



Application Notes for Configuring Alestra Enlace IP SIP Trunk Service with Avaya Aura® Communication Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2 – Issue 1.0

Abstract

These Application Notes describe the procedures required for configuring Session Initiation Protocol (SIP) trunking between the Alestra Enlace IP SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2.

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

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.....	3
2.	General Test Approach and Test Results.....	3
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results	5
2.3.	Support	6
3.	Reference Configuration	6
4.	Equipment and Software Validated	8
5.	Configure Avaya Aura® Communication Manager	9
5.1.	Licensing and Capacity	9
5.2.	System Features.....	10
5.3.	IP Node Names.....	11
5.4.	Codecs	11
5.5.	IP Network Regions	12
5.6.	Signaling Group	13
5.7.	Trunk Group.....	15
5.8.	Calling Party Information.....	17
5.9.	Inbound Routing.....	17
5.10.	Outbound Routing	18
6.	Configure Avaya Session Border Controller for Enterprise	20
6.1.	System Access.....	20
6.2.	System Management	21
6.3.	Global Profiles.....	22
6.3.1.	Server Interworking	22
6.3.2.	Signaling Manipulation.....	27
6.3.3.	Server Configuration.....	28
6.3.4.	Routing Profiles	31
6.3.5.	Topology Hiding.....	33
6.4.	Domain Policies	35
6.4.1.	Signaling Rules	35
6.4.2.	End Point Policy Groups.....	38
6.5.	Device Specific Settings.....	40
6.5.1.	Network Management.....	40
6.5.2.	Media Interface	41
6.5.3.	Signaling Interface	42
6.5.4.	End Point Flows.....	44
7.	Alestra Enlace IP SIP Trunk Configuration.....	46
8.	Verification and Troubleshooting.....	46
8.1.	General Verification Steps	46
8.2.	Communication Manager Verification.....	46
8.3.	Avaya SBCE Verification	47
9.	Conclusion	49
10.	References.....	49

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the Alestra Enlace IP SIP Trunk service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.3, Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.2 and various Avaya endpoints. The solution does not include Avaya Aura® Session Manager and consequently SIP endpoints are not supported.

The Alestra Enlace IP SIP Trunk Service referenced within these Application Notes is designed for enterprise business customers in Mexico. Customers using this service with the Avaya SIP-enabled 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 the Alestra Enlace IP SIP Trunk service 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, 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, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones in the “This Computer” and “Other Phone” modes (H.323).
- Various call types, including: local, long distance and international.
- Codecs G729A and G.711A and proper codec negotiation.
- DTMF tone transmissions 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 forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- T.38 Fax.

Items not supported or not tested included the following:

- Network Call Redirection methods using REFER or 302 Temporarily Unavailable messages are not supported by Alestra and were not tested.
- Operator services such as dialing 0 or 0 + 10 digits are not supported.
- 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 Enlace IP SIP Trunk service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the exception of the observations/limitations described below:

- **Caller ID on outbound calls:** On outbound calls, the caller ID number shown on the PSTN user was always the main number assigned to the SIP trunk by Alestra, regardless of the specific DID number sent in the origination headers from the enterprise. This seems to be the desired configuration on the Alestra network, and it is listed here just as an observation.
- **Caller ID on incoming calls from the U.S.:** Calls originating from PSTN telephones in the U.S. to DID numbers in Mexico assigned to the SIP trunk to the Avaya solution will display **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. This behavior is not necessarily indicative of a limitation of the combined Alestra/Avaya solution, and it is listed here simply as an observation.
- **“To” header on incoming calls:** Incoming calls from Alestra to the enterprise contained the last 4 digits of the assigned DID number in the Request-URI header, but the To header contained 18 digit numbers, consisting of the complete 10 digit DID number preceded by a constant 8 digit prefix. This issue was sent to Alestra for investigation. There was no noticeable effect to the user.
- **Outbound Calling Party Number (CPN) Block:** When an enterprise extension user activated “CPN Block” on an outbound call, the INVITE sent to Alestra included the From: “anonymous” and the “Privacy: id” headers as expected, but the caller ID on the receiving end at the PSTN still showed the main number assigned to the SIP trunk by Alestra. This may be a requirement on the PSTN in Mexico and it is listed here just as an observation.
- **Calls to Busy Numbers:** Alestra did not send “486 Busy Here” for calls made from an enterprise extension to busy PSTN numbers. Since busy tone was heard by the caller, this observation had no direct impact to the user.
- **T.38 Fax:** During testing of T.38 fax using voice interworking with codec G.711, Alestra responded with “488 Not Acceptable Here” to the re-INVITE with T.38 SDP sent from the enterprise, and the fax calls failed in this scenario. T.38 fax using voice interworking with codec G.729A was successfully tested and worked as expected. Since G.729A is the preferred codec by Alestra and the first option on the SIP trunk, the voice setup will generally be established at G.729A, hence there should not be any real impact to the user.
- **SIP header optimization:** During the compliance test, the “Alert-Info” and “AV-Global-Session-ID” SIP headers used by Communication Manager, as well as the “Remote-Address” header used by the Avaya SBCE, had no specific use in the Alestra network. Since these headers contain private IP addresses and other enterprise information that should not be propagated outside of the enterprise boundaries, and in order to optimize the size of the packets entering the service provider’s network, they were removed by using Signaling Rules and a Sigma Script in the Avaya SBCE. See **Sections 6.3.2 and 6.4.1** later in this document.

2.3. Support

For technical support on the Alestra Enlace IP 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 Enlace IP SIP Trunk 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.

