



## Application Notes for Configuring Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0 to support Alestra SIP Trunking on the Sonus Platform – Issue 1.0

### Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0, to interoperate with the Alestra SIP Trunk Service on the Sonus platform.

The SIP trunking service offered by Alestra provides customers with PSTN access via a SIP trunk between the enterprise and the service provider's network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results .....	6
2.3.	Support .....	7
3.	Reference Configuration .....	8
4.	Equipment and Software Validated .....	11
5.	Configure Avaya Aura® Communication Manager .....	12
5.1.	Licensing and Capacity .....	12
5.2.	System Features.....	13
5.3.	IP Node Names.....	14
5.4.	Codecs .....	14
5.5.	IP Network Regions .....	15
5.6.	Signaling Group .....	16
5.7.	Trunk Group.....	18
5.8.	Calling Party Information.....	20
5.9.	Inbound Routing.....	21
5.10.	Outbound Routing .....	22
6.	Configure Avaya Aura® Session Manager .....	24
6.1.	System Manager Login and Navigation.....	25
6.2.	SIP Domain .....	26
6.3.	Locations .....	26
6.4.	Adaptations.....	29
6.5.	SIP Entities .....	30
6.6.	Entity Links .....	34
6.7.	Routing Policies .....	35
6.8.	Dial Patterns .....	36
7.	Configure Avaya Session Border Controller for Enterprise .....	39
7.1.	System Access.....	39
7.2.	System Management .....	40
7.3.	Network Management .....	41
7.4.	Media Interfaces .....	42
7.5.	Signaling Interfaces.....	43
7.6.	Server Interworking.....	45
7.6.1.	Server Interworking Profile – Enterprise.....	45
7.6.2.	Server Interworking Profile – Service Provider.....	48
7.7.	Signaling Manipulation .....	50
7.8.	Server Configuration .....	51
7.8.1.	Server Configuration Profile – Enterprise .....	51
7.8.2.	Server Configuration Profile – Service Provider .....	52
7.9.	Routing .....	54
7.9.1.	Routing Profile – Enterprise .....	54

7.9.2.	Routing Profile – Service Provider .....	55
7.10.	Topology Hiding.....	56
7.10.1.	Topology Hiding Profile – Enterprise .....	56
7.10.2.	Topology Hiding Profile – Service Provider.....	57
7.11.	End Point Policy Groups .....	58
7.11.1.	End Point Policy Group – Enterprise .....	58
7.11.2.	End Point Policy Group – Service Provider.....	59
7.12.	End Point Flows.....	60
7.12.1.	End Point Flow – Enterprise .....	60
7.12.2.	End Point Flow – Service Provider .....	61
8.	Alestra SIP Trunking Configuration .....	62
9.	Verification and Troubleshooting .....	62
9.1.	General Verification Steps .....	62
9.2.	Communication Manager Verification.....	62
9.3.	Session Manager Verification .....	63
9.4.	Avaya SBCE Verification .....	64
10.	Conclusion .....	67
11.	References.....	67
12.	Appendix A: SigMa Script.....	68

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Alestra SIP Trunking, operating on the Sonus platform, and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.0 and various Avaya endpoints, as listed in **Section 4**.

The SIP trunking service provided Alestra and referenced within these Application Notes is designed for business customers in Mexico. Customers using this service with this Avaya enterprise solution are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

## 2. General Test Approach and Test Results

A simulated enterprise site containing all the equipment for the Avaya SIP-enabled solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to Alestra SIP Trunking via a broadband connection to the public Internet.

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

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk via the service provider network.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones using “This Computer” and “Other Phone” modes. (H.323, SIP).
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows softphones (SIP).
- Inbound and outbound PSTN calls to/from SIP remote workers using Avaya 96x1 deskphones, and the Avaya one-X® Communicator and Avaya Communicator for Windows softphones.
- Various call types including: local, long distance national, long distance international and outbound toll free.
- Codecs G.729A, G.711A and G.711MU.
- Inbound and outbound PSTN calls using VoIP media resources in Avaya Media Gateways and the Avaya Aura® Media Server at the enterprise network.
- DTMF tones passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail redirection and navigation.
- User features such as hold and resume, transfer and conference.
- Off-net call transferring, call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Fax support.

Items not supported or not tested included the following:

- Network Call Redirection using the REFER or 302 Temporarily Unavailable methods are not supported by Alestra and they were not tested.
- Operator services such as dialing 0, 0 + 10 digits and Local Directory assistance are not supported by Alestra.
- Inbound toll-free and emergency calls are supported but were not tested as part of the compliance test.

## 2.2. Test Results

Interoperability testing of the Alestra SIP Trunking service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations and limitations noted below:

- **Caller ID on incoming calls from the U.S.:** Calls originating from PSTN telephones in the U.S. to the DID numbers in Mexico assigned to the SIP trunk to the enterprise displayed *Restricted/Unavailable* on the enterprise extensions. This seems to be a PSTN restriction for all calls from the U.S. to Mexico, not limited just to Alestra. Inbound calls originating from local PSTN test numbers in Monterrey, Mexico showed the correct calling party caller ID.
- **“To” header on incoming calls:** Incoming calls from Alestra to the enterprise contained in the “Request-URI” header the last 4 digits of the DID number called, while the “To” header contained 18 digit strings, which included the complete 10 digit DID number preceded by a constant 8 digit prefix. This issue had no noticeable effect to the end user.
- **SDP Attributes on Incoming Calls:** On incoming calls from numbers on the PSTN in Mexico, Alestra normally sent in the SDP of the incoming INVITE codecs G.711A, G.711U and G.729A, in this order of preference, and DTMF with Payload Type 100. But on test calls made from the U.S., Alestra sent on the SDP of the incoming INVITE codec G.711A only, and DTMF “Inband”. This issue was sent to Alestra for investigation. Even though inband DTMF was still recognized and operational on the calls made from the U.S., shuffling (media redirection) was impacted by the mismatch between the offered codec and the codec list set in Communication Manager. Shuffling did not take place on incoming calls from the U.S. when using SIP endpoints at the enterprise
- **Caller ID on outbound calls:** On calls originating from enterprise extensions to PSTN telephones, the caller ID number shown on the PSTN endpoint was always the BDN or main DID number assigned by Alestra to the SIP trunk, not the specific DID assigned to that extension. This includes incoming calls that are forwarded or transferred back on the SIP trunk to the PSTN, and also EC500 (extension to cellular) calls. This is the expected behavior on the Alestra service for outbound calls on the SIP trunk; it is listed here simply as an observation.
- **Outbound Calling Party Number (CPN) Block:** When an enterprise user activated “CPN Block” on an outbound call with the purpose of privacy, Communication Manager sent “anonymous” in the “From” header and included the “Privacy:id” header, but on the receiving end at the PSTN the display still showed the BDN number assigned by Alestra to the SIP trunk.
- **Fax Support:** T.38 fax is not supported on the Alestra network. G.711 fax pass-through was successfully tested during the compliance test. Due to the unpredictability of pass-through techniques, which only work well on networks with very few hops and with limited end-to-end delay, G.711 fax pass-through is delivered in Communication Manager on a “best effort” basis; its success is not guaranteed, and it should be used at the customer’s discretion.

- **Conference in Avaya Communicator softclients:** The Communication Manager Conference feature is not supported in the Avaya Communicator current software release 2.1.2.75. An Avaya Aura® Conferencing server is required for ad-hoc conferences. This feature should be available in the upcoming release 3.0 of Avaya Communicator.
- **SIP header optimization:** There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider's network. These headers were removed with the purposes of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider's network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector and P-Location (**Section 6.4**). Additionally, the parameters "gsid" and "epv" were removed from outbound Contact headers using a Signaling Script in the Avaya SBCE (**Section 7.7**).

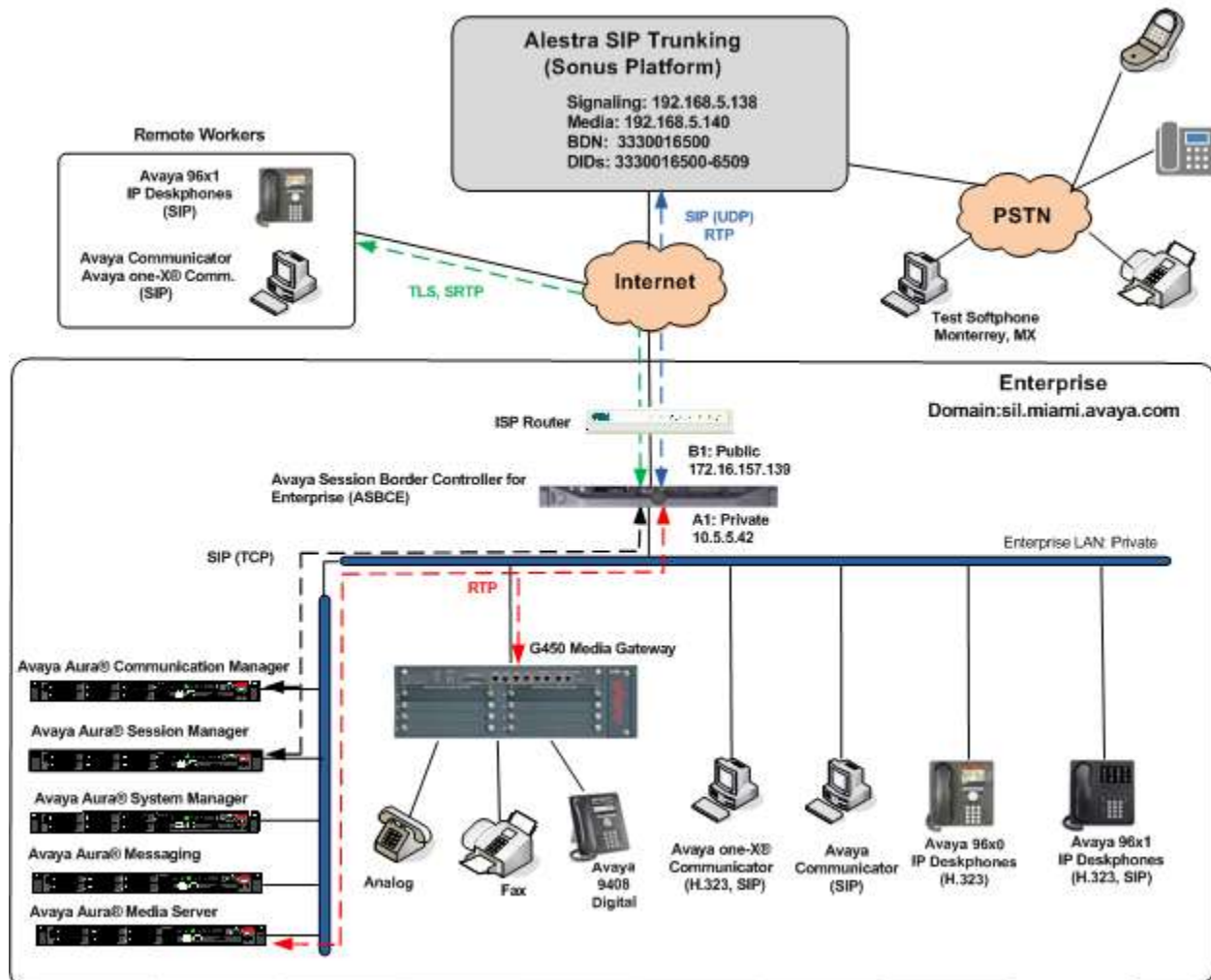
## 2.3. Support

For technical support on the Alestra SIP Trunk service offer, visit <http://www.alestra.com.mx/>

### 3. Reference Configuration

**Figure 1** illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Alestra SIP Trunking service through a public Internet WAN connection.

For security purposes, references to any public IP addresses used during the compliance test have been replaced in these Application Notes with private addresses. Also, PSTN routable phone numbers used in the test have been changed to non-routable numbers.



**Figure 1: Avaya SIP Enterprise Solution connected to Alestra SIP Trunking.**



The components used to create the simulated enterprise customer site included:

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya Aura® Messaging.
- Avaya Aura® Media Server.
- Avaya G450 Media Gateway.
- Avaya 96x0 and 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Communicator for Windows softphones.
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to the Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test, using the following endpoints and protocols:

- Avaya 96x1 SIP Deskphones (using TLS and SRTP).
- Avaya Communicator for Windows (using TLS and SRTP).
- Avaya one-X® Communicator SIP (using TCP and RTP).

For security reasons, TLS and SRTP are the recommended protocols to be used by all remote workers endpoints. During the tests, TCP and RTP were used with Avaya one-X® Communicator for tracing and troubleshooting purposes.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult [5] in the **References** section for additional information on this topic.

The Avaya SBCE was located at the edge of the enterprise. Its public side was connected to the external network, while its private side was connected to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flowed through the Avaya SBCE, protecting in this way the enterprise against any SIP-based attacks. The Avaya SBCE also performed network address translation at both the IP and SIP layers.

The transport protocol between the Avaya SBCE and Alestra across the public IP network was UDP. The transport protocol between the Avaya SBCE and the enterprise Session Manager across the enterprise IP network was TCP.

For inbound calls, the calls flowed from the service provider to the Avaya SBCE, then to Session Manager. Session Manager used the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case the Communication Manager) and on which link to send the call. Once the call arrived at Communication Manager, further incoming call treatment, such as incoming digit translation was performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the Alestra network.

