



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to support UPC Business SIPTrunk - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between UPC Business SIPTrunk 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. UPC 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 UPC Business SIPTrunk and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with UPC Business SIPTrunk are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

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

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

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

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for UPC Business SIPTrunk with the following observations:

- When an incoming call was made to an unassigned number, Communication Manager returned a “404 Not Found” message typical for this type of call failure. The network re-attempted the call however, and a significant delay of over three minutes was observed before the caller heard a tone.
- When an outgoing call was made to a PSTN destination and the call wasn’t answered, a “500 Internal Server Error” was received from the network. This is a generic failure message and could have been more informative.
- When an outgoing call was made to a busy PSTN destination, a “500 Internal Server Error” was received from the network. This has since been rectified by UPC and the network is returning 486 Busy Here, but it has not been retested in Avaya Labs.
- When an outgoing call was made to an unallocated PSTN destination, a “500 Internal Server Error” was received from the network. This is a generic failure message and could have been more informative, for example “404 Not Found”. A number of call failures are handled in this way by the network, and although an appropriate tone is heard, the call failures could be more graceful.
- When an incoming call was made and Communication Manager could not provide any of the codecs in the SDP offer, it sent a “488 Not Acceptable Here” which is typical for this type of call failure. The network however, re-attempted the call several times and there was a significant delay, around two minutes, before a tone was heard.
- Incoming Toll-Free numbers were not tested as no Toll-Free access to the enterprise was available.
- Outgoing Toll-Free calls were unsuccessful, the likely reason is that access to Toll-Free numbers is not available from the UPC Labs.
- Operator calls were unsuccessful, the likely reason is that access to the Operator is not available from the UPC Labs.
- No test calls were made to the Emergency Services as no test was booked with the Emergency Services Operator.
- When testing CLI restriction from the network, the P-Asserted-ID and Privacy headers were not present in the INVITE coming in from the network. This is not a significant issue as a meaningful message was still displayed on the screen of the Communication Manager extension.
- When testing EC500, significant post dial delay made it necessary to increase the “Redirect On OPTIM Failure” timer from 5000 to 10000. This is likely to be a limitation of the test environment.

2.3. Support

For technical support on UPC products please contact the UPC support team at:

<http://business.upc.nl/klantenservice/>

Telephone number: +31 (0) 88 - 12 12 500.

