



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.3 Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to support BT Business Voice IP Connect - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between BT Business Voice IP Connect 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 Germany 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 BT Business Voice IP Connect and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with BT Business Voice IP Connect 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.

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, calls made to SIP and H.323 telephones at the enterprise
- Outgoing calls from the enterprise site completed via BT Business Voice to PSTN destinations, calls made from SIP and H.323 telephones
- Calls using the G.711A, G.711MU, G.729A and G.726 codecs
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Direct IP-to-IP media (also known as “shuffling”) with SIP and H.323 telephones
- Call coverage and call forwarding for endpoints at the enterprise site
- Transmission and response of SIP OPTIONS messages sent by BT Business Voice requiring Avaya response and sent by Avaya requiring BT response

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for BT Business Voice IP Connect with the following observations:

- Speech quality was very poor on the Flare ADVD when testing the G.726 codec. This is a limitation of the ADVD.
- Calls from incoming Toll-Free numbers were not tested as toll-free access was not available to the test network
- Operator calls were not tested as they are not available from the BT Labs though calls to test access for Emergency Services were successful.
- Fragmented UDP messages were not successfully re-assembled in the test environment. Unused headers were removed in the Avaya SBCE to prevent fragmentation.

2.3. Support

For technical support on BT products please visit the website at www.bt.com or contact an authorized BT representative.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the BT Business Voice IP Connect. 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 a one-X Communicator soft phone running on a laptop PC configured for SIP.

