



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise R7.0 to support Colt SIP Trunk - Issue 0.1

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Colt SIP Trunk 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. Colt 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 the Colt SIP Trunk and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R7.0 (Communication Manager); Avaya Aura® Session Manager R7.0 (Session Manager); Avaya Session Border Controller for Enterprise R7.0 (Avaya SBCE). Note that the shortened names shown in brackets will be used throughout the remainder of the document. Customers using this Avaya SIP-enabled enterprise solution with the Colt SIP Trunk are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

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

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 Colt SIP Trunk, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the Colt SIP Trunk to PSTN destinations, calls made from SIP and H.323 telephones.
- Calls using the G.729A, G.711A and G.726-32 codecs.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media between the Avaya SBCE and the SIP and H.323 telephones.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by the Colt SIP Trunk requiring Avaya response and sent by Avaya requiring Colt response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Colt SIP Trunk with the following observations:

- No OPTIONS were received from the network during testing. This was noted as under certain failure conditions, call failures may not be handled as effectively as possible.
- When testing outbound calls with no matching codec, the network responded to the INVITE with a 180 Ringing and an alternative codec listed in the SDP. A more appropriate response in this case is “488 Not Acceptable Here”. Communication Manager sent a CANCEL and failure tone was heard on the calling phone.
- No inbound Toll-Free access was available to test.
- Routing was not in place to test Operator or Directory Enquiries calls.
- Emergency calls were not tested as there was no test call booked with the Emergency Services Operator
- Initial testing of outbound T.38 Fax calls was unsuccessful. When the network sent a re-INVITE to change to T.38 and Communication Manager responded with 200 OK, the network did not send an ACK. After repeated sending of 200 OK, Communication Manager released the call. A fix was put in place by Colt and outbound Fax was retested successfully.
- When testing congestion and failure of the SIP Trunk, it was approximately 15 seconds before a failure tone was heard on the calling phone. This was because the call was re-attempted from the network a number of times before it was rejected.

2.3. Support

For technical support on Colt products please contact Colt on 0800 358 3999 or visit their website at www.colt.net

3. Reference Configuration

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

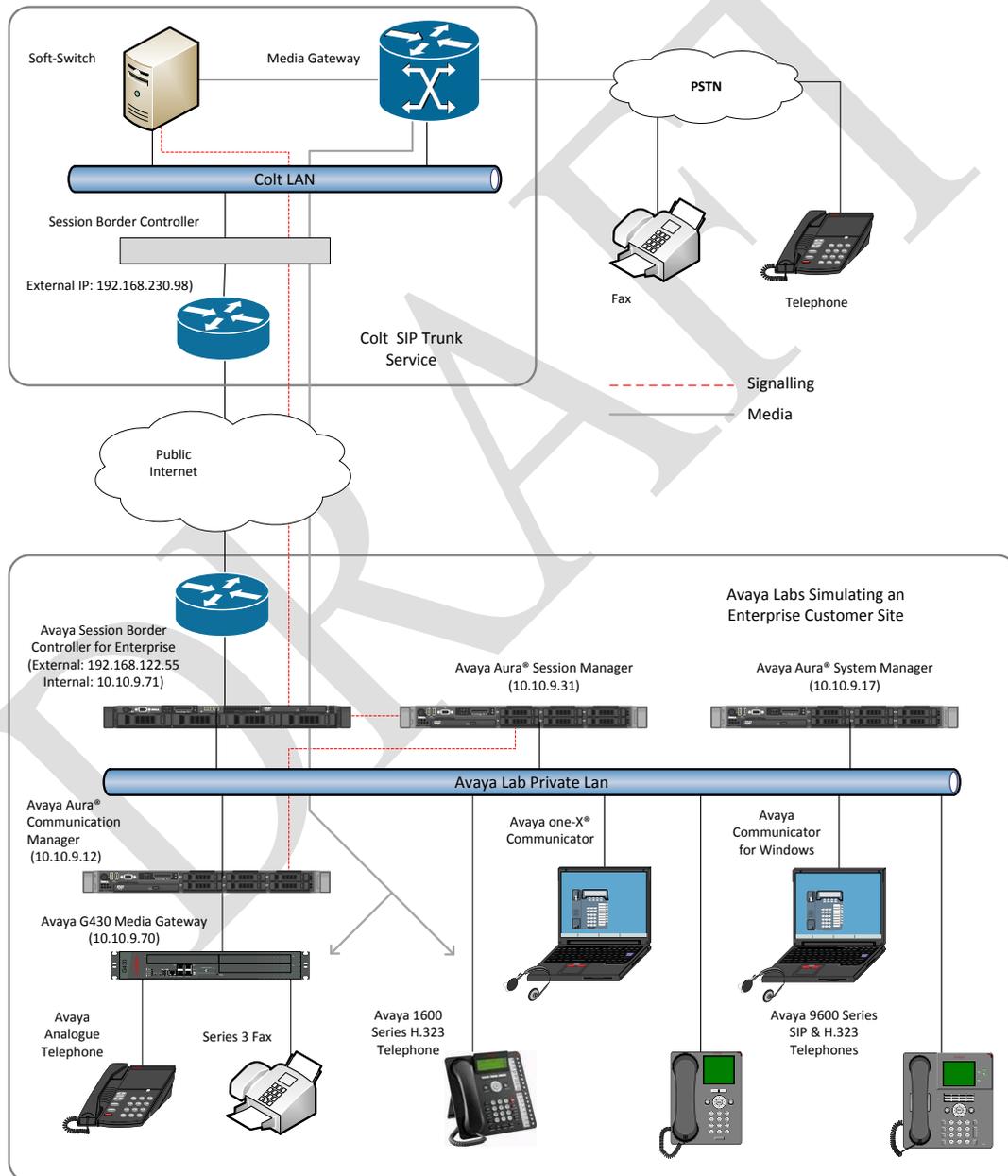


Figure 1: Test Setup Colt SIP Trunk to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Aura® System Manager	7.0.0.0.16266
Avaya Aura® Communication Manager	7.0-441 Build 0.22477
Avaya Session Border Controller for Enterprise	7.0.0-21-6602
Avaya G430 Media Gateway	37.19.0
Avaya 96x0 Phone (SIP)	2_6_14_5
Avaya 9608 Phone (SIP)	7.0.0 R39
Avaya 96x0 Phone (H.323)	3.230A
Avaya 9608 Phone (H.323)	6.3116
Avaya 1616 Phone (H.323)	1.380B
Avaya One-X Communicator	6.2.7.03-SP7
Avaya Communicator for Windows	2.1.2.75
Avaya 2400 Series Digital Handsets	N/A
Analogue Handset	N/A
Analogue Fax	N/A
Colt	
Sonus GSX	9.2.4
Sonus PSX	V08.04.08A002

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

```
display system-parameters customer-options                               Page 2 of 12
                                OPTIONAL FEATURES

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

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

```

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

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

IP Attendant Consoles? y
  
```

5.2. Administer IP Node Names

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

```

display node-names ip                                               IP NODE NAMES

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

5.3. Administer IP Network Region

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

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

```
change ip-network-region 1                                     Page 1 of 20
                                                              IP NETWORK REGION
Region: 1
Location: 1          Authoritative Domain: avaya.com
Name: default       Stub Network Region: n
MEDIA PARAMETERS    Intra-region IP-IP Direct Audio: yes
                    Codec Set: 1       Inter-region IP-IP Direct Audio: yes
                    UDP Port Min: 2048 IP Audio Hairpinning? n
                    UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS  AUDIO RESOURCE RESERVATION PARAMETERS
                    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** by typing **change ip-codec set 1**. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codecs supported by Colt were configured, namely **G.729A**, **G.711A** and **G.726A-32K**.