3. Reference Configuration

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

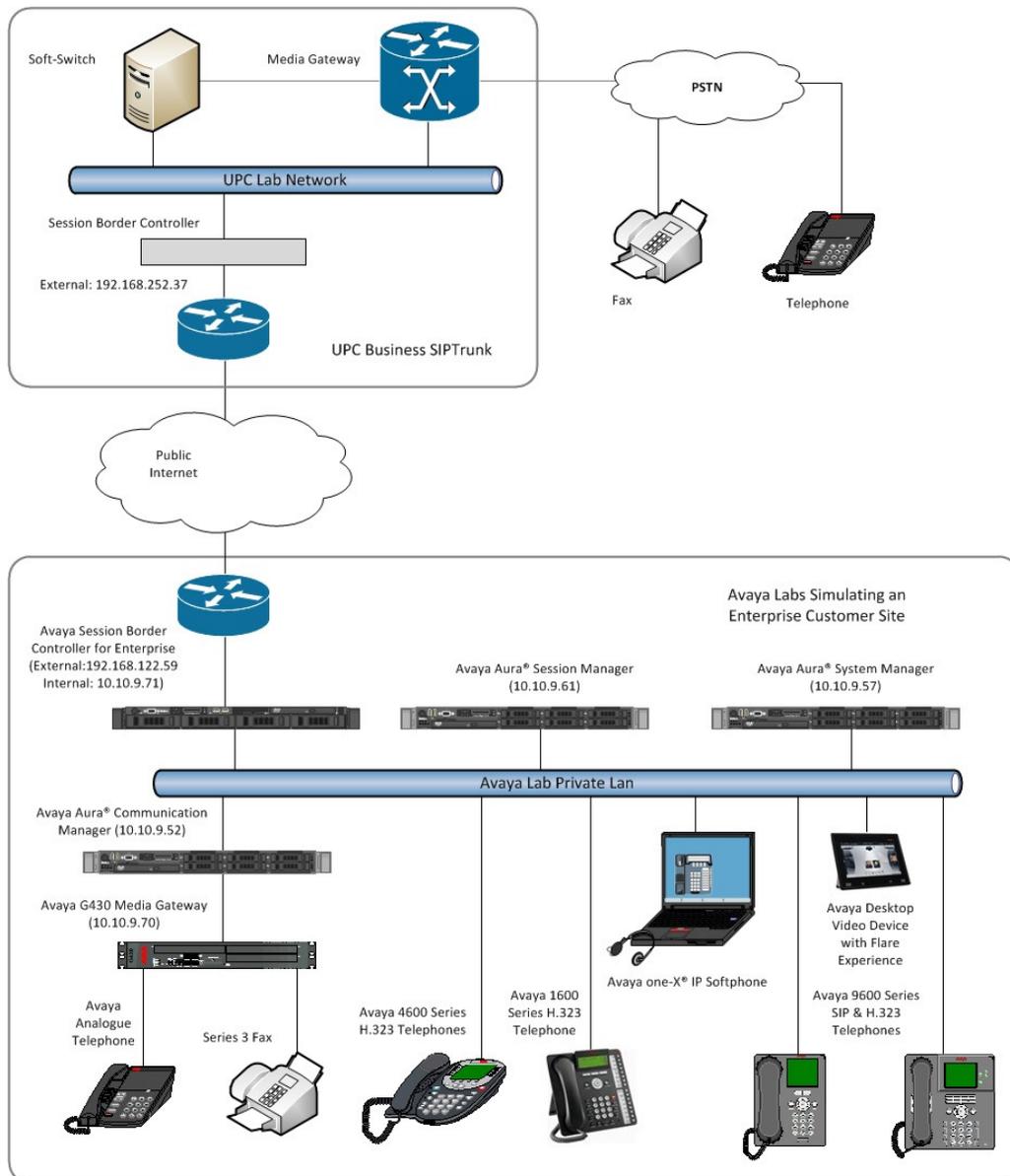


Figure 1: Test Setup UPC Business SIPTrunk to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Dell PowerEdge R620 running Session Manager on VM Version 8	SM-6.3.2.0.632023-e50-00
Dell PowerEdge R620 running System Manager on VM Version 8	SMGR-6.3.0.8.5682-e50-64 (Build 5682)
Dell PowerEdge R620 running Communication Manager on VM Version 8	R016x.03.0.124.0
Avaya Session Border Controller Advanced for Enterprise Server	6.2.0.Q48
Avaya 1616 Phone (H.323)	1.302
Avaya 4621 Phone (H.323)	2.902
Avaya 9670 Phone (H.323)	3.200
Avaya A175 Desktop Video Device (SIP)	Flare Experience Release 1.1.2
Avaya 9630 Phone (SIP)	R2.6 SP9
Avaya 9608 Phone (SIP)	R6.2 SP1
Avaya one-X® Communicator (H.323) on Lenovo T510 Laptop PC	6.1.8.06-SP8-40314
Analogue Handset	NA
Analogue Fax	NA
UPC	
Genband S3 SBC	software version 7.1.14.3

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 UPC Business SIPTrunk. For incoming calls, the Session Manager receives SIP messages from the Avaya SBC for Enterprise (Avaya SBCE) and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the UPC Business SIPTrunk 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 UPC Business SIPTrunk network, and any other SIP trunks used.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	0
Maximum Concurrently Registered IP Stations:	18000	3
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	41000	0
Maximum Video Capable IP Softphones:	18000	0
Maximum Administered SIP Trunks:	24000	10
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	0
Maximum Media Gateway VAL Sources:	250	1
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0

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

```
display system-parameters customer-options                               Page 4 of 11
                                OPTIONAL FEATURES

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

IP Attendant Consoles? y
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SMVM1** and **10.10.79.61** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```
display node-names ip
                                IP NODE NAMES

Name          IP Address
SMVM1       10.10.79.61
default      0.0.0.0
procr        10.10.79.52
procr6       ::
```

5.3. Administer IP Network Region

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

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

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

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

IP Codec Set

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1: G.711A	n	2	20
2: G.711MU	n	2	20
3: G.729A	n	2	20

UPC Business SIPTrunk 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 the default value of **y**

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

IP Codec Set

Allow Direct-IP Multimedia? n

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

5.5. Administer SIP Signaling Groups

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

- Set **Group Type** to **sip**
- Set **Transport Method** to **tcp**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SMVM1** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region **1**)
- Leave **Far-end Domain** blank (allows the CM to accept calls from any SIP domain on the associated trunk)
- Set **Direct IP-IP Audio Connections** to **y**
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.

```
add signaling-group 1                               Page 1 of 2
                                           SIGNALING GROUP

Group Number: 1                                Group Type: sip
IMS Enabled? n                                Transport Method: tcp
Q-SIP? n
IP Video? n                                    Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

Near-end Node Name: procr                       Far-end Node Name: SMVM1
Near-end Listen Port: 5060                      Far-end Listen Port: 5060
                                           Far-end Network Region: 1

Far-end Domain:

Incoming Dialog Loopbacks: eliminate            Bypass If IP Threshold Exceeded? n
                                           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:

- Set the **Redirect On OPTIM Failure** to **10000** to overcome potential issues with post-dial delay and EC500 (see **Section 2.2**)
- Set the Preferred **Minimum Session Refresh Interval (sec)** field to a value mutually agreed with UPC to prevent unnecessary SIP messages during call setup. A value of **900** was used for testing

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

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

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

    Numbering Format: public
                                                    UUI Treatment: service-provider
                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n
```

On **Page 4** of this form:

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

```
add trunk-group 1                                     Page 4 of 21
                                                    PROTOCOL VARIATIONS
                                                    Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
    Send Transferring Party Information? y
    Network Call Redirection? n

    Send Diversion Header? y
    Support Request History? n
    Telephone Event Payload Type: 101

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

5.7. Administer Calling Party Number Information

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

```

change public-unknown-numbering 0                               Page 1 of 2
                                NUMBERING - PUBLIC/UNKNOWN FORMAT
Ext  Ext      Trk      CPN      Total
Len  Code     Grp(s)  Prefix   CPN
                                Len
                                Total Administered: 8
                                Maximum Entries: 9999
4    2000      1        31103nnnnn0  11
4    2298      1        31103nnnnn3  11
4    2316      1        31103nnnnn5  11
4    2346      1        31103nnnnn2  11
4    2396      1        31103nnnnn1  11
4    2402      1        31103nnnnn6  11
4    2403      1        31103nnnnn6  11
4    2611      1        31103nnnnn4  11
                                Note: If an entry applies to
                                a SIP connection to Avaya
                                Aura(R) Session Manager,
                                the resulting number must
                                be a complete E.164 number.
                                Communication Manager
                                automatically inserts
                                a '+' digit in this case.

```

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to UPC Business SIPTrunk. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

```

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

```

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