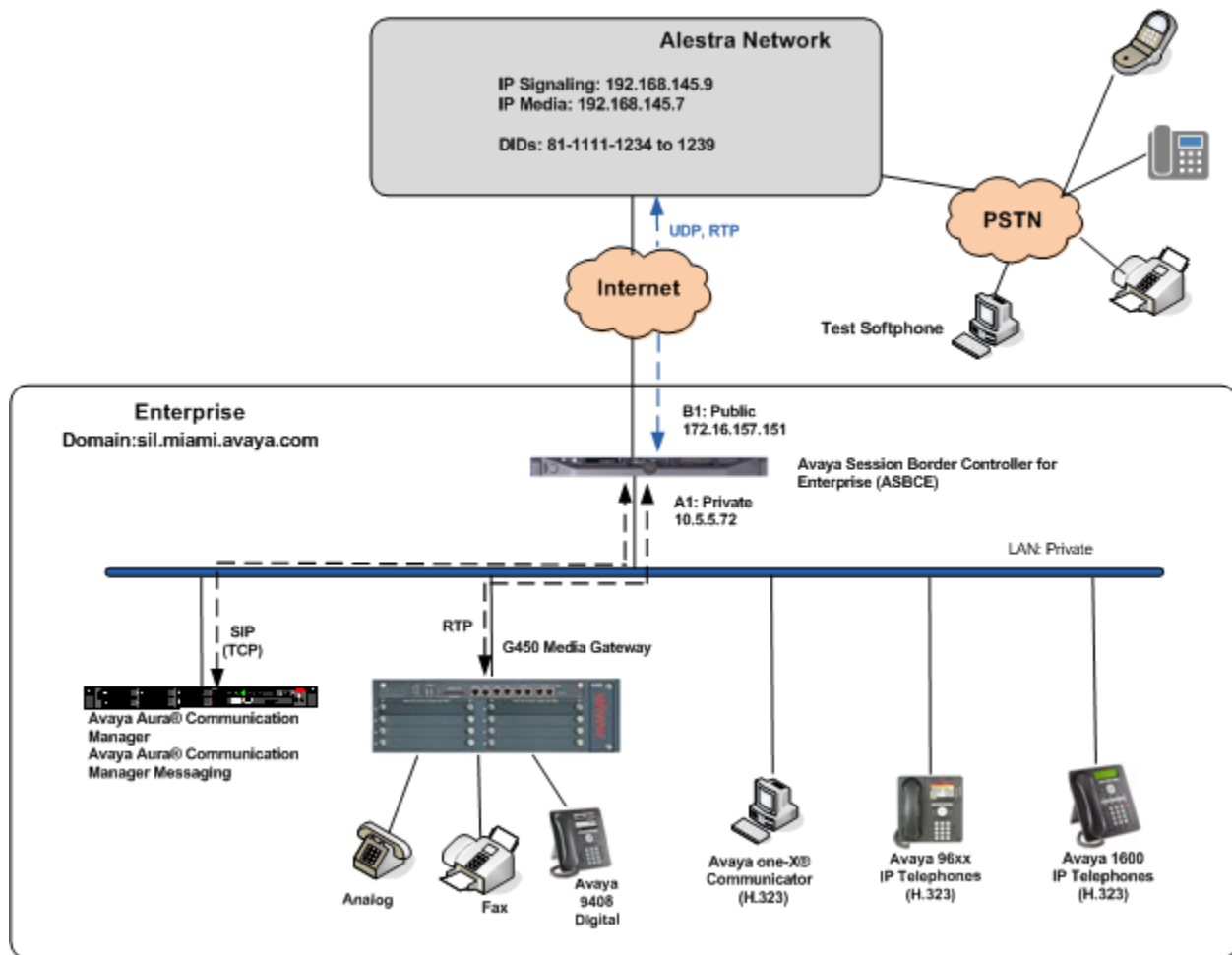


Figure 1: Avaya SIP Enterprise Solution connected to Alestra Enlace IP SIP Trunk Service

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

- Avaya Aura® Communication Manager.
- Avaya Aura® Communication Manager Messaging.
- Avaya Session Border Controller for Enterprise.
- Avaya G450 Media Gateway.
- Avaya 96xx and 16xx Series IP Telephones (H.323).
- Avaya one-X® Communicator softphones (H.323).
- Avaya digital and analog telephones.

The Avaya SBCE is located at the edge of the enterprise. It has a public interface that connects to the external network and a private interface that connects to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flows through the Avaya SBCE, which in this way can protect the enterprise against any SIP-based attacks. The Avaya SBCE also performs network address translation at both the IP and SIP layers.

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

For inbound calls, the calls flow from the service provider to the Avaya SBCE. After the Avaya SBCE performs the necessary security checks and interworking manipulation, the call is sent to Communication Manager, where incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to the Avaya SBCE for additional interworking treatment before egress to the Alestra network.

A separate SIP trunk was created between Communication Manager and the Avaya SBCE 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 traffic. The trunk carried both inbound and outbound traffic.

During the compliance test, in addition to the DID numbers assigned to the SIP trunk, Alestra provided a local test number in Monterrey, Mexico. A SIP-based softphone was registered to this local PSTN number and was used to originate and terminate local PSTN calls to and from the enterprise.

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® Communication Manager on HP® Proliant DL360 G7 Server	6.3 Service Pack 5 (patch 03.0.124-0-21460) (System Platform 6.3.1.08002.0)
Avaya Aura® Communication Manager Messaging	6.3 Service Pack 2 (CMM-03.0.124.0-0002)
Avaya Session Border Controller for Enterprise on a Dell R210 V2 Server	6.2.1.Q07
Avaya G450 Media Gateway	35.8.0
Avaya 96xx Series IP Telephones (H.323)	Avaya one-X Deskphone Edition 3.2.1
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition H.323 6.3.1
Avaya 16xx Series IP Telephones (H.323)	1.3 SP3
Avaya one-X Communicator (H.323)	6.2.2.07-SP2
Avaya 9408 Digital Telephone	Rel 12.0
Avaya 6210 Analog Telephone	N/A
Alestra Enlace IP	
Sonus Softswitch	V07.03.06 R003
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 Communication Manager and Media Gateway platforms running similar software versions.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Alestra SIP Trunk service. A SIP trunk is established between Communication Manager and the Avaya SBCE for use by signaling traffic to and from Alestra. It is assumed that the general installation of Communication Manager and the G450 Media Gateway 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 **395** 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 to add additional capacity.

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		12000	10	
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	6	
Maximum Administered SIP Trunks:		24000	395	
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0	
Maximum Number of DS1 Boards with Echo Cancellation:		522	0	
Maximum TN2501 VAL Boards:		128	0	
Maximum Media Gateway VAL Sources:		250	1	
Maximum TN2602 Boards with 80 VoIP Channels:		128	0	
Maximum TN2602 Boards with 320 VoIP Channels:		128	0	
Maximum Number of Expanded Meet-me Conference Ports:		300	0	
(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 20
FEATURE-RELATED SYSTEM PARAMETERS
  Self Station Display Enabled? y
    Trunk-to-Trunk Transfer: all
  Automatic Callback with Called Party Queuing? n
  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 highlighted below. The compliance test used the value of ***restricted*** for restricted calls and ***unavailable*** for unavailable calls.

```
change system-parameters features                               Page 9 of 20
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 private interface of the Avaya SBCE (**ASBCE_A1**). These node names will be needed when configuring the service provider signaling group in **Section 5.6**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
ASBCE_A1	10.5.5.72	
Acme_s1p0	192.168.10.52	
HG_CM	172.16.5.12	
HG_SM	172.16.5.32	
asm	192.168.10.32	
default	0.0.0.0	
ip_office	192.168.10.60	
msgserver	192.168.10.12	
procr	192.168.10.12	

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.729A and G.711A, in this order of preference. Enter **G.729A** and **G.711A** 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
1: G.729A	<u>n</u>	<u>2</u>
2: G.711A	<u>n</u>	<u>2</u>

On **Page 2**, set the **Fax Mode** to **t.38-standard**.

change ip-codec-set 2		Page 2 of 2
IP CODEC SET		
Allow Direct-IP Multimedia? <u>n</u>		
FAX	Mode	Redundancy
Modem	<u>t.38-standard</u>	<u>0</u>
TDD/TTY	<u>off</u>	<u>0</u>

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 necessary.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

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

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 R	G L	t c e t
1	2	y	NoLimit						n			t
2	2										all	
3												
4												

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Avaya SBCE 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 for this purpose and was configured using the parameters highlighted below:

- 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.
- Set the **Transport Method** field to the transport protocol to be used between Communication Manager and the Avaya SBCE. For the compliance test, *tcp* was used.
- Set the **Peer Detection Enabled** field to *y*. The **Peer-Server** field defaults to **Others**.
- Set the **Near-end Node Name** field 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** field to *ASBCE_A1*. This node name maps to the IP address of the private interface of the Avaya SBCE, as defined in **Section 5.3**.

change signaling-group 2		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? <u>n</u>	Transport Method: <u>tcp</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>		
Near-end Node Name: <u>procr</u>	Far-end Node Name: <u>ASBCE_A1</u>	
Near-end Listen Port: <u>5060</u>	Far-end Listen Port: <u>5060</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. The default well-known port value for SIP over TCP is 5060. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5060**.
- 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 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, these resources may be depleted during high call volume preventing additional calls from completing.
- Set **Enable Layer 3 Test** to **y**. This will enable Communication Manager to send SIP OPTIONS to the Avaya SBCE and subsequently to Alestra, to monitor the health of the SIP trunk.
- 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** field to the signaling group shown in the previous step.
- 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.

```
change trunk-group 2                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 2      Group Type: sip      CDR Reports: y
Group Name: Alestra      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: 10
```

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. For the compliance test, the default value of **600** seconds was used.