```
change ip-codec-set 1                                     Page 1 of 2

                                IP CODEC SET

Codec Set: 1

Audio          Silence      Frames   Packet
Codec          Suppression  Per Pkt  Size(ms)
1: G.729A      n             2        20
2: G.711A      n             2        20
3: G.726A-32K n             2        20
4:
5:
```

The Colt SIP Trunk supports T.38 for transmission of fax. Navigate to **Page 2** and define T.38 fax as follows:

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

```
change ip-codec-set 1                                     Page 2 of 2

                                IP CODEC SET

                                Allow Direct-IP Multimedia? n

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

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

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Colt SIP Trunk. During test, this was configured to use TCP and port 5060 though it's recommended to use TLS and port 5061 in the live environment to enhance security. Configure the **Signaling Group** using the **add signaling-group 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 the Session Manager (node name **Session_Manager** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** 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**.
- 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
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr                      Far-end Node Name: Session_Manager
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
                                           RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload                    Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3           IP Audio Hairpinning? n
  Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing 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-netwrk**.
- 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 Colt to prevent unnecessary SIP messages during call setup. During testing, a value of **600** was used that sets Min-SE to 1200 in the SIP signalling.

```
add trunk-group 1                                     Page 2 of 21
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                     Redirect On OPTIM Failure: 5000
  SCCAN? n          Digital Loss Group: 18
                                     Preferred Minimum Session Refresh Interval(sec): 600
Disconnect Supervision - In? y Out? y
```

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

```
add trunk-group 1                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                   Measured: none
                                                    Maintenance Tests? y

  Numbering Format: private
                                                    UII Treatment: service-provider
                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n
```

On **Page 4** of this form:

- Set **Support Request History** to **y**.
- Set **Send Diversion Header** to **y**. Note – History-Info and Diversion headers may not both be required but were sent during compliance testing.
- Set the **Telephone Event Payload Type** to **100** to match the value preferred by Colt (this Payload Type is not applied to calls from SIP end-points).
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on Communication Manager extension.

```
add trunk-group 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? y
  Telephone Event Payload Type: 100

  Convert 180 to 183 for Early Media? n
  Always Use re-INVITE for Display Updates? n
  Identity for Calling Party Display: From
  Block Sending Calling Party Location in INVITE? n
  Accept Redirect to Blank User Destination? n
  Enable Q-SIP? n
```

Note: - The above screenshot shows **Network Call Redirection** set to **n**. This was temporarily set to **y** for some of the last tests that involved testing of 302 Moved Temporarily and REFER messages. When set, REFER messages are sent that are not acted on by the Colt SIP Trunk and so are unnecessary additional signalling.

5.7. Administer Calling Party Number Information

Use the **change private-unknown-numbering** command to configure Communication Manager to send the calling party number in the format required. In test, calling party numbers were sent as Communication Manager extension numbers to be modified in the Session Manager.

Adaptations are used in Session Manager to format the number as described in **Section 6.4**.

These calling party numbers are sent in the SIP From, Contact and PAI headers as well as the Diversion header for forwarded calls. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network.

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

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the Colt 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: 8
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
```

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