```

change ars analysis 0
ARS DIGIT ANALYSIS TABLE
Location: all
Percent Full: 0
Dialed      Total      Route      Call      Node      ANI
String      Min Max    Pattern    Type      Num      Reqd
0           11 14     1         pubu     7        n
00          13 15     1         pubu     7        n
0035391    13 13     1         pubu     7        n
0900       8  8      1         pubu     7        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
Pattern Number: 1      Pattern Name:
SCCAN? n              Secure SIP? n
Grp FRL NPA Pfx Hop Toll No.  Inserted      DCS/  IXC
No      Mrk Lmt List Del  Digits        QSIG
Dgts
1: 1    0
2:
3:
4:
5:
6:
BCC VALUE  TSC CA-TSC      ITC BCIE Service/Feature PARM  No. Numbering LAR
0 1 2 M 4 W      Request
Subaddress
1: y y y y y n  n      rest      unk-unk  none
2: y y y y y n  n      rest      none
3: y y y y y n  n      rest      none
4: y y y y y n  n      rest      none
5: y y y y y n  n      rest      none
6: y y y y y n  n      rest      none
  
```

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the Communication Manager extensions. The incoming digits sent in the INVITE message from UPC Business SIPTrunk can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by UPC for testing are assigned to the internal extensions of the test equipment configured within the Communication Manager. The **change inc-call-handling-trmt trunk-group x** command is used to translate numbers **31103nnnnn0** to **31103nnnnn6** to the 4 digit extension by deleting all (**10**) of the incoming digits and inserting the extension number. Note that the significant digits beyond the area code have been obscured.

change inc-call-handling-trmt trunk-group 1					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/ Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	11	31103nnnnn0	11	2000	
public-ntwrk	11	31103nnnnn1	11	2396	
public-ntwrk	11	31103nnnnn2	11	2346	
public-ntwrk	11	31103nnnnn3	11	2298	
public-ntwrk	11	31103nnnnn4	11	2611	
public-ntwrk	11	31103nnnnn5	11	2316	
public-ntwrk	11	31103nnnnn6	11	2501	

5.10. EC500 Configuration

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

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386nnnnnnn**)
- 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 2396								Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION								
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode	
2396	EC500	-	-	0035386nnnnnnn	1	1		

Note: The phone number is in international format as it is a test mobile phone used at Avaya Labs in Galway.

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

6. Configuring Avaya Aura® Session Manager

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

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

6.1. Log in to Avaya Aura® System Manager

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

The screenshot displays the Avaya Aura® System Manager 6.3 web interface. At the top left is the AVAYA logo. The page title is "Avaya Aura® System Manager 6.3". On the top right, it shows "Last Logged on at September 3, 2013 7:25 AM" and links for "Help | About | Change Password | Log off admin". The main content area is divided into three columns:

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

6.2. Administer SIP Domain

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

Routing

Home / Elements / Routing / Domains

Domain Management

New Edit Delete Duplicate More Actions

1 Item Refresh

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

Select : All, None

6.3. Administer Locations

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

Home / Elements / Routing / Locations Help ?

Location Details Commit Cancel

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

2 Items Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.79.*	VMWare subnet
<input type="checkbox"/>	* 10.10.9.*	Lab subnet

6.4. Administer Adaptations

An Adaptation is used to convert international called numbers to E.164 format with leading “+”. This adaptation is applied to the Avaya SBCE SIP Entity.

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

- Under **Matching Pattern** enter the international dialling prefix to be removed, in this case **00**.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the dialled number, the range set during test was large enough to accommodate any possible dialled number.
- Under **Delete Digits** enter the number required to remove the international dialling prefix, in this case **2**.
- Under **Insert Digits** enter the value required to convert the number to the standard format used for E.164 in SIP, that is the full E.164 number prefixed with a **+**.
- Under **Address to Modify** choose **destination** from the drop down box to apply this rule to the To and Request URI headers only.

Home / Elements / Routing / Adaptations Help ?

Adaptation Details Commit Cancel

General

* Adaptation name: International
Module name: DigitConversionAdapter
Module parameter: fromto=true

Egress URI Parameters:
Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
--------------------------	------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*00	*2	*36		*2	+	both		

Note: During test, the **Address to modify** was left as **both**. This is not required as the origination addresses did not have an international dialling prefix and were unaffected by the adaptation.

6.5. Administer SIP Entities

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

Under **General**:

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

In this configuration there are three SIP Entities:

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

6.5.1. Avaya Aura® Session Manager SIP Entity

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

The screenshot displays the configuration page for a SIP Entity. The breadcrumb trail at the top reads "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details" with "Commit" and "Cancel" buttons in the top right. The "General" section is active and contains the following fields:

- Name:** Session Manager BGVM1
- FQDN or IP Address:** 10.10.79.61