```
change 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 *public*. 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 enabled CPN block.

change 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>public</u>		
UII 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** field set to the default value *n*. Alestra does not support Network Call Redirection methods using “REFER” or “302 Temporarily Unavailable” messages. Set **Send Diversion Header** to *y* and the **Support Request History** field to *n*. Set the **Telephone Event Payload Type** field 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.

change 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>y</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>		

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected in the trunk group to define the format of this number (**Section 5.7**), use the **change public-unknown-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) and they are used to authenticate the caller with the Service Provider. In the sample configuration, five DID numbers were assigned for testing. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from these extensions.

change public-unknown-numbering 1					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	55001	2	8111111234	10	Total Administered: 14 Maximum Entries: 9999 Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
5	55002	2	8111111235	10	
5	55003	2	8111111236	10	
5	55004	2	8111111237	10	
5	55005	2	8111111238	10	
—	—	—	—	—	

5.9. Inbound Routing

DID numbers received from Alestra can be mapped to internal extensions or Vector Directory Numbers (VDNs) on the enterprise, 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	1234	4	55001	
public-ntwrk	4	1235	4	55002	
public-ntwrk	4	1236	4	55003	
public-ntwrk	4	1237	4	55004	
public-ntwrk	4	1238	4	55005	
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						Page 1 of 12
			Location: all			Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	1	attd							
1	5	ext							
2	5	ext							
3	4	ext							
4	5	ext							
5	5	ext							
6	3	dac							
7	5	ext							
8	5	ext							
9	1	fac							
*	3	dac							
#	3	dac							

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

change feature-access-codes				Page 1 of 10	
FEATURE ACCESS CODE (FAC)					
Abbreviated Dialing List1		Access Code:		<u>*10</u>	
Abbreviated Dialing List2		Access Code:		<u>*12</u>	
Abbreviated Dialing List3		Access Code:		<u>*13</u>	
Abbreviated Dial - Prgm Group List		Access Code:		<u>*14</u>	
Announcement		Access Code:		<u>*19</u>	
Answer Back		Access Code:		<u> </u>	
Auto Alternate Routing (AAR)		Access Code:		<u>*00</u>	
Auto Route Selection (ARS) - Access Code 1:		<u>9</u>		Access Code 2: <u> </u>	
Automatic Callback Activation:		<u>*33</u>		Deactivation: <u>#33</u>	
Call Forwarding Activation Busy/DA:		<u>*30</u>		All: <u>*31</u> Deactivation: <u>#30</u>	
Call Forwarding Enhanced Status:		<u> </u>		Act: <u> </u> Deactivation: <u> </u>	

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 Req'd			
00	12	22	2	intl		n			
001	13	13	2	intl		n			
01	12	12	2	natl		n			
040	3	3	2	svcl		n			
2	8	8	2	hnpa		n			
8	8	8	2	hnpa		n			
						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 for the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 2 was used.
- **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.
- Default values were used for all other fields.

change route-pattern 2														Page	1 of	3				
Pattern Number: 2														Pattern Name: Alestra						
SCCAN? n														Secure SIP? n						
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC							
No			Mrk	Lmt	List	Del	Dgts					QSIG								
												Intw								
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	No.	Numbering	LAR
0 1 2 M 4 W Request																		Dgts	Format	
														Subaddress						
1:	y	y	y	y	y	n	n	rest							none					

6. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, the Avaya SBCE is used as the edge device between the Avaya CPE and the Alestra Enlace IP SIP Trunk service. It is assumed that the initial installation of the Avaya SBCE and the assignment of the management interface IP Address have already been completed; hence these tasks are not covered in these Application Notes. For more information on the SBC installation and initial provisioning, consult the Avaya SBCE documentation listed in the **References** section.

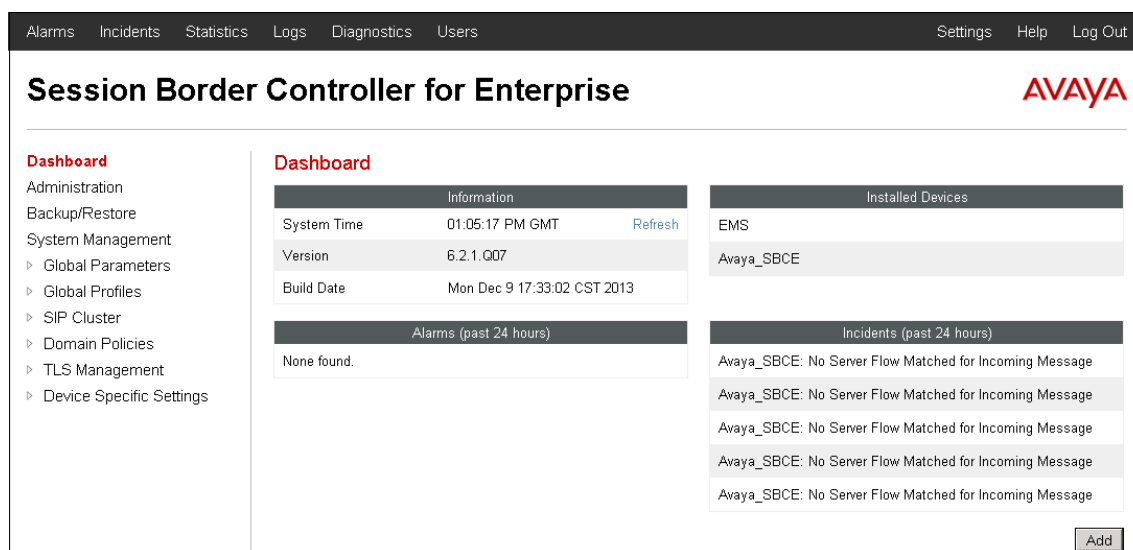
6.1. System Access

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 in red 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 disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." This is followed by a statement: "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials." Below that, it says: "All users must comply with all corporate instructions regarding the protection of information assets." At the very bottom, the copyright notice reads: "© 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.



The dashboard has a top navigation bar with links: Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. On the left is a navigation pane with "Dashboard" selected, and sub-items: Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled "Dashboard" and contains three sections: "Information" with a table of system details, "Installed Devices" with a table listing devices, and "Alarms (past 24 hours)" and "Incidents (past 24 hours)" sections, both showing "None found." An "Add" button is at the bottom right.

Information	
System Time	01:05:17 PM GMT Refresh
Version	6.2.1.Q07
Build Date	Mon Dec 9 17:33:02 CST 2013

Installed Devices
EMS
Avaya_SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
Avaya_SBCE: No Server Flow Matched for Incoming Message
Avaya_SBCE: No Server Flow Matched for Incoming Message
Avaya_SBCE: No Server Flow Matched for Incoming Message
Avaya_SBCE: No Server Flow Matched for Incoming Message
Avaya_SBCE: No Server Flow Matched for Incoming Message

6.2. 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 **Avaya_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.

Session Border Controller for Enterprise

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

SIP Cluster

Domain Policies

TLS Management

Device Specific Settings

System Management

Devices

Updates

SSL VPN

Licensing

Device Name (Serial Number)	Management IP	Version	Status	
Avaya_SBCE (PES37020432)	192.168.10.70	6.2.1.Q07	Commissioned	Reboot Shutdown Restart Application View Edit Delete

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 and the network settings. Note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces for the Avaya SBCE. The highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to Alestra.

System Information: Avaya_SBCE

General Configuration

Appliance Name	Avaya_SBCE
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.5.5.72	10.5.5.72	255.255.255.0	10.5.5.254	A1
172.16.157.151	172.16.157.151	255.255.255.0	172.16.157.129	B1
10.5.5.73	10.5.5.73	255.255.255.0	10.5.5.254	A1
172.16.157.146	172.16.157.146	255.255.255.0	172.16.157.129	B1
172.16.157.145	172.16.157.145	255.255.255.0	172.16.157.129	B1

DNS Configuration

Primary DNS	172.16.216.122
Secondary DNS	10.10.153.242
DNS Location	DMZ
DNS Client IP	172.16.157.148

Management IP(s)

IP	192.168.10.70
----	---------------

6.3. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

6.3.1. 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, Communication Manager functions as the Call Server and the Alestra SIP Proxy as the Trunk Server.

To configure the interworking profile in the enterprise direction, select **Global Profiles** → **Server Interworking** on the left navigation pane. Click **Add**.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left navigation pane is expanded to 'Global Profiles' > 'Server Interworking'. The main content area is titled 'Interworking Profiles: cs2100'. It features an 'Add' button and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this, there are tabs for 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is selected, showing a table of interworking parameters.

