



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Fibrenoire SIP Trunking Service with Avaya Aura® Communication Manager Release 6.3, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.3 – Issue 1.0**

## **Abstract**

These Application Notes describe the steps to configure a Session Initiation Protocol (SIP) trunk between Fibrenoire SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 6.3, Avaya Aura® Session Manager 6.3, Avaya Session Border Controller for Enterprise 6.3 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Session Border Controller for Enterprise.

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

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

Fibrenoire is a member of the Avaya DevConnect Service Provider Program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing is 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 .....	4
2.2.	Test Results .....	5
2.3.	Support.....	5
3.	Reference Configuration .....	6
4.	Equipment and Software Validated .....	8
5.	Configure Avaya Aura® Communication Manager .....	9
5.1.	Licensing and Capacity .....	9
5.2.	System Features .....	10
5.3.	IP Node Names .....	11
5.4.	Codecs.....	11
5.5.	IP Network Region .....	12
5.6.	Signaling Group .....	13
5.7.	Trunk Group.....	14
5.8.	Calling Party Information .....	16
5.9.	Inbound Routing .....	17
5.10.	Outbound Routing.....	17
5.11.	Saving Communication Manager Configuration Changes .....	19
6.	Configure Avaya Aura® Session Manager .....	20
6.1.	System Manager Login and Navigation .....	20
6.2.	Specify SIP Domain.....	21
6.3.	Add Location .....	22
6.4.	Add SIP Entities.....	23
6.5.	Add Entity Links.....	25
6.6.	Add Routing Policies .....	27
6.7.	Add Dial Patterns.....	28
6.8.	Add/View Session Manager .....	30
7.	Configure Avaya Session Border Controller for Enterprise .....	32
7.1.	Avaya Session Border Controller for Enterprise Login.....	32
7.2.	Global Profiles .....	33
7.2.1.	Uniform Resource Identifier (URI) Groups.....	33
7.2.2.	Routing Profiles .....	33
7.2.3.	Topology Hiding.....	35
7.2.4.	Server Interworking .....	36
7.2.5.	Server Configuration.....	40
7.3.	Domain Policies .....	43
7.3.1.	Signaling Rules .....	43
7.3.2.	Endpoint Policy Groups.....	44
7.4.	Device Specific Settings .....	46
7.4.1.	Network Management.....	46
7.4.2.	Media Interface .....	47
7.4.3.	Signaling Interface .....	47
7.4.4.	End Point Flows - Server Flow .....	48

8.	Fibreoptic Service Configuration .....	50
9.	Verification and Troubleshooting .....	50
9.1.	Verification Steps.....	50
9.2.	Protocol Traces .....	50
9.3.	Troubleshooting: .....	51
9.3.1.	The Avaya SBCE.....	51
9.3.2.	Communication Manager.....	51
10.	Conclusion .....	51
11.	References .....	52

# 1. Introduction

These Application Notes describe the steps to configure a SIP trunk between Fibrenoire SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.3 (Communication Manager) configured as an Evolution Server, Avaya Aura® Session Manager 6.3 (Session Manager), Avaya Session Border Controller for Enterprise 6.3 (Avaya SBCE) and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with Fibrenoire are able to place and receive PSTN calls via a broadband Internet connection. This converged network solution is an alternative to a traditional PSTN trunk such as analog and/or ISDN-PRI.

## 2. General Test Approach and Test Results

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.

Fibrenoire is a member of the Avaya DevConnect Service Provider Program. The general test approach is to connect a simulated enterprise to Fibrenoire via the Internet and exercise the features and functionalities listed in **Section 2.1**.

### 2.1. Interoperability Compliance Testing

To verify Fibrenoire interoperability, the following features and functionalities are covered in the compliance testing:

- Inbound PSTN calls to various phone types including H.323, SIP, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types including H.323, SIP, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phone. Both the 1XC Computer Mode (where 1XC is used for call control as well as audio path) and the 1XC Telecommuter Mode (where 1XC is used for call control and a separate telephone is used for audio path) are tested.
- Dialing plans including local, long distance, international, outbound toll-free, calls etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Codec G.711MU.
- Media and Early Media transmissions.
- Incoming and outgoing fax using T.38 and G.711.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.

- User features such as hold and resume, transfer, forward and conference.
- Off-net call forward with Diversion method.
- EC500 mobility (extension to cellular) with Diversion method.
- Routing inbound vector call to call center agent queues.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

Items that are supported and not tested including the following:

- Inbound toll-free is supported but was not tested as part of the compliance test.
- Operator Call 0 and operator call assisted (0 + 10 digits) were not supported.
- Local Directory Assistance Calls 411 was not supported.
- Call redirection (i.e. Blind and Consultative Transfers) using REFER method was not supported.
- Incoming call redirection after answer of incoming VDN calls using REFER method is not supported.

## 2.2. Test Results

Interoperability testing of Fibrenoire with the Avaya SIP-enabled enterprise solution is completed with successful results for all test cases with the exception of the observations and limitations described below.

- **OPTIONS** – Fibrenoire supports OPTIONS, but it is not needed on standard configuration. The OPTIONS can be activated upon request per vendor. It will also be activated for redundancy configuration.

## 2.3. Support

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

For technical support on Fibrenoire SIP Trunking, contact Fibrenoire Inc. at <http://www.fibrenoire.ca/en>.

### 3. Reference Configuration

**Figure 1** illustrates the sample Avaya SIP-enabled enterprise solution connected to the Fibrenoire (Vendor Validation circuit (not shown)) through a public Internet connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

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

- Avaya S8800 Server running Avaya Aura® Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Avaya Aura® System Manager
- Avaya S8800 Server running Avaya Aura® Session Manager
- Avaya S8800 Server running Avaya Aura® Messaging
- Avaya Session Border Controller for Enterprise
- Avaya 9600 Series IP Deskphones (H.323, SIP)
- Avaya one-X® Communicator soft phones (H.323, SIP)
- Avaya digital and analog telephones