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text field)
- Location:** Galway (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (empty text field)

The "SIP Link Monitoring" section at the bottom shows the "SIP Link Monitoring" dropdown menu set to "Use Session Manager Configuration".

The Session Manager must be configured with the port numbers of 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

Port

TCP Failover port:

TLS Failover port:

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP	avaya.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	UDP	avaya.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="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** the Adaptation to that defined in **Section 6.4** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV:

* SIP Timer B/F (in seconds):

Credential name:

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: Off

SIP Link Monitoring
SIP Link Monitoring: Use Session Manager Configuration

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* **Name:** ASBCE_50

* **FQDN or IP Address:** 10.10.9.75

Type: SIP Trunk

Notes:

Adaptation: International

Location: Galway

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV:

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

Credential name:

Call Detail Recording: egress

Loop Detection
Loop Detection Mode: Off

SIP Link Monitoring
SIP Link Monitoring: Use Session Manager Configuration

6.6. Administer Entity Links

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

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

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

Home / Elements / Routing / Entity Links Help ?

Entity Links

5 Items [Refresh](#) Filter: Enable

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

Select : All, None

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

6.7. Administer Routing Policies

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

Under **General**:

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

The following screen shows the routing policy for Communication Manager.

The screenshot shows the 'Routing Policy Details' configuration page. The breadcrumb trail is 'Home / Elements / Routing / Routing Policies'. There are 'Commit' and 'Cancel' buttons in the top right. The 'General' section contains fields for '* Name' (Internal_CM_VM1), 'Disabled' (checkbox), '* Retries' (0), and 'Notes'. The 'SIP Entity as Destination' section has a 'Select' button. Below it is a table with columns: Name, FQDN or IP Address, Type, and Notes. The table contains one entry: CM_VM1, 10.10.79.52, CM. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. Below is a table with columns: Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The table shows one item with Ranking 0, Name 24/7, and Start/End times 00:00 and 23:59. There is a 'Filter: Enable' option and a 'Select : All, None' dropdown at the bottom.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CM_VM1	10.10.79.52	CM	

Time of Day

1 Item Refresh Filter: Enable

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

Select : All, None

The following screen shows the routing policy for the Avaya SBCE and onward routing to the PSTN via UPC Business SIPTrunk.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
ASBCE_50	10.10.9.75	SIP Trunk	

Time of Day

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	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 UPC Business SIPTrunk.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern: 0
 * Min: 8
 * Max: 15

Emergency Call:
 Emergency Priority: 1
 Emergency Type:
 SIP Domain: -ALL-
 Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		UPC		<input type="checkbox"/>	ASBCE_50	

Select : All, None

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

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern: 31103nnnnn
 * Min: 10
 * Max: 11

Emergency Call:
 Emergency Priority: 1
 Emergency Type:
 SIP Domain: -ALL-
 Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

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

Note: The pattern to be matched is a public DDI number, and has been obscured with “nnnnn”.

6.9. Administer Application for Avaya Aura® Communication Manager

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

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

The screenshot shows the 'Application Editor' window. The breadcrumb path is 'Home / Elements / Session Manager / Application Configuration / Applications'. The form contains the following fields:

- Name:** CMV1_App
- SIP Entity:** CM_VM1
- CM System for SIP Entity:** CM_VM1 (with a 'Refresh' button and a link to 'View/Add CM Systems')
- Description:** (empty text box)

Buttons for 'Commit' and 'Cancel' are located at the top right of the form.

6.10. Administer Application Sequence for Avaya Aura® Communication Manager

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

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

The screenshot shows the 'Application Sequence Editor' window. The breadcrumb path is 'Home / Elements / Session Manager / Application Configuration / Application Sequences'. The form contains the following sections:

- Application Sequence:**
 - Name:** CMV1_App_Seq
 - Description:** (empty text box)
- Applications in this Sequence:**
 - Buttons: Move First, Move Last, Remove
 - Table with 1 item:
- Available Applications:**
 - Buttons: Refresh, Filter: Enable
 - Table with 2 items:

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

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

6.11. Administer SIP Extensions

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

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of user@domain e.g. **2460@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

The screenshot shows the 'Identity' configuration tab for a SIP extension. The interface includes a navigation bar with tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Identity' tab is active, showing a form with the following fields:

- Last Name:** Windows
- First Name:** Flare
- Middle Name:** (empty)
- Description:** (empty)