General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No

Enter a descriptive name for the new profile. Click **Next**.

The 'Interworking Profile' dialog box is shown. It has a title bar with 'Interworking Profile' and a close button 'X'. Inside, there is a text input field labeled 'Profile Name' with the value 'Com. Manager' entered. Below the field is a 'Next' button.

On the **General** screen, check the **T.38 Support** box. All other parameters retain their default values. Click **Next**.

Interworking Profile	
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
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Back Next

Click **Next** on the **Privacy/DTMF** and **SIP Timers/Transport Timers** tabs (not shown). On the **Advanced Settings** tab, uncheck the **Topology Hiding: Change Call-ID** box and check the **AVAYA Extensions** box. Click **Finish** to save and exit.

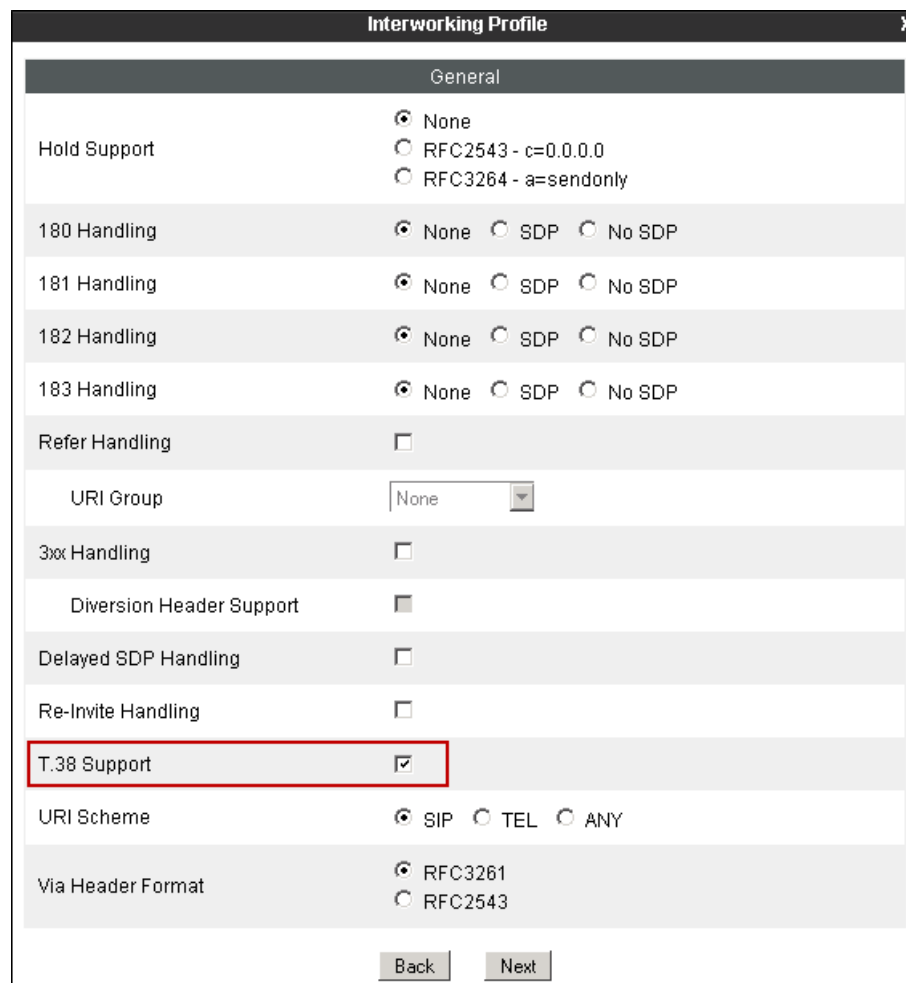
Interworking Profile	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include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

A second interworking profile named **Service Provider** in the direction of the SIP trunk to Alestra was similarly created. For this profile default values were used for all parameters except for **T.38 Support**, which was enabled.



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.

General tab:



The screenshot shows the "General" tab of the "Interworking Profile" dialog box. The tab is titled "General" and has a close button (X) in the top right corner. The settings are as follows:

Setting	Value
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
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

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

Advanced Settings tab:

Interworking Profile

Record Routes

☐ None

☐ Single Side

☒ Both Sides

Topology Hiding: Change Call-ID

☒

Call-Info NAT

☐

Change Max Forwards

☒

Include End Point IP for Context Lookup

☐

OCS Extensions

☐

AVAYA Extensions

☐

NORTEL Extensions

☐

Diversion Manipulation

☐

Diversion Header URI

Metaswitch Extensions

☐

Reset on Talk Spurt

☐

Reset SRTP Context on Session Refresh

☐

Has Remote SBC

☒

Route Response on Via Port

☐

Cisco Extensions

☐

Back

Finish

6.3.2. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform a granular header manipulation on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult [6] on the **References** section for more information on this topic.

A Sigma script was created during the compliance test to remove the “Remote-Address” header, used by the Avaya SBCE, from all outbound messages. This header contains private IP addresses that should not be propagated outside the enterprise limits.

Note: Additional Avaya SBCE header manipulation will be performed by implementing Signaling Rules, in **Section 6.4.1** later in this document.

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. The screen below shows the finished Signaling Manipulation script named *Remote_Address*.

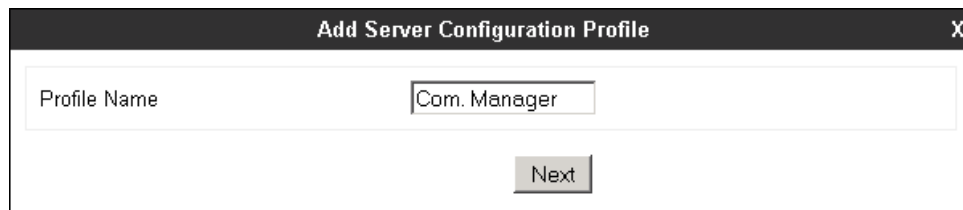
The screenshot displays the Avaya Session Border Controller for Enterprise web interface. On the left, a navigation menu shows 'System Management' with sub-items like 'Global Parameters', 'Global Profiles', and 'Signaling Manipulation' (highlighted in red). The main content area is titled 'Signaling Manipulation' and contains a list of scripts: 'Request_URI', 'T38MaxRate', 'OTG', 'Remove_Audio...', 'T.38', 'Remove phone...', 'Frontier script', 'Max-Forwards...', 'Frontier Script 2', 'Axtel Outbound', and 'Remote_Addr...' (highlighted in red). An 'Add' button is visible above the list. The script editor shows a Sigma script for removing the 'Remote-Address' header from outbound INVITE and 200 OK messages. The script text is:

```
//Remove Remote-Address header in outbound INVITE and 200 OK
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Remote-Address"])[1];
  }
}
```

 An 'Edit' button is located below the script text. At the top right of the main area, there are buttons for 'Download', 'Clone', and 'Delete'.