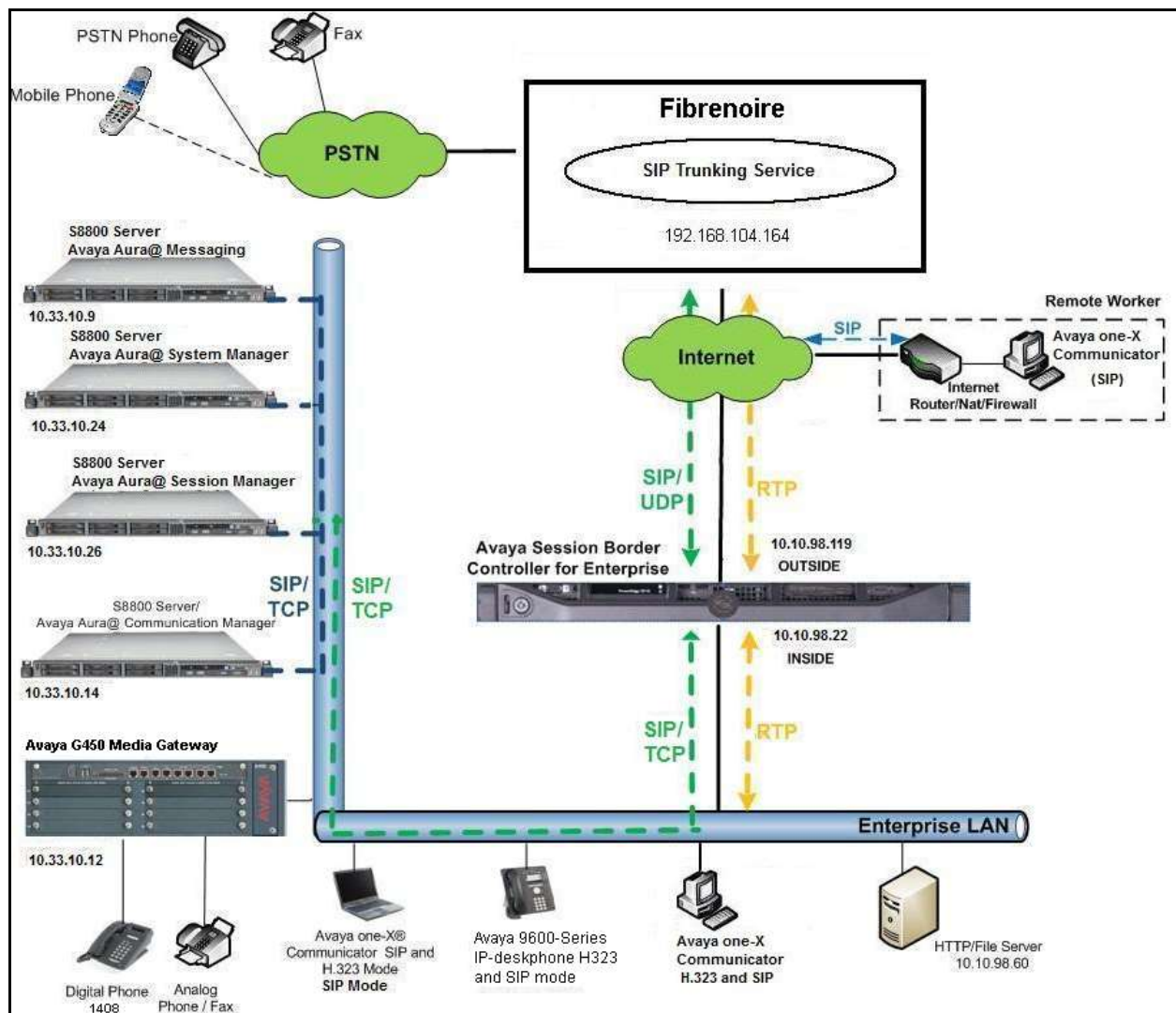
Located at the edge of the enterprise network is the Avaya SBCE. It has a public side that connects to Fibrenoire via Internet and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flows through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Fibrenoire across the public network is UDP. The transport protocol between the Avaya SBCE, Session Manager and Communication Manager is TCP.

In the compliance testing, the Avaya Customer-Premises Equipment (CPE) environment was configured with SIP domain “avayalab.com” for the enterprise. The Avaya SBCE is used to adapt the enterprise SIP domain to the IP address based URI-Host known to Fibrenoire. **Figure 1** below illustrates the network diagram for the enterprise. All voice application elements are connected to internal trusted LAN.

Additionally, the reference configuration included remote worker functionality, introduced with Avaya SBCE. A remote worker is a SIP endpoint that resides in the untrusted network, registered to Avaya Session Manager via the Avaya SBCE. Remote workers feature the same functionality as any other endpoint within the enterprise. This functionality was successfully tested during the compliance test, using the Avaya one-X Communicator for Windows using TLS and SRTP. The configuration tasks required to support remote workers are referenced in **Section 11**.

In this configuration, Avaya SBCE on enterprise side is configured to periodically perform OPTIONS ping to Fibrenoire system. Outbound calls from enterprise Communication Manager to PSTN do not require authentication or registration with Fibrenoire system but it can be done per request.

For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.



**Figure 1: Avaya IP Telephony Network connecting to Fibrenoire Networks**

## 4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on an Avaya S8800 Server	6.3.9 (CM: R016x.03.0.124 Patch 21971)
Avaya G450 Media Gateway	35.8.0
Avaya Aura® System Manager running on an Avaya S8800 Server	6.3.9 (Build No 6.3.9.1.2.538)
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.3.7 (6.3.7.0.637008)
Avaya Aura® Messaging running on an Avaya S8800 Server	MSG-03.0.124.0-315_0007
Avaya Session Border Controller for Enterprise	6.3.000-19-4338
Avaya 9650C IP Deskphone (H.323)	Avaya one-X® Deskphone Edition S3.220A
Avaya 9630G IP Deskphone (SIP)	Avaya one-X® Deskphone Edition 6.4.0.33
Avaya one-X Communicator (H.323/SIP)	6.2.3.05-FP5
Avaya 1408 Digital Deskphone	1400R10
Avaya 6210 Analog Telephone	n/a
Fibrenoire SIP Trunking Service Components	
Equipment/Software	Release/Version
Broadsoft Broadworks	20sp1
Sonus SBC 5100	4.0.7

**Table 1: Equipment and Software Tested**

**Note:** This solution will be compatible with other Avaya Server and Media Gateway platforms running similar version of Communication Manager.



## 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for Fibrenoire. It is assumed the general installation of Communication Manager and Avaya G450 Media Gateway has been previously completed and is not discussed here.

The configuration of Communication Manager 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 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 sale representative to add the additional capacity or feature.

<b>display system-parameters customer-options</b>		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	4000	50
Maximum Concurrently Registered IP Stations:	2400	1
Maximum Administered Remote Office Trunks:	4000	0
Maximum Concurrently Registered Remote Office Stations:	2400	0
Maximum Concurrently Registered IP eCons:	68	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	2400	0
Maximum Video Capable IP Softphones:	2400	3
<b>Maximum Administered SIP Trunks:</b>	<b>24000</b>	<b>289</b>
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0
Maximum Number of DS1 Boards with Echo Cancellation:	80	0
Maximum TN2501 VAL Boards:	10	0
Maximum Media Gateway VAL Sources:	50	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 an incoming call from the PSTN to be transferred to another PSTN destination. 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
```

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. The compliance test used the value of ***anonymous*** for restricted calls and 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: anonymous
      CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

      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: 1
      International Access Code: 001

      ENBLOC DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

      CALLER ID ON CALL WAITING PARAMETERS
      Caller ID on Call Waiting Delay Timer (msec): 200
```

### 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 Session Manager (*SM*). These node names will be needed for defining the service provider signaling groups in **Section 5.6**.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
<b>SM</b>	<b>10.33.10.26</b>	
default	0.0.0.0	
<b>procr</b>	<b>10.33.10.14</b>	
procr6	::	

### 5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to be used for calls between the enterprise and the service provider. This compliance test used ip-codec-set 1. Fibrenoire only supports G.711MU codec. To use this codec, enter *G.711MU* in the **Audio Codec** column of the table.

