



Application Notes for Configuring Avaya Aura® Solution for Midsize Enterprise 6.2.2 and Avaya Session Border Controller for Enterprise 6.2 with Alestra Enlace IP SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the procedures 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® Solution for Midsize Enterprise 6.2.2 and Avaya Session Border Controller for Enterprise 6.2.

The Enlace IP 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.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	6
2.3.	Support	6
3.	Reference Configuration.....	7
4.	Equipment and Software Validated	10
5.	Configure Avaya Aura® Communication Manager.....	11
5.1.	Licensing and Capacity	11
5.2.	System Features.....	12
5.3.	IP Node Names.....	13
5.4.	Codecs.....	13
5.5.	IP Network Regions	14
5.6.	Signaling Group	15
5.7.	Trunk Group.....	17
5.8.	Calling Party Information.....	19
5.9.	Inbound Routing.....	19
5.10.	Outbound Routing	20
6.	Configure Avaya Aura® Session Manager	22
6.1.	System Manager Login and Navigation.....	23
6.2.	SIP Domain	24
6.3.	Locations	24
6.4.	SIP Entities.....	25
6.5.	Entity Links.....	29
6.6.	Routing Policies	30
6.7.	Dial Patterns	31
6.8.	Add/View Session Manager Instance	33
7.	Configure Avaya Session Border Controller for Enterprise.....	35
7.1.	System Access.....	35
7.2.	System Management	36
7.3.	Global Profiles.....	37
7.3.1.	Server Interworking	37
7.3.2.	Server Configuration.....	42
7.3.3.	Routing Profiles	45
7.3.4.	Topology Hiding.....	47
7.4.	Domain Policies	49
7.4.1.	Signaling Rules	49
7.4.2.	End Point Policy Groups.....	53
7.5.	Device Specific Settings.....	54
7.5.1.	Network Management.....	54
7.5.2.	Media Interface	55
7.5.3.	Signaling Interface.....	56

7.5.4. End Point Flows.....	58
8. Alestra Enlace IP SIP Trunk Service Configuration.....	60
9. Verification and Troubleshooting	60
9.1. General Verification Steps	60
9.2. Communication Manager Verification.....	60
9.3. Session Manager Verification	61
9.4. Avaya SBCE Verification	62
10. Conclusion	64
11. References.....	64

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 a HP® Proliant DL360 server running the Avaya Aura® Solution for Midsize Enterprise 6.2.2 template, an Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.2 and various Avaya endpoints.

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:

- Response to SIP OPTIONS queries.
- 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 to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones.
- Avaya one-X® Communicator supports placing and receiving calls using the local computer or by controlling an external telephone. Usage modes “This Computer” and “Other Phone” were tested. Avaya one-X® Communicator also supports two signaling protocols: H.323 and SIP. Each supported protocol was tested.
- Inbound and outbound PSTN calls to/from Avaya Flare® Experience for Windows softphones.
- 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:

- Inbound toll-free and emergency calls are supported but were not tested as part of the compliance test
- 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.

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 and limitations described below:

- **Calls to Busy Numbers:** Alestra does not send “486 Busy Here” for calls from an enterprise extension to busy PSTN numbers. Since busy tone is heard by the caller this observation has no impact to the user.
- **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.

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, private addresses are shown in these Application Notes for the Avaya SBCE and the Service Providers public network interfaces, instead of the real public IP addresses used during the tests. Also, PSTN routable phone numbers used in the compliance test have been changed to non-routable numbers.

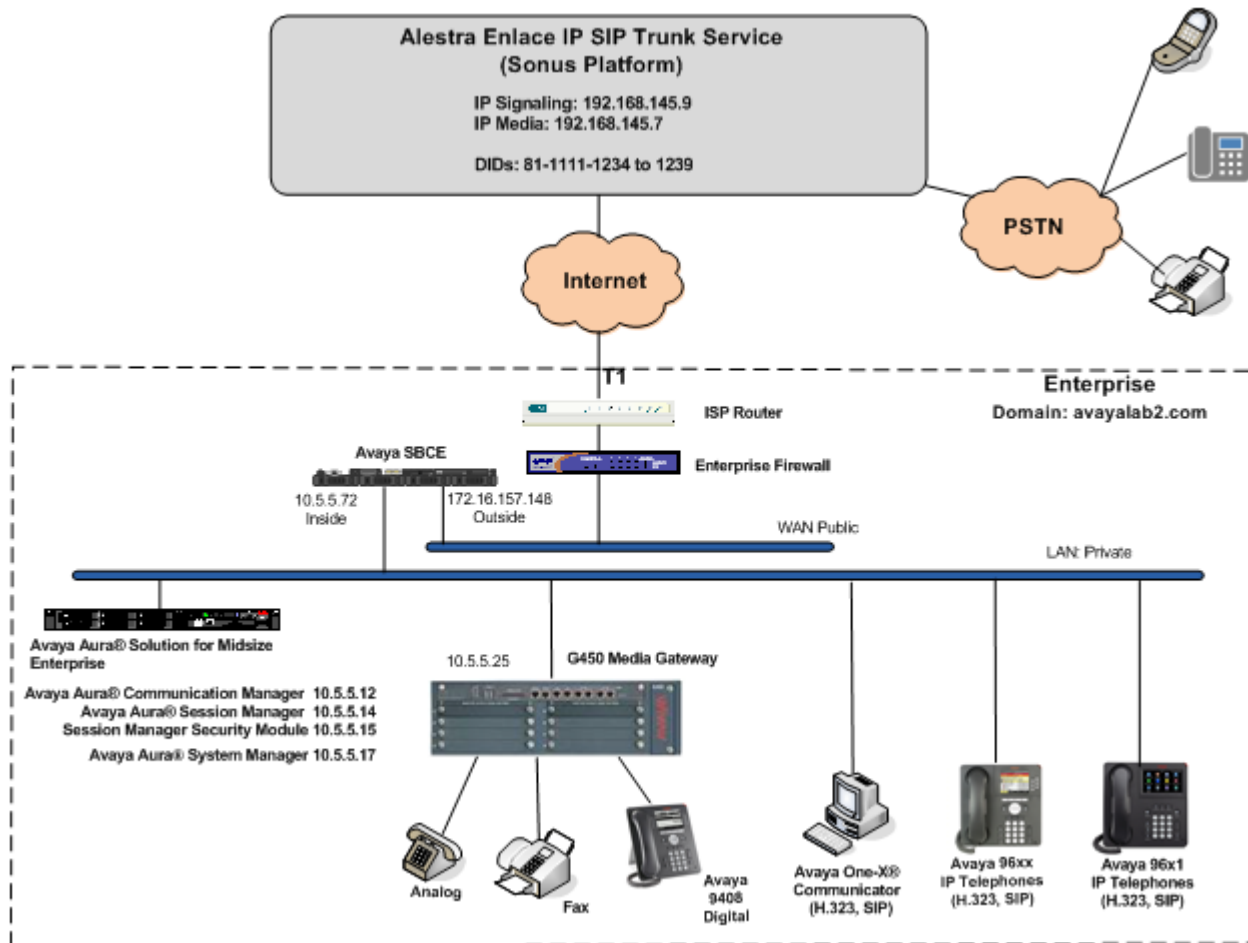


Figure 1: Avaya SIP Enterprise Solution connected to Alestra Enlace IP SIP Trunk Service

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

- Avaya Aura® Solution for Midsize Enterprise 6.2.2
- Avaya Session Border Controller for Enterprise 6.2
- Avaya G450 Media Gateway
- Avaya 96x0 and 96x1 Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator soft phones (H.323 and SIP)


- Avaya Flare® Experience for Windows softphones (SIP)
- Avaya digital and analog telephones

The Avaya Aura® Solution for Midsize Enterprise Release 6.2.2 Template delivers the following applications as virtual machines running on top of System Platform 6.3.0:

- Communication Manager 6.3.0
- Communication Manager Messaging 6.3.0
- Session Manager 6.3.2
- System Manager 6.3.2
- Presence Services 6.2.0
- Utility Services 6.3.0
- Application Enablement Services 6.3.0

These Application Notes will not cover the software installation of System Platform and the loading of the Midsize Enterprise Template. Consult the documentation on the **References** section for more information and instructions on the software installation of System Platform, the Midsize Enterprise Template and initial configuration.

The following screen shows the list of the applications installed and running on the server, as seen from the Virtual Machine Management screen in System Platform.



Avaya Aura® System Platform
 admin
Previous successful login: Wed Aug 14 17:43:16 EDT 2013
 Failed login attempts since: 1

[Home](#)
[About](#)
[Help](#)
[Log Out](#)


Virtual Machine Management

- Templates
- Manage
- View Install/Upgrade Log

Server Management







- System Information
- Patch Management**
- Download/Upload
- Manage
- Platform Upgrade
- Log Viewer
- Date / Time Configuration
- Logging Configuration
- System Configuration
- Network Configuration
- Static Route Configuration
- Ethernet Configuration
- Alarm Configuration
- Certificate Management
- License Management
- SAL Gateway Management
- High Availability

Virtual Machine Management

Virtual Machine List 

System Domain Uptime: 14 days, 3 hours, 44 minutes, 47 seconds

Current template installed: Midsize_Ent 6.2.2.0.1120 (smgr 6.3.8.0, aes 6.3.0.0.212, cm 06.3-03.0.124.0, utility_server 6.3.0.0.20, sm 6.3.2.0.632028, presence_va 6.2.0.0.0182) [Refresh](#)

	Name	Version	IP Address	Max Memory	Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.3.0.0.18002	10.5.5.10	864.0 MB	12	1d 16h 3m 39s	Running	N/A
✓	sm	6.3.2.0.632028	10.5.5.14	6.0 GB	6	1d 0h 26m 51s	Running	Running
✓ 	cm	06.3-03.0.124.0	10.5.5.12	4.5 GB	1	12h 49m 42s	Running	Running
✓ 	aes	6.3.0.0.212	10.5.5.18	4.0 GB	4	12h 26m 24s	Running	Running
✓ 	cdom	6.3.0.0.18002	10.5.5.11	512.0 MB	1	15h 6m 59s	Running	N/A
✓ 	utility_server	6.3.0.0.20	10.5.5.13	1024.0 MB	1	2h 51m 51s	Running	Running
✓ 	presence_va	6.2.0.0.0182	10.5.5.16	12.0 GB	6	4h 20m 53s	Running	N/A
✓ 	smgr	6.3.2.4.1529	10.5.5.17	9.0 GB	4	1d 22h 7m 16s	Running	Running

Note: Application Enablement and Presence Services are installed as part of the Midsize Enterprise Template, but since these applications were not used during the compliance testing, the configuration of these services is not covered in these Application Notes.