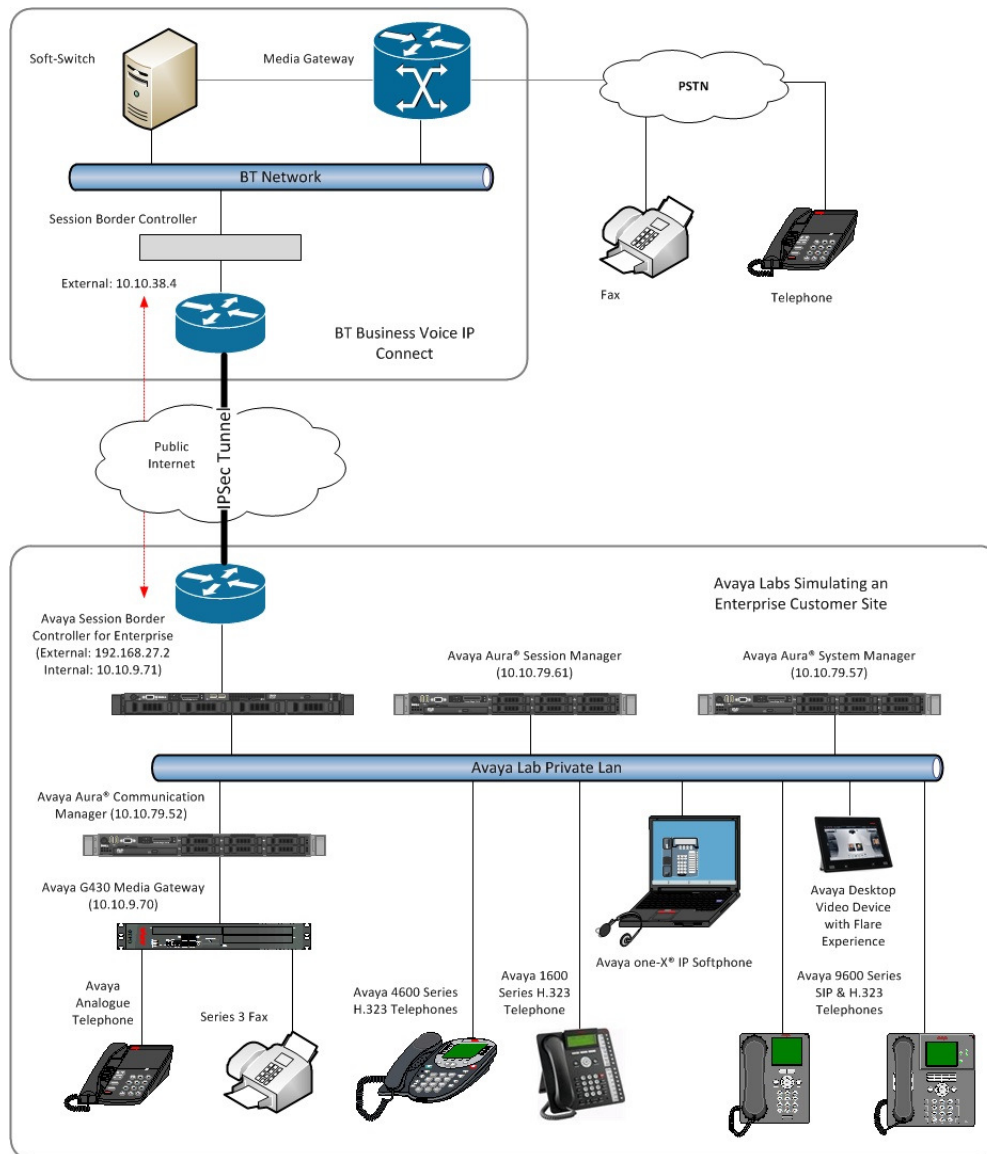


Figure 1: Test Setup BT Business Voice IP Connect to Avaya Enterprise

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	SM-6.3.2.0.632023-e50-00
Dell PowerEdge R620 running System Manager on VM Version 8	SMGR-6.3.0.8.5682-e50-64 (Build 5682)
Dell PowerEdge R620 running Communication Manager on VM Version 8	R016x.03.0.124.0
Avaya Session Border Controller Advanced for Enterprise Server	6.2.0.Q48
Avaya 1616 Phone (H.323)	1.302
Avaya 4621 Phone (H.323)	2.902
Avaya 96x0 Phone (H.323)	3.200
Avaya A175 Desktop Video Device (SIP)	Flare Experience Release 1.1.2
Avaya 9630 Phone (SIP)	R2.6 SP9
Avaya 9608 Phone (SIP)	R6.2 SP1
Avaya one-X® Communicator (H.323) on Lenovo T510 Laptop PC	6.1.8.06-SP8-40314
Analogue Handset	NA
Analogue Fax	NA
BT	
Nokia Siemens Networks hiE 9200	S 4.3
Media Gateway hiG1200	V9
SBC Acme Packet Net-Net SD 4xxx	SC6.2
ISDN Headset	NA
SNOM IP Phone	8.x

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 BT Business Voice IP Connect. 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 Business Voice 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 Business Voice 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 **node-names-ip** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM-SMVM1** and **10.10.79.61** 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	
SMVM1	10.10.79.61	
default	0.0.0.0	
procr	10.10.79.52	
procr6	::	

5.3. Administer IP Network Region

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

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

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


5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form in **Section 5.3**. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec's supported by BT Business Voice were configured, namely **G.711A**, **G.711MU**, **G.729A** and **G.726**.

change ip-codec-set 1				Page 1 of 2
IP Codec Set				
Codec Set: 1				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)	
1: G.711A	n	2	20	
2: G.711MU	n	2	20	
3: G.729A	n	2	20	
4: G.726A-32K	n	2	20	

BT Business Voice IP Connect 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**
- Set **ECM** to **n**

change ip-codec-set 1				Page 2 of 2
IP Codec Set				
Allow Direct-IP Multimedia? n				
FAX	Mode	Redundancy	ECM: n	
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 BT Business Voice 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 **node-names-ip** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SMVM1** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region **1**)
- Leave **Far-end Domain** blank (allows the CM to accept calls from any SIP domain on the associated trunk)
- Set **Direct IP-IP Audio Connections** to **y**
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.

add signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? 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: SMVM1	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
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 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 BT to prevent unnecessary SIP messages during call setup.

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

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

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

On **Page 4** of this form:

- Set **Support Request History** to **n** as the required information for forwarded and transferred calls will be sent in the **Diversion Header** and **Transferring Party Information**
- Set **Send Transferring Party Information** to **y**
- Set **Send Diversion Header** to **y**
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by BT Business Voice (this Payload Type is not applied to calls from SIP end-points)
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on the Communication Manager extension

add trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
	Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
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? n	
Identity for Calling Party Display: From	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number in E.164 format. In the test configuration, individual stations were mapped to send numbers allocated from the BT Business Voice DDI range supplied. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Note that the digits identifying the DDI range are not shown.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	2000	1	49689nnnn00	11	Total Administered: 8
4	2298	1	49689nnnn03	11	Maximum Entries: 9999
4	2316	1	49689nnnn05	11	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
4	2346	1	49689nnnn02	11	
4	2396	1	49689nnnn01	11	
4	2611	1	49689nnnn04	11	
					Communication Manager automatically inserts a '+' digit in this case.

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the BT Business Voice IP Connect. 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 or 1 in the case of some Operator calls. 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	
	032	9 18	1	pubu		n	
	0900	8 8	1	pubu		n	
	113	3 3	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						
														Intw						
1: 1	0											n	user							
2:											n	user								
3:											n	user								
4:											n	user								
5:											n	user								
6:											n	user								
BCC VALUE														TSC	CA-TSC	ITC BCIE Service/Feature PARM		No.	Numbering	LAR
0	1	2	M	4	W	Request								Dgts	Format					
														Subaddress						
1:	y	y	y	y	y	n	n	rest						unk-unk	none					
2:	y	y	y	y	y	n	n	rest							none					
3:	y	y	y	y	y	n	n	rest							none					
4:	y	y	y	y	y	n	n	rest							none					
5:	y	y	y	y	y	n	n	rest							none					
6:	v	v	v	v	v	n	n	rest							none					

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the Communication Manager extensions. The incoming digits sent in the INVITE message from BT Business Voice can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by BT for testing are assigned to the internal extensions of the test equipment configured within the Communication Manager. The **change inc-call-handling-trmt trunk-group x** command is used to translate numbers **0689nnnn00** to **0689nnnn08** to the 4 digit extension by deleting all (10) of the incoming digits and inserting the extension number. Note that the significant digits beyond the area code have been obscured.

change inc-call-handling-trmt trunk-group 1					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/ Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	10	0689nnnn00	10	2000	
public-ntwrk	10	0689nnnn01	10	2396	
public-ntwrk	10	0689nnnn02	10	2346	
public-ntwrk	10	0689nnnn03	10	2298	
public-ntwrk	10	0689nnnn04	10	2611	
public-ntwrk	10	0689nnnn05	10	2316	
public-ntwrk	10	0689nnnn06	10	6101	
public-ntwrk	10	0689nnnn07	10	2402	
public-ntwrk	10	0689nnnn08	10	2501	

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 2396. 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. **03201525nnnnnnnn**)
- Set the **Trunk Selection** to **1** so that Trunk Group 2 will be used for routing
- Set the **Config Set** to **1**

change off-pbx-telephone station-mapping 2396							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
2396	EC500	-		03201525nnnnnnnn	1	1	
		-					

Note: The phone number is in the format required to route off-net from the BT Germany Lab environment.