```
change ars analysis 0                                     Page 1 of 2
```

ARS DIGIT ANALYSIS TABLE							
Location: all							
Percent Full: 0							
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI	Reqd
0	11	14	1	pubu		n	
00	13	15	1	pubu		n	
118	5	6	1	pubu		n	
2	4	4	2	pubu		n	
7000	4	4	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: Session Manager			
SCCAN? n													Secure SIP? n		Used for SIP stations? n	
Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC		
							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	Sub	Numbering		LAR					
0	1	2	M	4	W	Request	Dgts	Format								
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 DDI calls to Communication Manager extensions. The incoming digits sent in the INVITE message from Colt can be manipulated as necessary to route calls to the desired extension. During test, the incoming DDI numbers were changed in the Session Manager to Communication Manager Extension number using an Adaptation as described in **Section 6.4**. When done this way, there is no requirement for any incoming digit translation in Communication Manager. If incoming digit translation is required, use the **change inc-call-handling-trmt trunk-group x** command where **x** is the Trunk Group defined in **Section 5.6**.

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

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

5.10. EC500 Configuration

When EC500 is enabled on a Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2396. Use the command **change off-pbx-telephone station-mapping x** where **x** is Communication Manager station.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration.
- For the **Phone Number** enter the phone that will also be called (e.g. **0035389434nnnn**).
- 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 2391								Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION										
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual			
Extension		Prefix			Selection	Set	Mode			
2391	EC500	-		0035389434nnnn	ars	1				

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

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

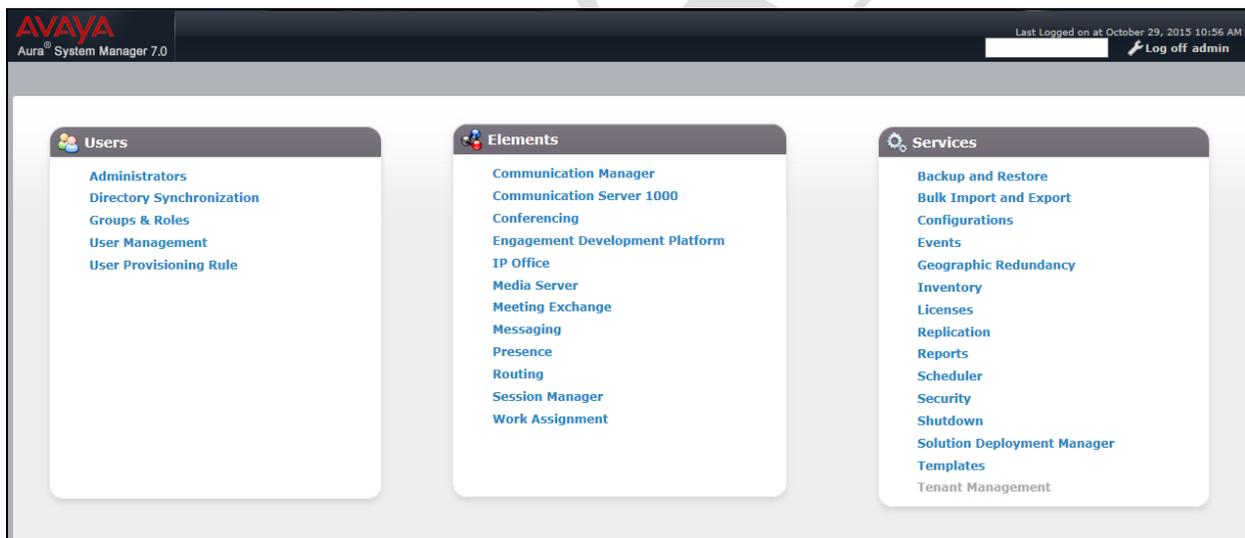
6. Configuring Avaya Aura® Session Manager

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

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

6.1. Log in to Avaya Aura® System Manager

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



6.2. Administer SIP Domain

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

The screenshot shows the 'Domain Management' interface. At the top, there are tabs for 'Home' and 'Routing'. Below the tabs is a breadcrumb trail: 'Home / Elements / Routing / Domains'. The left sidebar contains a menu with 'Routing' expanded, and 'Domains' selected. The main content area is titled 'Domain Management' and includes buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below these buttons, it indicates '1 Item' and shows a table with the following data:

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

At the bottom of the table, there is a 'Select' dropdown menu with options 'All' and 'None'.

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

6.3. Administer Locations

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

Home / Elements / Routing / Locations Help ?

Location Details

General

* Name:
Notes:

Dial Plan Transparency in Survivable Mode

Enabled:
Listed Directory Number:
Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:
Total Bandwidth:
Multimedia Bandwidth:
Audio Calls Can Take Multimedia Bandwidth:

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location): Kbit/Sec
* Minimum Multimedia Bandwidth: Kbit/Sec
* Default Audio Bandwidth:

Alarm Threshold

Overall Alarm Threshold: %
Multimedia Alarm Threshold: %
* Latency before Overall Alarm Trigger: Minutes
* Latency before Multimedia Alarm Trigger: Minutes

Location Pattern

1 Item Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	*10.10.9.x	<input type="text"/>

Select : All, None

6.4. Administer Adaptations

Calls from Colt are received at the enterprise in E.164 format with leading “+” on the Request URI. An Adaptation specific to Communication Manager is used to convert the called party number to a pre-defined extension number before onward routing to the Communication Manager SIP Entity and removes the requirement for incoming digit manipulation on Communication Manager.

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

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

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

* **Adaptation Name:**

* **Module Name:**

Module Parameter Type:

Egress URI Parameters:

Notes:

Scroll down and in the section **Digit Conversion for Outgoing Calls from SM**, click on **Add**. An additional row will appear (not shown). This allows information to be entered for the manipulation of numbers coming from the network. This is where the called party number is translated from E.164 format to the extension number for termination of calls on Communication Manager. In addition, the calling party number is adapted to diallable format for display on Communication Manager extensions.

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

- Under **Matching Pattern** enter the DDI number as received from the network.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the incoming DDI number.
- Under **Delete Digits** enter the number of digits to delete to leave only the extension number remaining, during test all had to be deleted as the extension number did not form part of the national number.
- Under **Insert Digits** enter digits to be inserted. During test, this was the full extension number. If the extension number forms part of the DDI number, there will be no entry required here.
- Under **Address to Modify** choose **destination** from the drop down box to apply this rule to the To and Request-Line headers only.

Digit Conversion for Outgoing Calls from SM

Add Remove

10 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*+	*12	*15		*1	00	origination		
<input type="checkbox"/>	*+44	*12	*13		*3	0	origination		
<input type="checkbox"/>	*+445511nnnn00	*13	*13		*13	2000	destination		
<input type="checkbox"/>	*+445511nnnn01	*13	*13		*13	2391	destination		
<input type="checkbox"/>	*+445511nnnn02	*13	*13		*13	2291	destination		
<input type="checkbox"/>	*+445511nnnn03	*13	*13		*13	2396	destination		
<input type="checkbox"/>	*+445511nnnn04	*13	*13		*13	2400	destination		
<input type="checkbox"/>	*+445511nnnn05	*13	*13		*13	7000	destination		
<input type="checkbox"/>	*+445511nnnn06	*13	*13		*13	6099	destination		
<input type="checkbox"/>	*+445511nnnn07	*13	*13		*13	6002	destination		

Select : All, None

Commit Cancel

Note: In the above screenshots the DDI numbers are partially obscured. If the number is to be changed to diallable format for display on Communication Manager extensions, additional rows will be required. These would replace the leading “+” with “00” for international calling party numbers and “+44” would be replaced by “0” for national calling party numbers.

An additional Adaptation is required to convert extension numbers to E.164 format. Calls from Communication Manager are received at the Session Manager with the extension number in the From header. An Adaptation specific to Colt is used to convert the calling party number to E.164 format with leading “+” before onward routing to the Colt SIP Trunk.