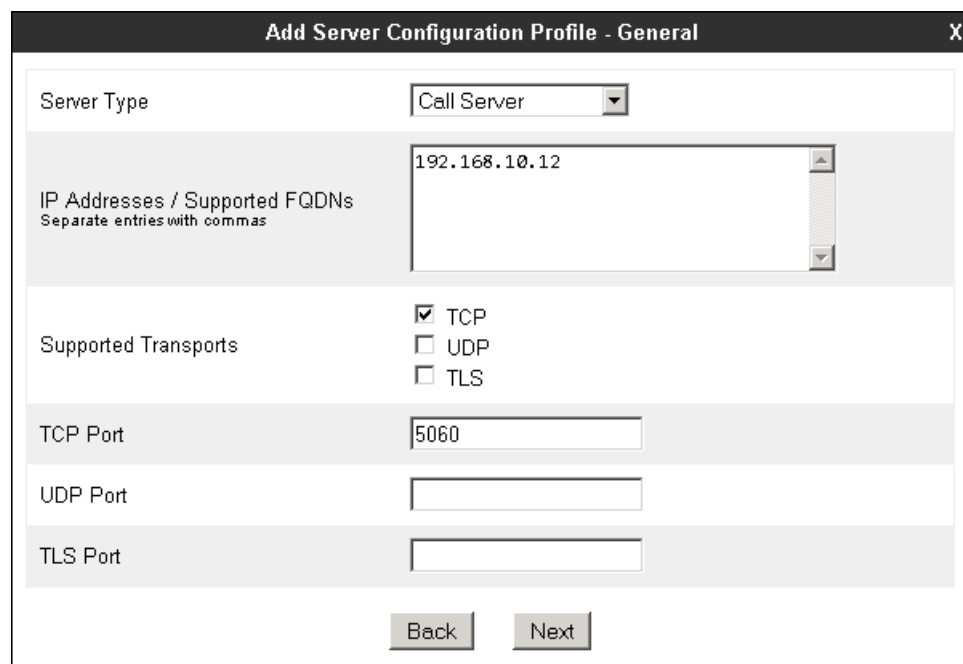
6.3.3. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE two peers, i.e., Communication Manager (Call Server) and the SIP Proxy at the service provider's network (Trunk Server). 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" 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 "Com. Manager". Below this field is a "Next" button.

On the **Add Server Configuration Profile - General** Tab select *Call Server* from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field, enter the IP address of the Communication Manager **procr** interface, as defined in **Section 5.3**. Select **TCP** for **Supported Transports**, and enter **5060** under **TCP Port**. The transport protocol and port selected here must match the values defined for the Communication Manager signaling group form in **Section 5.6**. Click **Next**.

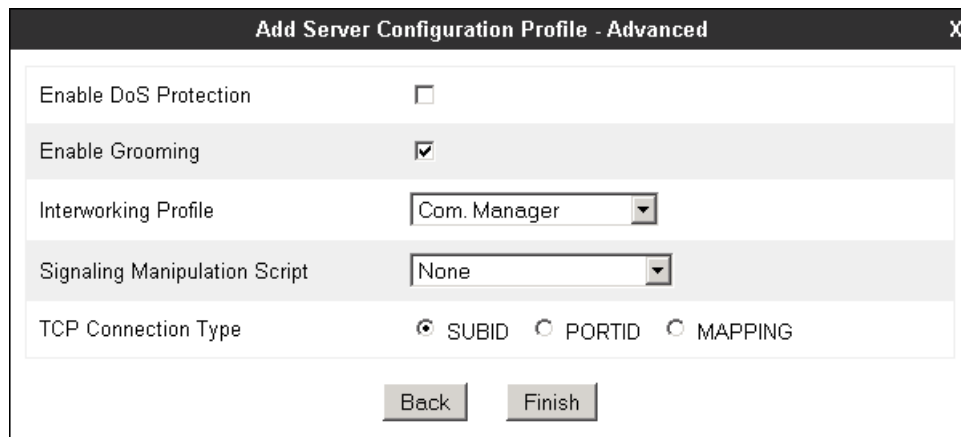


The screenshot shows a dialog box titled "Add Server Configuration Profile - General" with a close button (X) in the top right corner. The dialog contains several fields and checkboxes:

- Server Type**: A dropdown menu set to "Call Server".
- IP Addresses / Supported FQDNs**: A text area containing "192.168.10.12". Below the text area is the instruction "Separate entries with commas".
- Supported Transports**: Three checkboxes: ☒ TCP, ☐ UDP, and ☐ TLS.
- TCP Port**: A text input field containing "5060".
- UDP Port**: An empty text input field.
- TLS Port**: An empty text input field.

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 **Com. Manager** from the **Interworking Profile** drop down menu. Click **Finish**.

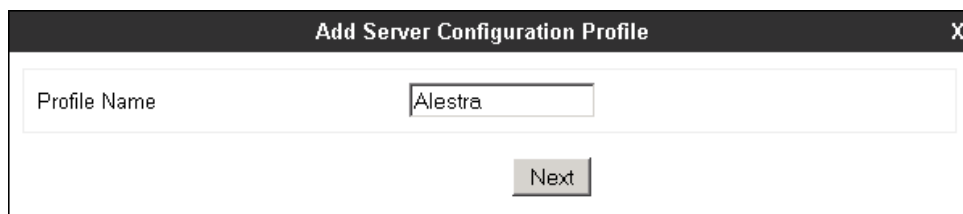


The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced" with a close button (X) in the top right corner. The dialog contains the following settings:

- Enable DoS Protection: ☐
- Enable Grooming: ☒
- Interworking Profile: Com. Manager (selected from a dropdown menu)
- Signaling Manipulation Script: None (selected from a dropdown menu)
- TCP Connection Type: ☒ SUBID, ☐ PORTID, ☐ MAPPING

At the bottom of the dialog are two buttons: "Back" and "Finish".

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**.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. The dialog contains the following settings:

- Profile Name: Alestra (entered in a text field)

At the bottom of the dialog is a button labeled "Next".

On the **Add Server Configuration Profile-General** Tab select **Trunk Server** from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field, enter the IP address of the Alestra SIP proxy server. Select **UDP** for **Supported Transports**, and enter **5060** under **UDP Port**, as specified by Alestra.

The screenshot shows the 'Add Server Configuration Profile - General' dialog box. It has a title bar with 'Add Server Configuration Profile - General' and a close button 'X'. The form contains the following fields and options:

- Server Type:** A dropdown menu with 'Trunk Server' selected.
- IP Addresses / Supported FQDNs:** A text area with '192.168.145.9' entered. Below the text area is the label 'Separate entries with commas'.
- Supported Transports:** Three checkboxes: 'TCP' (unchecked), 'UDP' (checked), and 'TLS' (unchecked).
- TCP Port:** An empty text input field.
- UDP Port:** A text input field containing '5060'.
- TLS Port:** An empty text input field.
- At the bottom are two buttons: 'Back' and 'Next'.

Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, select **Service Provider** from the **Interworking Profile** drop down menu. Under **Signaling Manipulation Script**, select the **Remote_Address** script created in **Section 6.3.2**. Click **Finish**.

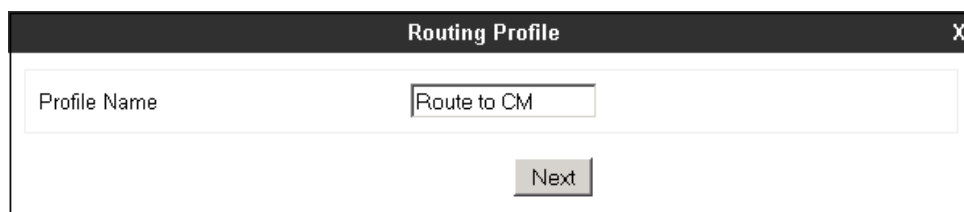
The screenshot shows the 'Add Server Configuration Profile - Advanced' dialog box. It has a title bar with 'Add Server Configuration Profile - Advanced' and a close button 'X'. The form contains the following fields and options:

- 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 'Remote_Address' selected.
- UDP Connection Type:** Three radio buttons: 'SUBID' (selected), 'PORTID' (unchecked), and 'MAPPING' (unchecked).
- At the bottom are two buttons: 'Back' and 'Finish'.