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. The Session Manager is configured via the System Manager. The procedures include the following areas:

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

6.1. Log in to Avaya Aura® System Manager

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

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at September 3, 2013 7:25 AM
Help | About | Change Password | Log off admin

Users	Elements	Services
Administrators Manage Administrative Users	Communication Manager Manage Communication Manager 5.2 and higher elements	Backup and Restore Backup and restore System Manager database
Directory Synchronization Synchronize users with the enterprise directory	Communication Server 1000 Manage Communication Server 1000 elements	Bulk Import and Export Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
Groups & Roles Manage groups, roles and assign roles to users	Conferencing Manage Conferencing Multimedia Server objects	Configurations Manage system wide configurations
User Management Manage users, shared user resources and provision users	IP Office Manage IP Office elements	Events Manage alarms, view and harvest logs
	Meeting Exchange Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements	Geographic Redundancy Manage Geographic Redundancy
	Messaging Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging	Inventory Manage, discover, and navigate to elements
	Presence Presence	Licenses View and configure licenses
	Routing Session Manager Routing Administration	Replication Track data replication nodes, repair replication nodes
		Scheduler Schedule, track, cancel, update and

6.2. Administer SIP Domain

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

Home / Elements / Routing / Domains

Domain Management

1 Item Refresh

<input type="checkbox"/>	Name	Type	Notes
<input type="checkbox"/>	avaya.com	sip	

Select : All, None

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the test enterprise.

Home / Elements / Routing / Locations

Location Details

CommitCancelHelp ?

General

* Name:Galway

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

Per-Call Bandwidth Parameters

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

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

* Minimum Multimedia Bandwidth:64Kbit/Sec

* Default Audio Bandwidth:80Kbit/sec

Alarm Threshold

Overall Alarm Threshold:80%

Multimedia Alarm Threshold:80%

* Latency before Overall Alarm Trigger:5Minutes

* Latency before Multimedia Alarm Trigger:5Minutes

Location Pattern

AddRemove

2 Items RefreshFilter: Enable

IP Address Pattern	Notes
* 10.10.79.*	VMWare subnet
* 10.10.9.*	Lab subnet

6.4. Administer Adaptations

Calls from BT Business Voice are received at the enterprise in E.164 format with a leading “+” on the Request URI. An Adaptation is used to convert the number to national format in the Session Manager before routing on to the Communication Manager. This simplifies the incoming trunk analysis on the Communication Manager.

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

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

In the section **Digit Conversion for Outgoing Calls from SM**.

- Under **Matching Pattern** enter **+49**.
- Under **Min** and **Max** enter the Minimum and Maximum digits expected for incoming calls. During test, a value of 12 was used as this was the length of the DDI range supplied by BT.
- Under **Delete Digits** enter **3** to remove the country code and the “+”.
- Under **Insert Digits** enter **0** to convert to national format.
- Under **Address to Modify** choose **both** from the drop down box if this is to be applied to the From header as well as the Request URI and To headers.

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

Help ?

General

* Adaptation name: DE_National

Module name: DigitConversionAdapter

Module parameter: fromto=true

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
*+49	*12	*12		*3	0	both		

6.5. Administer SIP Entities

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

Under **General**:

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

In this configuration there are three SIP Entities:

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

6.5.1. Avaya Aura® Session Manager SIP Entity

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

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is selected. A red box highlights the 'Name' field (containing 'Session Manager BGVM1'), the 'FQDN or IP Address' field (containing '10.10.79.61'), and the 'Type' dropdown menu (set to 'Session Manager'). Below these are the 'Notes' field, 'Location' dropdown (set to 'Galway'), 'Outbound Proxy' dropdown, 'Time Zone' dropdown (set to 'Europe/Dublin'), and 'Credential name' field. The 'SIP Link Monitoring' section at the bottom has a dropdown set to 'Use Session Manager Configuration'.

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* **Name:** Session Manager BGVM1

* **FQDN or IP Address:** 10.10.79.61

Type: Session Manager

Notes:

Location: Galway

Outbound Proxy:

Time Zone: Europe/Dublin

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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

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

Port

TCP Failover port:

TLS Failover port:

3 Items Refresh Filter: Enable

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

Select : All, None

6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the **Location** to that defined in **Section 6.3** the Adaptation to that defined in **Section 6.4** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: CM_VM1

* FQDN or IP Address: 10.10.79.52

Type: CM

Notes:

Adaptation: DE_National

Location: Galway

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

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

Loop Detection

Loop Detection Mode: 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 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: ASBCE_45

* FQDN or IP Address: 10.10.9.71

Type: SIP Trunk

Notes:

Adaptation: International

Location: Galway

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

* 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

Note: Although an adaptation is shown in the above screenshot, it only applies to numbers prefixed with 00. These were not used during test and so the adaptation is not described.

6.6. Administer Entity Links

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

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

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

Home / Elements / Routing / Entity Links Help ?