- Login Name:** 2460@avaya.com
- Authentication Type:** Basic
- Password:** (masked with dots)
- Confirm Password:** (masked with dots)
- Localized Display Name:** (empty)
- Endpoint Display Name:** (empty)
- Title:** (empty)
- Language Preference:** English (United Kingdom)
- Time Zone:** (+1:0)GMT : Dublin, Edinburgh
- Employee ID:** (empty)
- Department:** (empty)
- Company:** (empty)

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: 2460 @ avaya.com

Add Cancel

Expand the **Session Manager Profile** section.

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

Session Manager Profile ▾

SIP Registration

* **Primary Session Manager** ▾

Primary	Secondary	Maximum
5	0	5

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 ▾

Expand the CM **Endpoint Profile** section:

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

CM Endpoint Profile ▾

* **System** CM_VM1 ▾

* **Profile Type** Endpoint ▾

Use Existing Endpoints

* **Extension** 2460 Endpoint Editor

* **Template** 9630SIP_DEFAULT_CM_6_3 ▾

Set Type 9630SIP

Security Code

Port IP

Voice Mail Number

Preferred Handle (None) ▾

Enhanced Callr-Info display for 1-line phones

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

Override Endpoint Name

7. Configure Avaya Session Border Controller for Enterprise

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

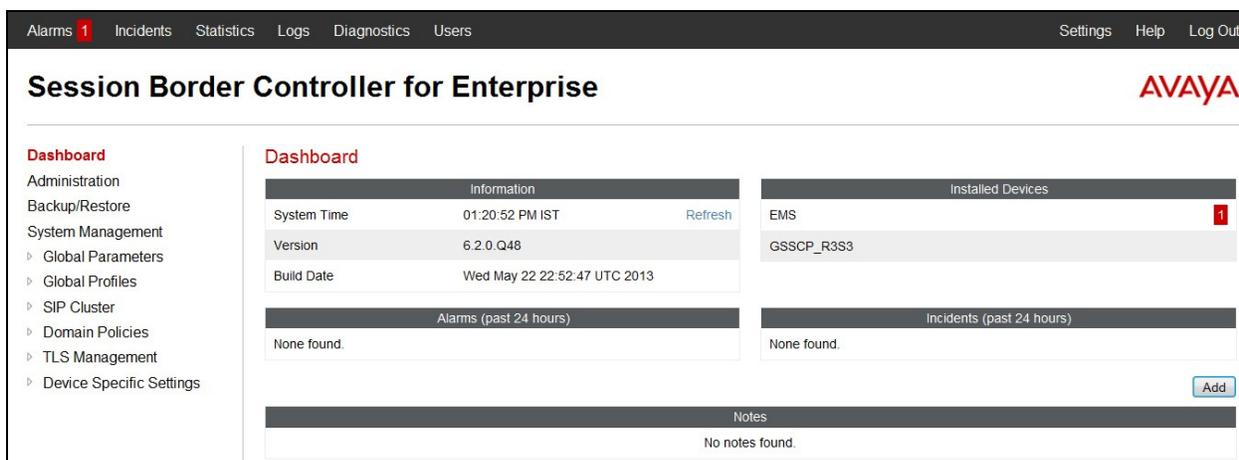
7.1. Access Avaya Session Border Controller for Enterprise

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



The login page features the Avaya logo in red on the left. To the right, under the heading "Log In", there are two input fields: "Username:" and "Password:". Below these fields is a blue "Log In" button. At the bottom right, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws."

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



The dashboard has a dark header with navigation links: Alarms (1), Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is titled "Session Border Controller for Enterprise" and includes the Avaya logo. A left-hand menu lists various sections: Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings), and Dashboard. The main dashboard area contains several panels: "Information" (System Time: 01:20:52 PM IST, Version: 6.2.0.Q48, Build Date: Wed May 22 22:52:47 UTC 2013), "Installed Devices" (listing EMS and GSSCP_R3S3), "Alarms (past 24 hours)" (None found), "Incidents (past 24 hours)" (None found), and "Notes" (No notes found). An "Add" button is located at the bottom right of the dashboard area.

7.2. Define Network Information

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

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

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

Session Border Controller for Enterprise AVAYA

Alarms 1 Incidents Statistics Logs Diagnostics Users Settings Help Log Out

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

Network Management: GSSCP_R3S3

Devices: GSSCP_R3S3

Network Configuration | Interface Configuration

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

A1 Netmask: 255.255.255.0 A2 Netmask: B1 Netmask: 255.255.255.128 B2 Netmask:

Add Save Clear

IP Address	Public IP	Gateway	Interface	
10.10.9.75		10.10.9.1	A1	Delete
192.168.122.59		192.168.122.51	B1	Delete

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

Network Management: GSSCP_R3S3

Devices: GSSCP_R3S3

Network Configuration | **Interface Configuration**

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

7.3. Define Interfaces

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

7.3.1. Signalling Interfaces

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

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

Signaling Interface: GSSCP_R3S3

Devices

GSSCP_R3S3

Signaling Interface

Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.9.75	5060	---	---	None	Edit Delete
Ext_Sig	192.168.122.59	---	5060	---	None	Edit Delete

7.3.2. Media Interfaces

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

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

Media Interface: GSSCP_R3S3

Devices

GSSCP_R3S3

Media Interface

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

Add

Name	Media IP	Port Range	Edit	Delete
Int_Med	10.10.9.75	35000 - 40000	Edit	Delete
Ext_Med	192.168.122.59	35000 - 40000	Edit	Delete

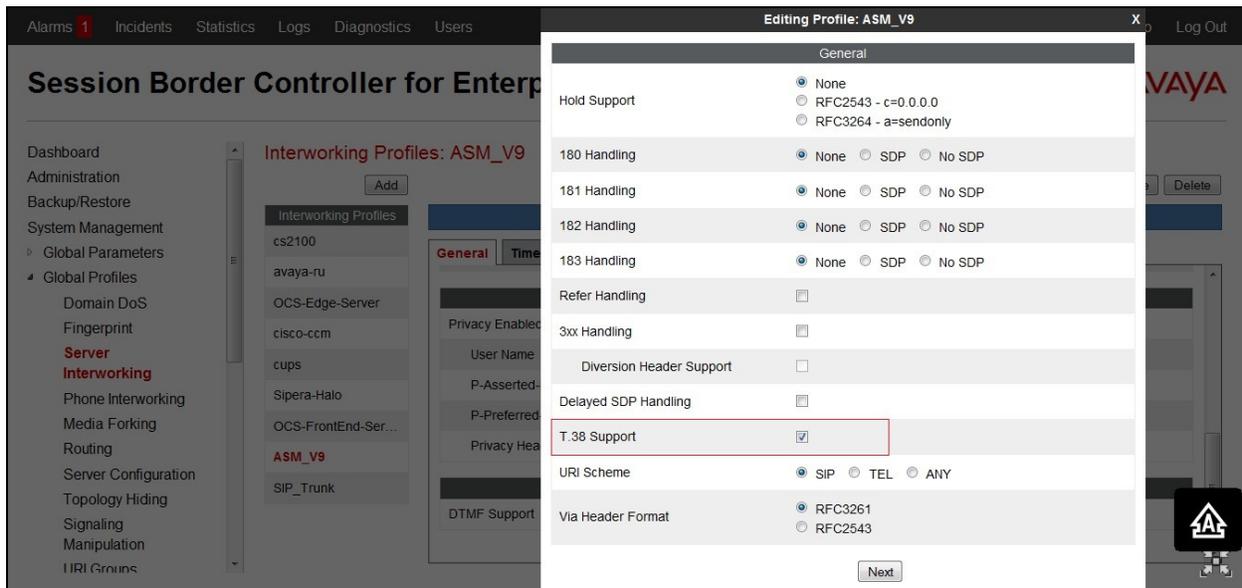
Note: During test the port ranges for the internal and external media interfaces were left at default values.

7.4. Define Server Interworking

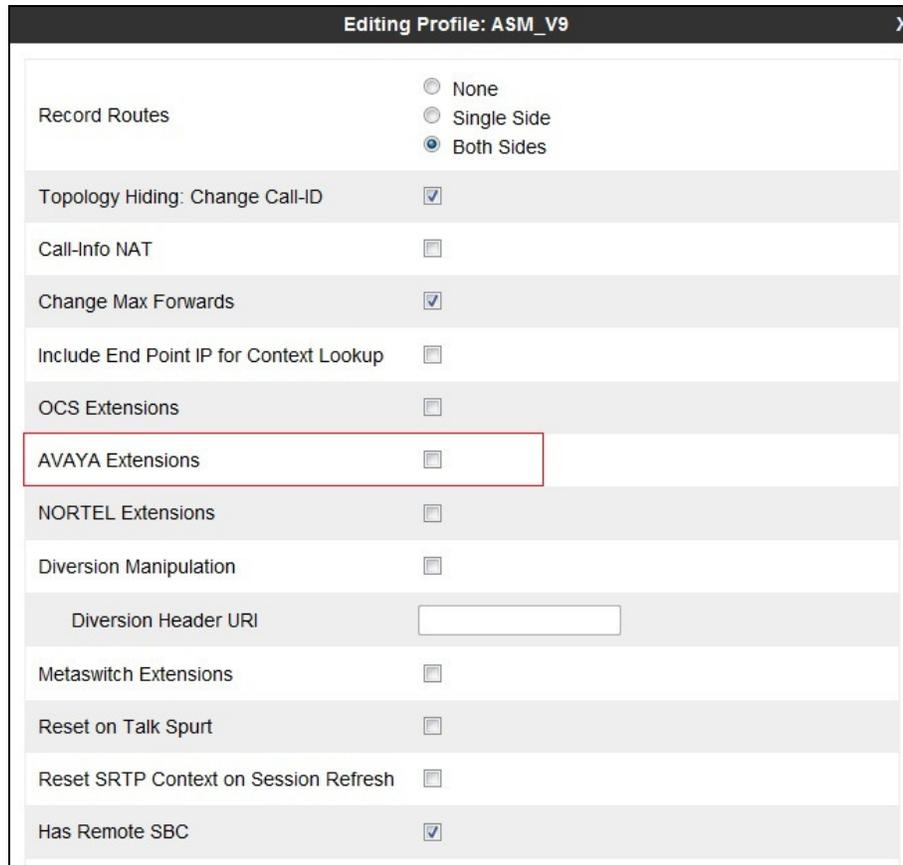
Server interworking is defined for each server connected to the Avaya SBCE. In this case, UPC Business SIPTrunk is connected as the Trunk Server and the Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

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

- In the **Clone Name** field enter a descriptive name for the Session Manager and click **Finish** – in test **ASM_V9** was used
- In the **General** tab (not shown) Select **Edit** and enter details in the pop-up menu
- Check the **T.38** box then click **Next** and **Finish** (not shown)



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



Editing Profile: ASM_V9	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>

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

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

7.5. Define Signalling Manipulation

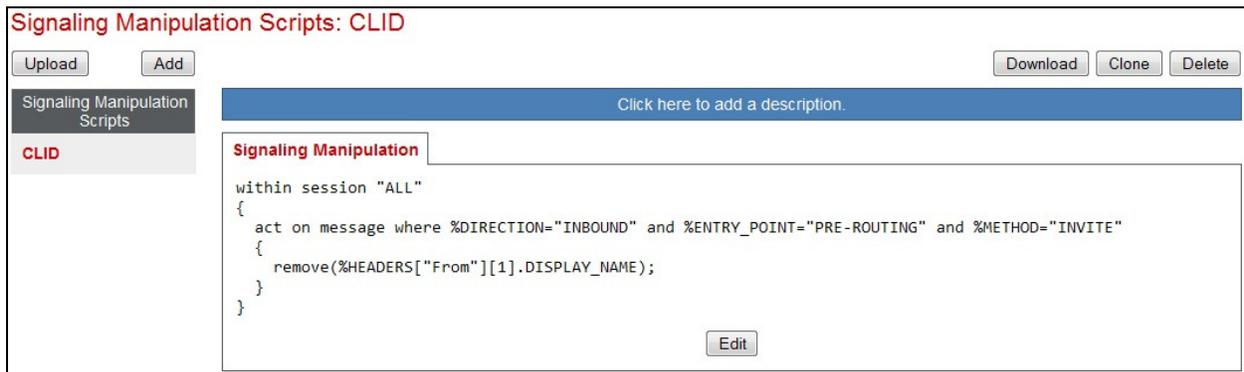
Signalling manipulation is required in some cases to ensure effective interworking. In the past, an issue has been found with enterprise phones connected to UPC where the calling party number is displayed twice. This happened because UPC send a display name parameter along with the URI in the From header that contains the full calling party number. The phone displays the display name plus the user portion of the URI and the result is that the calling party number

is displayed twice. If this issue is encountered and there is a requirement to remove the display name, a signalling manipulation script is available to do this.

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