change ip-codec-set 1		Page 1 of 2
		IP Codec Set
Codec Set: 1		
Audio Codec	Silence Suppression	Frames Per Pkt
1: <b>G.711MU</b>	<b>n</b>	<b>2</b>
2:		

On **Page 2**, set the **Fax Mode** to *T.38-G711-fallback* faxing which Fibrenoire supported both T.38 and G.711 fax modes.

change ip-codec-set 1		Page 2 of 2
		IP Codec Set
		Allow Direct-IP Multimedia? n
<b>FAX</b>	Mode	Redundancy
Modem	<b>t.38-G711-fallback</b>	<b>1</b>
TDD/TTY	off	0
Clear-channel	US	3
	n	0

## 5.5. IP Network Region

A separate IP network region for the service provider trunk group is created. This allows separate codec or quality of service setting to be used (if necessary) for a call between the enterprise and the service provider versus a call within the enterprise or elsewhere. For the compliance testing, ip-network-region 1 was created by the **change ip-network-region 1** command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance testing, the domain name is *avayalab.com*. This domain name appears in the “From” header of SIP message originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Media Gateway. By default, both **Intra-region** and **Inter-region IP-IP Direct Audio** are set to *yes*. Shuffling can be further restricted at the trunk level under 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 1		Page 1 of 20	
IP NETWORK REGION			
Region: 1			
Location: 1	Authoritative Domain: avayalab.com		
Name: ToSM			
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes	
Codec Set: 1		Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048		IP Audio Hairpinning? n	
UDP Port Max: 3329			
DIFFSERV/TOS PARAMETERS			
Call Control PHB Value: 46			
Audio PHB Value: 46			
Video PHB Value: 26			
...			

On **Page 4**, define the IP codec set to be used for traffic between region 1 and other regions. In the compliance testing, Communication Manager, the Avaya G450 Media Gateway, IP/SIP phones, Session Manager and the Avaya SBCE were assigned to the same region 1. To configure the IP codec set between regions, enter the desired IP codec set in the **codec set** column of the table with appropriate destination region (**dst rgn**). Default values may be used for all other fields. The example below shows codec set 1 will be used for a call between region 1 and other regions.

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

Non-IP telephones (e.g., analog, digital) derive network region from IP interface of the Avaya G450 Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping.

To define network region 1 for IP interface **procr**, use **change ip-interface procr** command as shown in the following screen.

<b>change ip-interface pr</b>		Page 1 of 2
IP INTERFACES		
Type: PROCR		
		Target socket load: 4800
Enable Interface? y	Allow H.323 Endpoints? y	
	Allow H.248 Gateways? y	
Network Region: 1	Gatekeeper Priority: 5	
...		

To define network region 1 for the Avaya G450 Media Gateway, use **change media-gateway** command as shown in the following screen.

<b>change media-gateway 1</b>		Page 1 of 2
MEDIA GATEWAY 1		
Type: g450		
Name: SPMGC		
Serial No: 12N517873797		
Encrypt Link? y	Enable CF? n	
Network Region: 1	Location: 1	
	Site Data:	
Recovery Rule: none		
...		

## 5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Avaya SBCE for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**.
- Set the **Transport Method** to **tcp**. The transport method specified here is used between Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to **5060**.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP interface of **procr** defined in **Section 5.3**.

- Set the **Far-end Node Name** to *SM*. This node name maps to the IP address of Avaya SBCE as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region *1* defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to *avayalab.com*.
- Set the **DTMF over IP** to *rtp-payload*. This setting enables Communication Manager to send or receive the DTMF transmissions using RFC2833.
- Set **Enable Layer 3 Test?** to *y*. This setting allows Communication Manager to send OPTIONS heartbeat to Session Manager on the SIP trunk.
- 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 G450 Media Gateway will remain in the media path between the SIP trunk and the endpoint for the duration of the call. Depending on the number of media resources available in the Avaya G450 Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **Direct IP-IP Early Media** is set to *n*.
- Set the **Alternate Route Timer** to *30*. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before canceling the call.
- Default values may be used for all other fields.

add signaling-group 2		Page 1 of 1	
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: 5060	Far-end Listen Port: 5060		
	Far-end Network Region: 1		
Far-end Domain: avayalab.com			
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n		
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n		
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y		
Enable Layer 3 Test? y	IP Audio Hairpinning? n		
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n		
	Alternate Route Timer(sec): 30		

## 5.7. Trunk Group

Use the **add trunk-group** command to create trunk group for the signaling group created in **Section 5.6**. For the compliance testing, 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 **Outgoing Display** to *y* to enable name display on the trunk.
- Set the **Service Type** field to *public-ntwrk*.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**.
- Set the **Number of Members** field to **32**. It is the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk group.
- Default values are used for all other fields.

<b>add trunk-group 2</b>		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: SP Trunk</b>	COR: 1	TN: 1	<b>TAC: #02</b>
Direction: two-way	<b>Outgoing Display? y</b>	Night Service:	
Dial Access? n			
Queue Length: 0			
<b>Service Type: public-ntwrk</b>	Auth Code? n		
	Member Assignment Method: auto		
	<b>Signaling Group: 2</b>		
	<b>Number of Members: 32</b>		

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to service provider. This value defines the interval a re-INVITEs must be sent to refresh the Session Timer. For the compliance testing, a default value of **600** seconds was used.

<b>add trunk-group 2</b>		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
<b>Redirect On OPTIM Failure: 15000</b>			
SCCAN? n	Digital Loss Group: 18		
<b>Preferred Minimum Session Refresh Interval(sec): 600</b>			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	

On **Page 3**, set the **Numbering Format** field to *public*. This field specifies the format of the CPN sent to the far-end. The public numbers are automatically preceded with a + sign when passed in the “From”, “Contact” and “P-Asserted Identity” headers. The addition of the + sign impacted interoperability with the service provider. Thus, the **Numbering Format** is set to *public* and the **Numbering Format** in the route pattern is set to *pub-unk* (see **Section 5.10**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on the local endpoint to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. Default values are used for all other fields.

<b>add trunk-group 2</b>		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
<b>Numbering Format: public</b>		
	UI Treatment: service-provider	
	<b>Replace Restricted Numbers? y</b>	
	<b>Replace Unavailable Numbers? y</b>	
Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y		

On **Page 4**, the **Network Call Redirection** field should be set to **n**. The setting of **Network Call Redirection** flag to **n** disables use of the SIP REFER message to transfer an inbound call back to the PSTN.

- Set **Mark Users as Phone** to **n**.
- Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound call back to PSTN and Extension to Cellular (EC500) call scenarios.
- Set the **Support Request History** field to **n**. This parameter determines if History-Info header will be excluded in the call-redirection INVITE from the enterprise.
- Set the **Telephone Event Payload Type** to **101**.

<b>add trunk-group 2</b>		Page 4 of 21
PROTOCOL VARIATIONS		
	<b>Mark Users as Phone? y</b>	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n		
	Send Transferring Party Information? n	
	<b>Network Call Redirection? n</b>	
	<b>Send Diversion Header? y</b>	
	<b>Support Request History? n</b>	
	<b>Telephone Event Payload Type: 101</b>	
...		