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise infrastructure. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE 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 the enterprise Session Manager across the enterprise IP network is TCP.

For inbound calls, the calls flow from the service provider to the external firewall, to the Avaya SBCE, then to Session Manager. Session Manager uses 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 arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be 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. The trunk carried both inbound and outbound traffic.

Communication Manager Messaging, defined as a separate SIP entity in Session Manager, was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of MWI (Message Waiting Indicator) messages to the enterprise telephones. Since the configuration tasks for Communication Manager Messaging are not directly related to the interoperability tests with the Alestra Enlace IP SIP trunk service, they are not included in these Application Notes.

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 calls to and from the PSTN to the enterprise.

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® Solution for Midsize Enterprise on a HP® Proliant DL360 G7 Server, including: <ul style="list-style-type: none">Avaya Aura® Communication ManagerAvaya Aura® Communication Manager MessagingAvaya Aura® System ManagerAvaya Aura® Session Manager	6.2.2.0.1120 (System Platform 6.3.0.0.18002) 6.3-03.0.124.0 6.3-26.0 6.3.0 -FP2 6.3.2.0.632028
Avaya Session Border Controller for Enterprise on a Dell R210 V2 Server	6.2.0.Q36
Avaya G450 Media Gateway	33.13.0
Avaya 96x0 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition 3.2
Avaya 96x1 Series IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 6.2.2.17
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition H.323 6.2.2 (SP2)
Avaya one-X® Communicator (H.323, SIP)	6.1.8.06-SP8-40314
Avaya Flare® Experience for Windows	1.1.3.14
Avaya 9408 Digital Telephone	2.00
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 Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Alestra Enlace IP SIP trunk service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from Alestra. It is assumed that the general installation of Communication Manager, the Avaya G450 Media Gateway and Session Manager 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 **12000** licenses are available and **263** 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	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:		128	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		36000	0
Maximum Video Capable IP Softphones:		18000	1
Maximum Administered SIP Trunks:		12000	263
Maximum Administered Ad-hoc Video Conferencing Ports:		12000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
Maximum TN2501 VAL Boards:		10	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 Session Manager Security module (**SM**). 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			
Acme_s0p0	192.168.10.53			
SM	10.5.5.15			
default	0.0.0.0			
me-aes	10.5.5.18			
procr	10.5.5.12			
procr6	::			

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. The Alestra Enlace IP SIP Trunk Service preferred codecs are 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	Packet Size(ms)	
1: G.729A	n	2	20	
2: G.711A	n	2	20	
3:				

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

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 trunks. 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 **avayalab2.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.
- 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: avayalab2.com
Name: Alestra SIP Trunk Stub Network Region: n
MEDIA PARAMETERS
Codec Set: 2 Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048 IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS RSVP Enabled? n
H.323 Link Bounce Recovery? 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	codec	direct	WAN-BW-limits		Video		Intervening		Dyn	G	A	t
rgn	set	WAN	Units	Total	Norm	Prio	Shr	Regions	CAC	R	L	c
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 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 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 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, **tcp** 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 with **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 **SM**. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**.

```

change signaling-group 2                                     Page 1 of 2
SIGNALING GROUP

Group Number: 2      Group Type: sip
IMS Enabled? n      Transport Method: tcp
Q-SIP? n
IP Video? n      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

Near-end Node Name: procr      Far-end Node Name: SM
Near-end Listen Port: 5062      Far-end Listen Port: 5062
Far-end Network Region: 2

Far-end Domain: avayalab2.com

Incoming Dialog Loopbacks: eliminate      Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload      RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3      IP Audio Hairpinning? n
Enable Layer 3 Test? y      Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n      Alternate Route Timer(sec): 6

```

- 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 TCP, the well-known port value is 5060). 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 **5062**.
- 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 SIP trunk 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.
- 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 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: Service Provider      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. 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 *private*. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign when passed in the SIP From, Contact and P-Asserted Identity 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 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>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 **101**, 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>n</u>		
Support Request History? <u>n</u>		
Telephone Event Payload Type: <u>101</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 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), and they are used to authenticate the caller. In the sample configuration, 6 DID numbers were assigned for testing. The example below shows these 6 numbers, mapped to 6 extensions used during testing. These 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

change private-numbering 1					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	5	3		5	Total Administered: 17
5	55001	2	8111111234	10	Maximum Entries: 540
5	55002	2	8111111235	10	
5	55003	2	8111111236	10	
5	55004	2	8111111237	10	
5	55005	2	8111111238	10	
5	55006	2	8111111239	10	

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	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	4	1239	4	55006	
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	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: *10					
Abbreviated Dialing List2 Access Code: *12					
Abbreviated Dialing List3 Access Code: *13					
Abbreviated Dial - Prgm Group List Access Code: *14					
Announcement Access Code: *19					
Answer Back Access Code: _____					
Auto Alternate Routing (AAR) Access Code: *00					
Auto Route Selection (ARS) - Access Code 1: 9			Access Code 2: _____		
Automatic Callback Activation: *33			Deactivation: #33		
Call Forwarding Activation Busy/DA: *30			Deactivation: #30		
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 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			

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.
- **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**.
- Default values were used for all other fields.

change route-pattern 2											Page	1 of	3
Pattern Number: 2											Pattern Name: Alestra SIP Trk		
SCCAN? <u>n</u>											Secure SIP? <u>n</u>		
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Dgts				DCS/ QSIG Intw	IXC	
1:	<u>2</u>	<u>0</u>	—	—	—	—	—				<u>n</u>	user	
2:	—	—	—	—	—	—	—				<u>n</u>	user	
3:	—	—	—	—	—	—	—				<u>n</u>	user	
4:	—	—	—	—	—	—	—				<u>n</u>	user	
5:	—	—	—	—	—	—	—				<u>n</u>	user	
6:	—	—	—	—	—	—	—				<u>n</u>	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:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	rest	—	—	<u>unk-unk</u>	none	
2:	<u>u</u>	<u>u</u>	<u>u</u>	<u>u</u>	<u>u</u>	<u>n</u>	<u>n</u>	rest	—	—	—	none	

6. Configure Avaya Aura® Session Manager

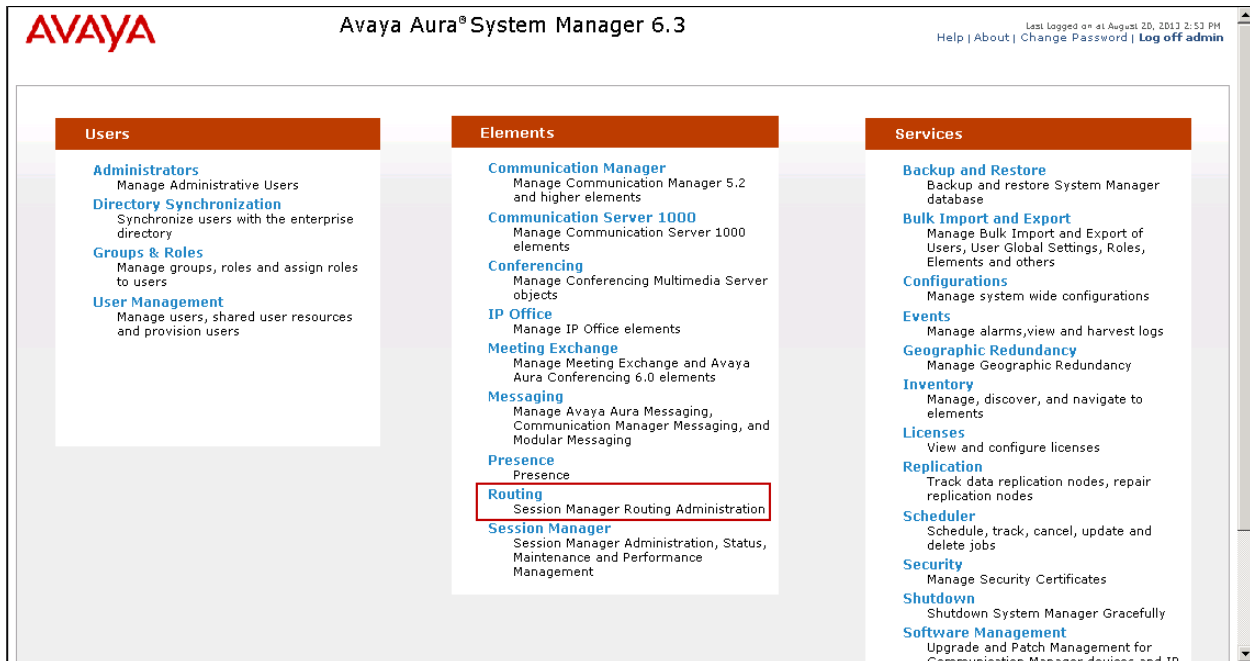
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- 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
- Session Manager instance, corresponding to the Session Manager Server to be managed by System Manager