Entity Links

New Edit Delete Duplicate More Actions ▾

5 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	ASBCE_45_Link	Session Manager BGVM1	TCP	5060	ASBCE_45	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	ASBCE_50_Link	Session Manager BGVM1	TCP	5060	ASBCE_50	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM_Lab1_Link	Session Manager BGVM1	TLS	5061	Communication Manager BG1	5061	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM_VM1_Link	Session Manager BGVM1	TCP	5060	CM_VM1	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Messaging_Link	Session Manager BGVM1	TCP	5060	Messaging	5060	trusted	<input type="checkbox"/>	

Select : All, None

Note: The Session Manager used for testing is also used with other test equipment. Only the Entity Links highlighted in the above screenshot are valid for this configuration.

6.7. Administer Routing Policies

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

Under **General**:

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

The following screen shows the routing policy for Communication Manager.

Home / Elements / Routing / Routing Policies

Help ?

Routing Policy Details

CommitCancel

General

* Name: Internal_CM_VM1

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM_VM1	10.10.79.52	CM	

Time of Day

AddRemoveView Gaps/Overlaps

1 Item Refresh

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 and onward routing to the PSTN via BT Business Voice.

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
ASBCE_45	10.10.9.71	SIP Trunk	

Time of Day

1 Item Refresh Filter: Enable

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

Select : All, None

6.8. Administer Dial Patterns

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

Under **General**:

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

Under **Originating Locations and Routing Policies**:

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

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to BT Business Voice.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern: 0

* Min: 8

* Max: 15

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- ▼

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		BT_Germany		<input type="checkbox"/>	ASBCE_45	

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: +49689nnnn

* Min: 10

* Max: 12

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- ▼

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		Internal_CM_VM1		<input type="checkbox"/>	CM_VM1	

Select : All, None

Note: The pattern to be matched has been obscured.

6.9. Administer Application for Avaya Aura® Communication Manager

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

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

The screenshot shows the 'Application Editor' window. The breadcrumb path is 'Home / Elements / Session Manager / Application Configuration / Applications'. The form has fields for 'Name' (CMV1_App), 'SIP Entity' (CM_VM1), 'CM System for SIP Entity' (CM_VM1), and 'Description'. There are 'Commit' and 'Cancel' buttons at the top right. A 'Refresh' button is next to the 'CM System for SIP Entity' field. A link 'View/Add CM Systems' is also present.

6.10. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Session Manager** → **Application Configuration** → **Application Sequences** and click on **New**.

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

The screenshot shows the 'Application Sequence Editor' window. The breadcrumb path is 'Home / Elements / Session Manager / Application Configuration / Application Sequences'. The form has fields for 'Name' (CMV1_App_Seq) and 'Description'. There are 'Commit' and 'Cancel' buttons at the top right. Below the form is a section 'Applications in this Sequence' with buttons 'Move First', 'Move Last', and 'Remove'. A table shows 1 item in the sequence:

Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
1	CMV1_App	CM_VM1	<input checked="" type="checkbox"/>	

Below the table is a 'Select : All, None' option. At the bottom is a section 'Available Applications' with a 'Refresh' button and a 'Filter: Enable' option. A table shows 2 items available:

Name	SIP Entity	Description
CM-App	Communication Manager BG1	Dell R610 Rack 3
CMV1_App	CM_VM1	

6.11. Administer SIP Extensions

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

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of user@domain e.g. **2208@trusted.voip.BT.fr** (entire name could not be displayed in the screenshot) which is used to create the user's primary handle
- The **Authentication Type** should be **Basic**
- In the **Password/Confirm Password** fields enter an alphanumeric password
- Set the **Language Preference** and **Time Zone** as required

The screenshot shows the 'Identity' tab of a configuration form for SIP extensions. The form includes the following fields and options:

- Identity** (selected tab, marked with a red asterisk)
- Communication Profile** (tab, marked with a red asterisk)
- Membership** (tab)
- Contacts** (tab)
- Identity** (dropdown menu)
- * Last Name:** 9608
- * First Name:** SIP
- Middle Name:** (empty field)
- Description:** (empty field with up/down arrows)
- * Login Name:** 2298@avaya.com
- * Authentication Type:** Basic (dropdown menu)
- Password:** (masked with dots)
- Confirm Password:** (masked with dots)
- Localized Display Name:** (empty field)
- Endpoint Display Name:** (empty field)
- Title:** (empty field)
- Language Preference:** English (United Kingdom) (dropdown menu)
- Time Zone:** (+1:0)GMT : Dublin, Edinburgh (dropdown menu)
- Employee ID:** (empty field)
- Department:** (empty field)
- Company:** (empty field)

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

Identity * Communication Profile * Membership Contacts

Communication Profile ▾

Communication Profile Password: ●●●●●●

Confirm Password: ●●●●●●

New Delete Done Cancel

Name
Primary

Select : None

* Name: Primary

Default : ☒

Communication Address ▾

New Edit Delete

Type	Handle	Domain
No Records found		

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

Communication Address ▾

New Edit Delete

Type	Handle	Domain
No Records found		

Type: Avaya SIP

* Fully Qualified Address: 2298 @ avaya.com

Add Cancel

Expand the **Session Manager Profile** section.

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

☒ **Session Manager Profile**

SIP Registration

*** Primary Session Manager**

Session Manager BGVM1

Secondary Session Manager

(None)

Survivability Server

(None)

Max. Simultaneous Devices

1

Block New Registration When Maximum Registrations Active?

☐

Primary	Secondary	Maximum
1	0	1

Application Sequences

Origination Sequence

CMV1_App_Seq

Termination Sequence

CMV1_App_Seq

Call Routing Settings

*** Home Location**

Galway

Conference Factory Set

(None)

Expand the **Endpoint Profile** section.