## 5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering is selected to define the format of this number (**Section 5.7**), use the **change public-**



**unknown-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the service provider. They are used to authenticate the caller.

The screen below shows a subset of the 10 digits DID numbers assigned for testing. These 3 numbers were mapped to the 3 enterprise extensions 60396, 60397 and 60398. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp (s)	Prefix	Len	
5	60396	2	5148640436		Total Administered: 3
5	60397	2	5148640437	10	Maximum Entries: 540
5	60398	2	5148640438	10	

## 5.9. Inbound Routing

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. DID number sent by Fibrenoire can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group. Use the **change inc-call-handling-trmt trunk-group** 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	10	5148640436	10	60396	
public-ntwrk	10	5148640437	10	60397	
public-ntwrk	10	5148640438	10	60398	
.....					

## 5.10. Outbound Routing

In these Application Notes, the **Automatic Route Selection (ARS)** feature is used to route an outbound call via the SIP trunk to the service provider. In the compliance testing, a single digit 9 was used as the ARS access code. An enterprise caller will dial 9 to reach an outside line. To define feature access code (**fac**) 9, use the **change dialplan analysis** command as shown below.

change dialplan analysis									Page 1 of 12
DIAL PLAN ANALYSIS TABLE									
Location: all									Percent Full: 1
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
11	4	ext							
3	4	udp							
6	1	fac							
7	4	ext							
9	1	fac							

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

<b>change feature-access-codes</b>	Page 1 of 10
FEATURE ACCESS CODE (FAC)	
Abbreviated Dialing List1 Access Code:	
Abbreviated Dialing List2 Access Code:	
Abbreviated Dialing List3 Access Code:	
Abbreviated Dial - Prgm Group List Access Code:	
Announcement Access Code: *05	
Answer Back Access Code:	
Attendant Access Code:	
Auto Alternate Routing (AAR) Access Code: *008	
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>	Access Code 2:

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 testing. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern **2** for an outbound call which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0

Page 1 of 2

ARS DIGIT ANALYSIS TABLE

Location: all

Percent Full: 0

Dialed String	Total		Route	Call	Node	ANI
	Min	Max	Pattern	Type	Num	Reqd
0	1	11	2	op		n
011	10	18	2	intl		n
1	11	11	2	pubu		n
300	10	10	2	pubu		n
411	3	3	2	svcl		n
613	10	10	2	pubu		n
866	10	10	2	pubu		n
911	3	3	2	svcl		n
514	10	10	2	pubu		n

As being mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for route pattern **2** in the following manner.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance testing, 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: Pub-unk** All calls using this route pattern will use the public numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

change route-pattern 2															Page 1 of 3	
Pattern Number: 2															Pattern Name: SP Route	
SCCAN? n															Secure SIP? n	
Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted								DCS/ IXC	
						Del	Digits								QSIG	
						Dgts								Intw		
1: 2	0		1								n	user				
2:											n	user				
....																
		BCC	VALUE	TSC	CA-TSC			ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR		
		0	1	2	M	4	W			Request			Dgts	Format		
											Subaddress					
1:	y	y	y	y	y	n	n			rest			pub-unk	none		
...																

## 5.11. Saving Communication Manager Configuration Changes

The command “**save translation all**” can be used to save the configuration changes made on Communication Manager.

## 6. Configure Avaya Aura® Session Manager

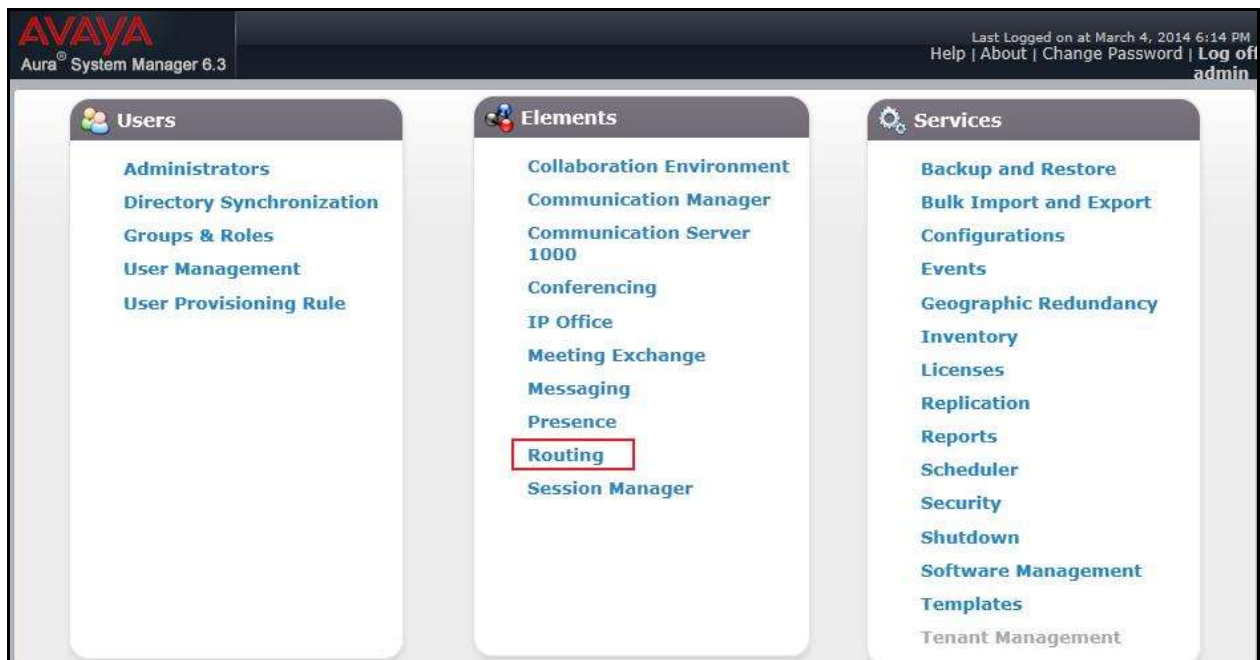
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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, 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 these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