6.3.4. Routing Profiles

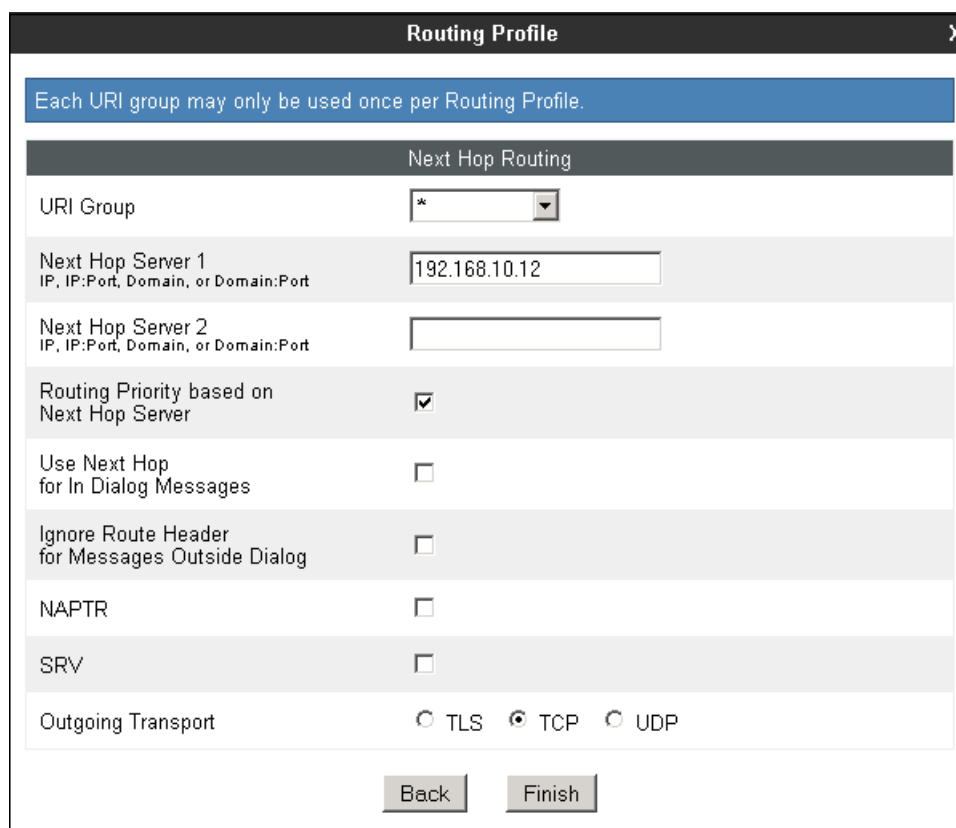
Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces.

Two Routing Profiles were created in the test configuration, one for inbound calls, with Communication Manager as the destination, and the second one for outbound calls, which are routed to the Alestra SIP trunk. 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 screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "Route to CM". Below the input field is a button labeled "Next".

On the **Next Hop Routing** tab, enter the IP Address of Communication Manager as **Next Hop Server 1**. Since the default well-known port value of 5060 for TCP was used, it is not necessary to enter the port number here. Check **Routing Priority based on Next Hop Server**. Choose **TCP** for **Outgoing Transport**. Click **Finish**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Below the title bar is a blue banner with the text "Each URI group may only be used once per Routing Profile." Below this is a section titled "Next Hop Routing". Inside this section, there are several fields and checkboxes:

- URI Group: A dropdown menu with an asterisk (*) as the selected option.
- Next Hop Server 1: A text input field containing "192.168.10.12". Below the field is the label "IP, IP:Port, Domain, or Domain:Port".
- Next Hop Server 2: An empty text input field. Below the field is the label "IP, IP:Port, Domain, or Domain:Port".
- Routing Priority based on Next Hop Server: A checkbox that is checked.
- Use Next Hop for In Dialog Messages: An unchecked checkbox.
- Ignore Route Header for Messages Outside Dialog: An unchecked checkbox.
- NAPTR: An unchecked checkbox.
- SRV: An unchecked checkbox.
- Outgoing Transport: Three radio buttons labeled "TLS", "TCP", and "UDP". The "TCP" radio button is selected.

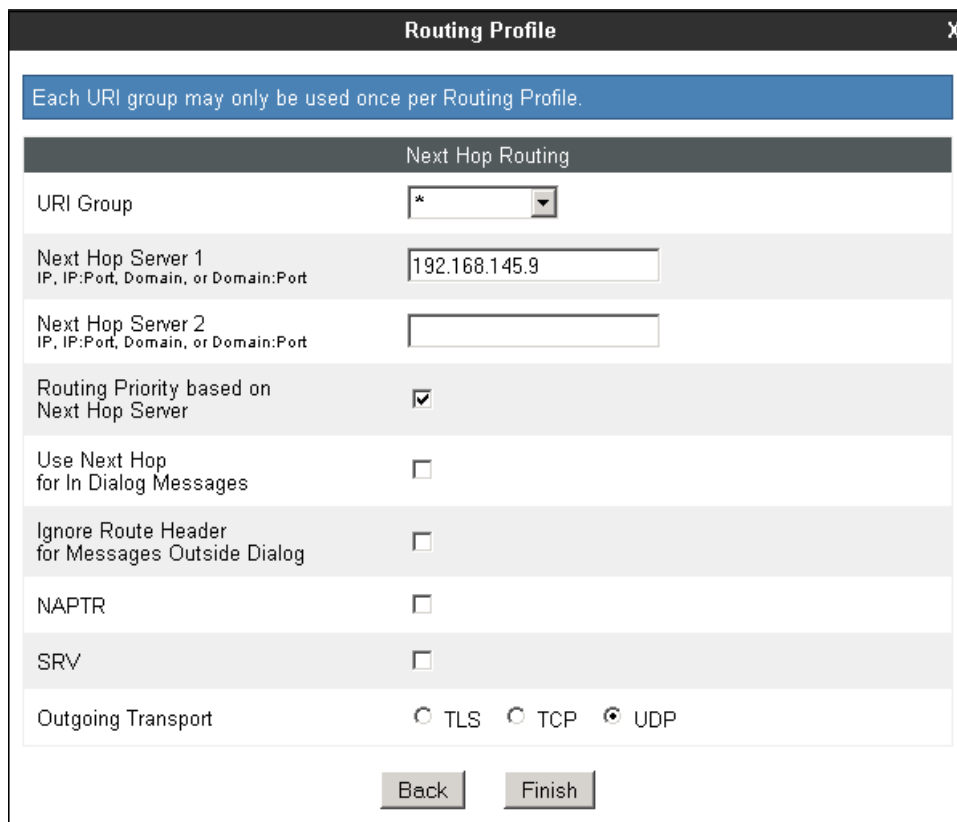
At the bottom of the window are two buttons: "Back" and "Finish".

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**. 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 labeled 'Profile Name' containing the text 'Route to Alestra'. Below the input field is a 'Next' button.

On the Next Hop Routing tab, enter the IP address of the service provider SIP proxy server as **Next Hop Server 1**. Since the default well-known port value of 5060 for UDP was used, it is not necessary to enter the port number here. Check the **Routing Priority based on Next Hop Server**. Choose **UDP** for **Outgoing Transport**. Click **Finish**.



The image shows the 'Routing Profile' dialog box with the 'Next Hop Routing' tab selected. At the top, a blue banner reads 'Each URI group may only be used once per Routing Profile.' Below this is a 'Next Hop Routing' section. It contains a 'URI Group' dropdown menu with an asterisk '*' selected. Below that are two text input fields for 'Next Hop Server 1' (containing '192.168.145.9') and 'Next Hop Server 2' (empty). Below these are several checkboxes: 'Routing Priority based on Next Hop Server' (checked), 'Use Next Hop for In Dialog Messages' (unchecked), 'Ignore Route Header for Messages Outside Dialog' (unchecked), 'NAPTR' (unchecked), and 'SRV' (unchecked). At the bottom, there are radio buttons for 'Outgoing Transport': 'TLS' (unchecked), 'TCP' (unchecked), and 'UDP' (checked). At the very bottom are 'Back' and 'Finish' buttons.

6.3.5. 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, 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.

To add the **Topology Hiding Profile** in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side and click the **Add** button (not shown). Enter a **Profile Name** such as the one shown below. Click **Next**.



On the **Topology Hiding Profile** screen, click the **Add Header** button repeatedly to show the rest of the headers in the profile.