A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk without affecting other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

As part of the Avaya Aura® version 7.0 release, Communication Manager incorporates the ability to use the Avaya Aura® Media Server (AAMS) as a media resource. The AAMS is a software-based, high density media server that provides DSP resources for IP-based sessions. Media resources from both the AAMS and a G450 Media Gateway were utilized during the compliance test. The configuration of the AAMS is not discussed in this document. For more information on the installation and administration of the AAMS in Communication Manager refer to [6] and [7] in the **References** section.

Avaya Aura® Messaging was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of Message Waiting Indicator (MWI) messages to the enterprise telephones. Since the configuration tasks for Messaging are not directly related to the interoperability tests with the service provider, they are not included in these Application Notes.

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya Aura® Communication Manager	7.0 Service Pack 1 (R017x.00.0.441.0 patch 22477)
Avaya Aura® Session Manager	7.0 (7.0.0.0.700007)
Avaya Aura® System Manager	7.0.0.0 (Update Revision 7.0.0.0.3929)
Avaya Session Border Controller for Enterprise	7.0.0-21-6602
Avaya Aura® Messaging	6.3.3
Avaya Aura® Media Server	7.7.0.226
Avaya G450 Media Gateway	37.19.0
Avaya 96x0 Series IP Deskphones (H.323)	Avaya one-X® Deskphone Edition S3.250A
Avaya 96x1 Series IP Deskphones (SIP)	Avaya one-X Deskphone Edition SIP 7.0.0.39
Avaya 96x1 Series IP Deskphones (H.323)	Avaya one-X® Deskphone Edition H.323 6.6
Avaya one-X® Communicator (H.323, SIP)	6.2.6.03-FP6
Avaya Communicator for Windows	2.1.2.75
Avaya 9408 Digital Telephone	Rel 12.0
Avaya 6210 Analog Telephone	N/A
<b>Alestra</b>	
Sonus Softswitch	V08.04.09R000
Acme Packet SBC	V6.2
Lucent 5ESS	V16.1

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Servers and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

**Note** - The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the table above were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 5.5) platforms. Consult the installation documentation on the **References** section for more information.

## 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to work with Alestra SIP Trunking. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager, the Avaya G450 Media Gateway and the Avaya Aura® Media Server has been previously completed and is not discussed here.

The 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.

### 5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **381** are in use. 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.

```
display system-parameters customer-options                               Page 2 of 12
                                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 2
      Maximum Video Capable IP Softphones: 18000 9
      Maximum Administered SIP Trunks: 24000 381
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
      Maximum Number of DS1 Boards with Echo Cancellation: 522 0

(NOTE: You must logoff & login to effect the permission changes.)
```

## 5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to ***all*** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons incoming calls should not be allowed to transfer back to the PSTN, then leave the field set to ***none***.

```
change system-parameters features                               Page 1 of 19
FEATURE-RELATED SYSTEM PARAMETERS
  Self Station Display Enabled? n
    Trunk-to-Trunk Transfer: all
  Automatic Callback with Called Party Queuing? y
  Automatic Callback - No Answer Timeout Interval (rings): 3
    Call Park Timeout Interval (minutes): 10
  Off-Premises Tone Detect Timeout Interval (seconds): 20
    AAR/ARS Dial Tone Required? y

  Music (or Silence) on Transferred Trunk Calls? no
  DID/Tie/ISDN/SIP Intercept Treatment: attendant
  Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
    Automatic Circuit Assurance (ACA) Enabled? n

  Abbreviated Dial Programming by Assigned Lists? n
  Auto Abbreviated/Delayed Transition Interval (rings): 2
    Protocol for Caller ID Analog Terminals: Bellcore
  Display Calling Number for Room to Room Caller ID Calls? n
```

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields under **CPN/ANI/ICLID PARAMETERS** on the screen below. The compliance test used the value of ***restricted*** for restricted calls and ***unavailable*** for unavailable calls.

```
change system-parameters features                               Page 9 of 19
FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable

DISPLAY TEXT
  Identity When Bridging: principal
  User Guidance Display? n
  Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
  Local Country Code:       
  International Access Code:       
```

### 5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (*procr*) and the Session Manager security module (*asm*). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

change node-names ip		Page	1 of	2
IP NODE NAMES				
Name	IP Address			
asm	10.10.5.32			
default	0.0.0.0			
media_server	192.168.10.46			
procr	10.10.5.12			
procr6	::			
tftp	192.168.10.150			

### 5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. Alestra used codecs G.711A, G711MU and G.729A on the SIP trunk, in this order of preference. Enter the corresponding codecs in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

On **Page 2**, since T.38 fax is not supported, set the **Fax Mode** to *off*.

change ip-codec-set 2		Page	2 of	2
IP CODEC SET				
Allow Direct-IP Multimedia? n				
	Mode	Redundancy	Packet Size(ms)	
FAX	off	0		
Modem	off	0		
TDD/TTY	off	3		
H.323 Clear-channel	n	0		
SIP 64K Data	n	0	20	

## 5.5. IP Network Regions

Create a separate IP network region for the service provider trunk group. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP Network Region 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is *sil.miami.avaya.com* as assigned to the shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to **yes**, the default setting. This will enable **IP-IP Direct Audio** (shuffling), to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Shuffling can be further restricted at the trunk level on the Signaling Group form if needed.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values may be used for all other fields.

change ip-network-region 2		Page 1 of 20
IP NETWORK REGION		
Region: 2		
Location: <u>1</u>	Authoritative Domain: <u>sil.miami.avaya.com</u>	
Name: <u>Service Provider</u>	Stub Network Region: <u>n</u>	
MEDIA PARAMETERS		
Codec Set: <u>2</u>	Intra-region IP-IP Direct Audio: <u>yes</u>	
UDP Port Min: <u>2048</u>	Inter-region IP-IP Direct Audio: <u>yes</u>	
UDP Port Max: <u>3329</u>	IP Audio Hairpinning? <u>n</u>	
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: <u>46</u>		
Audio PHB Value: <u>46</u>		
Video PHB Value: <u>26</u>		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: <u>6</u>		
Audio 802.1p Priority: <u>6</u>		
Video 802.1p Priority: <u>5</u>		
AUDIO RESOURCE RESERVATION PARAMETERS		
RSVP Enabled? <u>n</u>		
H.323 IP ENDPOINTS		
H.323 Link Bounce Recovery? <u>y</u>		
Idle Traffic Interval (sec): <u>20</u>		
Keep-Alive Interval (sec): <u>5</u>		
Keep-Alive Count: <u>5</u>		

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The following example shows the settings used for the compliance test. It indicates that codec set **2** will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

change ip-network-region 2										Page	4 of	20
Source Region: 2		Inter Network Region Connection Management								I		M
dst rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Intervening Prio Shr	Regions	Dyn CAC	A	G			
1	2	y	NoLimit				n					t
2	2										all	
3												

## 5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used and was configured using the parameters highlighted below, shown on the screen on the next page:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, *tls* was used.
- Set the **Peer Detection Enabled** field to *y*. The **Peer-Server** field will initially be set to *Others* and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to *SM* once Communication Manager detects its peer is a Session Manager.

**Note:** Once the **Peer-Server** field is updated to *SM*, the system changes the default values of the following fields, setting them to display-only:

- **Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to *y*.
- **Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to *n*.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *asm*. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.



add signaling-group 2		Page 1 of 2
<b>SIGNALING GROUP</b>		
Group Number: 2	Group Type: <u>sip</u>	
IMS Enabled? <u>n</u>	Transport Method: <u>tls</u>	
Q-SIP? <u>n</u>		
IP Video? <u>n</u>	Enforce SIPS URI for SRTP? <u>y</u>	
Peer Detection Enabled? <u>y</u>	Peer Server: Others	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? <u>n</u>		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? <u>y</u>		
Alert Incoming SIP Crisis Calls? <u>n</u>		
Near-end Node Name: <u>procr</u>	Far-end Node Name: <u>asm</u>	
Near-end Listen Port: <u>5063</u>	Far-end Listen Port: <u>5063</u>	
	Far-end Network Region: <u>2</u>	
Far-end Domain: <u>sil.miami.avaya.com</u>		
Incoming Dialog Loopbacks: <u>eliminate</u>	Bypass If IP Threshold Exceeded? <u>n</u>	
DTMF over IP: <u>rtp-payload</u>	RFC 3389 Comfort Noise? <u>n</u>	
Session Establishment Timer(min): <u>3</u>	Direct IP-IP Audio Connections? <u>y</u>	
Enable Layer 3 Test? <u>y</u>	IP Audio Hairpinning? <u>n</u>	
H.323 Station Outgoing Direct Media? <u>n</u>	Initial IP-IP Direct Media? <u>n</u>	
	Alternate Route Timer(sec): <u>6</u>	

- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so the SM can distinguish this trunk from the trunk used for other enterprise SIP traffic. For the compliance test both the **Near-end Listen Port** and **Far-end Listen Port** were set to **5063**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway or the AAMS will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and AAMS, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields.

## 5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 2 was configured using the parameters highlighted below.

- Set the **Group Type** field to *sip*.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to *public-ntwrk*.
- Set the **Signaling Group** to the signaling group shown in the previous section.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 2                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 2                      Group Type: sip      CDR Reports: y
  Group Name: SIP trunk to SP          COR: 1             TN: 1       TAC: 602
  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: 2
                                     Number of Members: 6
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. The default value of **600** seconds was used.

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

On **Page 3**, set the **Numbering Format** field to *private*. This field specifies the format of the calling party number (CPN) sent to the far-end. When *public* format is used, Communication Manager automatically inserts a “+” sign, preceding the numbers in the “From”, “Contact” and “P-Asserted Identity” (PAI) headers. The addition of the “+” sign impacted interoperability with Alestra. Thus, the **Numbering Format** was set to *private* and the **Numbering Format** in the route pattern was set to *unk-unk* (see **Section 5.10**). Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to *y*. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call has enabled CPN block.

add trunk-group 2		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? <u>n</u>	Measured: <u>none</u>	Maintenance Tests? <u>y</u>
Numbering Format: <u>private</u>		
UI Treatment: <u>service-provider</u>		
Replace Restricted Numbers? <u>y</u>		
Replace Unavailable Numbers? <u>y</u>		

On **Page 4**, leave the **Network Call Redirection** and the **Send Diversion Header** fields set to the default value *n*. Alestra does not support the use of the SIP REFER method or the Diversion header for calls that are transferred or forwarded back to the PSTN. Set the **Support Request History** field to *n*. Set the **Telephone Event Payload Type** to **100**, and **Convert 180 to 183 for Early Media** to *y*, the values preferred by Alestra. Default values were used for all other fields.

add trunk-group 2		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? <u>n</u>		
Prepend '+' to Calling/Alerting/Diverting/Connected Number? <u>n</u>		
Send Transferring Party Information? <u>n</u>		
Network Call Redirection? <u>n</u>		
Send Diversion Header? <u>n</u>		
Support Request History? <u>n</u>		
Telephone Event Payload Type: <u>100</u>		
Convert 180 to 183 for Early Media? <u>y</u>		
Always Use re-INVITE for Display Updates? <u>n</u>		
Identity for Calling Party Display: <u>P-Asserted-Identity</u>		
Block Sending Calling Party Location in INVITE? <u>n</u>		
Accept Redirect to Blank User Destination? <u>n</u>		
Enable Q-SIP? <u>n</u>		
Interworking of ISDN Clearing with In-Band Tones: <u>keep-channel-active</u>		
Request URI Contents: <u>may-have-extra-digits</u>		

## 5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, six DID numbers are assigned by the service provider for testing. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions.

change private-numbering 1					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	3001	2	3330016501	10	Total Administered: 10 Maximum Entries: 540
4	3002	2	3330016502	10	
4	3003	2	3330016503	10	
4	3004	2	3330016504	10	
5	3005	2	3330016505	10	
4	3006	2	3330016506	10	

**Note:** During the compliance test, Alestra inserted the BDN or main DID number assigned to the SIP trunk on all outbound calls sent to the PSTN, for caller ID purposes. Since the calling party information sent from the enterprise was not used for caller ID or authentication purposes by Alestra, the configuration shown on the screen above was not strictly required, and it is shown here simply for completeness.