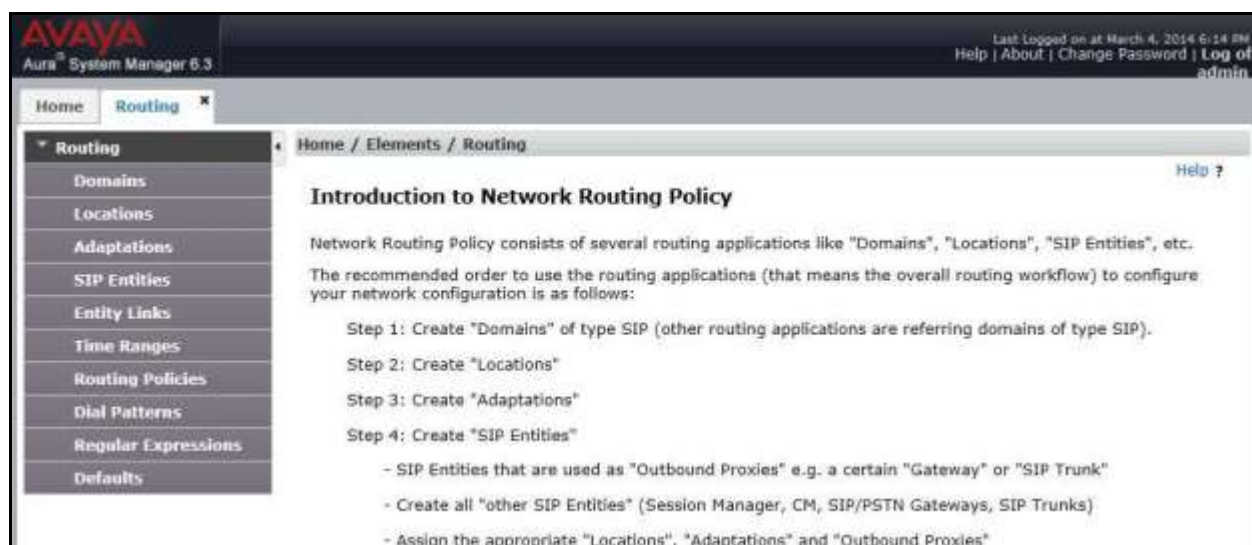
### 6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the Web GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. At the **System Manager Log On** screen, provide the appropriate credentials and click on **Login** (not shown). The initial screen shown below is then displayed.



Most of the configuration items are performed in the Routing element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen.

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



## 6.2. Specify SIP Domain

To view or change SIP domains, select **Routing** → **Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button (not shown) after changes are completed.

The following screen shows the list of configured SIP domains. The domain "avayalab.com" was already created for communication between Session Manager and Communication Manager. The domain "avayalab.com" is not known to Fibrenoire. It will be adapted by the Avaya SBCE to IP address based URI-Host to meet the SIP specification of Fibrenoire system.



## 6.3. Add Location

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

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

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

In the **Location Pattern** section (see the screen below), click **Add** and enter following values:

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

Displayed below are the screenshots for location **Belleville**, which includes all equipment on the **10.33.x**, **10.10.98.x** and **10.10.97.x** subnet including Communication Manager, Session Manager and Avaya SBCE. Click **Commit** to save.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 6.3', and a user status bar indicating 'Last Logged on at March 4, 2014 6:14 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left-hand navigation pane shows a tree structure with 'Routing' selected, and a sub-menu containing 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Home / Elements / Routing / Locations' and features a 'Location Details' section with 'Commit' and 'Cancel' buttons. The 'General' section contains fields for 'Name' (set to 'Belleville') and 'Notes' (set to 'GSSCP Belleville'). Below this is the 'Dial Plan Transparency in Survivable Mode' section, which includes an 'Enabled' checkbox, a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' dropdown. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' set to 'Kbit/sec', 'Total Bandwidth' set to '10000000', and 'Multimedia Bandwidth' set to '10000000'. A checkbox for 'Audio Calls Can Take Multimedia Bandwidth' is also present. The 'Location Pattern' section at the bottom includes 'Add' and 'Remove' buttons, a table with 3 items, and a 'Filter: Enable' option. The table has columns for 'IP Address Pattern' and 'Notes', with entries for '10.33.\*', '10.10.97.\*', and '10.10.98.\*'. A 'Select: All, None' option is at the bottom of the table.

IP Address Pattern	Notes
10.33.*	
10.10.97.*	
10.10.98.*	

## 6.4. Add 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 Avaya SBCE.

To add a new SIP Entity, navigate to **Routing** → **SIP Entities** in the left navigation pane and click **New** button in the right pane (not shown).

In **General** section, enter 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 *Other* for the Avaya SBCE.
- **Location:** Select one of the locations defined previously in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager SIP Entity. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top header shows the Avaya logo and 'Aura® System Manager 6.3'. On the right, it indicates 'Last Logged on at March 4, 2014 6:14 PM' and provides links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left navigation pane is expanded to 'Routing', which includes sub-items like Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area shows the 'SIP Entity Details' form under the 'General' tab. The breadcrumb trail is 'Home / Elements / Routing / SIP Entities'. The form fields are as follows: 'Name' (SM63), 'FQDN or IP Address' (10.33.10.26), 'Type' (Session Manager), 'Notes' (SM R6.3), 'Location' (Belleville), 'Outbound Proxy' (empty), 'Time Zone' (America/Toronto), and 'Credential name' (empty). At the bottom, the 'SIP Link Monitoring' section shows 'SIP Link Monitoring' set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are located at the top right of the form area.

SIP Entity Details	
<b>General</b>	
* Name:	SM63
* FQDN or IP Address:	10.33.10.26
Type:	Session Manager
Notes:	SM R6.3
Location:	Belleville
Outbound Proxy:	
Time Zone:	America/Toronto
Credential name:	
<b>SIP Link Monitoring</b>	
SIP Link Monitoring:	Use Session Manager Configuration

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

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

- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save (not shown).

The compliance test used **Port** entry **5060** with **TCP** for connecting to Communication Manager and **Port** entry **5060** with **TCP** for connecting to the Avaya SBCE.

The screenshot shows the 'Port' configuration section. At the top, there are input fields for 'TCP Failover port:' and 'TLS Failover port:', each followed by an empty text box. Below these are 'Add' and 'Remove' buttons. A table below shows 4 items. The table has columns: Port, Protocol, Default Domain, and Notes. The first two rows show '5060' in the Port column, 'TCP' in the Protocol column, and 'avayalab.com' in the Default Domain column. The Notes column is empty for both rows.

Port	Protocol	Default Domain	Notes
5060	TCP	avayalab.com	
5060	TCP	avayalab.com	

The following screen shows the addition of Communication Manager SIP Entity. In order for Session Manager to send SIP traffic on an entity link to Communication Manager, it is necessary to create a SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to IP address of Communication Manager. Select **Type** is **CM**.

The screenshot shows the 'SIP Entity Details' screen for a Communication Manager entity. The 'General' tab is selected. The 'Name' field is set to 'SP-CM63'. The 'FQDN or IP Address' field is set to '10.33.10.14'. The 'Type' dropdown is set to 'CM'. The 'Notes' field is empty. The 'Adaptation' dropdown is set to 'Belleville'. The 'Location' dropdown is set to 'America/Toronto'. The 'Time Zone' dropdown is set to 'America/Toronto'. The 'SIP Timer B/F (in seconds)' field is set to '4'. The 'Commit' and 'Cancel' buttons are visible at the bottom right.

**SIP Entity Details**

**General**

\* Name: SP-CM63

\* FQDN or IP Address: 10.33.10.14

Type: CM

Notes:

Adaptation: Belleville

Location: America/Toronto

Time Zone: America/Toronto

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



The following screen shows the addition of the SIP Entity for Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Select **Type** as *Other*. Select **SIP Link Monitoring** as **Link Monitoring Enabled** with the interval of **120** seconds. This setting allows Session Manager to send outbound OPTIONS heartbeat in every **120** seconds to service provider (which is forwarded by the Avaya SBCE) to query for the status of the SIP trunk connecting to service provider.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left navigation pane shows the 'Routing' menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and 'General'. The form contains the following fields and values:

- Name:** SBCE22
- FQDN or IP Address:** 10.10.98.22
- Type:** Other
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** Belleville
- Time Zone:** America/Toronto
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** none
- CommProfile Type Preference:** (empty)
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Link Monitoring Enabled
- Proactive Monitoring Interval (in seconds):** 120
- Reactive Monitoring Interval (in seconds):** 120
- Number of Retries:** 5

Buttons for 'Commit' and 'Cancel' are visible in the top right corner of the form area.