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

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

A Topology Hiding profile named **Service Provider** was similarly configured in the direction of the SIP trunk to Alestra. During the compliance test, IP addresses instead of domains were used in all SIP messages between the Alestra 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.

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

6.4. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

In the reference configuration, only a new Signaling Rule was defined. All other rules under Domain Policies, linked together on End Point Policy Groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. 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.

6.4.1. Signaling Rules

A Signaling Rule was created in the sample configuration to remove (block) the AV-Global-Session-ID and the Alert-Info headers. These headers are sent in SIP messages from Communication Manager to the Avaya SBCE. They contain private IP addresses and SIP domains from the enterprise, which should not be propagated outside of the enterprise boundaries.

In the **Domain Policies** menu on the left-hand side, select **Signaling Rules**, then **Add Rule** (not shown). Enter an appropriate name like in the example below. Click **Next**.



Signaling Rule		X
Rule Name	<input type="text" value="GSID-Alert-Info"/>	
		<input type="button" value="Next"/>

On the next three pages (not shown), leave sections **Inbound**, **Outbound** and **Content-Type Policies** with their default values. Click **Next**. On the **Signaling QoS** tab, default values were used. Click **Finish**.

On the newly created **GSID-Alert-Info** Signaling Rule, select the **Request Headers** tab to create the manipulations performed on request messages. Select **Add In Header Control**.

Signaling Rules: GSID-Alert-Info

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

Click here to add a description.

Tabs: General, Requests, Responses, **Request Headers**, Response Headers, Signaling QoS, UCID

Buttons: Add In Header Control, Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
No request header controls exist.						

In the **Add Header Control** screen select the following:

- **Header Name: Alert-Info**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove header**
- Click **Finish**

Add Header Control [X]

Proprietary Request Header ☐

Header Name: Alert-Info

Method Name: ALL

Header Criteria:

- ☒ Forbidden
- ☐ Mandatory
- ☐ Optional

Presence Action: Remove header

486 Busy Here

Finish

Select **Add In Header Control** again to similarly configure the header control rule or the AV-Global-Session-ID header. In this case, make sure to check the **Proprietary Request Header** box in the **Add Header Control** tab. This will allow typing the name of the specific header on the **Header Name** box. Once completed, the **Request Headers** tab should look like the following screen.

General		Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
					Add In Header Control	Add Out Header Control	
Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	
1	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
2	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit Delete

Select the **Response Headers** tab to similarly create the manipulations performed on response messages. Select **Add In Header Control** (not shown).

The screen below shows the settings for the Alert-Info header on response messages.

Add Header Control
X

Proprietary Response Header
☐

Header Name
Alert-Info

Response Code
2XX

Method Name
ALL

Header Criteria
☒ Forbidden
☐ Mandatory
☐ Optional

Presence Action
Remove header

486
Busy Here

Finish

Select **Add In Header Control** again to similarly configure the header control rule or the AV-Global-Session-ID header. In this case, make sure to check the **Proprietary Request Header** box in the **Add Header Control**. This will allow typing the name of the specific header on the **Header Name** box. Once completed, the **Response Headers** tab should look like the following screen.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID			
				Add In Header Control	Add Out Header Control				
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Alert-Info	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete

6.4.2. End Point Policy Groups

End Point Policy Groups associate the different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

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

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

Policy Group

Group Name

Enterprise

Next

In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration, with the exception of the **Signaling Rule**, where the *GSID-Alert-Info* rule created in **Section 6.4.1** was selected. Click **Finish**.

The screenshot shows a 'Policy Group' configuration window with a close button (X) in the top right corner. It contains six rows, each with a rule type and a dropdown menu:

- Application Rule: default-trunk
- Border Rule: default
- Media Rule: default-low-med
- Security Rule: default-low
- Signaling Rule: GSID-Alert-Info
- Time of Day Rule: default

At the bottom of the window are two buttons: 'Back' and 'Finish'.

The screen below shows the **Enterprise** End Point Policy Group after the configuration was completed.

Policy Group

Summary

Add

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default-trunk	default	default-low-med	default-low	GSID-Alert-Info	default	Edit	Clone

A second End Point Policy Group was created for the service provider, repeating the steps described above. Defaults were used in this case for all fields. The screen below shows the **Service Provider** End Point Policy Group after the configuration was completed.

Policy Group

Summary

Add

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default-trunk	default	default-low-med	default-low	default	default	Edit	Clone

6.5. Device Specific Settings

The **Device Specific Settings** determine server specific parameters that determine how the device will work when deployed on the network. Among parameters defined here are IP addresses, media and signaling interfaces, call flows, etc.

6.5.1. 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 made here.

Select **Network Management** from **Device Specific Settings** on the left-side menu (not shown). Under **Devices** in the center pane, select the device being managed, **Avaya_SBCE** in the sample configuration. On the **Network Configuration** tab, verify or enter the network information as needed. Note that the **A1** interface is used for the internal side and **B1** is used for the external side of the Avaya SBCE.

The screenshot displays the 'Network Management: Avaya_SBCE' web interface. On the left, a sidebar shows 'Devices' with 'Avaya_SBCE' selected. The main area has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. An orange warning banner states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from [System Management](#).' Below this, there are four input fields for netmasks: 'A1 Netmask' (255.255.255.0), 'A2 Netmask' (empty), 'B1 Netmask' (255.255.255.0), and 'B2 Netmask' (empty). An 'Add' button is to the left of the 'B1' and 'B2' fields, and 'Save' and 'Clear' buttons are to the right. Below the netmask fields is a table with four columns: 'IP Address', 'Public IP', 'Gateway', and 'Interface'. The table contains two rows of data. The first row has '10.5.5.72' for IP Address, an empty field for Public IP, '10.5.5.254' for Gateway, and 'A1' for Interface, with a 'Delete' link. The second row has '172.16.157.151' for IP Address, an empty field for Public IP, '172.16.157.129' for Gateway, and 'B1' for Interface, with a 'Delete' link.

IP Address	Public IP	Gateway	Interface	
10.5.5.72		10.5.5.254	A1	Delete
172.16.157.151		172.16.157.129	B1	Delete

Note: some customer deployments may use a router, firewall or some other kind of network device between the Avaya SBCE and the service provider's network. These customers may decide to assign IP addresses to the public and private sides of the Avaya SBCE that are both in the same private subnet of the enterprise. In these particular cases, the same physical interface (A1, for example) can be assigned to both the private and public sides of the Avaya SBCE. The rest of the configuration process, like the creation of separate Media Interfaces, Signaling Interfaces, etc. as specified in the next sections of this document still remains the same.

On the **Interface Configuration** tab, verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. Click the **Toggle** buttons if necessary to enable the interfaces.

<div>Devices</div> <div>Avaya_SBCE</div>	Network Configuration		Interface Configuration
	Name		Administrative Status
	A1	Enabled	Toggle
	A2	Disabled	Toggle
	B1	Enabled	Toggle
	B2	Disabled	Toggle

6.5.2. Media Interface

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 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 **Avaya_SBCE** device and click the **Add** button (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. The **Port Range** was left at the default values of **35000-40000**. Click **Finish**.

Add Media Interface

X

Name

Private_med

IP Address

10.5.5.72

Port Range

35000 - 40000

Finish

A second Media Interface facing the public network side was similarly created with the name **Public_med**, as shown below. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. The **Port Range** was left at the default values.

Add Media Interface

X

Name

Public_med

IP Address

172.16.157.151

Port Range

35000 - 40000

Finish

Once the configuration is complete, the **Media Interface** screen will appear as follows.

Media Interface: Avaya_SBCE

Devices

Avaya_SBCE

Media Interface

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

Add

Name	Media IP	Port Range	
Private_med	10.5.5.72	35000 - 40000	Edit Delete
Public_med	172.16.157.151	35000 - 40000	Edit Delete

6.5.3. Signaling Interface

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in both the inside and outside 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 **Avaya_SBCE** device and click the **Add** button (not shown). On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. Enter **5060** for **TCP Port**, since TCP port 5060 is used to listen to signaling traffic from Communication Manager in the sample configuration. Click **Finish**.