## 5.9. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Alestra is left unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. During the compliance test, Alestra sent to the enterprise the last 4 digits of the DID number. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

change inc-call-handling-trmt trunk-group 2					Page	1 of 30
INCOMING CALL HANDLING TREATMENT						
Service/ Feature	Number Len	Number Digits	Del	Insert		
public-ntwrk	4	6501	4	3001		
public-ntwrk	4	6502	4	3002		
public-ntwrk	4	6503	4	3003		
public-ntwrk	4	6504	4	3004		
public-ntwrk	4	6505	4	3005		
public-ntwrk	4	6506	4	3006		
public-ntwrk	—	—	—	—		

## 5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with **9** of length **1**, as a feature access code (*fac*).

change dialplan analysis								
DIAL PLAN ANALYSIS TABLE								
Location: all								
Percent Full: 2								
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	3	fac						
1	4	ext						
2	4	ext						
3	4	ext						
4	4	ext						
5	4	ext						
6	3	dac						
7	4	ext						
8	1	fac						
9	1	fac						
*	3	dac						
#	2	dac						

Use the **change feature-access-codes** command to configure **9** as the **Auto Route Selection (ARS) – Access Code 1**.

change feature-access-codes								
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: <u>099</u>								
Answer Back Access Code: <u>015</u>								
Attendant Access Code: _____								
Auto Alternate Routing (AAR) Access Code: <u>8</u>								
Auto Route Selection (ARS) - Access Code 1: <u>9</u>			Access Code 2: _____					
Automatic Callback Activation: <u>016</u>			Deactivation: <u>017</u>					
Call Forwarding Activation Busy/DA: <u>018</u>			All: <u>019</u>			Deactivation: <u>020</u>		
Call Forwarding Enhanced Status: _____			Act: _____			Deactivation: _____		

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2 which contains the SIP trunk group to the service provider.

change ars analysis 0							Page	1 of	2
ARS DIGIT ANALYSIS TABLE									
Location: all							Percent Full: 1		
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd			
00	12	22	2	intl		n			
001	13	13	2	intl		n			
01	12	12	2	natl		n			
3	8	8	2	locl		n			

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 2 in the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format:** Set to **unk-unk**. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

change route-pattern 2											Page	1 of	3
Pattern Number: 2											Pattern Name: To Serv Prov		
SCCAN? n		Secure SIP? n		Used for SIP stations? n									
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Dgts				DCS/ QSIG Intw	IXC	
1:	2	0									n	user	
2:											n	user	
3:											n	user	
4:											n	user	
5:											n	user	
6:											n	user	
BCC		VALUE		TSC	CA-TSC	ITC		BCIE	Service/Feature	PARM	Sub	Numbering	LAR
0 1 2 M 4 W					Request						Dgts	Format	
1:		y	y	y	y	y	n	n	rest			unk-unk	none
2:		y	y	y	y	y	n	n	rest				none

Enter the **save translation** command (not shown) to save all the changes made to the Communication Manager configuration.

## 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- Adaptation module to perform header manipulations.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.

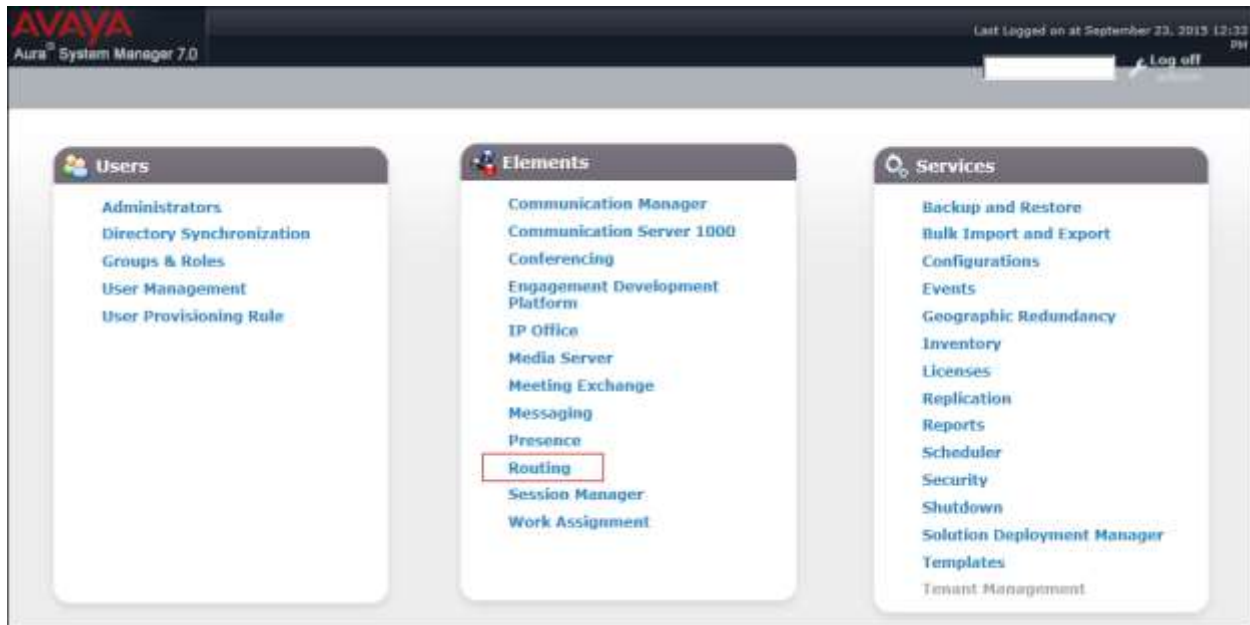
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.



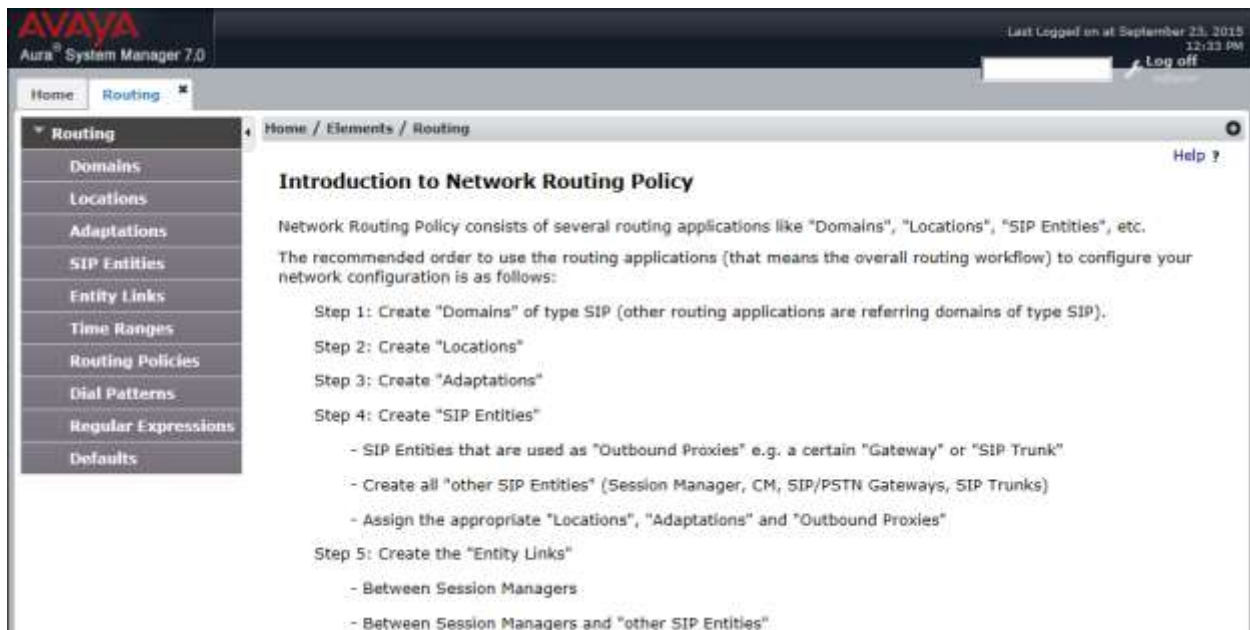
## 6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown).

The screen shown below is then displayed; click on **Routing**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in this section will be located under the **Routing** link shown below.

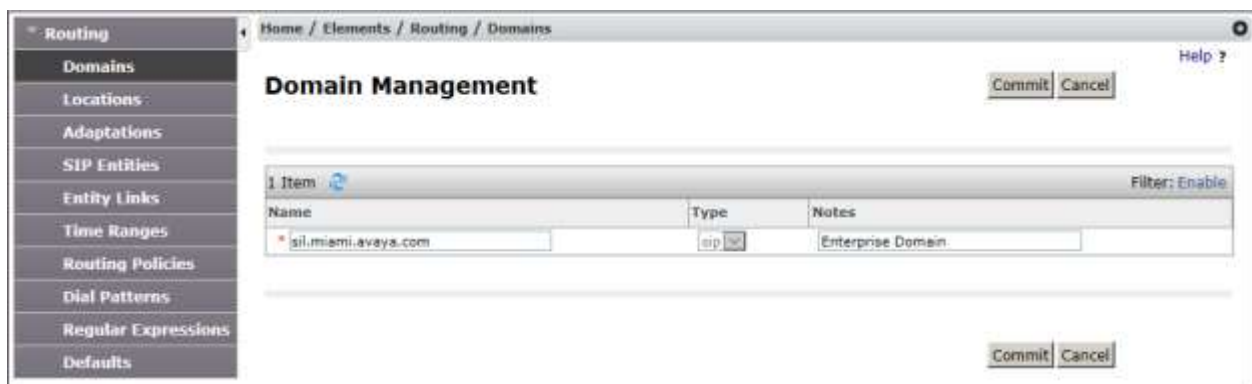


## 6.2. SIP Domain

Create an entry for each SIP domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this was the enterprise domain, *sil.miami.avaya.com*. Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the enterprise domain.



The screenshot shows the 'Domain Management' interface. On the left is a navigation pane with 'Routing' selected, and 'Domains' is highlighted. The main area has a breadcrumb 'Home / Elements / Routing / Domains' and a title 'Domain Management'. There are 'Commit' and 'Cancel' buttons at the top right. Below the title is a table with one item. The table has columns for Name, Type, and Notes. The entry is 'sil.miami.avaya.com', 'sip', and 'Enterprise Domain'. There are also 'Commit' and 'Cancel' buttons at the bottom right.

Name	Type	Notes
sil.miami.avaya.com	sip	Enterprise Domain

## 6.3. Locations

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

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

Defaults can be used for all other parameters.

The following screen shows the location details for the location named *Session Manager*. Later, this location will be assigned to the SIP Entity corresponding to Session Manager. Default values were used for all parameters.

The screenshot displays the 'Location Details' configuration page for a location named 'Session Manager'. The page is organized into several sections with expandable/collapsible headers. At the top, there is a breadcrumb trail 'Home / Elements / Routing / Locations' and a 'Help ?' link. The 'Location Details' section includes 'Commit' and 'Cancel' buttons. The 'General' section contains a required 'Name' field with the value 'Session Manager' and an empty 'Notes' field. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' dropdown menu. The 'Overall Managed Bandwidth' section includes 'Managed Bandwidth Units' (set to 'Kbit/sec'), 'Total Bandwidth' and 'Multimedia Bandwidth' fields, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section lists 'Maximum Multimedia Bandwidth (Intra-Location)' and '(Inter-Location)' both at 2000 Kbit/Sec, 'Minimum Multimedia Bandwidth' at 64 Kbit/Sec, and 'Default Audio Bandwidth' at 80 Kbit/sec. The 'Alarm Threshold' section shows 'Overall Alarm Threshold' and 'Multimedia Alarm Threshold' both at 80 %, and 'Latency before Overall Alarm Trigger' and 'Latency before Multimedia Alarm Trigger' both at 5 Minutes. The 'Location Pattern' section at the bottom has 'Add' and 'Remove' buttons, a table with 0 items, a 'Filter: Enable' button, and a table header with 'IP Address Pattern' and 'Notes'. 'Commit' and 'Cancel' buttons are also present at the bottom right.

The following screen shows the location details for the location named **Communication Manager**. Later, this location will be assigned to the SIP Entity corresponding to Communication Manager. Other location parameters (not shown) retained the default values.

The screenshot shows a web interface with a breadcrumb trail 'Home / Elements / Routing / Locations' at the top. Below this is a section titled 'Location Details' with 'Commit' and 'Cancel' buttons on the right. Under the 'General' tab, there is a required field '\* Name:' containing the text 'Communication Manager' and an empty 'Notes:' field below it.

The following screen shows the location details for the location named **Avaya SBCE**. Later, this location will be assigned to the SIP Entity corresponding to the Avaya SBCE. Other location parameters (not shown) retained the default values.

The screenshot shows a web interface with a breadcrumb trail 'Home / Elements / Routing / Locations' at the top. Below this is a section titled 'Location Details' with 'Commit' and 'Cancel' buttons on the right. Under the 'General' tab, there is a required field '\* Name:' containing the text 'Avaya SBCE' and an empty 'Notes:' field below it.

## 6.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 7.0 incorporates the ability to use Adaptation modules to remove specific headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements.

For the compliance test, an Adaptation named “Outbound\_Header\_Removal” was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

Navigate to **Routing → Adaptations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Adaptation Name:** Enter an appropriate name.
- **Module Name:** Select the *DigitConversionAdapter* option.
- **Module Parameter Type:** Select *Name-Value Parameter*.

Click **Add** to add the name and value parameters.

- **Name:** Enter *eRHdrs*. This parameter will remove the specified headers from messages in the egress direction.
- **Value:** Enter “*Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View*”

The screen below shows the adaptation created for the compliance test. This adaptation will later be applied to the SIP Entity corresponding to the Avaya SBCE. All other fields were left with their default values.

Home / Elements / Routing / Adaptations

**Adaptation Details** Commit Cancel

**General**

\* Adaptation Name: Outbound\_Header\_Removal

\* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Add Remove

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	eRHdrs	*Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-

Select : All, None

Egress URI Parameters:

Notes:

## 6.5. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**  
If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created and defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of the Session Manager SIP Entity. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.

Home / Elements / Routing / SIP Entities

### SIP Entity Details

Commit Cancel

#### General

\* Name: Session Manager

\* FQDN or IP Address: 10.10.5.32

Type: Session Manager

Notes: Security Module

Location: Session Manager

Outbound Proxy:

Time Zone: America/New\_York

Credential name:

#### SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the “**procr**” interface in Communication Manager, as seen in **Section 5.3**.