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

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

Home / Elements / Routing / Adaptations Help ?

Adaptation Details

General

* Adaptation Name:

* Module Name:

Module Parameter Type:

Add Remove	
<input type="checkbox"/> Name	Value
<input type="checkbox"/> fromto	true

Select : All, None

Egress URI Parameters:

Notes:

Note: When the Adaptation is viewed, **Module Parameter Type** appears as **Name-Value Parameter** and a box appears showing the parameters entered. For this adaptation, only **fromto** with a value of **true** is shown.

Scroll down and in the section **Digit Conversion for Outgoing Calls from SM**, click on **Add**. An additional row will appear (not shown). This allows information to be entered for the manipulation of numbers coming from Communication Manager. This is where the calling party number is translated from the extension number to E.164 format for display on the terminating PSTN phones as the diallable DDI number assigned to the extension. In addition, the called party number is adapted to E.164 format with leading “+” for both national and international numbers.

The screenshot below shows a translation for each calling party number. This is not normally necessary where the extension number forms part of the national number. When this is the case, a simple additional of the leading digits to build up the E.164 format is required.

- Under **Matching Pattern** enter the extension number as received from Communication Manager.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the incoming DDI number.
- Under **Delete Digits** enter the number of digits to delete to remove any digits that will not form part of the E.164 number, during test all had to be deleted as the extension number did not form part of the national number.
- Under **Insert Digits** enter digits to be inserted. During test, this was the full E.164 number with leading “+”. If the extension number forms part of the DDI number, only the necessary prefix digits will be required.
- Under **Address to Modify** choose **origination** from the drop down box to apply this rule to the From header only.

Digit Conversion for Outgoing Calls from SM

Add Remove

7 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*0	*10	*12		*1	+44	destination		
<input type="checkbox"/>	*00	*10	*17		*2	+	destination		
<input type="checkbox"/>	*2000	*4	*4		*4	+44207nnnnn50	origination		
<input type="checkbox"/>	*2291	*4	*4		*4	+44207nnnnn52	origination		
<input type="checkbox"/>	*2391	*4	*4		*4	+44207nnnnn54	origination		
<input type="checkbox"/>	*2396	*4	*4		*4	+44207nnnnn51	origination		
<input type="checkbox"/>	*2400	*4	*4		*4	+44207nnnnn53	origination		

Select : All, None

Commit Cancel

Note: In the above screenshots the DDI numbers are partially obscured. In addition, the international dialling prefix of “00” is replaced by “+” for international called party numbers and “0” is replaced by “+44” for national called party numbers.

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.

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

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

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

Listen Ports

TCP Failover port:

TLS Failover port:

Add Remove

3 Items

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

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**.

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

* SIP Timer B/F (in seconds):

Credential name:

Securable:

Call Detail Recording:

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: ▼

Loop Count Threshold:

Loop Detection Interval (in msec):

SIP Link Monitoring

SIP Link Monitoring: ▼

Supports Call Admission Control:

Shared Bandwidth Manager:

Primary Session Manager Bandwidth Association: ▼

Backup Session Manager Bandwidth Association: ▼

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 **Adaptation** to that defined in **Section 6.4**, the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type: ▼

Notes:

Adaptation: ▼

Location: ▼

Time Zone: ▼

* SIP Timer B/F (in seconds):

Credential name:

Securable:

Call Detail Recording: ▼

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.

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	ASBCE_Link	Session_Manager	TCP	5060	ASBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM_Entity_Link	Session_Manager	TCP	5060	CM_Entity	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Messaging_Link	Session_Manager	TCP	5060	Messaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

Note: The **Messaging_Link** Entity Link is used for the Avaya Aura ® Messaging system and is not described in this document.

6.7. Administer Routing Policies

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

Under **General**:

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

The following screen shows the routing policy for Communication Manager.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM_Entity	10.10.9.12	CM	

Time of Day

1 Item Filter: Enable

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

Select : All, None

The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed to the PSTN via the Colt SIP Trunk.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE	10.10.9.71	SIP Trunk	

Time of Day

1 Item Filter: Enable

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

Select : All, None

6.8. Administer Dial Patterns

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

Under **General**:

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

Under **Originating Locations and Routing Policies**:

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

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the PSTN via the Colt SIP Trunk.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details

General

* Pattern:

* Min:

* Max:

Emergency Call:

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item Filter: Enable

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

Select : All, None

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

Dial Pattern Details [Commit] [Cancel] [Help ?](#)

General

* Pattern: +44207nnnnn5

* Min: 12

* Max: 13

Emergency Call:

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- [v]

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-		CM_Terminating	0	<input type="checkbox"/>	CM_Entity	

Select : All, None

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

6.9. Administer Application for Avaya Aura® Communication Manager

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

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

Home Routing * Session Manager * [Home / Elements / Session Manager / Application Configuration / Applications](#)

Application Editor [Commit] [Cancel]

Application

* Name: CM_App [x]

* SIP Entity: CM_Entity

* CM System for SIP Entity: CM1_Element [Refresh] [View/Add CM Systems](#)

Description:

6.10. Administer Application Sequence for Avaya Aura® Communication Manager

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

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

Home / Elements / Session Manager / Application Configuration / Application Sequences Help ?