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

The screenshot shows the 'CM Endpoint Profile' configuration form. It includes fields for System (CM_VM1), Profile Type (Endpoint), Extension (2298), Template (9608SIP_DEFAULT_CM_6_2), Set Type (9608SIP), Security Code, Port (IP), Voice Mail Number, Preferred Handle (None), and checkboxes for 'Delete Endpoint on Unassign of Endpoint from User or on Delete User' and 'Override Endpoint Name'. A 'Use Existing Endpoints' checkbox is also present. A magnifying glass icon is next to the Extension field, and an 'Endpoint Editor' button is to its right.

☒ **CM Endpoint Profile**

* **System** CM_VM1

* **Profile Type** Endpoint

Use Existing Endpoints ☐

* **Extension** 2298

* **Template** 9608SIP_DEFAULT_CM_6_2

Set Type 9608SIP

Security Code

Port IP

Voice Mail Number

Preferred Handle (None)

Enhanced Callr-Info display for 1-line phones ☐

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

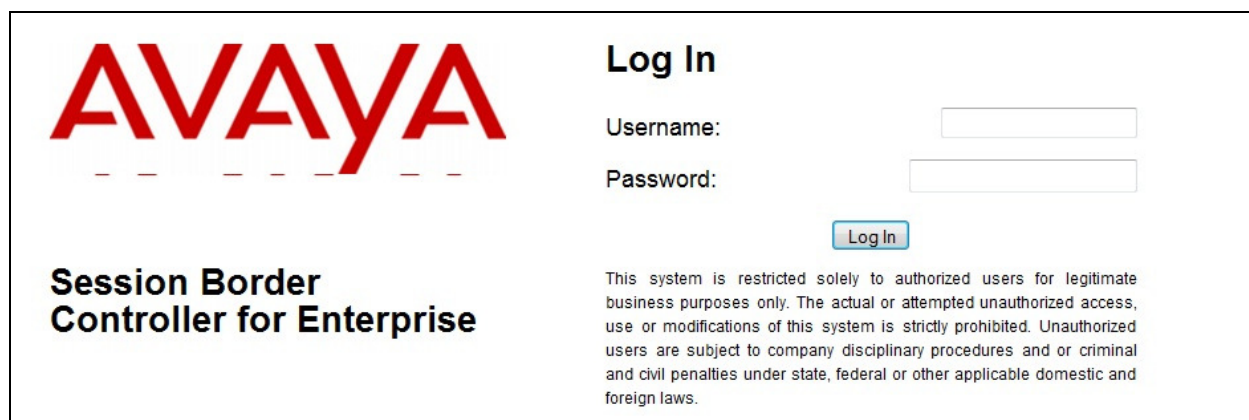
Override Endpoint Name ☒

7. Configure Avaya Session Border Controller for Enterprise

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

7.1. Access Avaya Session Border Controller for Enterprise

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



The login screen features the Avaya logo on the left. To the right, under the heading "Log In", are input fields for "Username:" and "Password:". Below these is a "Log In" button. A disclaimer text is located at the bottom right of the login area.

AVAYA

Log In

Username:

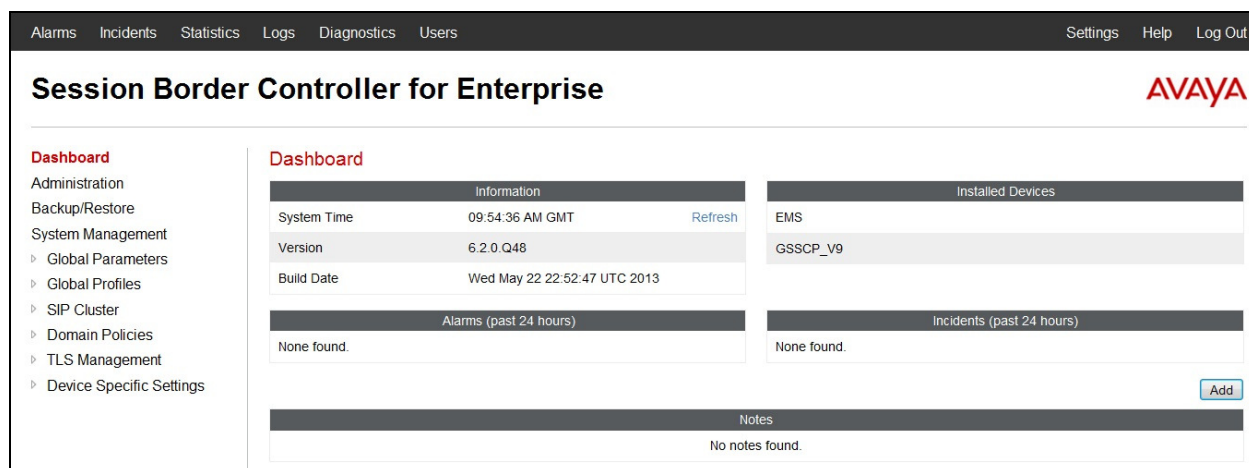
Password:

[Log In](#)

Session Border Controller for Enterprise

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

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



The dashboard has a top navigation bar with links: Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand menu lists various configuration options. The main content area displays several summary cards: "Information" (System Time, Version, Build Date), "Installed Devices" (EMS, GSSCP_V9), "Alarms (past 24 hours)", "Incidents (past 24 hours)", and "Notes".