```
within session "ALL"
{
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE-ROUTING" and
%METHOD="INVITE"
  {
    remove(%HEADERS["From"][1].DISPLAY_NAME);
  }
}
```

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



Note: This will only take effect when selected in the **Signalling Manipulation Script** drop down menu in the advanced Trunk Server settings. The Trunk server is defined in **Section 7.6** and is named **UPC_SIP_Trunk**.

7.6. Define Servers

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

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

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

The screenshot shows a window titled "Server Configuration: ASM_V9" with a sub-window "Edit Server Configuration Profile - General". On the left, there is a sidebar with "Server Profiles" containing "ASM_V9" and "UPC_SIP_Trunk". The main area contains the following fields:

- Server Type: Call Server (dropdown)
- IP Addresses / Supported FQDNs: 10.10.79.61 (text box)
- Supported Transports: TCP, UDP, TLS
- TCP Port: 5060 (text box)
- UDP Port: (empty text box)
- TLS Port: (empty text box)

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

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

The screenshot shows a window titled "Edit Server Configuration Profile - Advanced". The main area contains the following fields:

- Enable DoS Protection:
- Enable Grooming:
- Interworking Profile: ASM_V9 (dropdown)
- Signaling Manipulation Script: None (dropdown)
- TCP Connection Type: SUBID, PORTID, MAPPING

A "Finish" button is located at the bottom center of the dialog.

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

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

The screenshot shows the 'Edit Server Configuration Profile - General' dialog box. The title bar indicates the profile name is 'UPC_SIP_Trunk'. The main content area includes the following fields and settings:

- Server Type:** Trunk Server (dropdown)
- IP Addresses / Supported FQDNs:** 192.168.252.37 (text input)
- Supported Transports:** TCP (unchecked), UDP (checked), TLS (unchecked)
- TCP Port:** (empty text input)
- UDP Port:** 5060 (text input)
- TLS Port:** (empty text input)

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

- Click **Next** again then select the **Interworking Profile** for the UPC Business SIPTrunk defined in **Section 7.4** from the drop down menu
- If required, select the **Signaling Manipulation Script** defined in **Section 7.5**

The screenshot shows the 'Edit Server Configuration Profile - Advanced' dialog box. The main content area includes the following fields and settings:

- Enable DoS Protection:** (unchecked)
- Enable Grooming:** (unchecked)
- Interworking Profile:** SIP_Trunk (dropdown)
- Signaling Manipulation Script:** None (dropdown)
- UDP Connection Type:** SUBID (radio button selected), PORTID (radio button unselected), MAPPING (radio button unselected)

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

Note: See **Section 7.5** for the **Signalling Manipulation Script**. This is only required if there is a preference not to have the calling party number displayed twice on the enterprise phones. As stated in **Section 7.5**, UPC send a display name parameter along with the URI in the From header that contains the full calling party number. The phone displays the display name plus the user portion of the URI and the result is that the calling party number is displayed twice. Although the script has been tested successfully, it was not used in the SIP compliance testing that is the subject of these Application Notes.

7.7. Define Routing

Routing information is required for routing to the Session Manager on the internal side and UPC Business SIPTrunk on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used. To define routing to the Session Manager, navigate to **Global Profiles** → **Routing** in the main menu on the left hand side. Click on **Add** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Session Manager, in this case **ASM_V9**, and click **Next**
- Enter the Session Manager SIP interface address and port in the **Next Hop Server 1** field
- Select **TCP** for the **Outgoing Transport**
- Click **Finish**

The screenshot shows the 'Edit Routing Rule' dialog box. On the left, a sidebar displays 'Routing Profiles: ASM_V9' with an 'Add' button and a list of profiles: 'default', 'ASM_V9', and 'SIP_Trunk'. The 'Routing Profile' section shows 'Priority' set to '1'. The main dialog area has a blue header with the text 'Each URI group may only be used once per Routing Profile.' Below this is the 'Next Hop Routing' section with the following fields:

Next Hop Routing	
URI Group	* [dropdown]
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	10.10.79.61
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	[empty]
Routing Priority based on Next Hop Server	<input checked="" type="checkbox"/>
Use Next Hop for In Dialog Messages	<input type="checkbox"/>
Ignore Route Header for Messages Outside Dialog	<input type="checkbox"/>
NAPTR	<input type="checkbox"/>
SRV	<input type="checkbox"/>
Outgoing Transport	<input type="radio"/> TLS <input checked="" type="radio"/> TCP <input type="radio"/> UDP

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

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

- In the **Profile Name** field enter a descriptive name for UPC Business SIPTrunk, in this case a generic name of **SIP_Trunk** was used, and click **Next**
- Enter the UPC Business SIPTrunk IP address and port in the **Next Hop Server 1** field
- Select **UDP** for the **Outgoing Transport**
- Click **Finish**

The screenshot shows the 'Edit Routing Rule' dialog box. The left sidebar shows 'Routing Profiles: SIP_Trunk' with an 'Add' button and a list of profiles including 'default', 'ASM_V9', and 'SIP_Trunk'. The main area is titled 'Edit Routing Rule' and contains a warning: 'Each URI group may only be used once per Routing Profile.' Below this is the 'Next Hop Routing' section with the following fields:

Next Hop Routing	