Application Sequence Editor

Application Sequence

*Name x

Description

Applications in this Sequence

1 Item

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

Select : All, None

Available Applications

1 Item Filter: Enable

	Name	SIP Entity	Description
<input type="button" value="+"/>	CM_App	CM_Entity	

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. 2291@avaya.com which is used to create the user's primary handle.
- The **Authentication Type** should be **Basic**.
- In the **Password/Confirm Password** fields enter an alphanumeric password.
- Set the **Language Preference** and **Time Zone** as required.

Home / Users / User Management / Manage Users

New User Profile

Commit & Continue Commit

Identity * Communication Profile Membership Contacts

User Provisioning Rule

User Provisioning Rule: [dropdown]

Identity

* Last Name: SIP
Last Name (Latin Translation): SIP

* First Name: 9608
First Name (Latin Translation): 9608

Middle Name: [text box]

Description: [dropdown]

* Login Name: 2291@avaya.com
Authentication Type: Basic [dropdown]

Password: [masked]
Confirm Password: [masked]

Localized Display Name: [text box]

Endpoint Display Name: [text box]

Title: [text box]

Language Preference: English (United Kingdom) [dropdown]

Time Zone: (0:0)GMT : Dublin, Edinburgh, L [dropdown]

Employee ID: [text box]

Department: [text box]

Company: [text box]

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: 2291 @ 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 Sequence** field configured in **Section 6.10**.
- Select the appropriate application sequence from the drop-down menu in the **Termination Sequence** field configured in **Section 6.10**.
- Select the appropriate location from the drop-down menu in the **Home Location** field.

Session Manager Profile ▾

SIP Registration

* Primary Session Manager

Primary	Secondary	Maximum
4	0	4
< [Progress Bar] >		

Secondary Session Manager

Survivability Server

Max. Simultaneous Devices ▾

Block New Registration When Maximum Registrations Active?

Application Sequences

Origination Sequence ▾

Termination Sequence ▾

Call Routing Settings

* Home Location ▾

Conference Factory Set ▾

Call History Settings

Enable Centralized Call History?

Expand the **Endpoint Profile** section.

- Select Communication Manager 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 Communication Manager user configuration automatically.

The screenshot shows the 'CM Endpoint Profile' configuration form. The form is titled 'CM Endpoint Profile' with a dropdown arrow. It contains several fields and checkboxes:

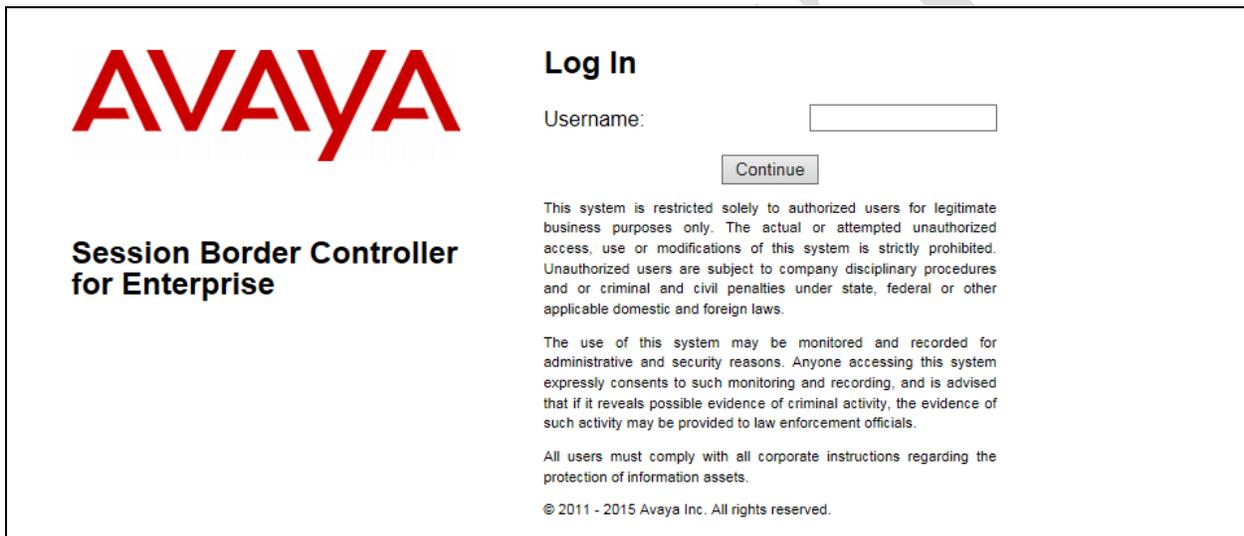
- * System:** CM1_Element (dropdown)
- * Profile Type:** Endpoint (dropdown)
- Use Existing Endpoints:**
- * Extension:** 2291 (text field) with an 'Endpoint Editor' button to its right.
- * Template:** 9608SIP_DEFAULT_CM_7_0 (dropdown)
- Set Type:** 9608SIP (text field)
- Security Code:** (empty text field)
- Port:** IP (text field)
- Voice Mail Number:** (empty text field)
- Preferred Handle:** (None) (dropdown)
- Calculate Route Pattern:**
- Sip Trunk:** aar (text field)
- Enhanced Callr-Info display for 1-line phones:**
- Delete Endpoint on Unassign of Endpoint from User or on Delete User:**
- Override Endpoint Name and Localized Name:**
- Allow H.323 and SIP Endpoint Dual Registration:**

7. Configure Avaya Session Border Controller for Enterprise

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

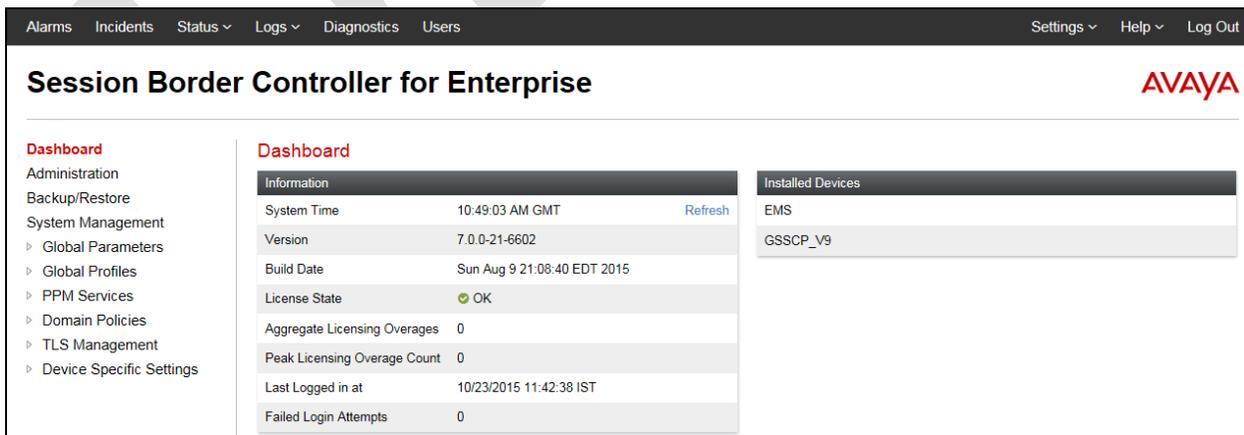
7.1. Access Avaya Session Border Controller for Enterprise

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



The login page features the Avaya logo in red on the left. To the right, under the heading "Log In", there is a "Username:" label followed by a text input field and a "Continue" button. Below the input field, there are three paragraphs of legal disclaimer text and a copyright notice at the bottom: "© 2011 - 2015 Avaya Inc. All rights reserved."

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



The dashboard has a top navigation bar with "Alarms", "Incidents", "Status", "Logs", "Diagnostics", and "Users" on the left, and "Settings", "Help", and "Log Out" on the right. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand menu lists "Dashboard" (selected) and "Administration" (with sub-items: Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings). The main content area is titled "Dashboard" and contains two panels: "Information" and "Installed Devices".

Information	
System Time	10:49:03 AM GMT Refresh
Version	7.0.0-21-6602
Build Date	Sun Aug 9 21:08:40 EDT 2015
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	10/23/2015 11:42:38 IST
Failed Login Attempts	0

Installed Devices	
EMS	
GSSCP_V9	

7.2. Define Network Management

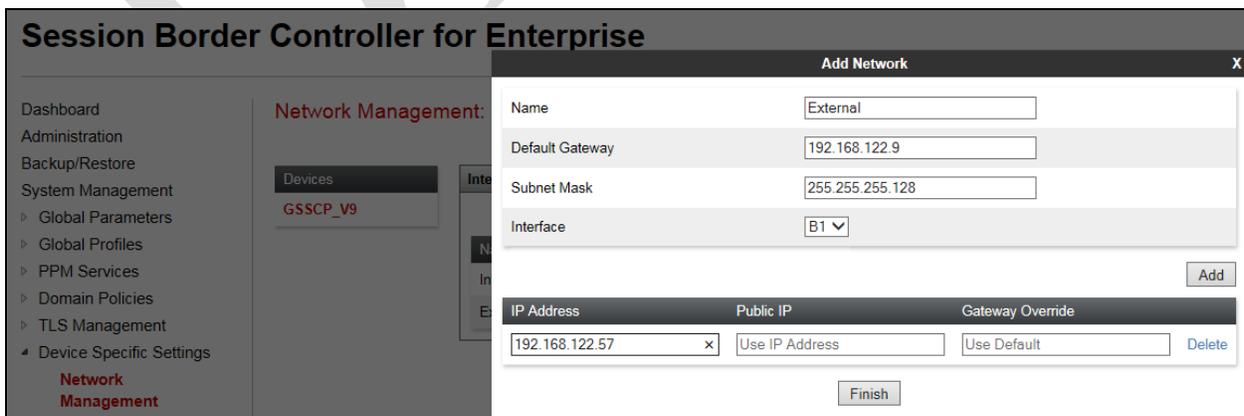
Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one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

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



Enter details for the external interface in the dialogue box (not shown):

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



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

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

The following screenshot shows the completed Network Management configuration:

Name	Gateway	Subnet Mask	Interface	IP Address	Edit	Delete
Internal	10.10.9.1	255.255.255.0	A1	10.10.9.71	Edit	Delete
External	192.168.122.9	255.255.255.128	B1	192.168.122.57	Edit	Delete

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

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

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

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

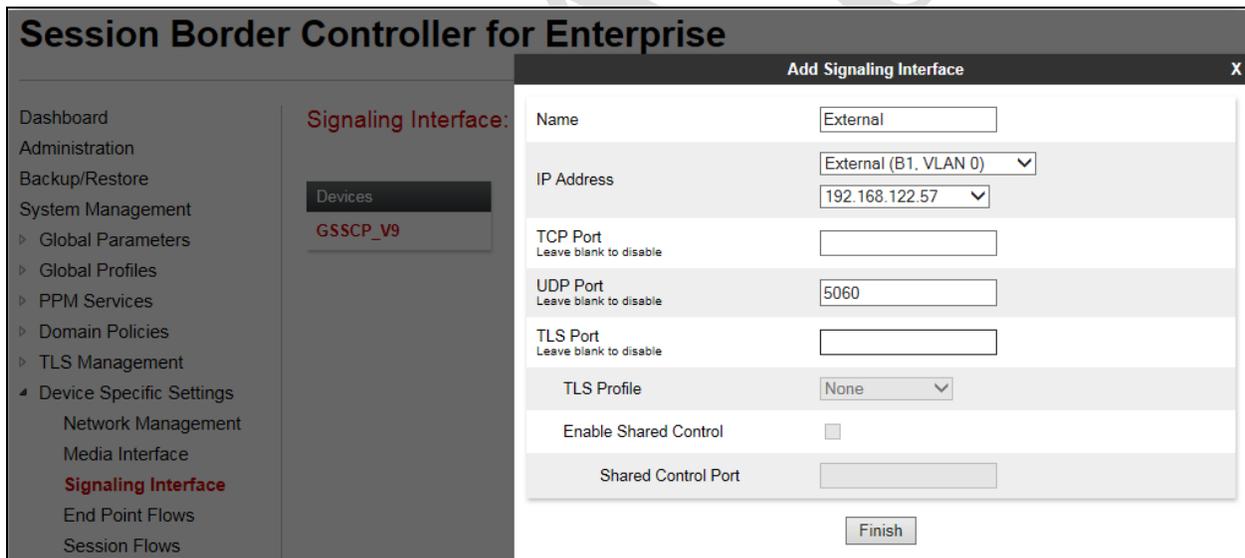
7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces. Testing was carried out with TCP used for transport of signalling between the Session Manager and the Avaya SBCE, and UDP for transport of signalling between the Avaya SBCE and the Colt SIP Trunk. This document shows the configuration for TCP and UDP, if additional security is required, it's recommended to use TLS and port 5061.

7.3.1. Signalling Interfaces

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

- Select **Add** and enter details of the external signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was a single IP address **192.168.122.57**.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for the Colt SIP Trunk.



The screenshot shows the 'Session Border Controller for Enterprise' configuration interface. On the left is a navigation menu with 'Device Specific Settings' expanded to 'Signaling Interface'. The main area displays the 'Add Signaling Interface' dialog box with the following fields:

Field	Value
Name	External
IP Address	External (B1, VLAN 0) [192.168.122.57]
TCP Port	[Leave blank to disable]
UDP Port	5060
TLS Port	[Leave blank to disable]
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	[]

A 'Finish' button is located at the bottom right of the dialog box.

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

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

The following screenshot shows details of the media interfaces:

Name	Media IP Network	Port Range	
Internal	10.10.9.71 Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