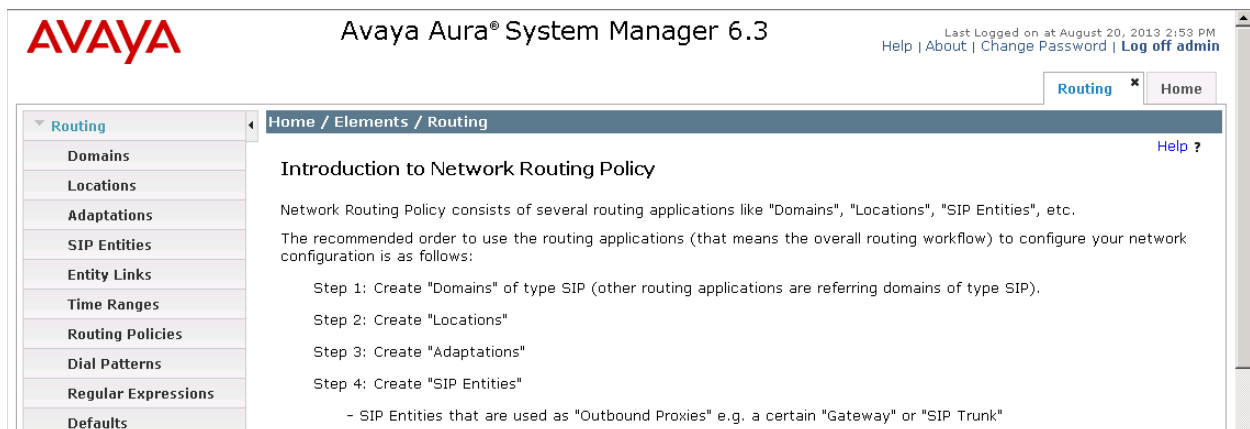
It may not be necessary to create all the items above when creating a connection to the service provider, since some of them would have already been defined as part of the initial Midsize Enterprise Solution template installation. This includes entries such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

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 a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this will be the enterprise domain, **avayalab2.com**.

Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) 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' expanded and 'Domains' selected. The main area has a breadcrumb 'Home / Elements / Routing / Domains' and a 'Help ?' link. Below the breadcrumb is a 'Domain Management' section with 'Commit' and 'Cancel' buttons. A table below shows one item: 'avayalab2.com' with type 'sip' and notes 'Lab Domain'. The table has columns 'Name', 'Type', and 'Notes'. There are 'Commit' and 'Cancel' buttons at the bottom right.

Name	Type	Notes
* avayalab2.com	sip	Lab 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. For the compliance test, only one location was defined, named **Miami Lab**, which contains all the equipment at the enterprise. 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).

The screenshot shows the 'Location Details' interface. On the left is a navigation pane with 'Routing' expanded and 'Locations' selected. The main area has a breadcrumb 'Home / Elements / Routing / Locations' and 'Commit' and 'Cancel' buttons. Below the breadcrumb is a 'Location Details' section with 'Commit' and 'Cancel' buttons. The 'General' section is active, showing fields for 'Name' (Miami Lab) and 'Notes'.

Name: Miami Lab

Notes:

In the **Location Pattern** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **IP Address Pattern:** Add IP address patterns used to identify the location.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.

The screenshot shows the 'Location Pattern' configuration window. At the top, there are 'Add' and 'Remove' buttons. Below them, it says '2 Items' and 'Refresh'. On the right, there is a 'Filter: Enable' link. The main area contains a table with two columns: 'IP Address Pattern' and 'Notes'. The first row has a checkbox, the pattern '10.5.5.*', and the note 'CM/SM/ASBCE'. The second row has a checkbox, the pattern '192.168.10.*', and the note 'Phones/Others'. Below the table, there is a 'Select : All, None' dropdown. At the bottom right, there are 'Commit' and 'Cancel' buttons.

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	*10.5.5.*	CM/SM/ASBCE
<input type="checkbox"/>	*192.168.10.*	Phones/Others

Select : All, None

Commit Cancel

6.4. 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. For the compliance test, all components were located in location **Miami Lab**.
- **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 for **FQDN or IP Address**.

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* **Name:** SessionManager1

* **FQDN or IP Address:** 10.5.5.15

Type: Session Manager

Notes:

Location: Miami Lab

Outbound Proxy:

Time Zone: America/New_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

To define the ports that Session Manager will use to listen for SIP requests, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. The screen below shows the ports used by Session Manager in the shared lab environment. Only TCP ports 5060 and 5062 are directly relevant to these Application Notes.

Port

TCP Failover port:

TLS Failover port:

Add Remove

4 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avayalab2.com	
<input type="checkbox"/>	5061	TLS	avayalab2.com	
<input type="checkbox"/>	5062	TCP	avayalab2.com	
<input type="checkbox"/>	6060	TCP	avayalab2.com	

Select : All, None

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 to the one created during the Template installation to be 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.

Home / Elements / Routing / SIP Entities

SIP Entity Details

CommitCancel

General

* Name:

C.M. Trunk 2

* FQDN or IP Address:

10.5.5.12

Type:

CM

Notes:

Adaptation:

Location:

Miami Lab

Time Zone:

America/New_York

Override Port & Transport with DNS SRV:

☐

* SIP Timer B/F (in seconds):

4

Credential name:

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**).

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities](#)

SIP Entity Details

CommitCancel

General

* Name: Avaya SBCE

* FQDN or IP Address: 10.5.5.72

Type: SIP Trunk

Notes:

Adaptation:

Location: Miami Lab

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5. 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 the 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. The breadcrumb trail is 'Home / Elements / Routing / Entity Links'. There are 'Commit' and 'Cancel' buttons. Below the title, there is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Connection Policy. The first row shows a link named 'SM to CM Trunk 2' with SIP Entity 1 set to 'SessionManager1', Protocol to 'TCP', Port to '5062', SIP Entity 2 set to 'C.M. Trunk 2', Port to '5062', and Connection Policy set to 'trusted'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* SM to CM Trunk 2	* SessionManager1	TCP	* 5062	* C.M. Trunk 2	* 5062	trusted

Entity Link to the Avaya SBCE:

The screenshot shows the 'Entity Links' configuration page. The breadcrumb trail is 'Home / Elements / Routing / Entity Links'. There are 'Commit' and 'Cancel' buttons. Below the title, there is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Connection Policy. The first row shows a link named 'SM to ASBCE' with SIP Entity 1 set to 'SessionManager1', Protocol to 'TCP', Port to '5060', SIP Entity 2 set to 'Avaya SBCE', Port to '5060', and Connection Policy set to 'trusted'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* SM to ASBCE	* SessionManager1	TCP	* 5060	* Avaya SBCE	* 5060	trusted

6.6. 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 must be added: one for Communication Manager and one for 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). Select 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

Home / Elements / Routing / Routing Policies [Help ?](#)

Routing Policy Details [Commit](#) [Cancel](#)

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
C.M. Trunk 2	10.5.5.12	CM	

Home / Elements / Routing / Routing Policies [Help ?](#)

Routing Policy Details [Commit](#) [Cancel](#)

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.5.5.72	SIP Trunk	

6.7. 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 Alestra 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.
- **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.

Two examples of the Dial Patterns used for the compliance test are shown, one for outbound calls from the enterprise to the PSTN and one for inbound calls. Other Dial Patterns (e.g., 01 for long distance national, 001 for international calls to the U.S., etc.) were similarly defined.

The example in this screen shows that in the test environment, 8 digit dialed numbers for outbound local calls in Monterrey, Mexico, beginning with 8 and originating from the Miami Lab location uses route policy **Outbound to ASBCE**, which sends the call out to the PSTN via the Avaya SBCE to the Alestra SIP Trunk.

Home / Elements / Routing / Dial Patterns
[Help ?](#)

Dial Pattern Details
Commit Cancel

General

* Pattern: 8

* Min: 8

* Max: 8

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avayalab2.com

Notes: Outbound local

Originating Locations and Routing Policies

Add Remove

1 Item Refresh
Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Miami Lab		Outbound to ASBCE	0	<input type="checkbox"/>	Avaya SBCE	

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

On incoming calls, Alestra sent to the enterprise during the compliance test only the last 4 digits of the DID number. The example below shows that a 4 digit number starting with **1**, which is the DID range assigned by Alestra, will use route policy **Incoming to CM Trunk 2** to Communication Manager.

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

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"/>	Miami Lab		Incoming to CM Trunk 2		<input type="checkbox"/>	C.M. Trunk 2	

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

6.8. Add/View Session Manager Instance

The creation of a Session Manager Instance provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description:** Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

The screen below shows the Session Manager values used for the compliance test.

The screenshot displays the 'View Session Manager' configuration page. The left sidebar shows a navigation menu with 'Session Manager' expanded, containing 'Dashboard', 'Session Manager Administration' (selected), 'Communication Profile Editor', 'Network Configuration', 'Device and Location Configuration', 'Application Configuration', 'System Status', 'System Tools', and 'Performance'. The main content area has a breadcrumb trail: 'Home / Elements / Session Manager / Session Manager Administration'. Below this is a 'Return' button and a list of tabs: 'General' (selected), 'Security Module', 'NIC Bonding', 'Monitoring', 'CDR', 'Personal Profile Manager (PPM)', 'Connection Settings', and 'Event Server'. The 'General' tab shows the following fields: 'SIP Entity Name' (SessionManager1), 'Description' (empty), 'Management Access Point Host Name/IP' (10.5.5.14), 'Direct Routing to Endpoints' (Enable), and 'VMware Virtual Machine' (checkbox, unchecked).

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows Security Module values used for the compliance test.