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	192.168.252.37
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	<input checked="" type="checkbox"/>
Use Next Hop for In Dialog Messages	<input type="checkbox"/>
Ignore Route Header for Messages Outside Dialog	<input type="checkbox"/>
NAPTR	<input type="checkbox"/>
SRV	<input type="checkbox"/>
Outgoing Transport	<input type="radio"/> TLS <input type="radio"/> TCP <input checked="" type="radio"/> UDP

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

7.8. Topology Hiding

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

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

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

Topology Hiding Profiles: ASM_V9

Add Rename Clone Delete

Topology Hiding Profiles

- default
- cisco_th_profile
- ASM_V9**
- UPC_SIP_Trunk

Click here to add a description.

Topology Hiding

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

Edit

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

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

Topology Hiding Profiles: UPC_SIP_Trunk

Buttons: Add, Rename, Clone, Delete

Topology Hiding Profiles list: default, cisco_th_profile, ASM_V9, **UPC_SIP_Trunk**

Click here to add a description.

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

Edit

7.9. Signalling Rules

Signalling rules are a mechanism on the Avaya SBCE to handle any unusual signalling scenarios that may be encountered for a particular Service Provider. In the case of UPC Business SIPTrunk, unnecessary and proprietary headers were removed to simplify the signalling. This is not strictly necessary for effective SIP trunk operation, but removes these headers as a possible cause of signalling issues.

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

- In the **Rule Name** field enter a descriptive name for the UPC Business SIPTrunk signalling rule and click **Next** and **Next** again, then **Finish**
- Click on the **Request Headers** tab and then click on **Add In Header Control**
- Check the **Proprietary Request Header** box
- Enter the name of the proprietary header in the Header Name field, in the example shown it's **P-Location**, and **ALL** in the Method Name field
- Check **Forbidden** in the Header Criteria options
- In the **Presence Action** drop down menu, select **Remove Header**
- Click **Finish**

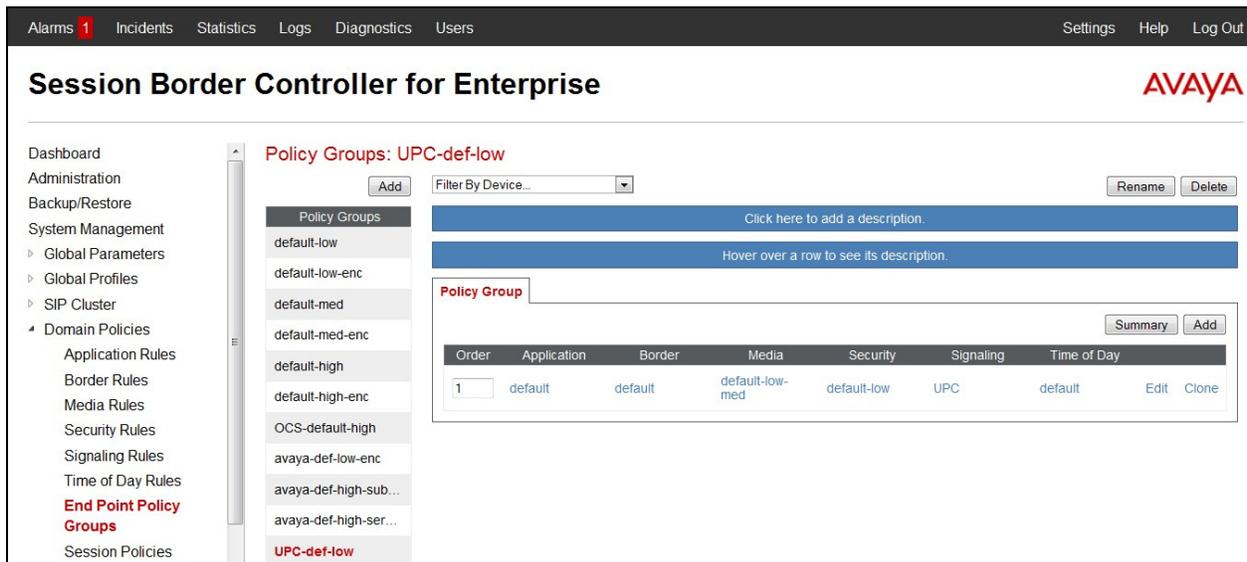
Note: The above is an example of the proprietary headers. During test, the same was done for Alert-Info, AV-Global-Session-ID, P-AV-Message-Id, P-Asserted-Identity, P-Charging-Vector and P-Location.

When finished, all the Request Headers defined will be shown under the Request Headers tab:

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

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

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



7.10. Server Flows

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

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

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for the Session Manager, in this case **Session Manager** 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 **Routing Profile** drop-down menu, select the routing profile of UPC Business SIPTrunk defined in **Section 7.7**.
- Leave the **End Point Policy Group** drop down menu at the default value.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.8** and click **Finish**.

Edit Flow: Session_Manager	
Flow Name	Session_Manager
Server Configuration	ASM_V9
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Med
End Point Policy Group	default-low
Routing Profile	SIP_Trunk
Topology Hiding Profile	ASM_V9
File Transfer Profile	None

Finish

To define a Server Flow for UPC Business SIPTrunk, 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 UPC Business SIPTrunk, in this case a generic name of **Trunk Server** 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 UPC Business SIPTrunk 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 UPC Business SIPTrunk 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 UPC Business SIPTrunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.7**.
- In the **End Point Policy Group** drop down menu, select the End Point Policy Group that contains the Signalling Rules for UPC Business SIPTrunk defined in **Section 7.9**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the UPC Business SIPTrunk defined in **Section 7.8** and click **Finish**.

Edit Flow: SIP_Trunk	
Flow Name	SIP_Trunk
Server Configuration	UPC_SIP_Trunk
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Med
End Point Policy Group	UPC-def-low
Routing Profile	ASM_V9
Topology Hiding Profile	UPC_SIP_Trunk
File Transfer Profile	None

Finish

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

Session Border Controller for Enterprise AVAYA

Alarms 1 Incidents Statistics Logs Diagnostics Users Settings Help Log Out

End Point Flows: GSSCP_R3S3

Devices: GSSCP_R3S3

Subscriber Flows | **Server Flows** Add

Click here to add a row description.

Server Configuration: ASM_V9

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

Server Configuration: UPC_SIP_Trunk

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SIP_Trunk	*	Int_Sig	Ext_Sig	UPC-def-low	ASM_V9	View Clone Edit Delete

8. Configure UPC Business SIPTrunk Equipment

The configuration of the UPC equipment used to support UPC Business SIPTrunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on UPC equipment and system configuration please contact an authorised UPC representative.

9. Verification Steps

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

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

Home / Elements / Session Manager / System Status / SIP Entity Monitoring Help ?

SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: ASBCE_50

Summary View

Status Details for the selected Session Manager:

1 Items Refresh Filter: Enable

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> Session Manager BGVM1	10.10.9.75	5060	TCP	FALSE	UP	200 OK	UP

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