Home / Elements / Routing / SIP Entities

## SIP Entity Details

CommitCancel

### General

\* Name:CM Trunk 2

\* FQDN or IP Address:10.10.5.12

Type:CM

Notes:For Service Provider calls

Adaptation:

Location:Communication Manager

Time Zone:America/New\_York

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

Credential name:

Securable:

Call Detail Recording:none

### Loop Detection

Loop Detection Mode:Off

### SIP Link Monitoring

SIP Link Monitoring:Use Session Manager Configuration



The following screen shows the addition of the Avaya SBCE Entity. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**). On the **Adaptation** field, the adaptation module *Outbound\_Header\_Removal* previously defined in **Section 6.4** is selected.

Home / Elements / Routing / SIP Entities

**SIP Entity Details** Commit Cancel

**General**

\*

Name:

Avaya SBCE

\*

FQDN or IP Address:

10.10.5.42

Type:

SIP Trunk

▼

Notes:

Avaya SBCE

Adaptation:

Outbound\_Header\_Removal

▼

Location:

Avaya SBCE

▼

Time Zone:

America/New\_York

▼

\*

SIP Timer B/F (in seconds):

4

Credential name:

Securable:

☐

Call Detail Recording:

egress

▼

**Loop Detection**

Loop Detection Mode:

Off

▼

**SIP Link Monitoring**

SIP Link Monitoring:

Use Session Manager Configuration

▼

## 6.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.

Click **Commit** to save.

The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.

The screenshot shows the 'Entity Links' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Entity Links'. Below this, the title 'Entity Links' is displayed next to 'Commit' and 'Cancel' buttons. A table with 10 columns is shown: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, and Deny New Service. The first row contains the following values: Name: '\* SM-CM Trunk 2', SIP Entity 1: '\* Session Manager', Protocol: 'TLS', Port: '\* 5063', SIP Entity 2: '\* CM Trunk 2', DNS Override: (empty), Port: '\* 5063', Connection Policy: 'trusted', and Deny New Service: (empty). Below the table, there is a 'Select' dropdown menu with 'All, None' options.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service
* SM-CM Trunk 2	* Session Manager	TLS	* 5063	* CM Trunk 2		* 5063	trusted	

The Entity Link to the Avaya SBCE is show below. **TCP** and port **5060** were used.

The screenshot shows the 'Entity Links' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Entity Links'. Below this, the title 'Entity Links' is displayed next to 'Commit' and 'Cancel' buttons. A table with 10 columns is shown: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, and Deny New Service. The first row contains the following values: Name: '\* SM-ASBCE', SIP Entity 1: '\* Session Manager', Protocol: 'TCP', Port: '\* 5060', SIP Entity 2: '\* Avaya SBCE', DNS Override: (empty), Port: '\* 5060', Connection Policy: 'trusted', and Deny New Service: (empty). Below the table, there is a 'Select' dropdown menu with 'All, None' options.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service
* SM-ASBCE	* Session Manager	TCP	* 5060	* Avaya SBCE		* 5060	trusted	

## 6.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies were added: an incoming policy with Communication Manager as the destination, and an outbound policy to the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screens show the Routing Policies for Communication Manager and the Avaya SBCE.

The screenshot shows the 'Routing Policy Details' page for a policy named 'To CM Trunk 2'. The 'General' section includes fields for Name, Disabled (checkbox), Retries (0), and Notes ('Incoming Calls'). The 'SIP Entity as Destination' section shows a table with one entry: 'CM Trunk 2' with FQDN or IP Address '10.10.5.12', Type 'CM', and Notes 'For Service Provider calls'.

Name	FQDN or IP Address	Type	Notes
CM Trunk 2	10.10.5.12	CM	For Service Provider calls

The screenshot shows the 'Routing Policy Details' page for a policy named 'To ASBCE'. The 'General' section includes fields for Name, Disabled (checkbox), Retries (0), and Notes ('Outbound Calls'). The 'SIP Entity as Destination' section shows a table with one entry: 'Avaya SBCE' with FQDN or IP Address '10.10.5.42', Type 'SIP Trunk', and Notes 'Avaya SBCE'.

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.10.5.42	SIP Trunk	Avaya SBCE

## 6.8. Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to the service provider and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

In the **General** section, enter the following values:

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria, or select “**ALL**” to route incoming calls to all SIP domains.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. On incoming calls, Alestra sent to the enterprise the last 4 digits of the DID number. The example below shows that a 4 digit number starting with **65**, which is the DID range assigned by Alestra, arriving from location **Avaya SBCE**, used route policy **To CM Trunk 2** to Communication Manager.

**Dial Pattern Details** [Commit] [Cancel] [Help ?]

**General**

\* Pattern: 65

\* Min: 4

\* Max: 4

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: sil.miami.avaya.com

Notes: Alestra Inbound

**Originating Locations and Routing Policies**

[Add] [Remove]

1 Item [Filter: Enable]

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Avaya SBCE		To CM Trunk 2	0	<input type="checkbox"/>	CM Trunk 2	Incoming Calls

Repeat this procedure as needed to define additional dial patterns for other range of numbers assigned by the service provider to the enterprise, to be routed to Communication Manager.

The following screen illustrates an example dial pattern used to verify outbound calls from the Enterprise to the PSTN during the compliance test. The example in this screen shows that 12 digit dialed numbers, beginning with the digits **01**, used for Long Distance National calls, arriving from the **Communication Manager** location, will use route policy **To ASBCE**, which sends the call out to the PSTN via Avaya SBCE and the Alestra SIP Trunk.

Home / Elements / Routing / Dial Patterns Help ?

### Dial Pattern Details

Commit Cancel

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Communication Manager		To ASBCE	0	<input type="checkbox"/>	Avaya SBCE	Outbound Calls

Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the service provider's network via the Avaya SBCE.

## 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

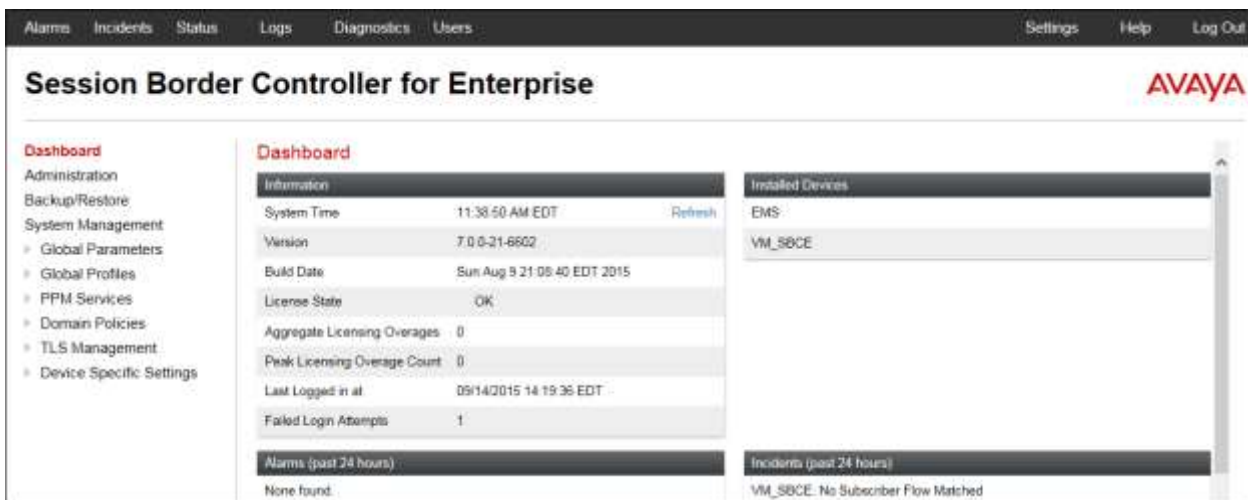
### 7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



The login page features the Avaya logo on the left. To the right, under the heading "Log In", are input fields for "Username:" and "Password:", followed by a "Log In" button. Below the login fields, there is a block of legal disclaimer text regarding unauthorized access and system monitoring. At the bottom left of the page, it says "Session Border Controller for Enterprise". At the bottom right, it shows the copyright "© 2011 - 2013 Avaya Inc. All rights reserved."

Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.



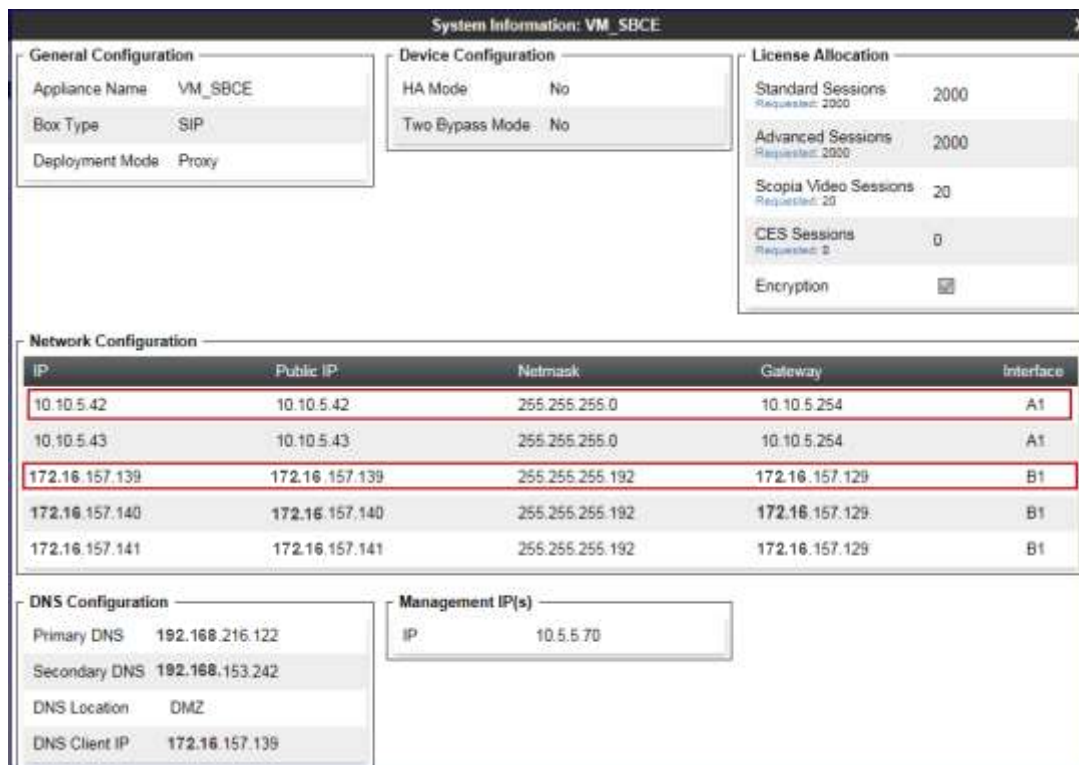
The dashboard has a top navigation bar with links: Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left sidebar lists navigation items: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings). The main content area is titled "Dashboard" and contains several sections: "Information" with fields for System Time (11:38:50 AM EDT), Version (7.0.0-21-6602), Build Date (Sun Aug 9 21:09:40 EDT 2015), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (09/14/2015 14:19:36 EDT), and Failed Login Attempts (1); "Alarms (past 24 hours)" showing "None found"; "Installed Devices" listing "EMS" and "VM\_SBCE"; and "Incidents (past 24 hours)" showing "VM\_SBCE: No Subscriber Flow Matched".

## 7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named **VM\_SBCE** is shown. The management IP address that was configured during installation and the current software version are shown here. Note that the management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is **Commissioned**, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.



To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device configuration and network settings.





The **A1** and **B1** interfaces correspond to the private and public interfaces of the Avaya SBCE. Note that the highlighted **A1** and **B1** IP addresses are the ones used for the SIP trunk to the service provider, and the ones relevant to these Application Notes. Other IP addresses assigned to these interfaces are used to support remote workers and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

### 7.3. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, **VM\_SBCE** in the sample configuration. On the **Networks** tab, verify or enter the network information as needed. Note that the **A1** and **B1** interfaces correspond to the private and public interfaces for the Avaya SBCE.

In the configuration used during the compliance test, IP address **10.10.5.42** was assigned to interface **A1**, and IP address **172.16.157.139** was assigned to interface **B1**.



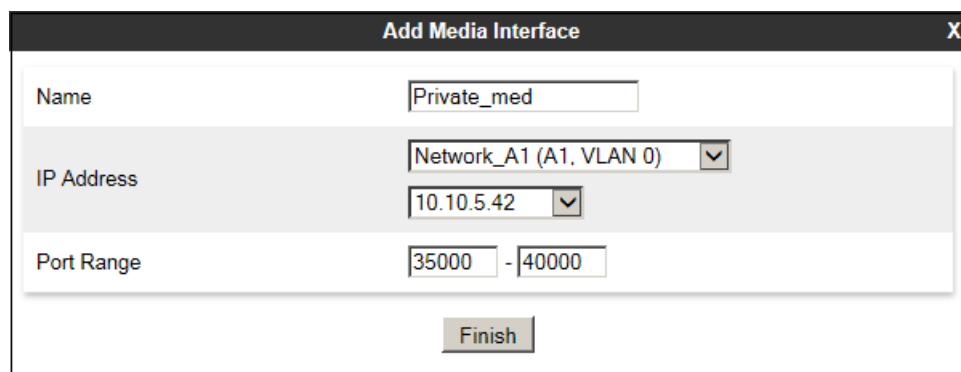
On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. Click the buttons under the **Status** column if necessary to enable the interfaces.