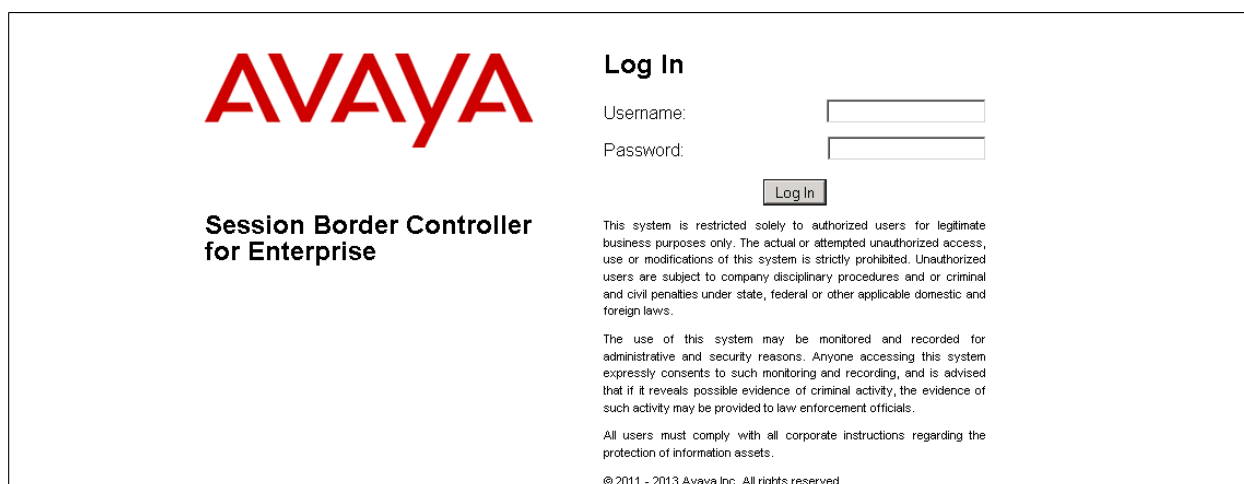
The screenshot shows the 'Security Module' configuration page. The 'Security Module' tab is selected in the left sidebar. The main content area displays the following fields: 'SIP Entity IP Address' (10.5.5.15), 'Network Mask' (255.255.255.0), 'Default Gateway' (10.5.5.254), 'Call Control PHB' (46), 'QOS Priority' (6), 'Speed & Duplex' (Auto), and 'VLAN ID' (empty).

7. 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 installation and initial provisioning of the Avaya SBCE consult [10] and [11] in the **References** section.

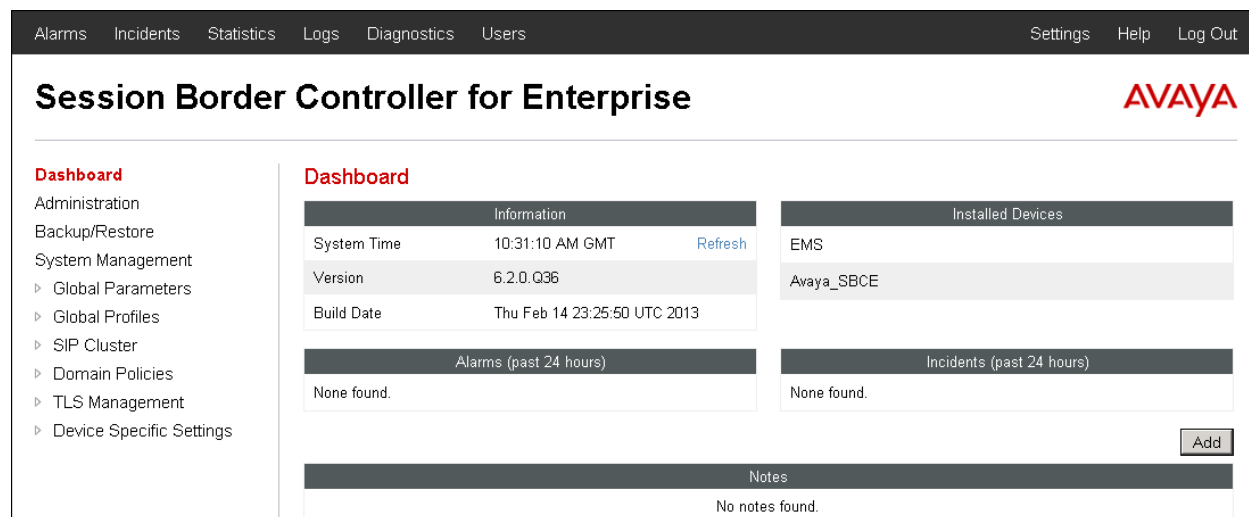
7.1. System Access

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 in red on the left. To the right, under the heading "Log In", are input fields for "Username:" and "Password:". Below these is a "Log In" button. Further down, 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 is another statement: "All users must comply with all corporate instructions regarding the protection of information assets." At the very bottom, it says "© 2011 - 2013 Avaya Inc. All rights reserved."

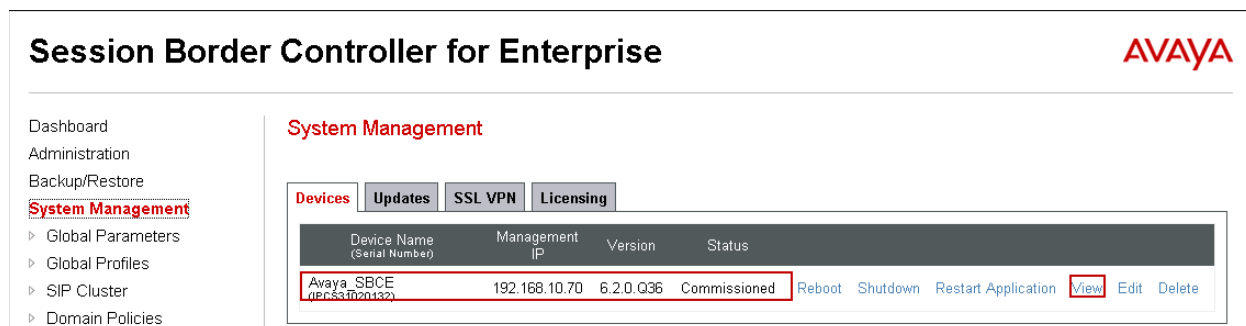
Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE.



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 several sections: "Information" with System Time (10:31:10 AM GMT), Version (6.2.0.Q36), and Build Date (Thu Feb 14 23:25:50 UTC 2013); "Installed Devices" with EMS and Avaya_SBCE; "Alarms (past 24 hours)" and "Incidents (past 24 hours)" both showing "None found."; and "Notes" showing "No notes found." with an "Add" button.

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 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 the other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify the device shows the status of **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

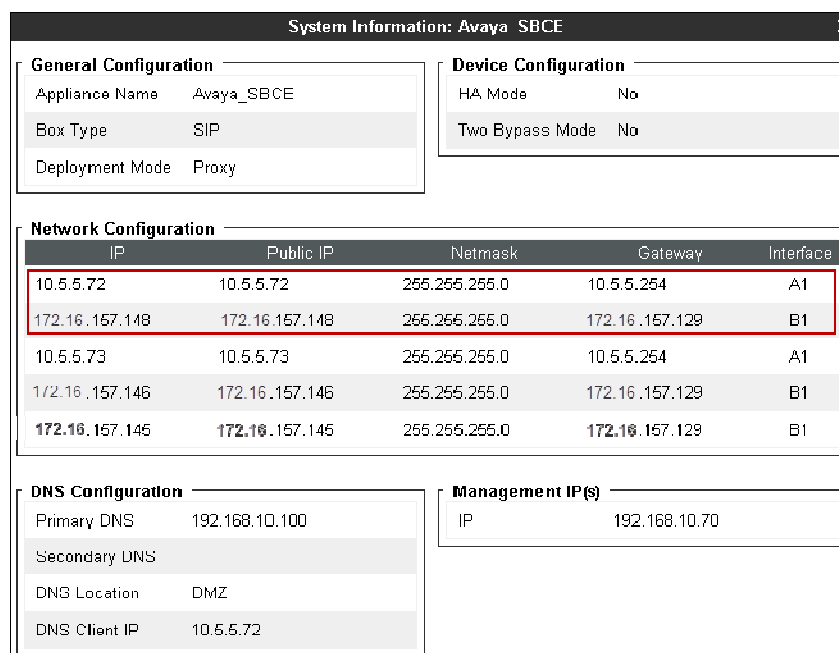
System Management

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies

Devices Updates SSL VPN Licensing

Device Name (Serial Number)	Management IP	Version	Status	
Avaya_SBCE (9PC8310201432)	192.168.10.70	6.2.0.Q36	Commissioned	Reboot Shutdown Restart Application View Edit Delete

To view the network information assigned to the Avaya SBCE, click **View** on the previous screen. The **System Information** window is displayed as shown below, 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, as shown in **Figure 1** in **Section 3**. Note that in the shared lab environment, multiple IP addresses are assigned to these interfaces, but only the highlighted ones are relevant to these Application Notes.



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
172.16.157.148	172.16.157.148	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: 192.168.10.100
Secondary DNS:
DNS Location: DMZ
DNS Client IP: 10.5.5.72

Management IP(s)

IP: 192.168.10.70

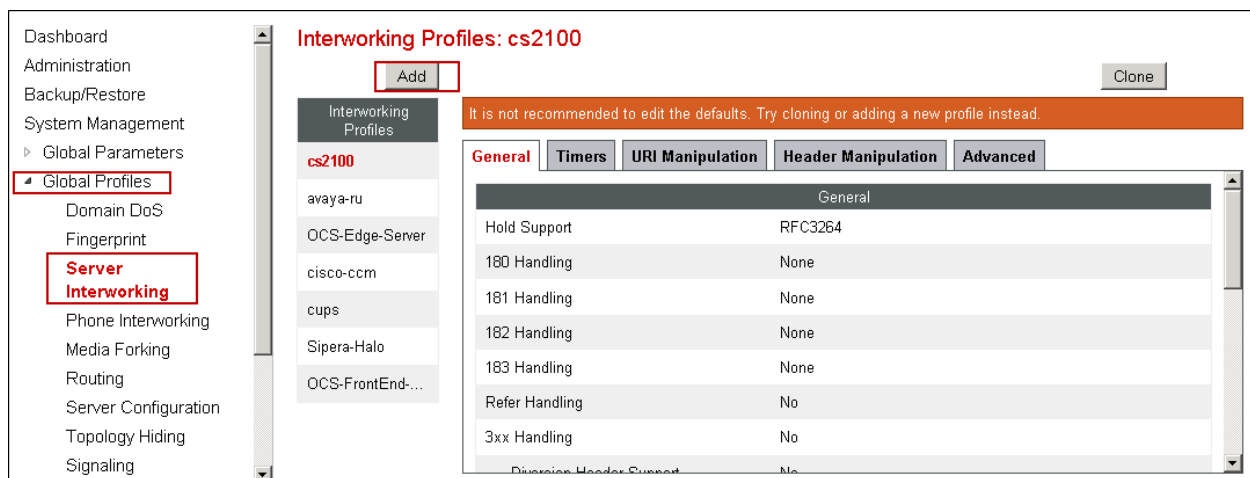
7.3. Global Profiles

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

7.3.1. 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, Session 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**.