External	192.168.122.57 External (B1, VLAN 0)	35000 - 40000	Edit Delete

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the Colt SIP Trunk is connected as the Trunk Server and the Session Manager is connected as the Call Server.

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

Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

- In the General dialogue box shown in the previous screenshot, check the **T.38 Support** box. During testing, the rest of the parameters were left at default values.
- Click on **Next** and **Next** again to go through the next two dialogue boxes. During testing, these were left at default values.

The image shows two screenshots of the 'Interworking Profile' configuration dialog. The left screenshot displays the 'SIP Timers' section with the following fields and ranges:

Field	Unit	Range
Min-SE	seconds	[90 - 86400]
Init Timer	milliseconds	[50 - 1000]
Max Timer	milliseconds	[200 - 8000]
Trans Expire	seconds	[1 - 64]
Invite Expire	seconds	[180 - 300]

The right screenshot displays the 'Privacy' section with the following fields:

Field	Control
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

In the final dialogue box, select the required extensions from the **Extensions** drop down menu. Note that Avaya extensions are not supported for the SIP Trunk though they were applied to the Session Manager during testing. Click on **Finish**

The image shows the 'Editing Profile: ASM' dialog with the following configuration:

Field	Value
Record Routes	<input checked="" type="radio"/> Both Sides
Include End Point IP for Context Lookup	<input type="checkbox"/>
Extensions	Avaya
Diversion Manipulation	<input type="checkbox"/>
Diversion Condition	None
Diversion Header URI	
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
DTMF Support	<input checked="" type="radio"/> None

To define Server Interworking for the Colt SIP Trunk, click on **Add** (not shown). A pop-up menu (not shown) is generated. In the **Name** field enter a descriptive name for the Colt SIP Trunk and click **Next**.

In the General dialogue box that appears, check the **T.38** box

The screenshot shows a 'General' dialog box with the following settings:

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

Finish

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

Interworking Profile		Interworking Profile	
All fields are optional.		Privacy	
SIP Timers		Privacy Enabled	<input type="checkbox"/>
Min-SE	<input type="text"/> seconds, [90 - 86400]	User Name	<input type="text"/>
Init Timer	<input type="text"/> milliseconds, [50 - 1000]	P-Asserted-Identity	<input type="checkbox"/>
Max Timer	<input type="text"/> milliseconds, [200 - 8000]	P-Preferred-Identity	<input type="checkbox"/>
Trans Expire	<input type="text"/> seconds, [1 - 64]	Privacy Header	<input type="text"/>
Invite Expire	<input type="text"/> seconds, [180 - 300]		
<input type="button" value="Back"/> <input type="button" value="Next"/>		<input type="button" value="Back"/> <input type="button" value="Next"/>	

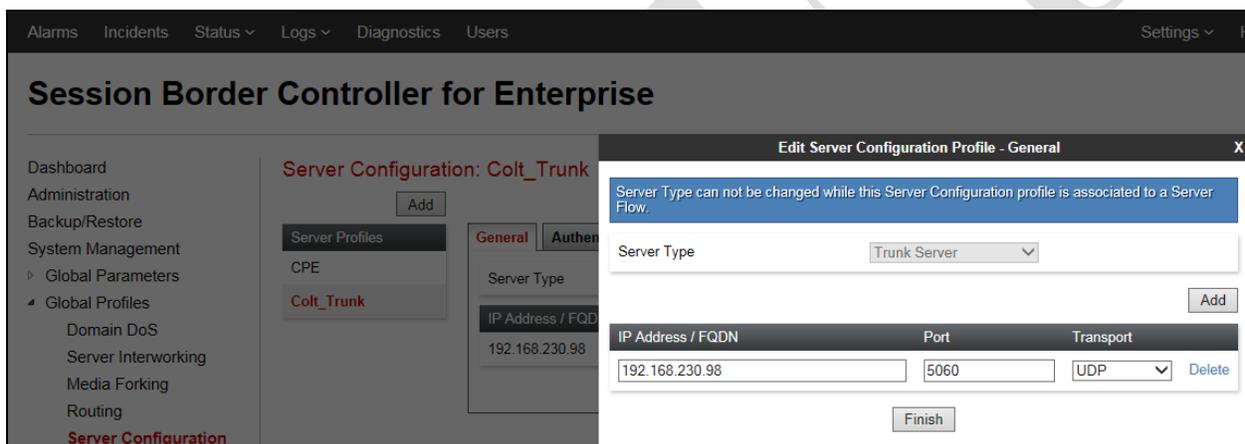
In the final dialogue box, select **None** from the **Extensions** box and click on **Finish**.

Interworking Profile	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides <input type="radio"/> Dialog-Initiate Only (Single Side) <input type="radio"/> Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	<input type="checkbox"/>
Extensions	<input type="text" value="None"/> ▼
Diversion Manipulation	<input type="checkbox"/>
Diversion Condition	<input type="text" value="None"/> ▼
Diversion Header URI	<input type="text"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

7.5. Define Servers

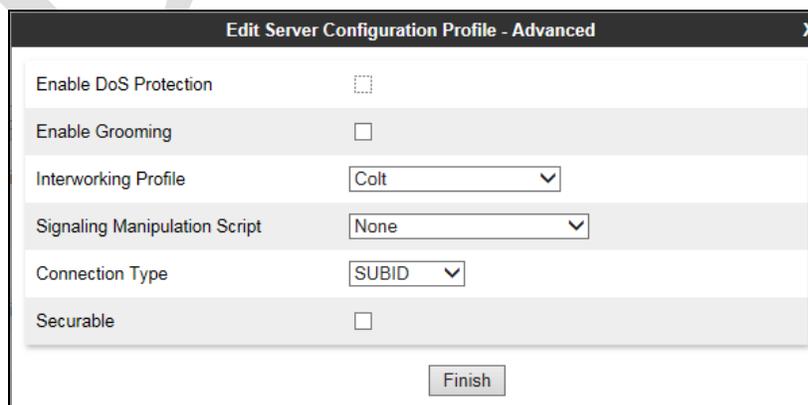
A server definition is required for each server connected to the Avaya SBCE. In this case, the Colt SIP Trunk is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the Colt SIP Trunk Server, navigate to **Global Profiles** → **Server Configuration** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up menu (not shown). Click on **Next** and enter details in the dialogue box.

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



The screenshot displays the 'Edit Server Configuration Profile - General' dialog box. The 'Server Type' is set to 'Trunk Server'. The 'IP Address / FQDN' field contains '192.168.230.98', the 'Port' is '5060', and the 'Transport' is 'UDP'. A 'Delete' button is next to the IP address field. The 'Finish' button is at the bottom. A warning message at the top reads: 'Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.'

- Click on **Next** and **Next** again to go through the next two dialogue boxes. During testing, these were left at default values. Final dialogue box is the **Advanced** settings:
- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for the Colt SIP Trunk defined in **Section 7.4**.
- Click **Finish**.



The screenshot displays the 'Edit Server Configuration Profile - Advanced' dialog box. The settings are: 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (Colt), 'Signaling Manipulation Script' (None), 'Connection Type' (SUBID), and 'Securable' (checkbox). The 'Finish' button is at the bottom.

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

- Ensure that **Call Server** is selected in the **Server Type** drop down menu in the **General** dialogue box.
- Ensure that the Interworking Profile defined for the Session Manager in **Section 7.4** is selected in the **Interworking Profile** drop down menu in the Advanced dialogue box (not shown).

IP Address / FQDN	Port	Transport	
10.10.9.31	5060	TCP	Delete

7.6. Define Routing

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

To define routing to the Session manager, navigate to **Global Profiles** → **Routing** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the dialogue box (not shown), click on Next and enter details for the Routing Profile:

- Click on **Add** to specify an IP address for the Session Manager.
- Assign a priority in the **Priority / Weight** field, with a single IP address a value of **1** can be used
- Select the Server Configuration defined in **Section 7.5** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.

The screenshot shows the 'Profile : LAN - Edit Rule' configuration window. The left sidebar contains a navigation menu with 'Routing' selected. The main area shows configuration options for the LAN profile:

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

Below these options is a table for defining routing rules:

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	CPE	10.10.9.31:5060 (TCP)	None	Delete

A 'Finish' button is located at the bottom right of the configuration area.

Repeat the above process for the Routing Profile for the Colt SIP Trunk:

The screenshot shows the 'Profile : WAN - Edit Rule' configuration window. The configuration options are similar to the LAN profile but with specific values for the WAN profile:

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

The routing rule table is as follows:

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Colt_Trunk	192.168.230.98:5060 (UDP)	None	Delete

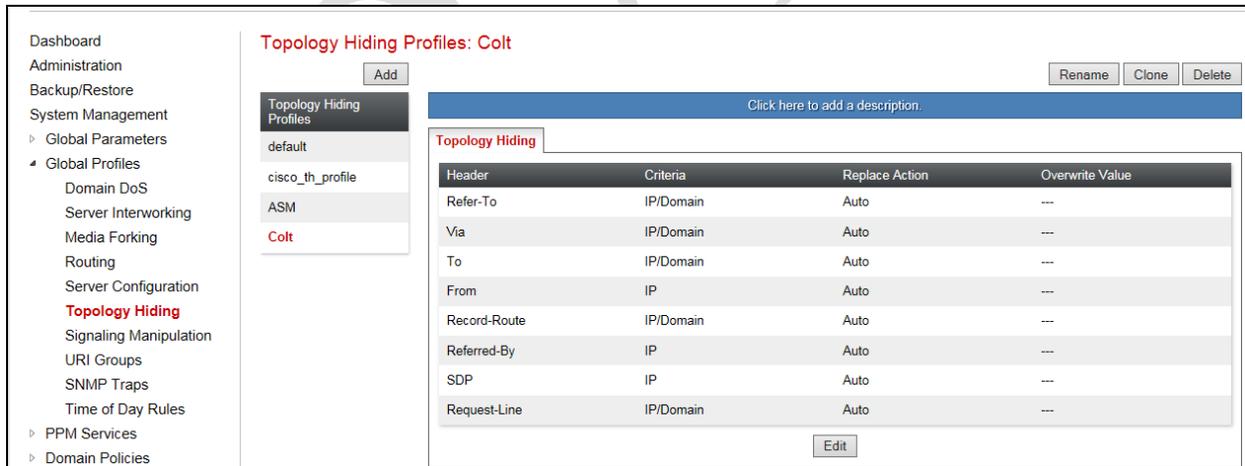
A 'Finish' button is located at the bottom center of the configuration area.

7.7. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop or external interfaces. 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 Colt SIP Trunk, 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 Colt SIP Trunk and click **Next**.