## 7.4. Media Interfaces

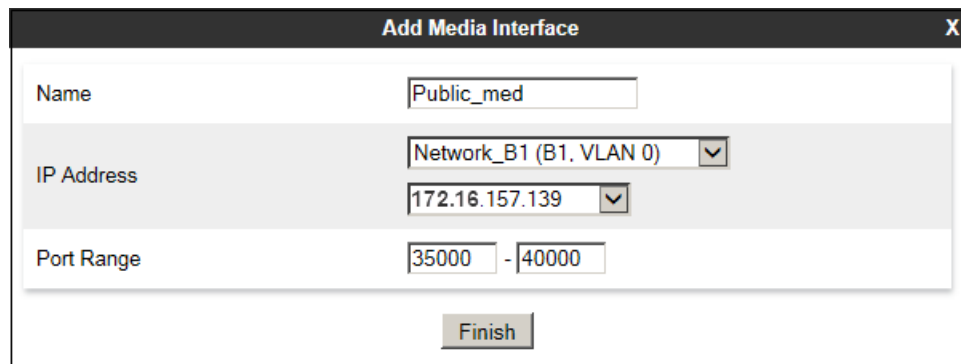
Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which it will accept media from the Call or the Trunk Server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Under **IP Address**, select from the drop-down menus the network and IP address associated with the private interface of the Avaya SBCE (A1). The **Port Range** was left at the default values of **35000-40000**. Click **Finish**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. It contains three main sections: "Name" with a text input field containing "Private\_med"; "IP Address" with two dropdown menus, the first showing "Network\_A1 (A1, VLAN 0)" and the second showing "10.10.5.42"; and "Port Range" with two text input fields containing "35000" and "40000" separated by a hyphen. A "Finish" button is located at the bottom center.

A Media Interface facing the public network side was similarly created with the name **Public\_med**, as shown below. Under **IP Address**, the network and IP address associated with the public interface of the Avaya SBCE (B1) were selected from the drop-down menus. The **Port Range** was left at the default values. Click **Finish**.

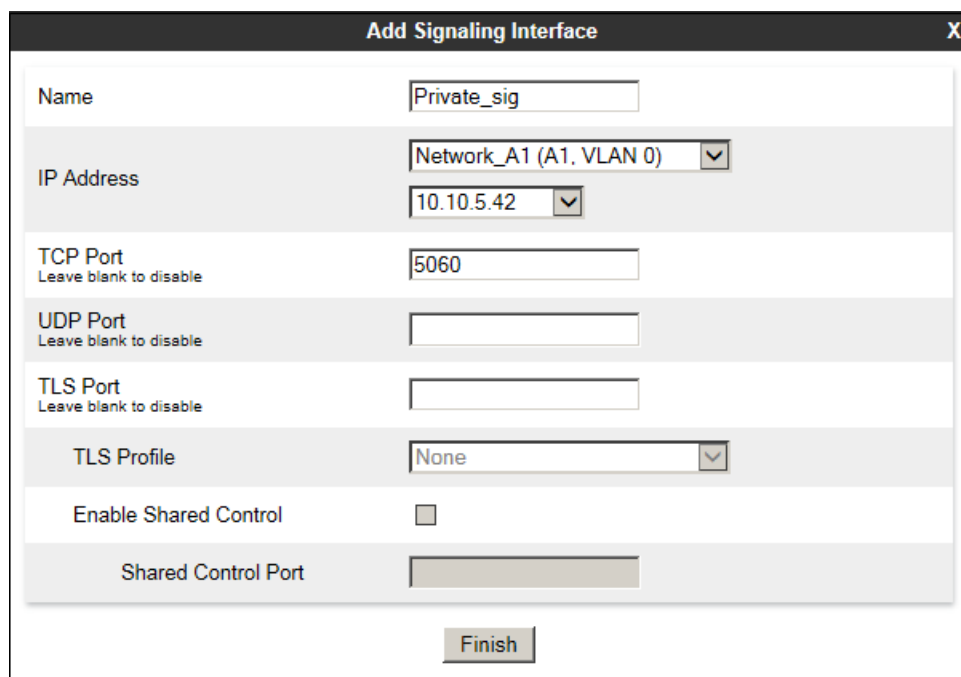


The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. It contains three main sections: "Name" with a text input field containing "Public\_med"; "IP Address" with two dropdown menus, the first showing "Network\_B1 (B1, VLAN 0)" and the second showing "172.16.157.139"; and "Port Range" with two text input fields containing "35000" and "40000" separated by a hyphen. A "Finish" button is located at the bottom center.

## 7.5. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

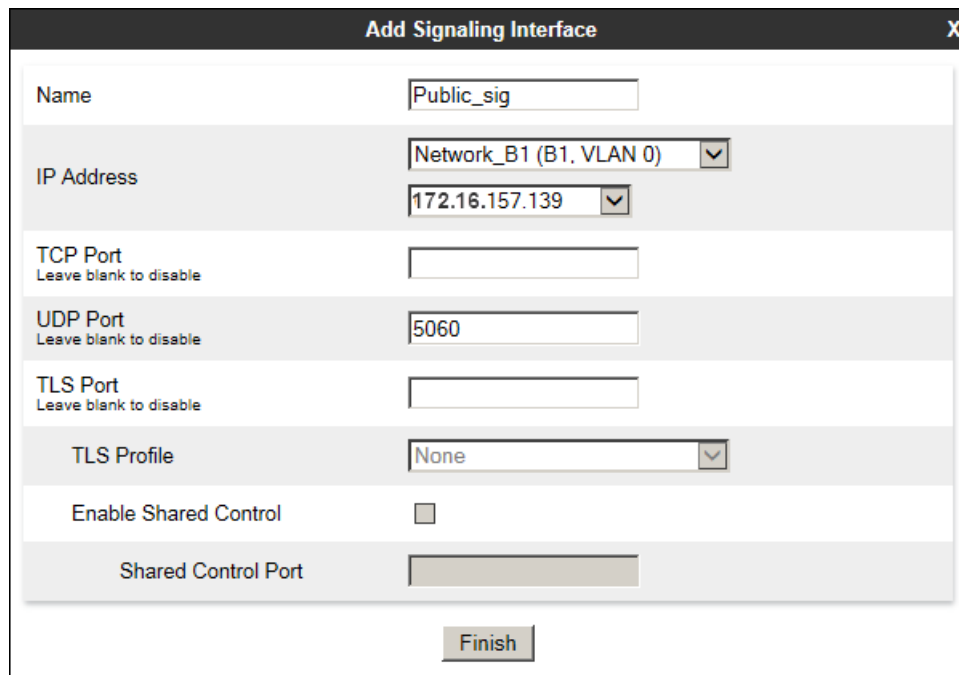
To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown). On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Under **IP Address**, select from the drop-down menus the network and IP address associated with the private interface of the Avaya SBCE (A1). Enter **5060** for **TCP Port**, since TCP port 5060 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.6**. Click **Finish**.



The screenshot shows a web-based configuration window titled "Add Signaling Interface" with a close button (X) in the top right corner. The form contains the following fields and controls:

- Name:** A text input field containing "Private\_sig".
- IP Address:** A section with two dropdown menus. The first dropdown is set to "Network\_A1 (A1, VLAN 0)". The second dropdown is set to "10.10.5.42".
- TCP Port:** A text input field containing "5060". Below the field is the text "Leave blank to disable".
- UDP Port:** An empty text input field. Below the field is the text "Leave blank to disable".
- TLS Port:** An empty text input field. Below the field is the text "Leave blank to disable".
- TLS Profile:** A dropdown menu set to "None".
- Enable Shared Control:** An unchecked checkbox.
- Shared Control Port:** An empty text input field.
- Finish:** A button at the bottom center of the form.

A second Signaling Interface with the name **Public\_sig** was similarly created in the service provider's direction. Under **IP Address**, the network and IP address associated with the public interface of the Avaya SBCE (B1) were selected from the drop-down menus. Enter **5060** for **UDP Port**, since this is the protocol and port that was used by the Avaya SBCE to listen to the service provider's SIP traffic. Click **Finish**.



The screenshot shows a configuration window titled "Add Signaling Interface" with a close button (X) in the top right corner. The window contains several fields for configuring a signaling interface:

- Name:** A text field containing "Public\_sig".
- IP Address:** A section with two dropdown menus. The first menu is set to "Network\_B1 (B1, VLAN 0)" and the second menu is set to "172.16.157.139".
- TCP Port:** A text field that is currently empty. Below it is the text "Leave blank to disable".
- UDP Port:** A text field containing "5060". Below it is the text "Leave blank to disable".
- TLS Port:** A text field that is currently empty. Below it is the text "Leave blank to disable".
- TLS Profile:** A dropdown menu set to "None".
- Enable Shared Control:** A checkbox that is currently unchecked.
- Shared Control Port:** A text field that is currently empty.

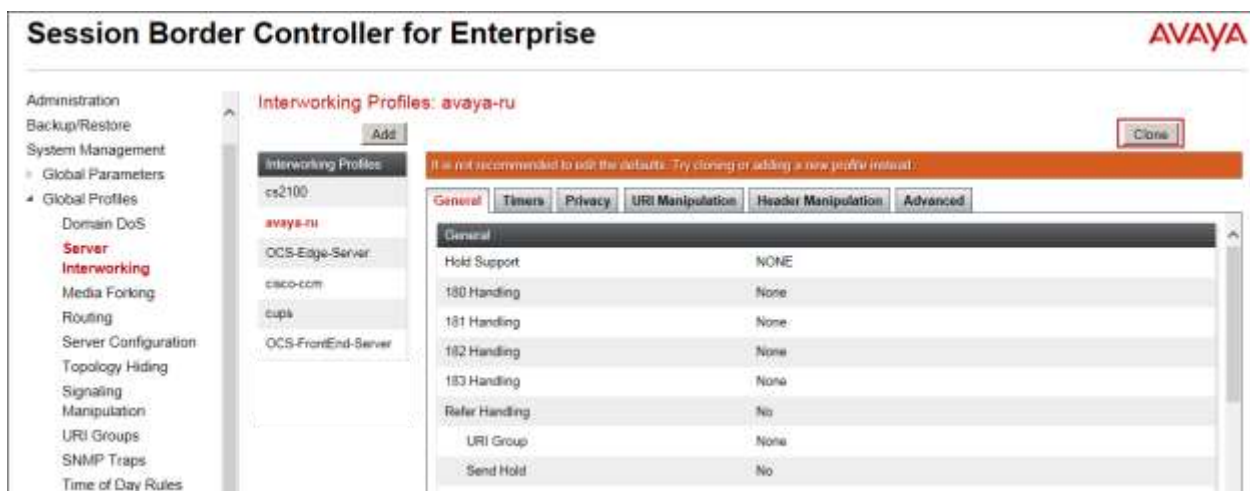
At the bottom center of the window is a button labeled "Finish".

## 7.6. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server). In the reference configuration, Session Manager functions as the Call Server and the Alestra SIP Proxy as the Trunk Server.

### 7.6.1. Server Interworking Profile – Enterprise

Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Global Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select *avaya-ru* from the list of pre-defined profiles. Click **Clone**.



Enter a descriptive name for the cloned profile. Click **Finish**.

Clone Profile

Profile Name

avaya-ru

Clone Name

Session Manager

Finish

On the newly cloned **Session Manager** interworking profile, on the **General** tab, scroll down to the bottom of the page and click **Edit** (not shown). All parameters retain their default values, as shown on the screen below. Click **Finish**.