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

Interworking Profile X

Profile Name

Next

On the **General** screen, set Hold Support to RFC2543 and check the **T.38 Support** box. All other parameters retain their default values. Click **Next**.

Interworking Profile

General

Hold Support

☐ None

☒ RFC2543 - c=0.0.0.0

☐ RFC3264 - a=sendonly

180 Handling

☒ None

☐ SDP

☐ No SDP

181 Handling

☒ None

☐ SDP

☐ No SDP

182 Handling

☒ None

☐ SDP

☐ No SDP

183 Handling

☒ None

☐ SDP

☐ No SDP

Refer Handling

☐

3xx Handling

☐

Diversion Header Support

☐

Delayed SDP Handling

☐

T.38 Support

☒

URI Scheme

☒ SIP

☐ TEL

☐ ANY

Via Header Format

☒ RFC3261

☐ 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

☐ 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

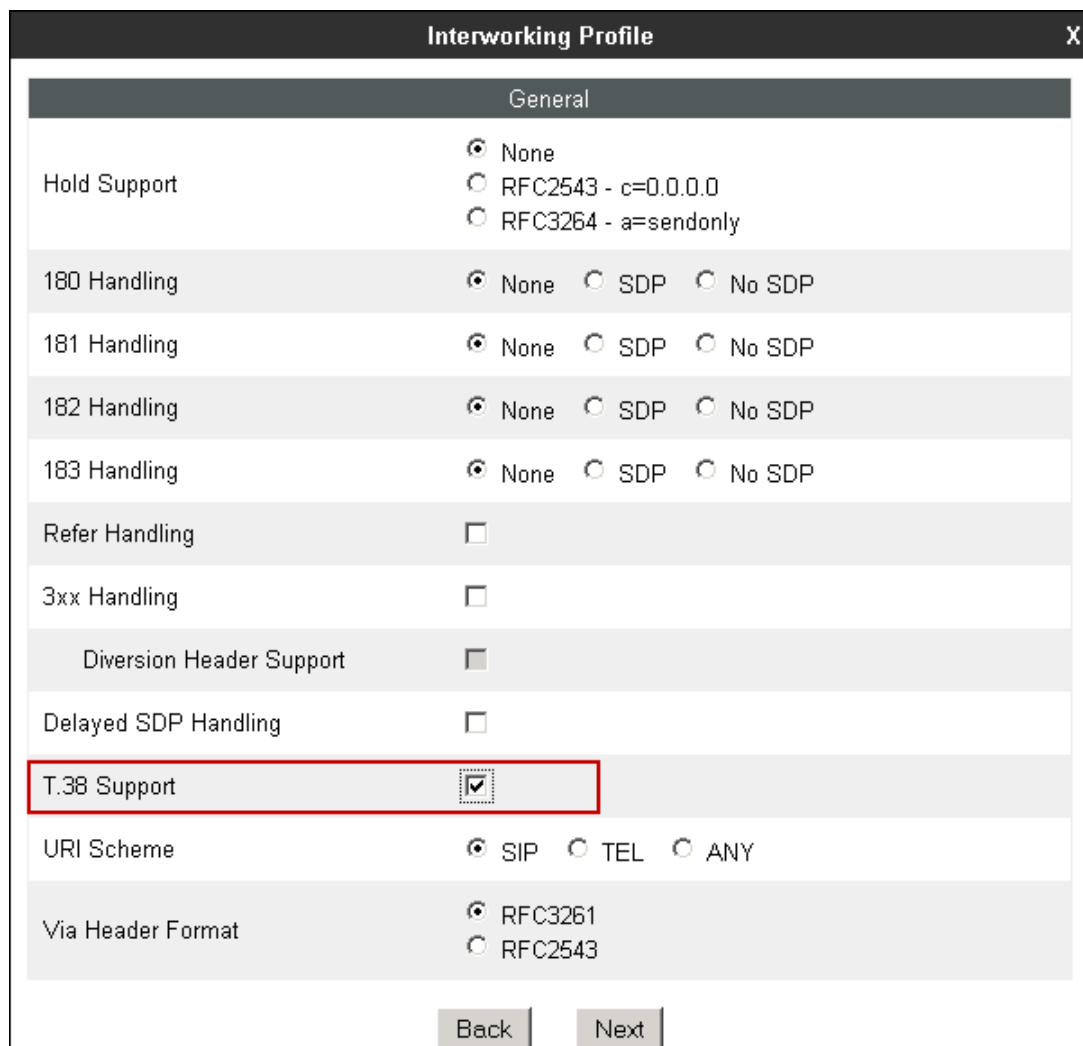
Finish

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 "Interworking Profile" dialog box with the "General" tab selected. The dialog contains the following settings:

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"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP 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 are "Back" and "Next" buttons. The "T.38 Support" row is highlighted with a red border.

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

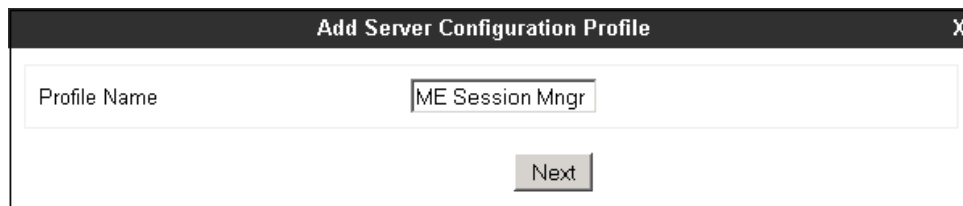
☐

Back

Finish

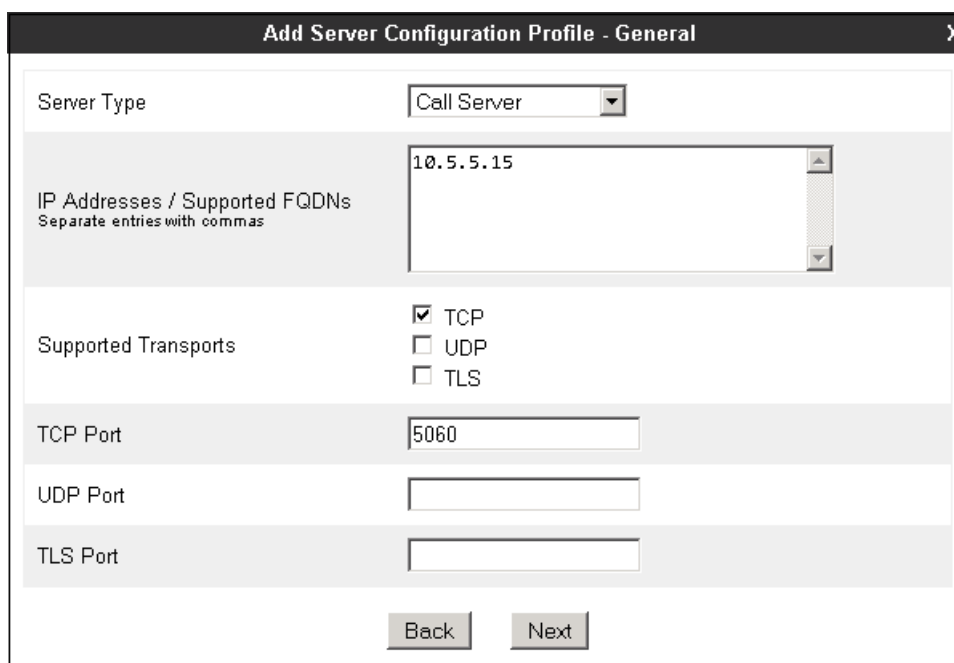
7.3.2. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE two peers, i.e., Session 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 "ME Session Mngr". Below this field is a button labeled "Next".

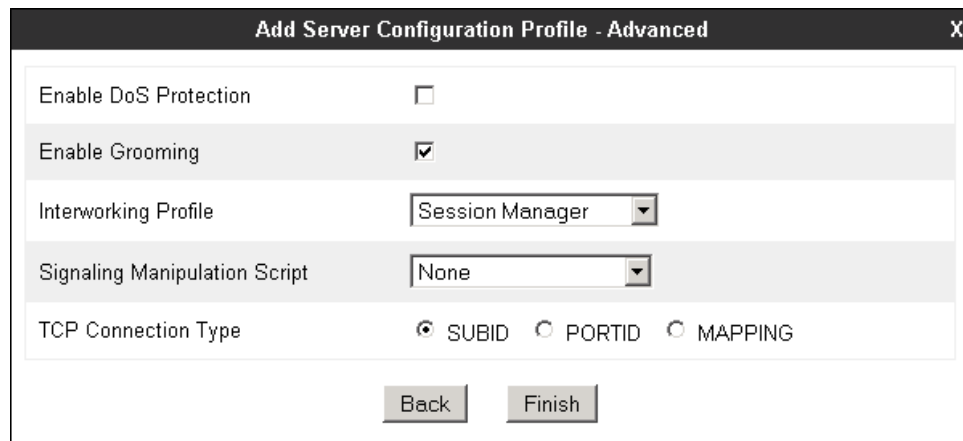
On the **Add Server Configuration Profile - General** Tab select **Call Server** from the drop down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field, enter the IP address of the Session Manager Security Module. Select **TCP** for **Supported Transports**, and enter **5060** under **TCP Port**. The transport protocol and port selected here must match the values defined for the Session Manager SIP entity in **Section 6.4**. 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 options:

- Server Type:** A dropdown menu set to "Call Server".
- IP Addresses / Supported FQDNs:** A text area containing "10.5.5.15". Below the text area is the instruction "Separate entries with commas".
- Supported Transports:** A section with 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, there are two buttons: "Back" and "Next".