- Click on **Add Header** and select from the **Header** drop down menu.
- Select **IP** or **IP/Domain** from the **Criteria** drop down menu depending on requirements. During testing **IP** was used for the From header so that the domain name of “anonymous.invalid” for CLI restricted calls was not overwritten.
- Leave the **Replace Action** at the default value of **Auto** unless a specific domain name is required. In this case, select **Overwrite** and define a domain name in the **Overwrite Value** field.
- Topology hiding was defined for all headers where the function is available.



The screenshot shows the configuration page for 'Topology Hiding Profiles: Colt'. The sidebar on the left contains a navigation menu with 'Topology Hiding' highlighted. The main content area shows a table of headers with their respective criteria, replace actions, and overwrite values.

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

To define Topology hiding for the Session Manager, follow the same process. This can be simplified by cloning the profile defined for the Colt SIP Trunk. Do this by highlighting the profile defined for the Session Manager and clicking on **Clone**.

Enter an appropriate name for the Session Manager and click on Next. Make any changes where required, in the test environment the settings were left at the same values.

Topology Hiding Profiles: ASM

Topology Hiding Profiles

Click here to add a description.

Topology Hiding

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

Topology Hiding Profiles

default

cisco_th_profile

ASM

Colt

7.8. End Point Policy Groups

End Point Policy Groups are used to bring together a number of different rules for use in a server flow described in **Section 7.9**. The Colt SIP Trunk was tested with a signalling rule to remove unnecessary and Avaya proprietary SIP headers. This was not necessary for the effective functioning of the SIP Trunk but was used to reduce the SIP message size.

7.8.1. Signalling Rules

Signalling rules are a mechanism on the Avaya SBCE to handle any non-standard signalling that may be encountered on the SIP Trunk of a particular Service Provider. In the case of the Colt SIP Trunk, this was the transmission of Avaya proprietary and unnecessary SIP message headers from the Avaya equipment.

To define the signalling rule, navigate to **Domain Policies** → **Signaling Rules** in the main menu on the left hand side. Click on **Add** and enter details in the Signaling Rule pop-up box. In the **Rule Name** field enter a descriptive name for the signalling rule and click **Next** and **Next** again, then **Finish**

- Click on the **Request Headers** tab and then click on **Add In Header Control** (not shown).
- Either select a standard header from the **Header Name** drop down menu or check the **Proprietary Request Header** box and enter the name manually. The example shows **P-Location**.
- Select **ALL** from the **Method Name** drop down menu.
- Check the **Forbidden** button in the **Header Criteria** menu.
- Select **Remove Header** from the **Presence Action** drop down menu.

Apply the above to the following SIP Headers: Accept; Alert-Info; Av-Global-Session-ID; Endpoint-View; P-AV-Message-Id; P-Charging-Vector; P-Location: The following screenshot shows the applied Request Header removal:

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

The same is required for Response Headers. In addition to applying the rule to the headers listed previously, the rule must also be applied to the response codes where the headers may be present. The screenshot below shows the applied Response Header removal:

Signaling Rules: Header_Removal

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

Response headers are defined in the same way as request headers. The screenshot over the page shows the additional drop down menu for **Response Code**. This is applied to **1XX** and **2XX** response codes so the header can be removed from 180 Ringing / 183 Session Progress and 200 OK messages.

SIP header “P-Location” is shown as an example. Click **Finish** to complete.

7.8.2. End Point Policy Group

An End Point Policy Group is required to implement the signalling rule. To define one for use in the Session Manager server flow, navigate to **Domain Policies** → **End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up box (not shown). Click on **Next** to configure the Policy Set. Enter details as follows:

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

7.9. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for the Colt SIP Trunk and another for the Session Manager. These End Point Server Flows allow calls to be routed from the Session Manager to the Colt SIP Trunk and vice versa. To define a Server Flow for the Colt SIP Trunk, navigate to **Device Specific Settings → End Point Flows**.

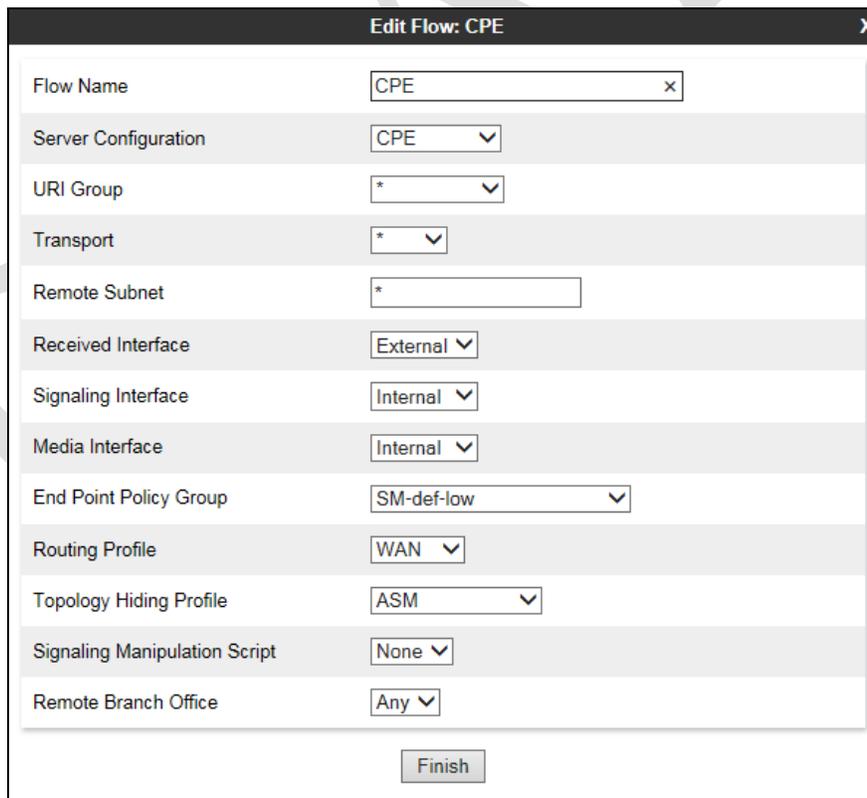
- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for the Colt SIP Trunk, in the test environment **Colt_Trunk** was used.
- In the **Received Interface** drop-down menu, select the internal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

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

Finish

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 **Name** field enter a descriptive name for the server flow for the Session Manager, in the test environment **CPE** was used.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that 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 **End Point Policy Group** drop-down menu, select the End Pint Policy Group defined in **Section 7.8**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Colt SIP Trunk defined in **Section 7.6**.
- 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 "Edit Flow: CPE" with a close button (X) in the top right corner. The dialog contains the following fields and values:

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

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

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

- Dashboard
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management
- ▾ Device Specific Settings
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows**
 - Session Flows
 - DMZ Services
 - TURN/STUN Service

End Point Flows: GSSCP_V9

Devices

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: CPE

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	CPE	*	External	Internal	SM-def-low	WAN	View Clone Edit Delete

Server Configuration: Colt_Trunk

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Colt_Trunk	*	Internal	External	default-low	LAN	View Clone Edit Delete

DRAFT

BG; Reviewed:
RRR m/d/y

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

54 of 59
Colt_CM70_SM

8. Configure the Colt SIP Trunk Equipment

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

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:

SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> CM_Entity	10.10.9.12	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/> ASBCE	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 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
          Port          State              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
```