## 6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. During compliance testing, two Entity Links were created, one for Communication Manager and other for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click **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 defined in **Section 6.4**.

- **Protocol:** Select the transport protocol used for this link, **TCP** for the Entity Link to Communication Manager and **TCP** for the Entity Link to the Avaya SBCE.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other systems. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**. For Avaya SBCE, select Avaya SBCE SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager in **Section 5.6**.
- **Connection Policy:** Select **Trusted**. **Note:** If this is not selected, calls from the associated SIP Entity specified in **Section 6.4** will be denied.
- Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and to Avaya SBCE.

#### Entity Link to Communication Manager

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, and Regular Expressions. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, and Connection Policy. The row shows: \*SM63\_SP-CM63, \*SM63, TCP, \*5060, \*SP-CM63, ☐, \*5060, and trusted. There are 'Commit' and 'Cancel' buttons at the top right of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
*SM63_SP-CM63	*SM63	TCP	*5060	*SP-CM63	<input type="checkbox"/>	*5060	trusted

#### Entity Link to Avaya SBCE

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, and Regular Expressions. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, and Connection Policy. The row shows: \*SM63\_SBCE22\_TCP, \*SM63, TCP, \*5060, \*SBCE22, ☐, \*5060, and trusted. There are 'Commit' and 'Cancel' buttons at the top right of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
*SM63_SBCE22_TCP	*SM63	TCP	*5060	*SBCE22	<input type="checkbox"/>	*5060	trusted

## 6.6. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies were added, one for Communication Manager and other for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click **New** button in the right pane (not shown). The following screen is displayed.

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

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

In **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity is displayed in 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.

AVAYA  
Aura System Manager 6.3

Last Logged on at October 6, 2014 9:27  
Log off  
admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

Name: To-SPCM63

Disabled: ☐

Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SP-CH63	10.33.10.14	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select: All, None

The following screens show the Routing Policies for the Avaya SBCE.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane is expanded to 'Routing', and the 'Routing Policies' sub-item is selected. The main content area displays the 'Routing Policy Details' for a policy named 'To-SBCE22'. The 'General' tab is active, showing fields for Name, Disabled, Retries, and Notes. The 'SIP Entity as Destination' section shows a table with one entry: 'SBCE22' with FQDN or IP Address '10.10.98.22' and Type 'Other'. The 'Time of Day' section shows a table with one entry: '24/7' with Start Time '00:00' and End Time '23:59'.

**Routing Policy Details**

**General**

\* Name: To-SBCE22

Disabled: ☐

\* Retries: 0

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
SBCE22	10.10.98.22	Other	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select: All, None

## 6.7. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to Fibrenoire and vice versa. Dial Patterns define which routing 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 **New** button in the right pane (not shown).

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 testing were shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise.

The first example shows a 3 to 10-digit dialed numbers, which starts with 3 digits show in capture below, that has a destination domain of “avayalab.com” uses route policy to Avaya SBCE as defined in **Section 6.6**.

**AVAYA**  
Aura® System Manager 6.3

Routing

Home / Elements / Routing / Dial Patterns

**Dial Pattern Details**

**General**

\* Pattern: 514

\* Min: 3

\* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avayalab.com

Notes: To Service Provider

**Originating Locations and Routing Policies**

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville		To-SBCE22	0	<input type="checkbox"/>	SBCE22	

Select : All, None

The second example shows that inbound 10-digit numbers that start with 5148 to domain “avayalab.com” uses route policy to Communication Manager as defined in **Section 6.6**. These are the DID numbers assigned to the enterprise by Fibrenoire.

## 6.8. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This is most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click **New** button in the right pane (not shown). If the Session Manager Instances 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.
- **Directs Routing to Endpoints:** Enabled, to enable call routing on the Session Manager.

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name.
- **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 **Commit** to save (not shown).

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

AVAYA  
Aura® System Manager 6.3

Last Logged on at March 5, 2014 11:35 AM  
Help | About | Change Password | Log off admin

Home Session Manager x

Home / Elements / Session Manager / Session Manager Administration

### View Session Manager

Help ?  
Return

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |  
Expand All | Collapse All

#### General

SIP Entity Name

Description

Management Access Point Host Name/IP

Direct Routing to Endpoints ☒ Enable

VMware Virtual Machine ☐

#### Security Module

SIP Entity IP Address

Network Mask

Default Gateway

Call Control PHB

QOS Priority

Speed & Duplex

VLAN ID

\*SIP Firewall Configuration



## 7. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, an Avaya SBCE is used as the edge device between the Avaya Customer Premise Equipment (CPE) and Fibrenoire SIP Trunking Service.

These Application Notes assume that the installation of the Avaya SBCE and the assignment of a management IP Address have already been completed.

In this session, the naming convention for Fibrenoire is Service Provider (SP) which is connecting to external interface of Avaya SBCE. And for Avaya side is Enterprise (EN) which is connected to internal interface of Avaya SBCE.

### 7.1. Avaya Session Border Controller for Enterprise Login

Use a Web browser to access the Avaya SBCE web interface, enter `https://<ip-addr>/ucsec` in the address field of the web browser (not shown), where `<ip-addr>` is the management LAN IP address of Avaya SBCE.

Enter appropriate credentials and click **Log In**.



The login page features the Avaya logo on the left. The main heading is "Session Border Controller for Enterprise". On the right, there is a "Log In" section with fields for "Username:" and "Password:", followed by a "Log In" button. Below the login fields, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and/or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." Another paragraph states: "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." At the bottom, it says: "All users must comply with all corporate instructions regarding the protection of information assets." and "© 2011 - 2013 Avaya Inc. All rights reserved."

The main page of the Avaya SBCE will appear as shown below.



The dashboard has a left sidebar with a "Dashboard" link and a list of navigation items: Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled "Dashboard" and contains a warning message: "Application DEBUG level log messages are currently enabled on one or more subsystems. Leaving this log level enabled for extended periods of time may cause severe performance degradation." Below the warning, there are two panels. The "Information" panel displays system details: System Time (01:55:19 AM CST), Version (6.3.000-19-4338), Build Date (Fri Sep 26 09:14:23 EDT 2014), License State (OK), Aggregate Licensing Overages (0), and Peak Licensing Overage Count (0). The "Installed Devices" panel shows a table with one device: EMS SBCE62.

Information	
System Time	01:55:19 AM CST
Version	6.3.000-19-4338
Build Date	Fri Sep 26 09:14:23 EDT 2014
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0

Installed Devices
EMS SBCE62



## 7.2. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

### 7.2.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, “\*” is used for all incoming and outgoing traffic.

### 7.2.2. Routing Profiles

Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

To create a Routing Profile, select **Global Profiles → Routing**. Click on the **Add** button.