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" with a close button (X) in the top right corner. The dialog contains several configuration options:

- Enable DoS Protection**: A checkbox that is currently unchecked.
- Enable Grooming**: A checkbox that is checked.
- Interworking Profile**: A dropdown menu with "Session Manager" selected.
- Signaling Manipulation Script**: A dropdown menu with "None" selected.
- TCP Connection Type**: Three radio buttons labeled "SUBID", "PORTID", and "MAPPING". "SUBID" is selected.

At the bottom of the dialog, there 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 a single text input field labeled "Profile Name" with the text "Service Provider" entered. Below the input field is a "Next" button.

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 *192.168.145.9*, the IP Address of Alestra's 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 dialog contains several fields: 'Server Type' is a dropdown menu set to 'Trunk Server'; 'IP Addresses / Supported FQDNs' is a text box with '192.168.145.9' and a note 'Separate entries with commas'; 'Supported Transports' has three checkboxes: 'TCP' (unchecked), 'UDP' (checked), and 'TLS' (unchecked); 'TCP Port' is an empty text box; 'UDP Port' is a text box with '5060'; and 'TLS Port' is an empty text box. At the bottom are 'Back' and 'Next' buttons.

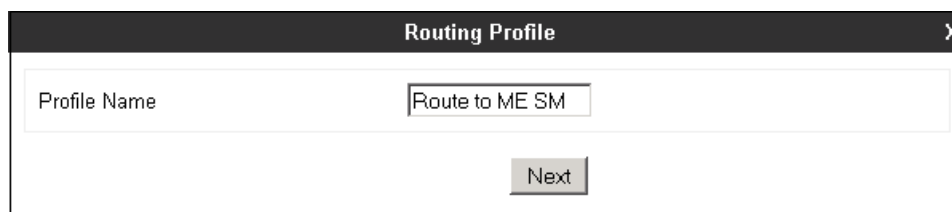
Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, select *Service Provider* from the **Interworking Profile** drop down menu. Click **Finish**

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 dialog contains several fields: 'Enable DoS Protection' and 'Enable Grooming' are checkboxes, both unchecked; 'Interworking Profile' is a dropdown menu set to 'Service Provider'; 'Signaling Manipulation Script' is a dropdown menu set to 'None'; and 'UDP Connection Type' has three radio buttons: 'SUBID' (selected), 'PORTID' (unchecked), and 'MAPPING' (unchecked). At the bottom are 'Back' and 'Finish' buttons.

7.3.3. Routing Profiles

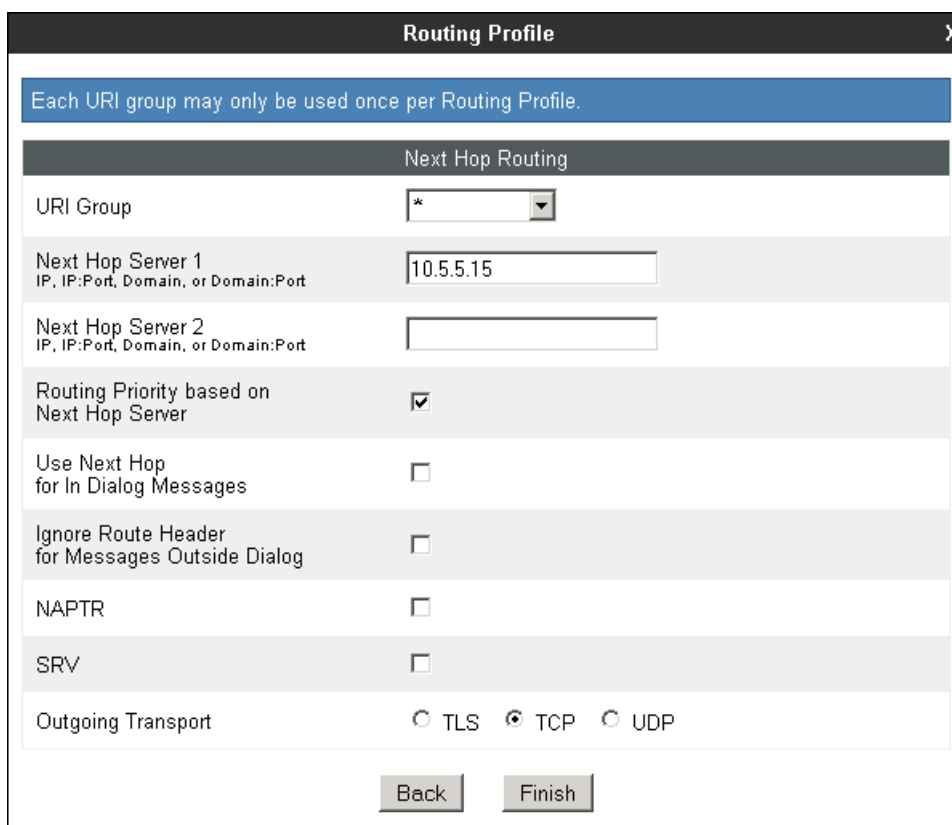
Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces.

Two Routing Profiles were created in the test configuration, one for inbound calls, with Session 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 ME SM". Below the input field is a button labeled "Next".

On the **Next Hop Routing** tab, enter the IP Address of Session 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**.

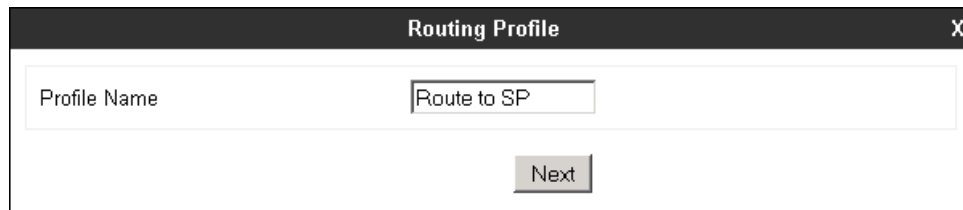


The screenshot shows the "Routing Profile" window with the "Next Hop Routing" tab selected. At the top, a blue banner states "Each URI group may only be used once per Routing Profile." Below this, the "Next Hop Routing" section contains the following fields and options:

- URI Group:** A dropdown menu with an asterisk (*) selected.
- Next Hop Server 1:** A text input field containing "10.5.5.15". 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: "TLS" (unchecked), "TCP" (checked), and "UDP" (unchecked).

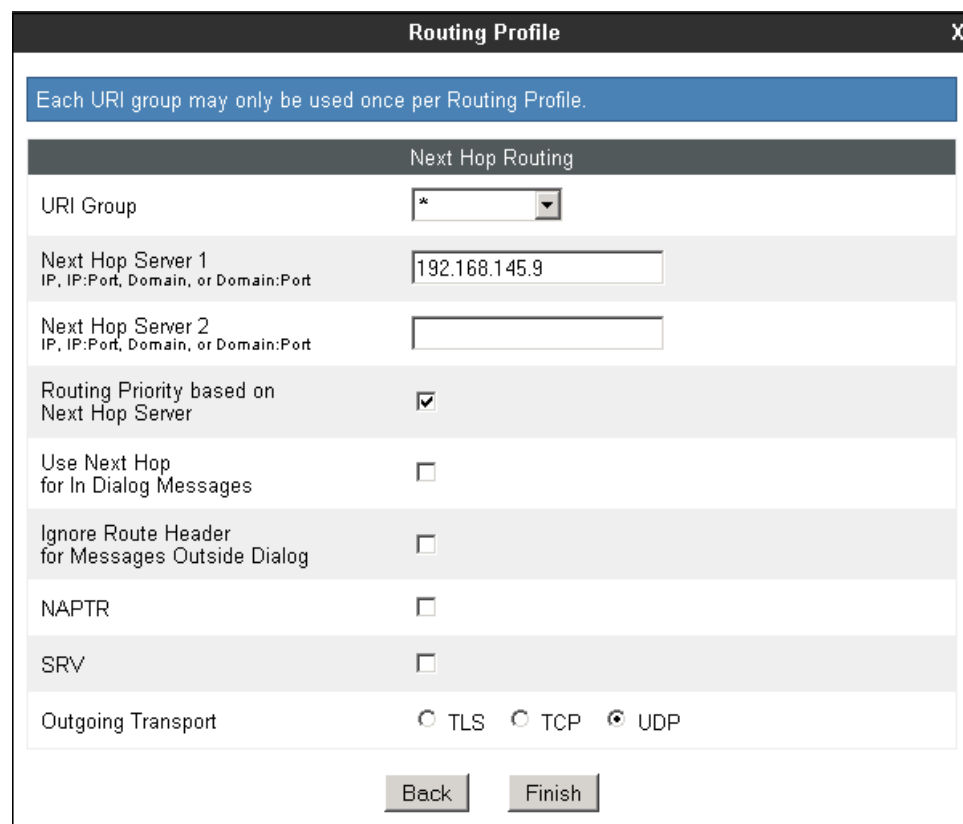
At the bottom of the window are two buttons: "Back" and "Finish".

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** 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 labeled 'Profile Name' containing the text 'Route to SP'. 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 **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, the 'Next Hop Routing' section contains the following fields and options:

- URI Group:** A dropdown menu with an asterisk (*) as the selected option.
- Next Hop Server 1:** A text input field containing '192.168.145.9'. Below it, the text 'IP, IP:Port, Domain, or Domain:Port' is displayed.
- Next Hop Server 2:** An empty text input field. Below it, the text 'IP, IP:Port, Domain, or Domain:Port' is displayed.
- 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: 'TLS' (unchecked), 'TCP' (unchecked), and 'UDP' (checked).

