000 - 51000	Edit Delete
Ext_Media	192.168.37.2	10000 - 51000	Edit Delete
Int_Media_B	10.10.3.35	10000 - 51000	Edit Delete

7.5. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to BT Ireland's SIP Trunk and incoming flows from BT Ireland's SIP Trunk to Session Manager. This configuration ties all the previously entered information together so that signalling can be routed from Session Manager to the PSTN via the BT Ireland 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 BT Ireland SBC A and BT Ireland 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 BT Ireland SIP Trunk service and vice versa. The following screenshot shows all configured flows.

Subscriber Flows

Server Flows

Add

Hover over a row to see its description.

Server Configuration: Avaya

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Call_Server_A	*	Ext_Sig	Int_Sig_A	default-low	BT_SBC_A	View Clone Edit Delete
2	Call_Server_B	*	Ext_Sig	Int_Sig_B	default-low	BT_SBC_B	View Clone Edit Delete

Server Configuration: BT_SBC_A

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Trunk_Server_A	*	Int_Sig_A	Ext_Sig	default-low	Avaya	View Clone Edit Delete

Server Configuration: BT_SBC_B

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Trunk_Server_B	*	Int_Sig_B	Ext_Sig	default-low	Avaya	View Clone Edit Delete

To define a Server Flow for 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 BT Ireland 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**.

The screenshot shows a configuration window titled "Flow: Call_Server_A". It contains a form with the following fields and values:

Field	Value
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
End Point Policy Group	default-low
Routing Profile	BT_SBC_A
Topology Hiding Profile	Avaya
File Transfer Profile	None

A "Finish" button is located at the bottom right of the form.

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 BT Ireland network SBCs (BT Ireland SBC A and BT Ireland 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 BT Ireland 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 BT Ireland 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 BT Ireland defined in **Section 7.2.6** and click **Finish**.

Flow: Trunk_Server_A

Flow Name	Trunk_Server_A
Server Configuration	BT_SBC_A
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig_A
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	BT
File Transfer Profile	None

Finish

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

8. Configure BT Ireland SIP Trunk Equipment

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

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"/>	Communication Manager	10.10.8.67	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Avaya SBCE	10.10.3.30	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	CS1K R7.6	10.10.9.21	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Avaya SBCE 2	10.10.9.71	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Messaging	10.10.2.82	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 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_V9

Devices	Call Trace	Packet Capture	Captures
GSSCP_V9	Packet Capture Configuration		
Status: Ready			
Interface: B1			
Local Address IP[:Port]: 192.168.37.2			
Remote Address: *			
Protocol: UDP			
Maximum Number of Packets to Capture: 10000			
Capture Filename: SP_Trunk_Test1.pcap <small>Using the name of an existing capture will overwrite it.</small>			
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 viewing traces. At the top, it says "Trace: GSSCP_V9". Below this, there are three tabs: "Devices", "Call Trace", and "Captures". The "Captures" tab is selected. On the left, under "Devices", there is a button labeled "GSSCP_V9". On the right, there is a "Refresh" button. Below the tabs is a table with the following columns: "File Name", "File Size (bytes)", and "Last Modified". The table contains one entry: "SP_Trunk_Test1_20140916074423.pcap" with a file size of "0" and a last modified date of "September 16, 2014 7:44:24 AM GMT". There is also a "Delete" link next to the file name.

File Name	File Size (bytes)	Last Modified
SP_Trunk_Test1_20140916074423.pcap	0	September 16, 2014 7:44:24 AM GMT

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 BT Ireland 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 BT Ireland's SIP Trunk Service. BT Ireland'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 2014
- [2] *Administering Avaya Aura® System Platform*, Release 6.3, May 2014
- [3] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, April 2014
- [4] *Avaya Aura® Communication Manager 6.3 Documentation library*, August 2014
- [5] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 April 2014
- [6] *Implementing Avaya Aura® System Manager* Release 6.3, May 2014
- [7] *Upgrading Avaya Aura® System Manager to 6.3* May 2014
- [8] *Administering Avaya Aura® System Manager* Release 6.3, May 2014
- [9] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 August 2014
- [10] *Implementing Avaya Aura® Session Manager* Release 6.3, May 2014
- [11] *Upgrading Avaya Aura® Session Manager* Release 6.3, May 2014
- [12] *Administering Avaya Aura® Session Manager* Release 6.3, June 2014
- [13] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2 June 2014
- [14] *Upgrading Avaya Session Border Controller for Enterprise* Release 6.2 July 2014
- [15] *Administering Avaya Session Border Controller for Enterprise* Release 6.2 March 2014
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2015 Avaya Inc. All Rights Reserved.

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

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