In the compliance testing, a Routing Profile **EN-to-SP** was created to use in conjunction with the server flow defined for EN. This entry is to route the outbound call from the enterprise to service provider.

In the opposite direction, a Routing Profile named **SP-to-EN** was created to be used in conjunction with the server flow defined for SP. This entry is to route the inbound call from service provider to the enterprise.

## Routing Profile for SP

The screenshot below illustrates the routing profile from Avaya SBCE to the SP network, **Global Profiles → Routing: EN-to-SP**. As shown in **Figure 1**, the SP SIP trunk is connected with transportation protocol UDP (not shown). If there is a match in the “To” or “Request URI” headers with the URI Group **SP** defined in **Section 7.2.1**, the call will be routed to the **Next Hop Server 1** which is the IP address of SP SIP trunk on port 5060.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Dashboard, Administration, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, and Routing (highlighted in red). The main content area is titled "Routing Profiles: EN-to-SP" and includes an "Add" button, "Rename", "Clone", and "Delete" buttons. Below this is a description field with the text "Click here to add a description." and a "Routing Profile" section with an "Update Priority" button and an "Add" button. A table lists the routing profile configuration:

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	192.168.104.164	UDP	Edit Delete

## Routing Profile for EN

The Routing Profile for SP to EN, **SP-to-EN**, was defined to route call where the “To” header matches the URI Group **SP** defined in **Section 7.2.1** to **Next Hop Server 1** which is the IP address of Session Manager, on port 5060 as a destination. As shown in **Figure 1**, the SIP trunk between EN and the Avaya SBCE is connected with transportation protocol TCP.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Dashboard, Administration, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, and Routing (highlighted in red). The main content area is titled "Routing Profiles: SP-to-EN" and includes an "Add" button, "Rename", "Clone", and "Delete" buttons. Below this is a description field with the text "Click here to add a description." and a "Routing Profile" section with an "Update Priority" button and an "Add" button. A table lists the routing profile configuration:

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	10.33.10.26	TCP	Edit Delete

### 7.2.3. Topology Hiding

Topology Hiding is an Avaya SBCE security feature which allows changing certain key SIP message parameters to ‘hide’ or ‘mask’ how the enterprise network may appear to an unauthorized or malicious user.

To create a Topology Hiding profile, select **Global Profiles → Topology Hiding**. Click on the **Add** button.

In the compliance testing, two Topology Hiding profiles **EN-to-SP** and **SP-to-EN** were created.

#### Topology Hiding Profile for SP

Profile **EN-to-SP** was defined to mask the enterprise SIP domain avayalab.com in “Request-URI” and “To” headers to SP IP address and “From” header to the Avaya SBCE external interface IP address; mask the enterprise SIP domain avayalab.com in the “From” and “PAI” headers to IP **10.10.98.119** (the Avaya SBCE public IP address). It is to secure the enterprise network topology and to meet the SIP requirement of the service provider.

#### Notes:

- The **Criteria** should be selected as **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “**From**” and “**To**” and “**Request-Line**” headers.

The screenshots below illustrate the Topology Hiding profile **EN-to-SP**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (highlighted), Signaling Manipulation, URI Groups, PPM Services, and Domain Policies. The main content area is titled 'Topology Hiding Profiles: EN-to-SP' and includes an 'Add' button, a list of profiles (EN-to-SP and SP-to-EN), and buttons for Rename, Clone, and Delete. A table titled 'Topology Hiding' shows the configuration for the EN-to-SP profile, with columns for Header, Criteria, Replace Action, and Overwrite Value.

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

## Topology Hiding Profile for EN

Profile **SP-to-EN** was also created to mask SP URI-Host in “Request-URI”, “From”, “To” headers to the enterprise domain *avayalab.com*, replace Record-Route, Via headers and SDP added by SP to internal IP address known to EN.

### Notes:

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “**From**”, “**To**” and “**Request-Line**” headers.

The screenshots below illustrate the Topology Hiding profile **SP-to-EN**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar shows the navigation menu with 'Global Profiles' expanded, and 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: SP-to-EN'. It includes an 'Add' button and a list of profiles: 'EN-to-SP' and 'SP-to-EN'. The 'SP-to-EN' profile is selected, showing a table of configuration rules. The table has columns: Header, Criteria, Replace Action, and Overwrite Value. The rules are as follows:

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

Buttons for 'Rename', 'Clone', 'Delete', and 'Edit' are visible at the top and bottom of the configuration area.

## 7.2.4. Server Interworking

Interworking Profile features are configured differently for Call Server and Trunk Server.

To create a Server Interworking profile, select **Global Profiles** → **Server Interworking**. Click on the **Add** button.

In the compliance testing, two Server Interworking profiles were created for SP and EN respectively.

## Server Interworking profile for SP

Profile **SP-SI** was defined to match the specification of SP. The **General** and **Advanced** settings are configured with the following parameters while the other settings for **Timers**, **URI Manipulation** and **Header Manipulation** are kept as default.

### General settings:

- **Hold Support** = *NONE*. The Avaya SBCE will not modify the hold/ resume signaling from EN to SP.
- **18X Handling** = *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from EN to SP.
- **Refer Handling** = *No*. The Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from EN to SP.
- **T.38 Support** = *Yes*. SP does support T.38 fax in the compliance testing.
- **Privacy Enabled** = *No*. The Avaya SBCE will not mask the “**From**” header with anonymous for the outbound call to SP.
- **DTMF Support** = *None*. The Avaya SBCE will send original DTMF method from EN to SP.
- Others are left as default.

The screenshots below illustrate the Server Interworking profile **SP-SI**, under the **General** tab.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar shows the navigation menu with 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: SP-SI' and includes an 'Add' button. Below this, there are tabs for 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is selected, showing a table of configuration parameters.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

### Advanced settings:

- **Record Routes = Both.** The Avaya SBCE will send “**Record-Route**” header to both call and trunk servers.
- **Topology Hiding: Change Call-ID = Yes.** The Avaya SBCE will modify “**Call-ID**” header for the call toward SP.
- **Change Max Forwards = Yes.** The Avaya SBCE will adjust the original Max-Forwards value from EN to SP by reducing the intermediate hops involving in the call flow.
- **Has Remote SBC = Yes.** SP has a SBC which interfaces its Central Office (CO) to the enterprise SIP trunk. This setting allows the Avaya SBCE to always use the SDP received from SP for the media.
- Others are left as default.