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

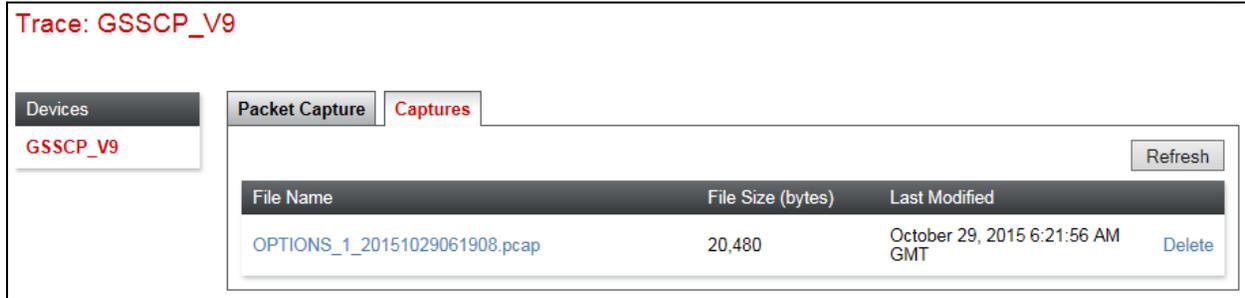
To define the trace, navigate to **Device Specific Settings** → **Advanced Options** → **Troubleshooting** → **Trace** in the main menu on the left hand side and select the **Packet Capture** tab.

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

The screenshot displays the 'Packet Capture Configuration' window in the Avaya SBCE management interface. The left-hand navigation pane is expanded to 'Trace'. The main configuration area is titled 'Trace: GSSCP_V9' and contains the following fields and controls:

- Status:** Ready
- Interface:** B1 (dropdown menu)
- Local Address (IP:Port):** All (dropdown menu) and an empty text input field.
- Remote Address (*, *Port, IP, IP:Port):** * (text input field)
- Protocol:** All (dropdown menu)
- Maximum Number of Packets to Capture:** 10000 (text input field)
- Capture Filename (Using the name of an existing capture will overwrite it.):** OPTIONS_1.pcap (text input field)
- Buttons:** Start Capture and Clear

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



The screenshot shows a web interface for viewing network traces. At the top, it says "Trace: GSSCP_V9". Below this, there are two tabs: "Packet Capture" and "Captures", with "Captures" being the active tab. On the left, there is a "Devices" sidebar with "GSSCP_V9" selected. In the main area, there is a table of captures and a "Refresh" button.

File Name	File Size (bytes)	Last Modified	
OPTIONS_1_20151029061908.pcap	20,480	October 29, 2015 6:21:56 AM GMT	Delete

The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response to OPTIONS in the form of a 200 OK will be seen from the Colt 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 the Colt SIP Trunk. The Colt SIP Trunk is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

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

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

©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.