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise **AVAYA**

Dashboard

- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - SIP Cluster
 - Domain Policies
 - TLS Management
 - Device Specific Settings

Information

System Time	09:54:36 AM GMT	Refresh
Version	6.2.0.Q48	
Build Date	Wed May 22 22:52:47 UTC 2013	

Installed Devices

EMS
GSSCP_V9

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found. [Add](#)

Notes

No notes found.

7.2. Define Network Information

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

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

- Define the internal IP address with mask and assign to interface **A1**
- Select **Save** to save the information
- Click on **Add**
- Define the external IP address with 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)

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

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

Network Management: GSSCP_V9

Devices
GSSCP_V9

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	
10.10.9.71		10.10.9.1	A1	Delete
192.168.27.2		192.168.27.2	B1	Delete

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

Network Management: GSSCP_V9

Devices
GSSCP_V9

Network Configuration **Interface Configuration**

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

7.3. Define Interfaces

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

7.3.1. Signalling Interfaces

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

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

Signaling Interface: GSSCP_V9

Devices

GSSCP_V9

Signaling Interface

Add

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

7.3.2. Media Interfaces

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

- Select **Add** and enter details of the internal media interface in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface
- For **Media IP**, select an **internal** media interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select **Add** and enter details of the external media interface in the pop-up menu
- In the **Name** field enter a descriptive name for the external media interface
- For **Media IP**, select an **external** media interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the media path with BT Business Voice

Media Interface: GSSCP_V9

Devices
GSSCP_V9

Media Interface

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

Add

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

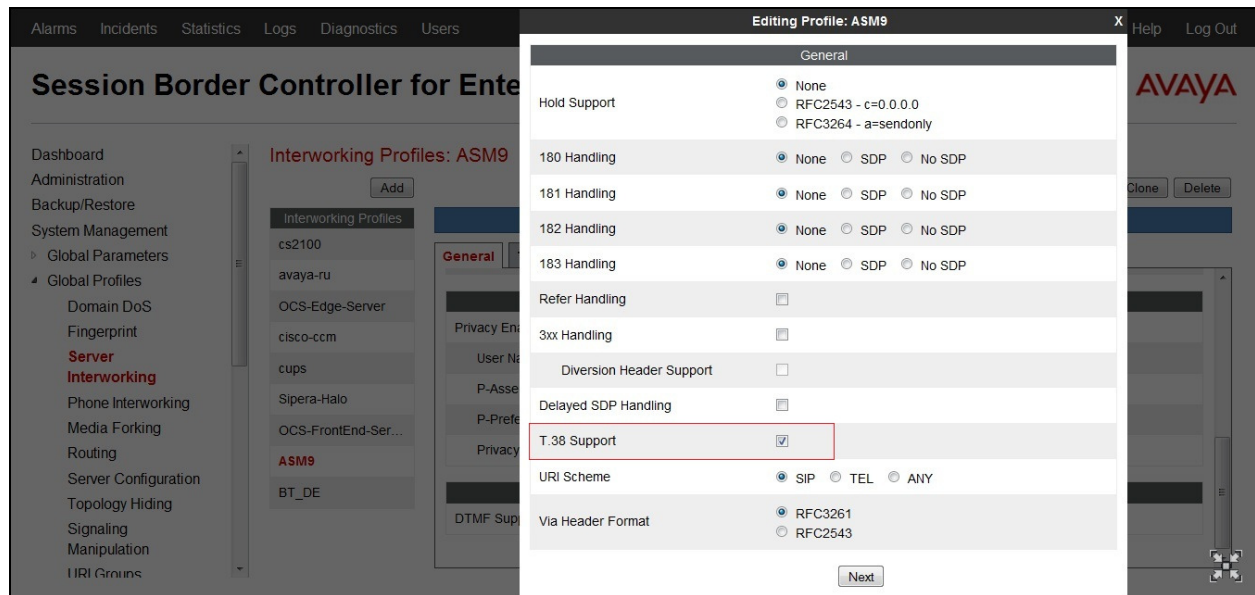
Note: During test the port ranges for the internal and external media interfaces were defined as the default values used by the Communication Manager.

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, BT Business Voice is connected as the Trunk Server and the Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. To define Server Interworking for the Session Manager, highlight the **avaya-ru** profile which is a factory setting appropriate for Avaya equipment and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown)

- In the **Clone Name** field enter a descriptive name for the Session Manager and click **Finish** – in test **ASM9** was used (not shown)
- In the **General** tab (not shown) Select **Edit** and enter details in the pop-up menu.
- Check the **T.38** box then click **Next** and **Finish** (not shown)



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

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

- In the **Clone Name** field enter a descriptive name for server interworking profile for BT Business Voice and click **Finish** – in test **BT_DE** was used
- Select **Edit** and enter details in the pop-up menu
- Check the **T.38** box
- Select **Next** three times and **Finish**

7.5. Define Servers

Servers are defined for each server connected to the Avaya SBCE. In this case, BT Business Voice is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the Session Manager, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side.