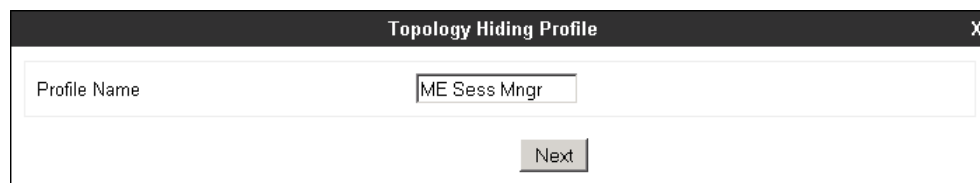
At the bottom of the dialog box are 'Back' and 'Finish' buttons.

7.3.4. 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.



Header	Criteria	Replace Action	Overwrite Value
RequestLine	IP/Domain	Auto	

For the **Request-Line**, **From** and **To** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain known by the Session Manager, **avayalab2.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	avayalab2.com
From	IP/Domain	Overwrite	avayalab2.com
To	IP/Domain	Overwrite	avayalab2.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
Request-Line	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---

7.4. 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 one 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.

7.4.1. Signaling Rules

A Signaling Rule was created in the sample configuration to remove (block) the following headers:

- AV-Global-Session-ID
- Alert-Info
- P-AV-Message-ID
- P-Location
- P-Charging-Vector

These headers are sent in SIP messages from the Session 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	Remove_headers	
		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 **Remove_headers** Signaling Rule, select the **Request Headers** tab to create the manipulations performed on request messages. Select **Add In Header Control**.

Signaling Rules configuration interface. The **Remove_headers** rule is selected. The **Request Headers** tab is active, and the **Add In Header Control** button is highlighted. The table below shows no existing request header controls.

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: INVITE**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- **Click Finish**

Add Header Control dialog box configuration:

- Proprietary Request Header: ☐
- Header Name: Alert-Info
- Method Name: INVITE
- Header Criteria: ☒ Forbidden, ☐ Mandatory, ☐ Optional
- Presence Action: Remove header
- Status: 486, Reason: Busy Here
- Finish button

Select **Add In Header Control** as needed to configure the remaining header control rules for the AV-Global-Session-ID, P-AV-Message-ID, P-Location and P-Charging-Vector headers. For these headers, 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							
				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
3	P-AV-Message-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
4	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
5	P-Location	ALL	Forbidden	Remove Header	Yes	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
200

Method Name
INVITE

Header Criteria
☒ Forbidden
☐ Mandatory
☐ Optional

Presence Action
Remove header

486
Busy Here

Finish

Select **Add In Header Control** as needed to configure the remaining header control rules for the AV-Global-Session-ID, P-AV-Message-ID, P-Location and P-Charging-Vector headers. For these headers, 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 **Response Headers** tab should look like the following screen.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS				
				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	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Alert-Info	200	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
3	P-AV-Message-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-Charging-Vector	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.4.2. 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**.

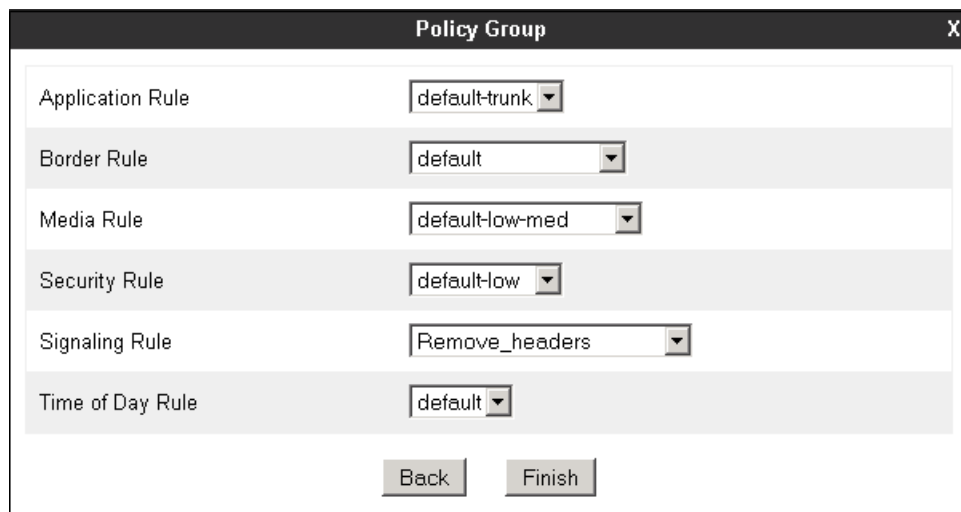


Policy Group X

Group Name

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 *Remove_headers* rule created in **Section 7.4.1** was selected. Click **Finish**.



Policy Group X

Application Rule

Border Rule

Media Rule

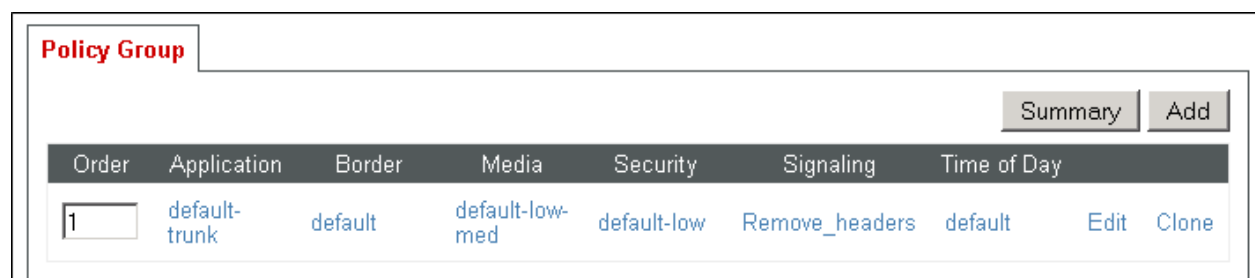
Security Rule

Signaling Rule

Time of Day Rule

Back 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	Remove_headers	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.

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

7.5. Device Specific Settings

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

7.5.1. 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 centre 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.

Network Management: Avaya_SBCE

Devices
Avaya_SBCE

Network Configuration **Interface Configuration**

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

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

Add Save Clear

IP Address	Public IP	Gateway	Interface	
10.5.5.72		10.5.5.254	A1	Delete
172.16.157.148		172.16.157.129	B1	Delete

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.

Devices	Network Configuration	Interface Configuration
Avaya_SBCE		
Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

7.5.2. 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
172.16.157.148

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	172.16.157.148	35000 - 40000	Edit Delete

7.5.3. 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 Session 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. **UDP Port 5060** was selected 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

172.16.157.148 ▼

TCP Port
Leave blank to disable

UDP Port
Leave blank to disable

Enable Stun
☐

TLS Port
Leave blank to disable

TLS Profile

AvayaSBCEServer ▼

Enable Shared Control
☐

Shared Control Port

Finish

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

<div style="background-color: #333; color: white; padding: 2px 5px; margin-bottom: 5px;">Devices</div> <div style="background-color: #f96; padding: 2px 5px; margin-bottom: 5px;">Avaya_SBCE</div>	<div style="display: flex; justify-content: space-between; align-items: center;"> Signaling Interface Add </div>					
	<div style="display: flex; justify-content: space-between;"> Name Signaling IP TCP Port UDP Port TLS Port TLS Profile </div>					
	Private_sig	10.5.5.72	5060	---	---	None
	Public_sig	172.16.157.148	---	5060	---	None

7.5.4. 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 **ME SM 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**.

Add FlowX

Flow Name	ME SM Flow
Server Configuration	ME Session Mngr.
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 SP
Topology Hiding Profile	ME Sess Mngr
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**.

Add Flow X

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 ME SM"/>
Topology Hiding Profile	<input type="text" value="Service Provider"/>
File Transfer Profile	<input type="text" value="None"/>
<input type="button" value="Finish"/>	

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

Devices

Avaya_SBCE

Subscriber Flows

Server Flows

Click here to add a row description.

Server Configuration: ME Session Mngr.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	ME SM Flow	*	Public_sig	Private_sig	Enterprise	Route to SP	<a>View <a>Clone <a>Edit <a>Delete

Server Configuration: Service Provider

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 ME SM	<a>View <a>Clone <a>Edit <a>Delete

8. Alestra Enlace IP SIP Trunk Service Configuration

Alestra is responsible for the configuration of the Enlace IP SIP Trunk Service on its network. 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 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, 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 useful troubleshooting 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**. Verify that the state of the Session Manager links under the **Conn. Status** and **Link Status** columns to Communication Manager and the Avaya SBCE is **UP**, like shown on the screen below.

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

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: [SessionManager1](#)

Summary View

Status Details for the selected Session Manager:

5 Items | [Refresh](#)Filter: [Enable](#)

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input checked="" type="radio"/>	CommunicationManager1	10.5.5.12	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Presence1	10.5.5.16	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Messaging	10.5.5.12	6060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	Avaya SBCE	10.5.5.72	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	C.M. Trunk 2	10.5.5.12	5062	TCP	FALSE	UP	200 OK	UP

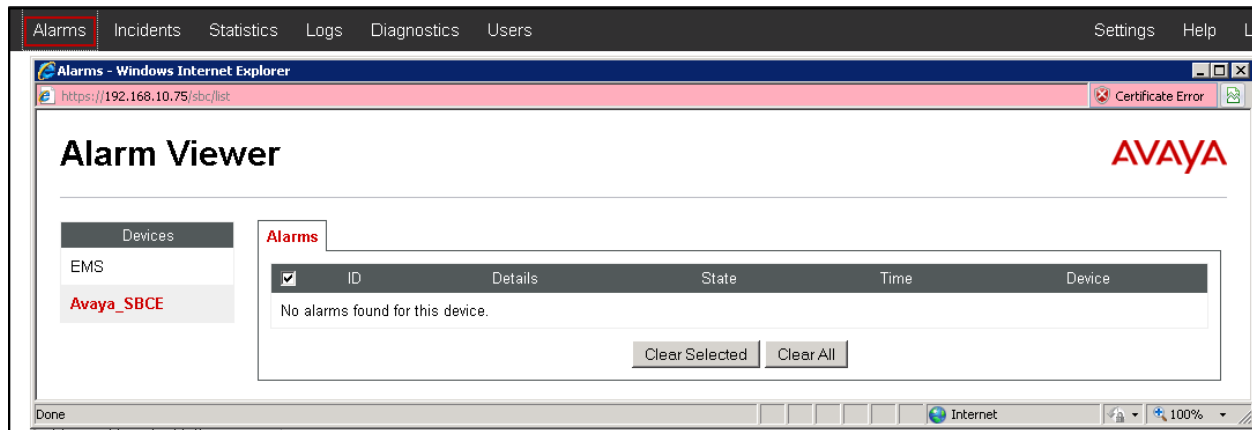
Other Session Manager useful verification and troubleshooting tools include:

- **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

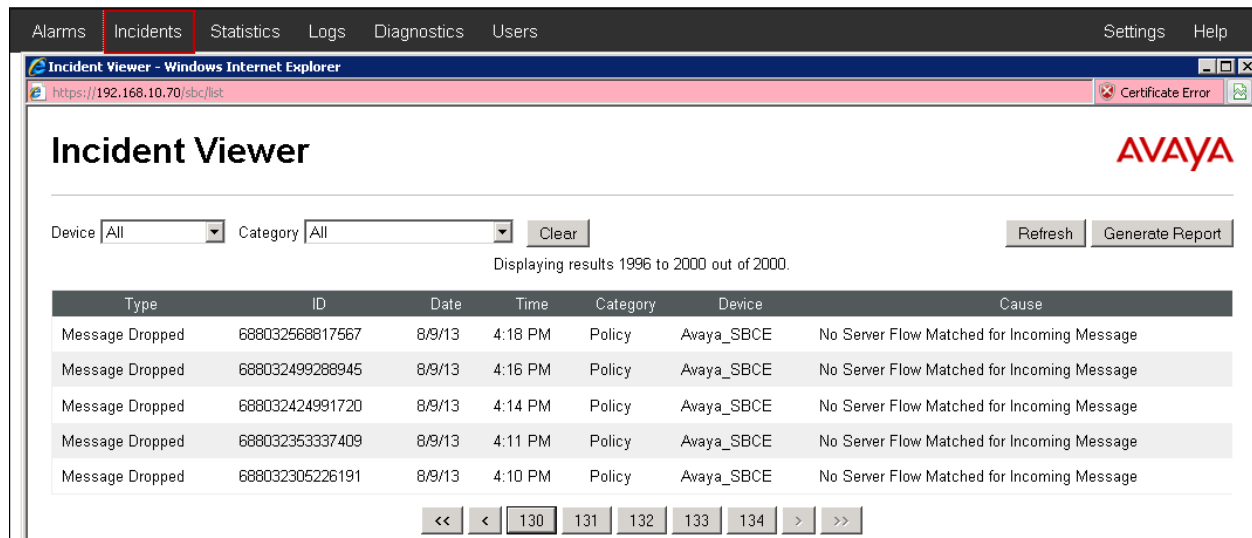
9.4. Avaya SBCE Verification

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.

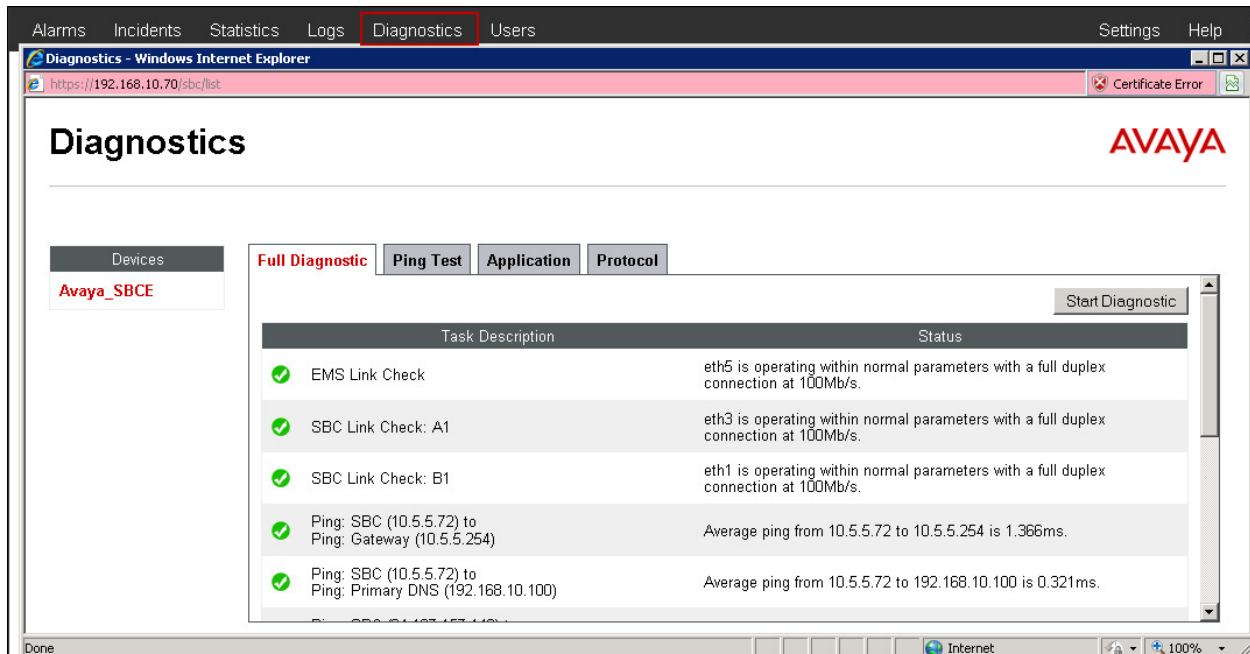
Alarms: Provides information about the health of the SBC.



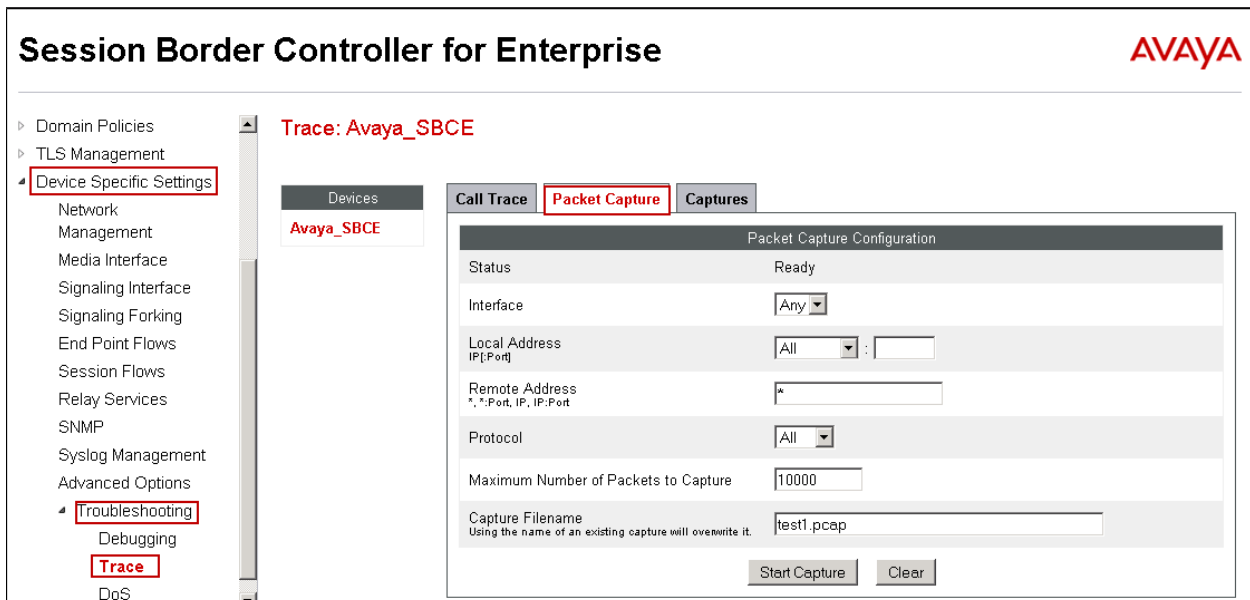
Incidents : Provides detailed reports of anomalies, errors, policies violations, etc.



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



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.

Call Trace	Packet Capture	Captures
Refresh		
File Name	File Size (bytes)	Last Modified
test1_20130830102339.pcap	393,216	August 30, 2013 10:24:04 AM GMT
		Delete

10. Conclusion

These Application Notes describe the procedures required to configure an Avaya Aura® Solution for Midsize Enterprise 6.2.2 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**.

11. References

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

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3, May 2013.
- [2] *Administering Avaya Aura® System Platform*, Release 6.3, May 2013.
- [3] *Avaya Aura® Solution for the Midsize Enterprise (ME) 6.2.2 Intelligent Workbook*, Version 1.3, August 2013
- [4] *Implementing Avaya Aura® Solution for the Midsize Enterprise*, Release 6.2.2, August 2013
- [5] *Upgrading Avaya Aura® Solution for Midsize Enterprise*, Release 6.2.2, August 2013
- [6] *Avaya Aura® Solution for the Midsize Enterprise 6.2.2 Release Notes*, August 2013
- [7] *Administering Avaya Aura® Communication Manager*, Release 6.3, May 2013, Document Number 03-300509.
- [8] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3, May 2013, Document Number 555-245-205.
- [9] *Administering Avaya Aura® Session Manager*, Release 6.3, June 2013.
- [10] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, June 2013
- [11] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, March 2013
- [12] *Administering Avaya one-X® Communicator*, December 2012.
- [13] *Using Avaya one-X® Communicator, Release 6.1*, October 2011.
- [14] *Implementing Avaya Flare® Experience for Windows*. Release 1.1 February 2013.
- [15] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>.
- [16] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

©2013 Avaya Inc. All Rights Reserved.

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

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