Editing Profile: Session Manager

X

General

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

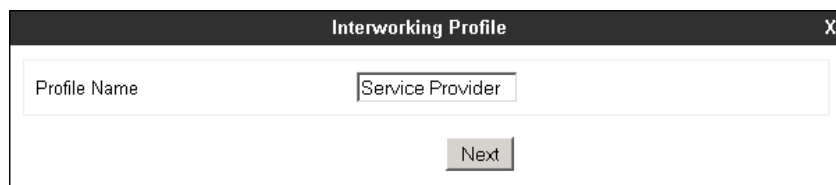
Finish

The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries. The **Advanced** tab settings are shown on the screen below:

General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
Record Routes		Both Sides			
Include End Point IP for Context Lookup		Yes			
Extensions		Avaya			
Diversion Manipulation		No			
Has Remote SBC		Yes			
Route Response on Via Port		No			
DTMF					
DTMF Support		None			
<div>Edit</div>					

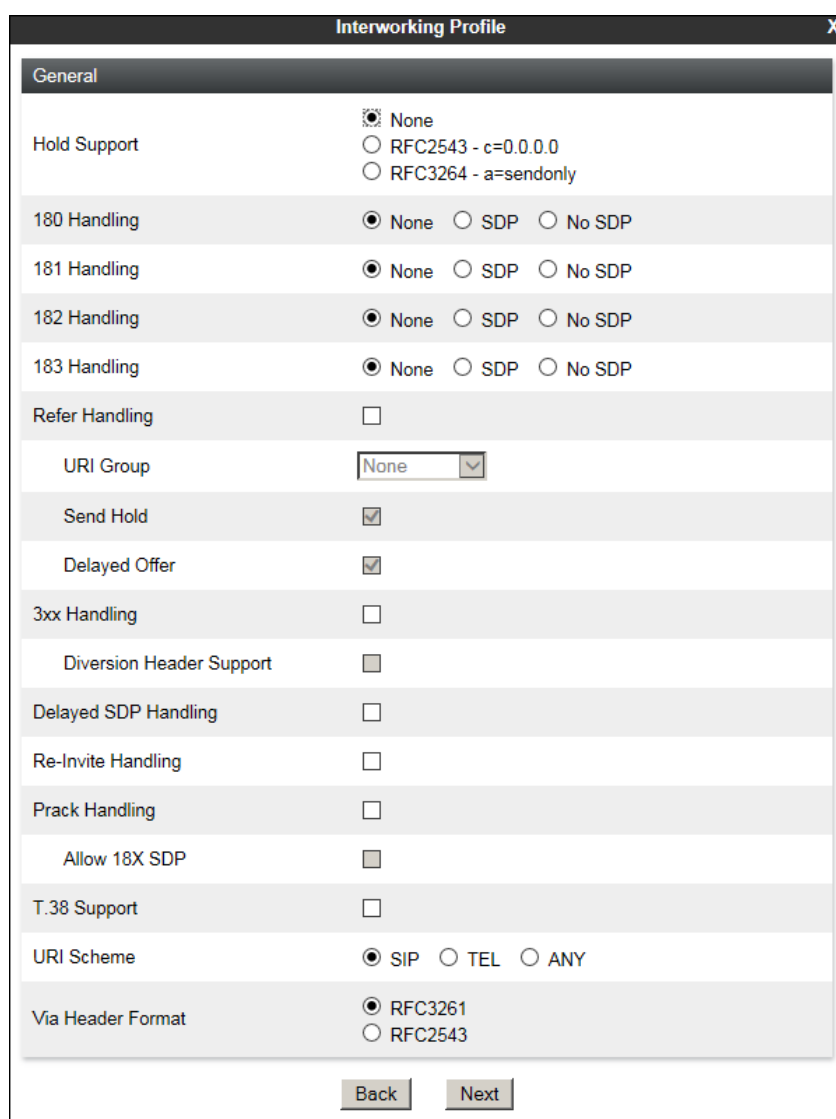
### 7.6.2. Server Interworking Profile – Service Provider

A second interworking profile in the direction of the SIP trunk was created, by adding a new profile in this case. Select **Global Profiles → Server Interworking** on the left navigation pane and click **Add** (not shown). Enter a descriptive name for the new profile. Click **Next**.



The screenshot shows a dialog box titled "Interworking Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Service Provider". Below the input field is a "Next" button.

On the **General** screen, all parameters retain their default values. Click **Next**.



The screenshot shows the "Interworking Profile" dialog box with the "General" tab selected. The dialog contains various configuration options with their default values:

- Hold Support:** Radio buttons for ☒ None, ☐ RFC2543 - c=0.0.0.0, and ☐ RFC3264 - a=sendonly.
- 180 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 181 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 182 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 183 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- Refer Handling:** ☐ checkbox.
- URI Group:** A dropdown menu showing "None".
- Send Hold:** ☒ checkbox.
- Delayed Offer:** ☒ checkbox.
- 3xx Handling:** ☐ checkbox.
- Diversion Header Support:** ☐ checkbox.
- Delayed SDP Handling:** ☐ checkbox.
- Re-Invite Handling:** ☐ checkbox.
- Prack Handling:** ☐ checkbox.
- Allow 18X SDP:** ☐ checkbox.
- T.38 Support:** ☐ checkbox.
- URI Scheme:** Radio buttons for ☒ SIP, ☐ TEL, and ☐ ANY.
- Via Header Format:** Radio buttons for ☒ RFC3261 and ☐ RFC2543.

At the bottom of the dialog are "Back" and "Next" buttons.



Click **Next** on the **SIP Timers** and **Privacy** tabs (not shown). On the **Advanced/DTMF** tab, select **Both Sides** under **Record Routes**. Accept the defaults settings for all other fields. Click **Finish**.

Interworking Profile

X

Record Routes

☐ None

☐ Single Side

☒ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup

☐

Extensions

None

Diversion Manipulation

☐

Diversion Condition

None

Diversion Header URI

Has Remote SBC

☒

Route Response on Via Port

☐

DTMF

DTMF Support

☒ None

☐ SIP NOTIFY

☐ SIP INFO

Back

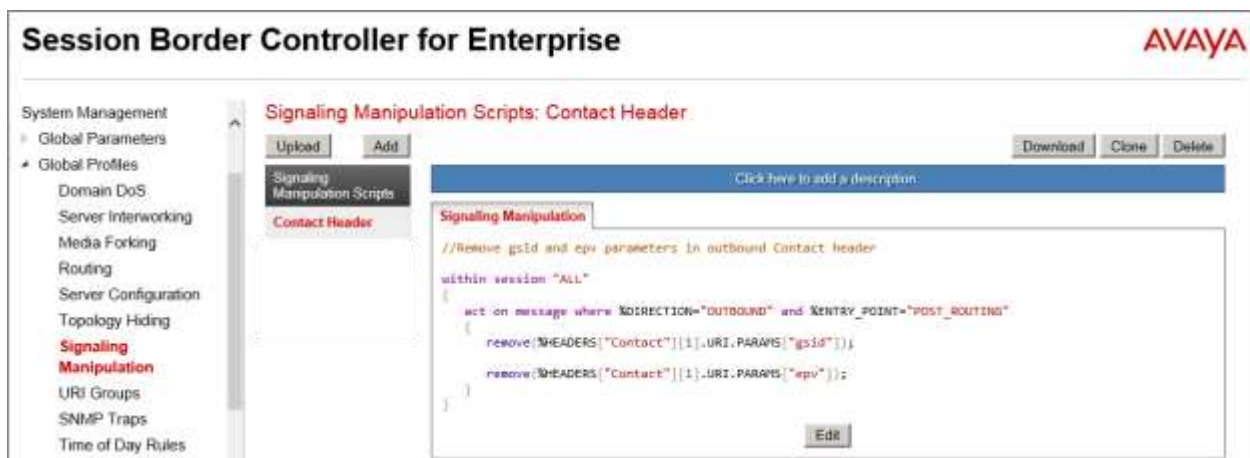
Finish

## 7.7. Signaling Manipulation

The screen below shows the finished Signaling Manipulation script named *Contact Header* created during the compliance test. This script was used to remove the “gsid” and “epv” parameters from outbound “Contact” headers. These parameters have no significance to the service provider and add unnecessary size to the outbound messages.

The script will later be applied to the Server Configuration profile corresponding to the service provider, later in **Section 7.8.2**.

To add a Signaling Manipulation script, from the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click **Add** to open the SigMa Editor screen, where the text of the script can be entered or copied.



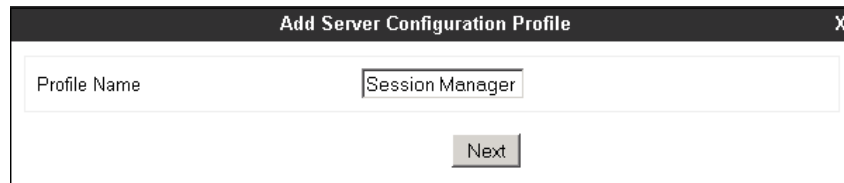
The details of the script used can be found in **Appendix A** in this document.

## 7.8. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and the SIP Proxy at the service provider network (Trunk Server).

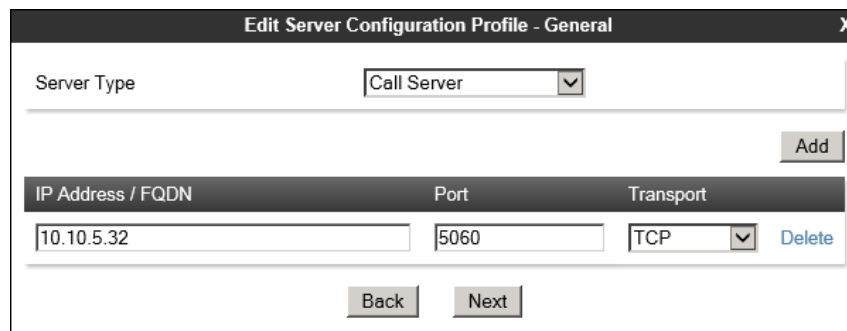
### 7.8.1. Server Configuration Profile – Enterprise

From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server. Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



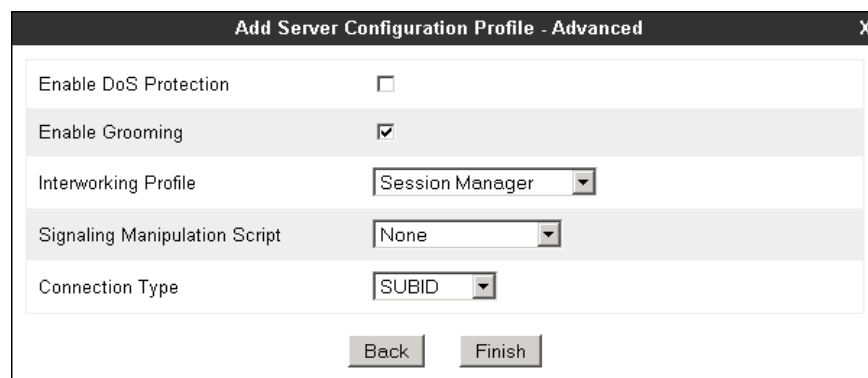
The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "Session Manager". Below this field is a "Next" button.

On the **Server Configuration Profile General** Tab select **Call Server** from the drop down menu under the **Server Type**. On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 6.5**). Enter **5060** under **Port** and select **TCP** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously in **Section 6.6**. Click **Next**.



The screenshot shows a dialog box titled "Edit Server Configuration Profile - General". It has a close button (X) in the top right corner. The "Server Type" dropdown menu is set to "Call Server". Below this is an "Add" button. There is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row contains the values "10.10.5.32", "5060", and "TCP" (selected from a dropdown). To the right of the "Transport" dropdown is a "Delete" link. At the bottom of the dialog are "Back" and "Next" buttons.

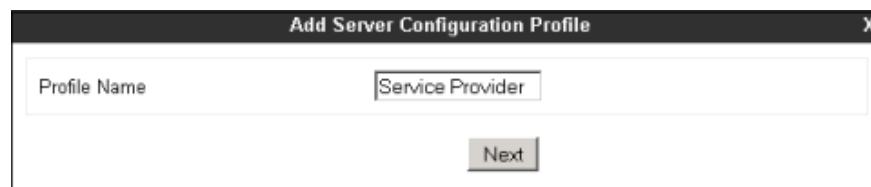
Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, since TCP is used, check the **Enable Grooming** box. Select **Session Manager** from the **Interworking Profile** drop down menu. Click **Finish**.



The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It has a close button (X) in the top right corner. It contains several settings: "Enable DoS Protection" (unchecked), "Enable Grooming" (checked), "Interworking Profile" (dropdown set to "Session Manager"), "Signaling Manipulation Script" (dropdown set to "None"), and "Connection Type" (dropdown set to "SUBID"). At the bottom are "Back" and "Finish" buttons.

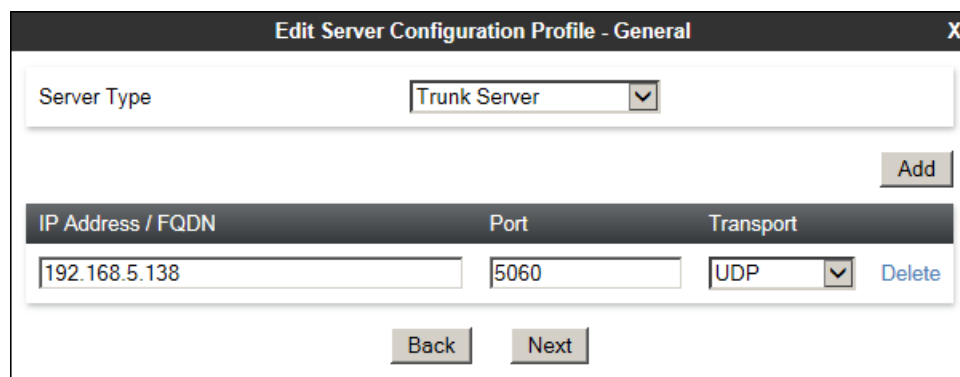
### 7.8.2. Server Configuration Profile – Service Provider

Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown). Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



A dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. It contains a text input field labeled "Profile Name" with the value "Service Provider" entered. Below the input field is a "Next" button.

On the **Add Server Configuration Profile** Tab select **Trunk Server** from the drop down menu for the **Server Type**. On the **IP Addresses / FQDN** field, enter the IP address of the service provider SIP proxy server. Enter **5060** under **Port**, and select **UDP** for **Transport**. Click **Next**.