Add Signaling Interface

Name: Private_sig

IP Address: 10.5.5.72

TCP Port: 5060
Leave blank to disable

UDP Port:
Leave blank to disable

Enable Stun: ☐

TLS Port:
Leave blank to disable

TLS Profile: AvayaSBCServer

Enable Shared Control: ☐

Shared Control Port:

Finish

A second Signaling Interface with the name **Public_sig** was similarly created in the network direction. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. Under **UDP Port**, enter **5060** since this is the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic.

Add Signaling Interface
X

Name

IP Address

TCP Port
Leave blank to disable

UDP Port
Leave blank to disable

Enable Stun

☐

TLS Port
Leave blank to disable

TLS Profile

Enable Shared Control

☐

Shared Control Port

Once the configuration is complete, the **Signaling Interface** screen will appear as follows:

Signaling Interface: Avaya_SBCE

Devices

Avaya_SBCE

Signaling Interface

Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	10.5.5.72	5060	---	---	None	Edit Delete
Public_sig	172.16.157.151	---	5060	---	None	Edit Delete

6.5.4. 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.

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 **Com. Manager Flow** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection, which is the reverse route of the flow. Click **Finish**.

Edit Flow: Com. Manager Flow	
Flow Name	Com. Manager Flow
Server Configuration	Com. 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
File Transfer Profile	None
Finish	

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 the **Routing Profile** selection, which is the reverse route of the flow. Click **Finish**.

Edit Flow: SIP Trunk Flow X

Flow Name	<input type="text" value="SIP Trunk Flow"/>
Server Configuration	<input type="text" value="Alestra"/>
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 CM"/>
Topology Hiding Profile	<input type="text" value="Service Provider"/>
File Transfer Profile	<input type="text" value="None"/>

The two Server Flows created in the sample configuration are summarized on the screen below:

End Point Flows: Avaya_SBCE

Devices

Avaya_SBCE

Subscriber Flows

Server Flows

Server Configuration: Alestra

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SIP Trunk Flow	*	Private_sig	Public_sig	Service Provider	Route to CM	View Clone Edit Delete

Server Configuration: Com. Manager

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Com. Manager Flow	*	Public_sig	Private_sig	Enterprise	Route to Alestra	View Clone Edit Delete

7. Alestra Enlace IP SIP Trunk Configuration

Alestra is responsible for the configuration of the Alestra Enlace IP SIP Trunk 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 Alestra 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 and the Avaya SBCE discussed in the previous sections.

8. 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.

8.1. 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.

8.2. 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.

8.3. 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: Provides information about the health of the Avaya SBCE.

The screenshot shows the 'Alarm Viewer' page in a web browser. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', and 'Help'. The 'Alarms' tab is selected. The page title is 'Alarm Viewer' with the Avaya logo on the right. On the left, there is a 'Devices' sidebar with 'EMS' and 'Avaya_SBCE' listed. The main area shows a table with columns: ID, Details, State, Time, and Device. A message states 'No alarms found for this device.' Below the table are 'Clear Selected' and 'Clear All' buttons.

Incidents : Provides detailed reports of anomalies, errors, policies violations, etc.

The screenshot shows the 'Incident Viewer' page in a web browser. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', and 'Help'. The 'Incidents' tab is selected. The page title is 'Incident Viewer' with the Avaya logo on the right. Below the title, there are filters for 'Device' (set to 'All') and 'Category' (set to 'All'), a 'Clear Filters' button, and 'Refresh' and 'Generate Report' buttons. A message states 'Displaying results 1996 to 2000 out of 2000.' Below this is a table with columns: Type, ID, Date, Time, Category, Device, and Cause. The table contains five rows of 'Message Dropped' incidents. At the bottom, there are pagination controls showing '<<', '<', '130', '131', '132', '133', '134', '>', and '>>'.

Type	ID	Date	Time	Category	Device	Cause
Message Dropped	700843420678324	6/2/14	5:27 AM	Policy	Avaya_SBCE	No Server Flow Matched for Incoming Message
Message Dropped	700843395024023	6/2/14	5:26 AM	Policy	Avaya_SBCE	No Server Flow Matched for Incoming Message
Message Dropped	700843371324294	6/2/14	5:25 AM	Policy	Avaya_SBCE	No Server Flow Matched for Incoming Message
Message Dropped	700843327298321	6/2/14	5:24 AM	Policy	Avaya_SBCE	No Server Flow Matched for Incoming Message
Message Dropped	700843321661703	6/2/14	5:24 AM	Policy	Avaya_SBCE	No Server Flow Matched for Incoming Message

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

Alarms Incidents Statistics Logs **Diagnostics** Users Settings He

https://192.168.10.70/~Diagnostics - Windows Internet Explorer

Diagnostics

AVAYA

Devices

Avaya_SBCE

Full Diagnostic Ping Test Application Protocol

Start Diagnostic

Task Description	Status
EMS Link Check	-
SBC Link Check: A1	-
SBC Link Check: B1	-
Ping: SBC (10.5.5.72) to Ping: Gateway (10.5.5.254)	-
Ping: SBC (10.5.5.72) to Ping: Primary DNS (172.16.216.122)	-
Ping: SBC (10.5.5.72) to Ping: Secondary DNS (172.16.153.242)	-
Ping: SBC (172.16.157.151) to Ping: Gateway (172.16.157.129)	-

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**.

Session Border Controller for Enterprise

AVAYA

Domain Policies TLS Management **Device Specific Settings**

Network Management Media Interface Signaling Interface Signaling Forking End Point Flows Session Flows Relay Services SNMP Syslog Management Advanced Options

Troubleshooting

Debugging **Trace** DoS

Trace: Avaya_SBCE

Devices

Avaya_SBCE

Call Trace **Packet Capture** Captures

Packet Capture Configuration

Status Ready

Interface Any

Local Address IP:Port All

Remote Address * : *Port, IP, IP:Port

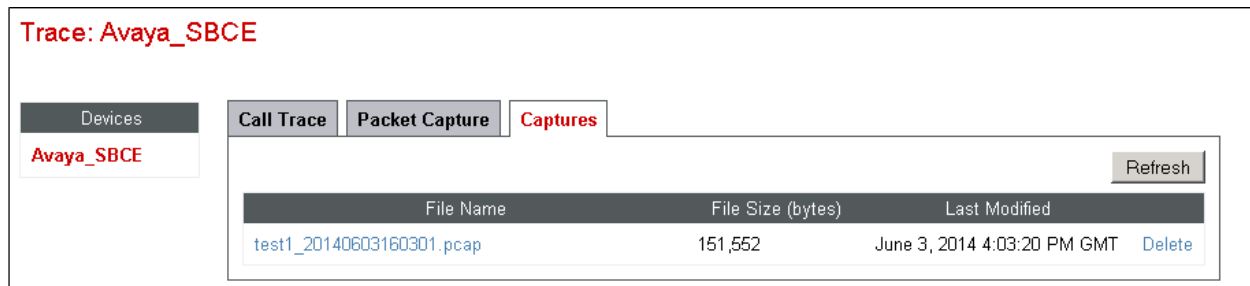
Protocol All

Maximum Number of Packets to Capture 10000

Capture Filename test1.pcap
Using the name of an existing capture will overwrite it.

Start Capture Clear

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.



9. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2, to connect to the Alestra Enlace IP SIP Trunk service, as shown in **Figure 1**.

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

10. References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.3, June 2014, Document Number 03-300509.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3, June 2014, Document Number 555-245-205.
- [3] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, June 2013
- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, January 2014
- [5] *Avaya Session Border Controller for Enterprise Release Notes*. Release 6.2. FP1, December 2013
- [6] *Administering Avaya one-X® Communicator*, Release 6.2, December 2013.
- [7] *Using Avaya one-X® Communicator*, Release 6.2, December 2013.
- [8] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>.
- [9] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

©2014 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.