Click on **Add** and enter details in the pop-up menu

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

Server Configuration: ASM9_Call_Server

Add

Server Profiles

ASM9_Call_Server

SP_Trunk_Server

Edit Server Configuration Profile - General

Server Type: Call Server

IP Addresses / Supported FQDNs: 10.10.79.61

Supported Transports: ☒ TCP, ☐ UDP, ☐ TLS

TCP Port: 5060

UDP Port:

TLS Port:

Finish

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

Edit Server Configuration Profile - Advanced

Enable DoS Protection: ☐

Enable Grooming: ☐

Interworking Profile: ASM9

Signaling Manipulation Script: None

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

Finish

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

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

Server Configuration: SP_Trunk_Server

Edit Server Configuration Profile - General

Server Type: Trunk Server

IP Addresses / Supported FQDNs: 10.10.38.4

Supported Transports: ☐ TCP, ☒ UDP, ☐ TLS

TCP Port:

UDP Port: 5060

TLS Port:

Finish

- Click **Next** again then select the **Interworking Profile** for the BT Business Voice defined in **Section 7.4** from the drop down menu

Edit Server Configuration Profile - Advanced

Enable DoS Protection: ☐

Enable Grooming: ☐

Interworking Profile: BT_DE

Signaling Manipulation Script: None

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

Finish

7.6. Define Routing

Routing information is required for routing to the Session Manager on the internal side and BT Business Voice 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. To define routing to the Session Manager, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Session Manager, in this case **Call Server**, and click **Next** (not shown)
- Enter the Session Manager SIP interface address and port in the **Next Hop Server 1** field
- Select **TCP** for the **Outgoing Transport**
- Click **Finish**

The screenshot shows the 'Edit Routing Rule' dialog box. On the left, a sidebar lists 'Routing Profiles: Call Server' with an 'Add' button. Below it, a 'Routing Profile' section shows 'default', 'Call Server' (selected), and 'Trunk Server'. A 'Priority' field is set to '1'. The main dialog area has a title bar 'Edit Routing Rule' and a close button 'X'. A blue banner at the top states: 'Each URI group may only be used once per Routing Profile.' Below this is a 'Next Hop Routing' section. It includes a 'URI Group' dropdown menu. The 'Next Hop Server 1' field is highlighted with a red box and contains '10.10.79.61'. Below it is the 'Next Hop Server 2' field. Further down are several checkboxes: 'Routing Priority based on Next Hop Server' (checked), 'Use Next Hop for In Dialog Messages' (checked), 'Ignore Route Header for Messages Outside Dialog' (unchecked), 'NAPTR' (unchecked), and 'SRV' (unchecked). The 'Outgoing Transport' section is highlighted with a red box and shows radio buttons for 'TLS', 'TCP' (selected), and 'UDP'. A 'Finish' button is at the bottom right.

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

- In the **Profile Name** field enter a descriptive name for BT Business Voice, in this case a generic name of **Trunk Server** was used, and click **Next** (not shown)
- Enter the BT Business Voice IP address and port in the **Next Hop Server 1** field
- Select **UDP** for the **Outgoing Transport**
- Click **Finish**

Controller for Enterprise

Routing Profiles: Trunk Server

Add

Routing Profiles

default

Call Server

Trunk Server

Routing Profile

Priority

1 *

Edit Routing Rule

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group *

Next Hop Server 1
IP, IP:Port, Domain, or Domain:Port 10.10.38.4

Next Hop Server 2
IP, IP:Port, Domain, or Domain:Port

Routing Priority based on Next Hop Server ☒

Use Next Hop for In Dialog Messages ☐

Ignore Route Header for Messages Outside Dialog ☐

NAPTR ☐

SRV ☐

Outgoing Transport ☐ TLS ☐ TCP ☒ UDP

Finish

7.7. Topology Hiding

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

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

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

Topology Hiding Profiles: ASM9

Add

Rename

Clone

Delete

Topology Hiding Profiles

default

cisco_th_profile

ASM9

BT_DE

Click here to add a description.

Topology Hiding

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

Edit

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

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

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

Topology Hiding Profiles: BT_DE

Add Rename Clone Delete

Topology Hiding Profiles

default

cisco_th_profile

ASM9

BT_DE

Click here to add a description.

Topology Hiding

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

Edit

7.8. Signalling Rules

Signalling rules are a mechanism on the Avaya SBCE to handle any unusual signalling scenarios that may be encountered for a particular Service Provider. In the case of BT Business Voice, the test environment was not successfully re-assembling fragmented UDP packets. As this issue could have been occurring anywhere in the test environment between the Avaya enterprise equipment and BT Business Voice, the approach was taken to reduce the SIP messages to below the Maximum Transmission Unit (MTU) so that fragmentation did not occur. A signalling rule was used to remove Avaya proprietary headers which resulted in the necessary reduction in size.

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

- In the **Rule Name** field enter a descriptive name for the BT Business Voice signalling rule and click **Next** and **Next** again, then **Finish** (not shown)
- Click on the **Request Headers** tab and then click on **Add In Header Control** (not shown)
- Check the **Proprietary Request Header** box
- Enter the name of the proprietary header in the Header Name field, in the example shown it's **P-Location**, and **ALL** in the Method Name field
- Check **Forbidden** in the Header Criteria options
- In the **Presence Action** drop down menu, select **Remove Header**
- Click **Finish**

Add Header Control

Proprietary Request Header ☒

Header Name

Method Name

Header Criteria ☒ Forbidden ☐ Mandatory ☐ Optional

Presence Action

Note: The above is an example of the proprietary headers. During test, the same was done for AV-Global-Session-ID and P-Charging-Vector.

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

Session Border Controller for Enterprise

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Signaling Rules: ASM9

Filter By Device...