```
status trunk 1

TRUNK GROUP STATUS

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

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.

- Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from the Session Manager via the Avaya SBCE to UPC Business SIPTrunk are receiving a response.

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

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded to 'Troubleshooting' and then 'Trace'. The main content area is titled 'Trace: GSSCP_R3S3' and contains three tabs: 'Call Trace', 'Packet Capture', and 'Captures'. The 'Packet Capture' tab is active, displaying the 'Packet Capture Configuration' form. The form fields are as follows:

Field	Value
Status	Ready
Interface	B1
Local Address (IP:Port)	All
Remote Address (*, *Port, IP, IP:Port)	*
Protocol	UDP
Maximum Number of Packets to Capture	1000
Capture Filename (Using the name of an existing capture will overwrite it.)	SIP_Trunk_Test.pcap

Buttons for 'Start Capture' and 'Clear' are visible at the bottom of the configuration form.

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

The screenshot shows the 'Captures' tab in the 'Trace: GSSCP_R3S3' view. A table lists the captured files:

File Name	File Size (bytes)	Last Modified	
SIP_Trunk_Test_20130905145207.pcap	4,096	September 5, 2013 2:53:40 PM IST	Delete

A 'Refresh' button is located in the top right corner of the table area.

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to UPC Business SIPTrunk. UPC Business SIPTrunk is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

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

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

©2013 Avaya Inc. All Rights Reserved.

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

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