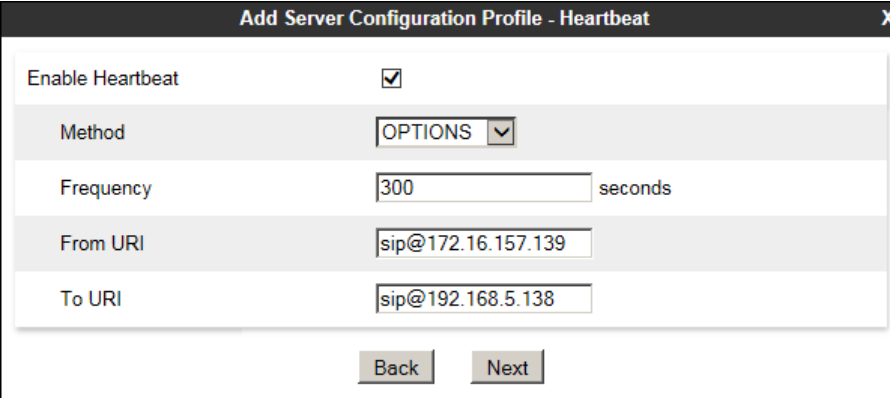
A dialog box titled "Edit Server Configuration Profile - General" with a close button (X) in the top right corner. It contains a "Server Type" dropdown menu set to "Trunk Server". Below this is an "Add" button. Underneath is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row contains the values "192.168.5.138", "5060", and "UDP" (selected from a dropdown). A "Delete" link is to the right of the "Transport" dropdown. At the bottom are "Back" and "Next" buttons.

IP Address / FQDN	Port	Transport
192.168.5.138	5060	UDP

Click **Next** on the **Authentication** tab (not shown).

On the **Heartbeat** tab, OPTIONS can be configured to periodically check the integrity of the SIP trunk to the service provider. To do this, set the following:

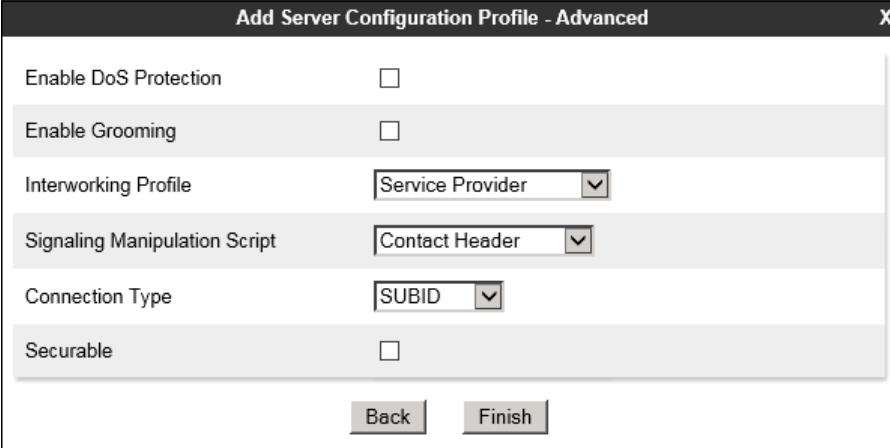
- Check the **Enable Heartbeat** box.
- Under **Method**, select **OPTIONS** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between OPTIONS messages that will be sent from the enterprise to the service provider proxy server. **300** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the OPTIONS messages were built using the IP addresses of the public interface of the Avaya SBCE and the service provider proxy server respectively.
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile - Heartbeat". It contains the following fields and controls:

- Enable Heartbeat**: A checkbox that is checked.
- Method**: A dropdown menu with "OPTIONS" selected.
- Frequency**: A text input field containing "300", followed by the label "seconds".
- From URI**: A text input field containing "sip@172.16.157.139".
- To URI**: A text input field containing "sip@192.168.5.138".
- At the bottom, there are two buttons: "Back" and "Next".

On the **Advanced** tab, select **Service Provider** from the **Interworking Profile** drop down menu. Under **Signaling Manipulation Script**, select the **Contact Header** script created in **Section 7.7**. Click **Finish**.



The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It contains the following fields and controls:

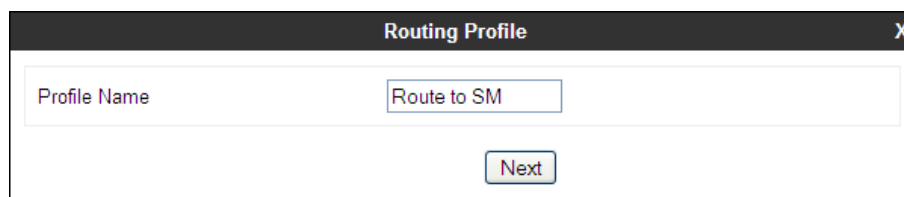
- Enable DoS Protection**: A checkbox that is unchecked.
- Enable Grooming**: A checkbox that is unchecked.
- Interworking Profile**: A dropdown menu with "Service Provider" selected.
- Signaling Manipulation Script**: A dropdown menu with "Contact Header" selected.
- Connection Type**: A dropdown menu with "SUBID" selected.
- Securable**: A checkbox that is unchecked.
- At the bottom, there are two buttons: "Back" and "Finish".

## 7.9. Routing

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the Alestra SIP trunk.

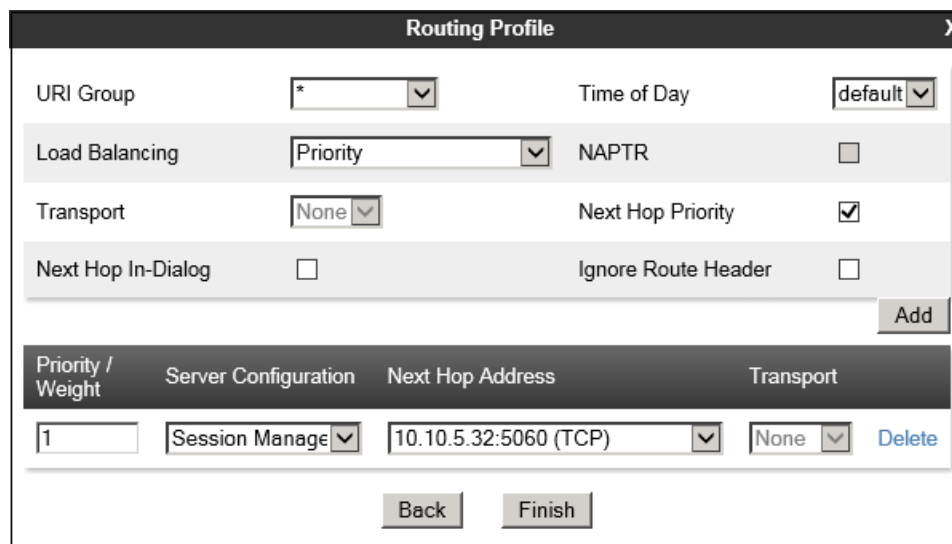
### 7.9.1. Routing Profile – Enterprise

To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown). Enter an appropriate **Profile Name** similar to the example below. Click **Next**.



The image shows a 'Routing Profile' dialog box. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a text input field for 'Profile Name' containing the text 'Route to SM'. Below the input field is a 'Next' button.

On the **Routing Profile** tab, click the **Add** button to enter the next-hop address. Enter **1** under **Priority/Weight**. Under **Server Configuration**, select **Session Manager**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile in **Section 7.8.1**. Defaults were used for all other parameters. Click **Finish**.



The image shows a 'Routing Profile' dialog box with various configuration options and a table of routing entries.

Configuration options:

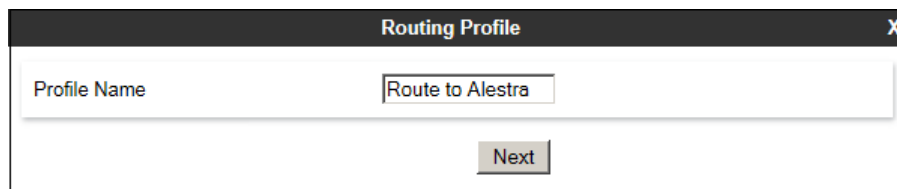
- URI Group: \*
- Time of Day: default
- Load Balancing: Priority
- NAPTR: ☐
- Transport: None
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐

Buttons: Add, Back, Finish

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Session Manager	10.10.5.32:5060 (TCP)	None	Delete

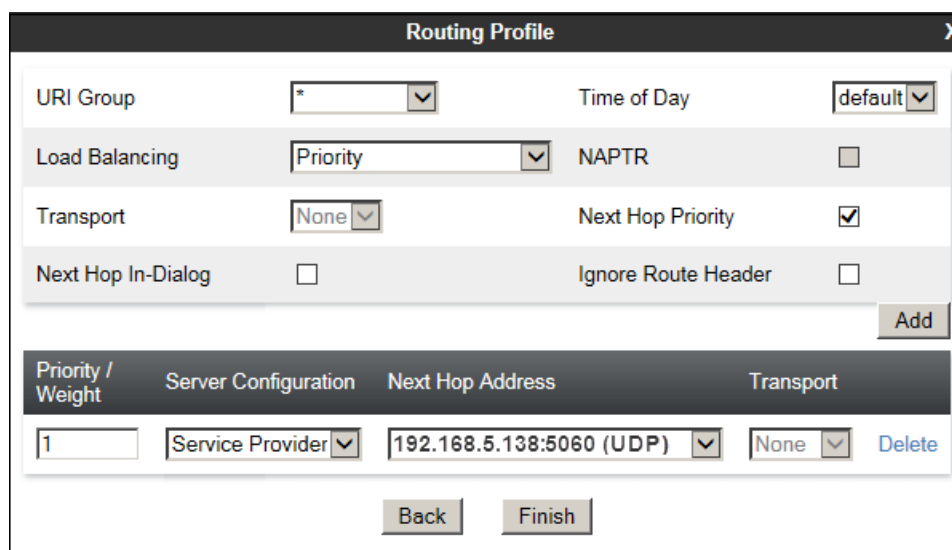
### 7.9.2. Routing Profile – Service Provider

Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route. Enter an appropriate **Profile Name** similar to the example below. Click **Next**.



The image shows a 'Routing Profile' dialog box. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a text field labeled 'Profile Name' containing the text 'Route to Alestra'. Below this field is a button labeled 'Next'.

On the **Routing Profile** tab, click the **Add** button to enter the next-hop address. Enter **1** under **Priority/Weight**. Under **Server Configuration**, select **Service Provider**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Service Provider Server Configuration Profile in **Section 7.8.2**. Defaults were used for all other parameters. Click **Finish**.



The image shows a 'Routing Profile' dialog box with various configuration options and a table.

Configuration options:

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

Buttons: Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Service Provider	192.168.5.138:5060 (UDP)	None	Delete

Buttons: Back, Finish

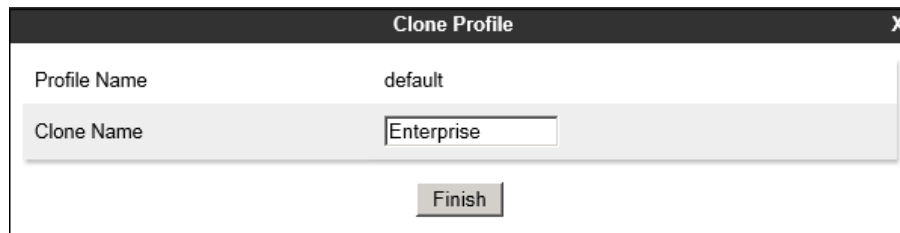
## 7.10. Topology Hiding

Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. Only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

### 7.10.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select *default* from the list of pre-defined profiles and click the **Clone** button (not shown). Enter a **Clone Name** such as the one shown below. Click **Finish**.



Clone Profile	
Profile Name	default
Clone Name	Enterprise
<div>Finish</div>	

On the newly cloned *Enterprise* profile screen, click the **Edit** button (not shown).



For the **To**, **From** and the **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **sil.miami.avaya.com**, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.2**. Default values were used for all other fields. Click **Finish**.

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

Finish

### 7.10.2. Topology Hiding Profile – Service Provider

A Topology Hiding profile named **Service Provider** was similarly created in the direction of the SIP trunk to the service provider. During the compliance test, IP addresses and not domains names were used in all SIP messages between the service provider SIP proxy server and the Avaya SBCE. Note that since the default action of **Auto** implies the insertion of IP addresses in the host portion of these headers, it was not necessary to modify any of the headers sent to the service provider. The screen below shows the **Service Provider** profile once the configuration was completed.

Topology Hiding Profiles: Service Provider

Add Rename Clone Delete

Click here to add a description

Topology Hiding

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

Edit

## 7.11. End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. In the reference configuration, the End Point Policy Groups defined used default sets of rules already pre-defined in the configuration. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule. Also note that even though the End Point Policy Groups for both the Enterprise and the Service Provider used the same set of rules, they were still separately defined, to allow for future changes to be made in one direction if needed, without affecting the other direction.

### 7.11.1. End Point Policy Group – Enterprise

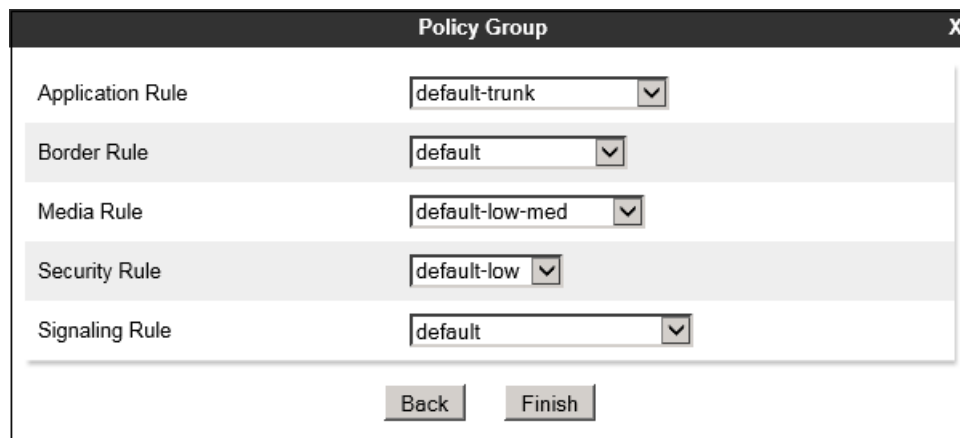
To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

Enter an appropriate name in the **Group Name** field. Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a label "Group Name" followed by a text input field containing the word "Enterprise". Below the input field is a "Next" button.