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

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Av-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
2	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
3	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete

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

- In the **Group Name** field enter a descriptive name for the Session Manager Policy Group, in this case **SM-def-low**, and click **Next**
- Leave the **Application**, **Border**, **Media**, **Security** and **Time of Day** fields at their default values
- In the **Signaling** drop down menu, select the recently added signalling rule for the Session Manager (**ASM9**)
- Leave the Time of Day field at its default value

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header is 'Session Border Controller for Enterprise' with the Avaya logo. The left sidebar shows a tree view with 'Domain Policies' expanded, and 'End Point Policy Groups' selected. The main content area is titled 'Policy Groups: SM-def-low'. It features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'avaya-def-high-su...', and 'avaya-def-high-ser...'. The 'SM-def-low' group is highlighted. To the right, there is a table with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The table contains one row with the following values: 1, default-trunk, default, default-low-med, default-low, ASM9, and default. There are buttons for 'Add', 'Filter By Device...', 'Rename', 'Delete', 'Summary', and 'Add'.

7.9. Server Flows

Server Flows combine the previously defined profiles into an outgoing flow from the Session Manager to BT Business Voice and an incoming flow from BT Business Voice to the Session Manager. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to BT Business Voice and vice versa.

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

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Flow Name** field enter a descriptive name for the server flow for the Session Manager, in this case **Session Manager** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.5** for the Session Manager
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that media bound for the Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of BT Business Voice defined in **Section 7.6**.
- In the **End Point Policy Group** drop down menu, select the End Point Policy Group that contains the Signalling Rules for the Session Manager defined in **Section 7.8**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.7** and click **Finish**.

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

Field Label	Value
Flow Name	Session Manager
Server Configuration	ASM9_Call_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Med
End Point Policy Group	SM-def-low
Routing Profile	Trunk Server
Topology Hiding Profile	ASM9
File Transfer Profile	None

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

To define a Server Flow for BT Business Voice, 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 Business Voice, in this case a generic name of **Trunk Server** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.5** for BT Business Voice
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for BT Business Voice is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for BT Business Voice is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for BT Business Voice is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.6**.
- In the **End Point Policy Group** drop down menu, select the End Point Policy Group that contains the Signalling Rules for BT Business Voice defined in **Section 7.8**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the BT Business Voice defined in **Section 7.7** and click **Finish**.

Edit Flow: Trunk Server	
Flow Name	Trunk Server
Server Configuration	SP_Trunk_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Med
End Point Policy Group	default-low
Routing Profile	Call Server
Topology Hiding Profile	BT_DE
File Transfer Profile	None
Finish	

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

The screenshot displays the Avaya SBCE web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand sidebar lists various configuration options, with "End Point Flows" highlighted in red. The main content area is titled "End Point Flows: GSSCP_V9" and features two tabs: "Subscriber Flows" and "Server Flows". The "Server Flows" tab is active, showing a table of server configurations. Above the table is a blue bar with the text "Click here to add a row description." and an "Add" button. The table is divided into two sections: "Server Configuration: ASM9_Call_Server" and "Server Configuration: SP_Trunk_Server". Each section contains a table with columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. The first section has one row with Priority 1, Flow Name "Session Manager", URI Group "*", Received Interface "Ext_Sig", Signaling Interface "Int_Sig", End Point Policy Group "SM-def-low", and Routing Profile "Trunk Server". The second section has one row with Priority 1, Flow Name "Trunk Server", URI Group "*", Received Interface "Int_Sig", Signaling Interface "Ext_Sig", End Point Policy Group "default-low", and Routing Profile "Call Server". Each row has "View", "Clone", "Edit", and "Delete" links.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Session Manager	*	Ext_Sig	Int_Sig	SM-def-low	Trunk Server	View Clone Edit Delete

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Trunk Server	*	Int_Sig	Ext_Sig	default-low	Call Server	View Clone Edit Delete

8. Configure BT Business Voice Equipment

The configuration of the BT equipment used to support BT Business Voice IP Connect is outside of the scope of these Application Notes and will not be covered. To obtain further information on BT equipment and system configuration please contact an authorised BT 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 Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring
[Help ?](#)

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: ASBCE_45

Summary View

Status Details for the selected Session Manager:

1 Items [Refresh](#)
Filter: Enable

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input checked="" type="radio"/> Session Manager BGVM1	10.10.9.71	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.

- 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 BT Business Voice 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 Service Provider's SBC in the **Remote Address** field or enter a * to capture all traffic
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example
- Specify the filename of the resultant pcap file in the **Capture Filename** field
- Click on **Start Capture**

The screenshot shows the Avaya SBCE web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header is "Session Border Controller for Enterprise" with the Avaya logo. On the left, a sidebar menu shows "Device Specific Settings" expanded, with "Trace" selected under "Troubleshooting". The main content area is titled "Trace: GSSCP_V9" and has three tabs: "Call Trace", "Packet Capture", and "Captures". The "Packet Capture" tab is active, showing the "Packet Capture Configuration" form. The form fields are: Status (Ready), Interface (B1), Local Address (All), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (SIP_Trunk_Test.pcap). There are "Start Capture" and "Clear" buttons at the bottom.

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

The screenshot shows the "Captures" tab in the "Trace: GSSCP_V9" section. It displays a table of captured files. The table has columns for File Name, File Size (bytes), and Last Modified. A "Refresh" button is in the top right, and a "Delete" link is next to the file name.

File Name	File Size (bytes)	Last Modified
SP_Trunk_Test_20130905113022.pcap	4,096	September 5, 2013 11:31:45 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 Service Provider.

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 Business Voice IP Connect. BT Business Voice IP Connect 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/>

©2013 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.