In the Policy Group tab, all fields used one of the default sets of rules already pre-defined in the configuration. Click **Finish**.



The screenshot shows the "Policy Group" dialog box with several dropdown menus. The "Application Rule" is set to "default-trunk", "Border Rule" is set to "default", "Media Rule" is set to "default-low-med", "Security Rule" is set to "default-low", and "Signaling Rule" is set to "default". At the bottom of the dialog are "Back" and "Finish" buttons.

### 7.11.2. End Point Policy Group – Service Provider

A second End Point Policy Group was created for the service provider, repeating the steps previously described. In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration.

The screen below shows the End Point Policy Group named *Service Provider* after the configuration was completed.

**Policy Groups: Service Provider**

Buttons: Add, Filter By Device..., Rename, Clone, Delete

Policy Groups List:

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- avaya-def-high-sub...
- avaya-def-high-server
- Enterprise
- Service Provider**

Click here to add a description.

Hover over a row to see its description.

**Policy Group**

Order	Application	Border	Media	Security	Signaling	
1	default-trunk	default	default-low-med	default-low	default	Edit

Summary

## 7.12. End Point Flows

End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. They also combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

### 7.12.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named *Session Manager Flow* created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 7.9.2**, which is the reverse route of the flow. Click **Finish**.

Edit Flow: Session Manager Flow	
Flow Name	Session Manager Flow
Server Configuration	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
End Point Policy Group	Enterprise
Routing Profile	Route to Alestra
Topology Hiding Profile	Enterprise
Signaling Manipulation Script	None
Remote Branch Office	Any
<b>Finish</b>	

### 7.12.2. End Point Flow – Service Provider

A second Server Flow with the name **SIP Trunk Flow** was similarly created in the network direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 7.9.1**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Since the script created in **Section 7.7** was previously applied to the service provider's Server Configuration Profile in **Section 7.8.2**, it is not necessary to make a selection here. Click **Finish**.

Edit Flow: SIP Trunk FlowX

Flow Name	<input type="text" value="SIP Trunk Flow"/>
Server Configuration	<input type="text" value="Service Provider"/>
URI Group	<input type="text" value="*/"/>
Transport	<input type="text" value="*/"/>
Remote Subnet	<input type="text" value="*/"/>
Received Interface	<input type="text" value="Private_sig"/>
Signaling Interface	<input type="text" value="Public_sig"/>
Media Interface	<input type="text" value="Public_med"/>
End Point Policy Group	<input type="text" value="Service Provider"/>
Routing Profile	<input type="text" value="Route to SM"/>
Topology Hiding Profile	<input type="text" value="Service Provider"/>
Signaling Manipulation Script	<input type="text" value="None"/>
Remote Branch Office	<input type="text" value="Any"/>

Finish

## 8. Alestra SIP Trunking Configuration

Alestra is responsible for the configuration of the Alestra SIP Trunking service. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise. Alestra will provide the customer the necessary information to configure the SIP trunk connection from the enterprise site to the network, including:

- IP address of the Alestra SIP Proxy server.
- Supported codecs and order of preference.
- DID numbers.
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

This information is used to complete the configuration of Communication Manager, Session Manager and the Avaya SBCE discussed in the previous sections.

## 9. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of commands that can be used to troubleshoot the solution.

### 9.1. General Verification Steps

- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

### 9.2. Communication Manager Verification

The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

- **list trace station** <extension number>  
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>  
Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>  
Displays signaling group service state.
- **status trunk** <trunk group number>  
Displays trunk group service state.
- **status station** <extension number>  
Displays signaling and media information for an active call on a specific station.

### 9.3. Session Manager Verification

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager** → **System Status** → **SIP Entity Monitoring**. Click the Session Manager instance (*Session Manager* in the example below).

The screenshot shows the 'SIP Entity Link Monitoring Status Summary' page. It includes a sidebar with navigation options like Dashboard, Session Manager, Administration, Communication, Profile Editor, Network, Configuration, Device and Location Configuration, Application Configuration, System Status, SIP Entity Monitoring, and SIP Entity Monitoring. The main content area has a title 'SIP Entity Link Monitoring Status Summary' and a description: 'This page provides a summary of Session Manager SIP entity link monitoring status.' Below this is a section 'SIP Entities Status for All Monitoring Session Manager Instances' with a 'Run Monitor' button. A table shows the status of monitored entities. The table has columns: Session Manager, Type, and Monitored Entities (Down, Partially Up, Up, Not Monitored, Down, Total). The data row shows 'Session Manager' as the entity, 'Core' as the type, and counts: Down: 0, Partially Up: 0, Up: 7, Not Monitored: 0, Down: 0, Total: 7.

Session Manager	Type	Down	Partially Up	Up	Not Monitored	Down	Total
Session Manager	Core	0	0	7	0	0	7

Verify that the state of the Session Manager links to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.

The screenshot shows the 'Session Manager Entity Link Connection Status' page. It includes a sidebar with navigation options like Dashboard, Session Manager, Administration, Communication, Profile Editor, Network, Configuration, Device and Location Configuration, Application Configuration, System Status, SIP Entity Monitoring, and SIP Entity Monitoring. The main content area has a title 'Session Manager Entity Link Connection Status' and a description: 'This page displays detailed connection status for all entity links from a Session Manager.' Below this is a section 'All Entity Links for Session Manager: Session Manager' with a 'Summary View' button. A table shows the status of entity links. The table has columns: SIP Entity Name, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The data rows show various entity links, including 'Avaya SBCE' and 'CM Trunk 2', all with 'UP' status.

SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
AA Messaging	10.10.5.92	5062	TLS	FALSE	UP	200 OK	UP
SBCE-2	10.10.5.42	5080	TCP	FALSE	UP	200 OK	UP
CM Trunk 9B	10.10.5.12	5064	TLS	FALSE	UP	200 OK	UP
C.M. Trunk 10	10.10.5.12	5080	TCP	FALSE	UP	200 OK	UP
CM Trunk 1	10.10.5.12	5061	TLS	FALSE	UP	200 OK	UP
Avaya SBCE	10.10.5.42	5060	TCP	FALSE	UP	200 OK	UP
CM Trunk 2	10.10.5.12	5063	TLS	FALSE	UP	200 OK	UP

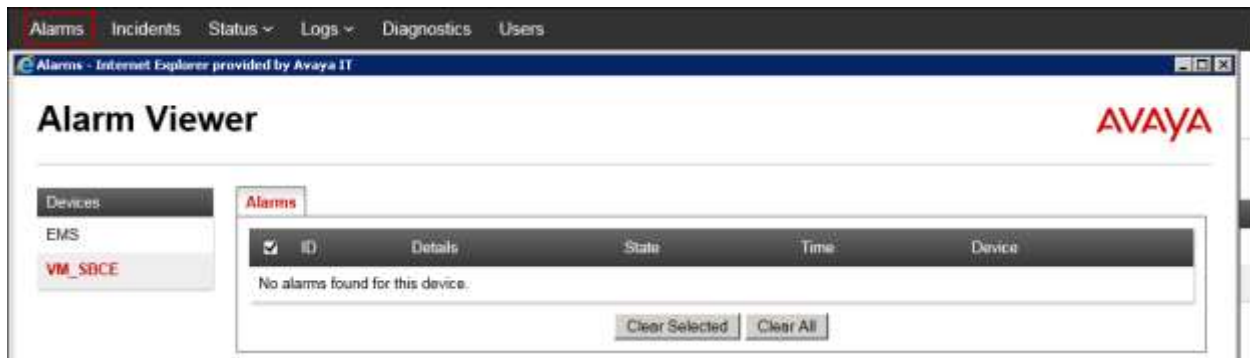
Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Enter the requested data to run the test.

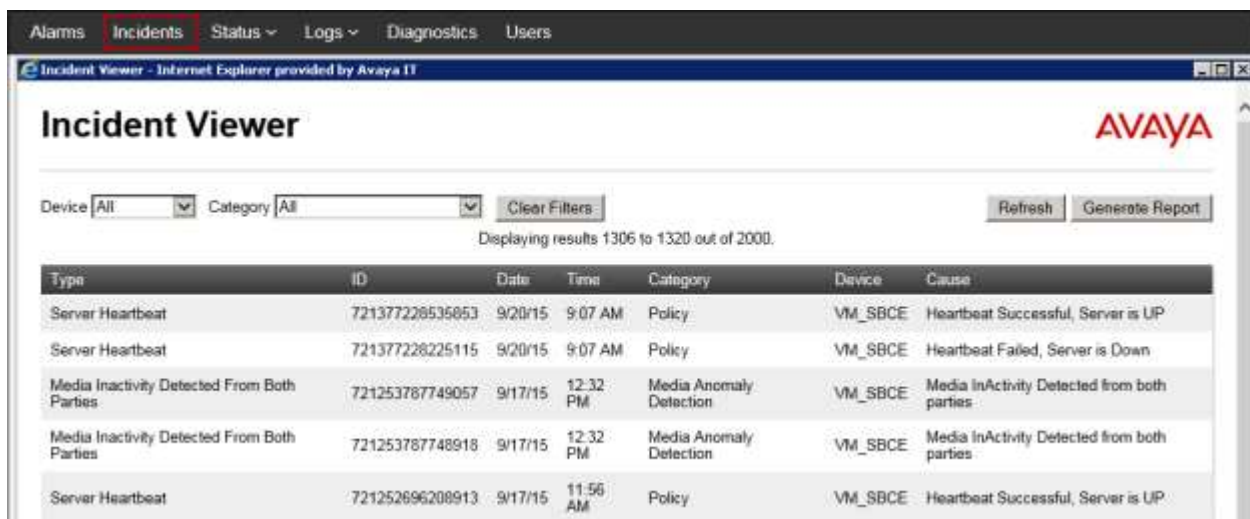
## 9.4. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

**Alarms:** This screen provides information about the health of the SBC.



**Incidents :** This screen provides detailed reports of anomalies, errors, policies violations, etc.





**Status:** Statistical and current status information. The **Server Status** screen below provides information about the condition of the connection to the Service Provider. In order to receive server status information, Heartbeat needs to be enabled on the Server Configuration profile, as configured in **Section 7.8.2**.



The screenshot shows the Avaya SBCE Status page. The top navigation bar includes Alarms, Incidents, Status (highlighted), Logs, Diagnostics, Users, and Settings. The left sidebar shows Session B, SIP Statistics, User Registrations, and Server Status (highlighted). The main content area is titled 'Status' and features the Avaya logo. Below the title, there is a 'Devices' section with 'VM\_SBCE' listed. The 'Server Status' section contains a table with the following data:

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Status	TimeStamp
Service Provider	192.168.5.138	192.168.5.138	5060	UDP	UP	10/29/2015 13:22:22 EDT

**Diagnostics:** This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.



The screenshot shows the Avaya SBCE Diagnostics page. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics (highlighted), and Users. The left sidebar shows Session B, SIP Statistics, User Registrations, and Server Status. The main content area is titled 'Diagnostics' and features the Avaya logo. Below the title, there is a 'Devices' section with 'VM\_SBCE' listed. The 'Diagnostics' section contains two tabs: 'Full Diagnostic' (highlighted) and 'Ping Test'. The 'Full Diagnostic' section has a message: 'Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.' Below this message is a 'Start Diagnostic' button. The 'Full Diagnostic' section also contains a table with the following data:

Task Description	Status
EMS Link Check	
SBC Link Check: A1	
SBC Link Check: B1	
Ping: SBC (A1) to Gateway (10.10.5.254)	

Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as *pcap* files. Navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

Once the capture is stopped, click the **Captures** tab and select the proper *pcap* file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.

Packet Capture		
Captures		
Last Modified ▼	Descending ▼	Sort Reset Refresh
File Name	File Size (bytes)	Last Modified
test_20150925183130.pcap	233,472	September 25, 2015 6:31:54 PM EDT <a href="#">Delete</a>

## 10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0, to connect to the Alestra SIP Trunk Service on the Sonus platform, as shown in **Figure 1**.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the observations/limitations described in **Section 2.2**.

## 11. References

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

- [1] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 7.0 August 2015.
- [2] *Administering Avaya Aura® Communication Manager*, Release 7.0, August 2015, Document Number 03-300509.
- [3] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, August 2015, Document Number 555-245-205.
- [4] *Deploying Avaya Aura® System Manager*, Release 7.0, October 2015.
- [5] *Deploying Avaya Aura® Session Manager on VMware®*, Release 7.0, August 2015.
- [6] *Administering Avaya Aura® Session Manager*, Release 7.0, August 2015.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
- [8] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.0, August 2015.
- [9] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
- [10] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.7. August 2015.
- [11] *Implementing and Administering Avaya Aura® Media Server*. Release 7.7. August 2015.
- [12] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager. White Paper*. August 2015.
- [13] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [14] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

## 12. Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the Avaya SBCE, on **Section 7.7**.

```
//Remove gsid and epv parameters in outbound Contact header
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
    remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
  }
}
```

---

**©2015 Avaya Inc. All Rights Reserved.**

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

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