The screenshots below illustrate the Server Interworking profile **SP-SI**, under the **Advanced** tab.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and SIP Cluster. The 'Global Profiles' section is expanded, showing 'Server Interworking' as the selected profile. The main content area is titled 'Interworking Profiles: SP-SI' and features a table of settings under the 'Advanced' tab. The table lists various settings and their values, such as 'Record Routes' set to 'Both' and 'Has Remote SBC' set to 'Yes'. Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

Setting	Value
Record Routes	Both
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No



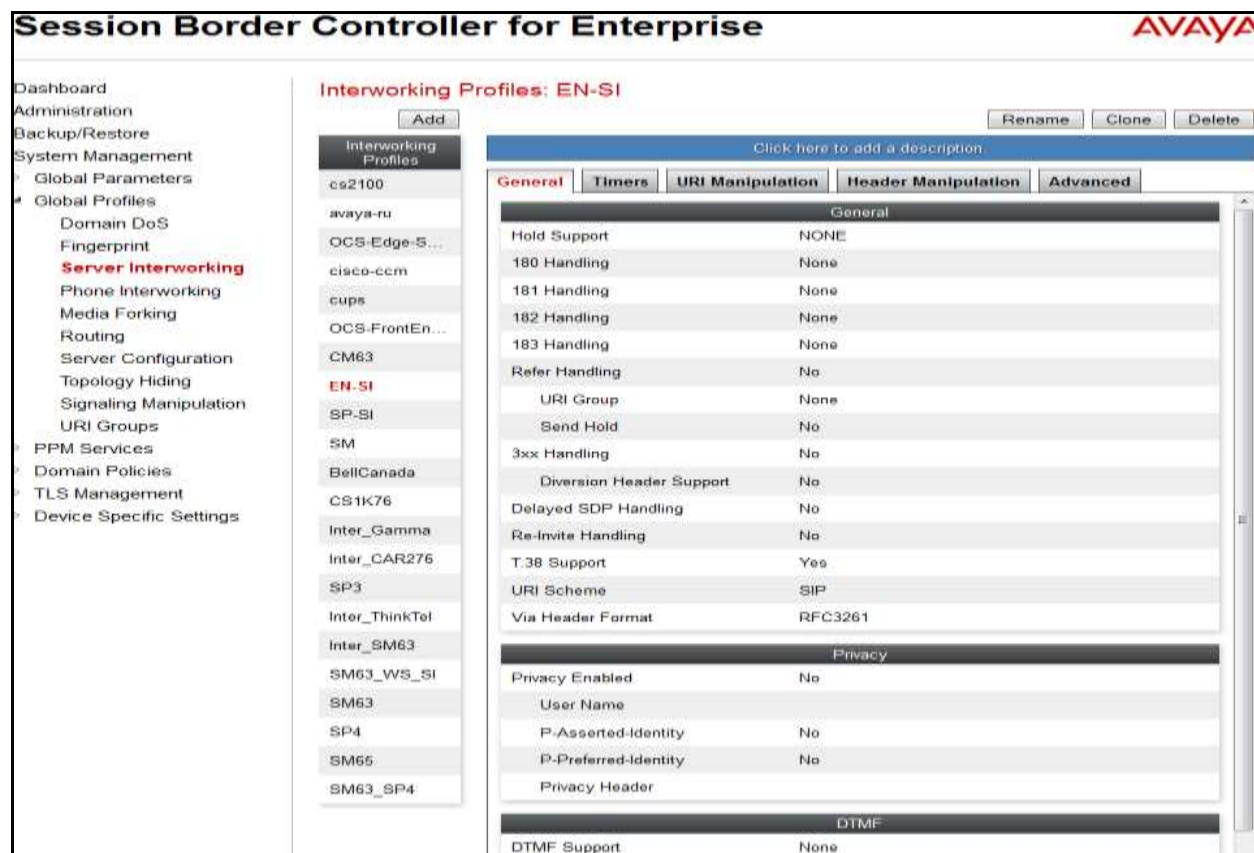
## Server Interworking profile for EN

Profile **EN-SI** was defined to match the specification of EN. The **General** and **Advanced** settings are configured with the following parameters while the other settings for **Timers**, **URI Manipulation** and **Header Manipulation** are kept as default.

### General settings:

- **Hold Support** = *NONE*.
- **18X Handling** = *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from SP to EN.
- **Refer Handling** = *No*. The Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from SP to EN.
- **T.38 Support** = *Yes*. EN does support T.38 fax.
- **Privacy Enabled** = *No*. The Avaya SBCE will not mask the “**From**” header with anonymous for an inbound call from SP. It depends on SP to enable/ disable privacy on an individual call basis.
- **DTMF Support** = *None*. The Avaya SBCE will send original DTMF method from SP to EN.
- Others are left as default.

The screenshots below illustrate the Server Interworking profile **EN-SI**, under the **General** tab.



The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) configuration interface. The left sidebar shows the navigation menu with 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: EN-SI' and includes an 'Add' button. Below this, a list of profiles is shown, with 'EN-SI' selected. The 'General' tab is active, displaying the following settings:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

### Advanced settings:

- **Record Routes = Both.** The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Topology Hiding: Change Call-ID = Yes.** The Avaya SBCE will modify “Call-ID” header for the call toward EN.
- **Change Max Forwards = Yes.** The Avaya SBCE will adjust the original Max-Forwards value from SP to EN by reducing the intermediate hops involving in the call flow.
- **Has Remote SBC = Yes.** This setting allows the Avaya SBCE to always use the SDP received from EN for the media.
- Others are left as default.

The screenshots below illustrate the Server Interworking profile **EN-SI**, under the **Advanced** tab.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar shows the navigation menu with 'Server Interworking' selected. The main content area is titled 'Interworking Profiles: EN-SI' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are tabs for 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'Advanced' tab is active, showing a table of settings for the EN-SI profile.

Setting	Value
Record Routes	Both
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No

An 'Edit' button is located at the bottom right of the settings table.

### 7.2.5. Server Configuration

Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.



To create a Server Configuration entry, select **Global Profiles → Server Configuration**. Click on the **Add** button.

In the compliance testing, two separate Server Configurations were created, server entry **SP-SC** for SP and server entry **EN-SC** for EN.

### Server Configuration for SP

Server Configuration named **SP-SC** was created for SP. It will be discussed in detail below. **General** and **Advanced** tabs are provisioned for SP on the SIP trunk for every outbound call from enterprise to PSTN. The additional **DoS Whitelist** and **DoS Protection** tabs are displayed after **DoS Protection** is enabled under **Advanced** tab, the settings for these tabs are kept as default. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from EN to SP to query the status of the SIP trunk.

In the **General** tab, click on the **Edit** button then set **Server Type** for SP as *Trunk Server*. In the compliance testing, SP supported **UDP** and listened on port **5060**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Global Parameters, Global Profiles, Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, and Server Configuration (highlighted in red). The main content area is titled "Server Configuration: SP-SC" and includes an "Add" button, a "Server Profiles" dropdown showing "SP-SC", and buttons for "Rename", "Clone", and "Delete". The "General" tab is active, showing "Server Type" set to "Trunk Server". Below this is a table with columns "IP Address / FQDN", "Port", and "Transport". The table contains one entry: IP Address / FQDN: 192.168.104.164, Port: 5060, Transport: UDP. An "Edit" button is located at the bottom right of the table.

IP Address / FQDN	Port	Transport
192.168.104.164	5060	UDP

- Under **Advanced** tab, check on **Enable DoS Protection**. From the **Interworking Profile** drop down list, select **SP-SI** as defined in Section 7.2.4. For **Signaling Manipulation Script**, select **None** as defined above. This configuration applies the specific SIP profile to the SP traffic. The other settings are kept as default.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar is the same as the previous screenshot. The main content area is titled "Server Configuration: SP-SC" and includes an "Add" button, a "Server Profiles" dropdown showing "SP-SC", and buttons for "Rename", "Clone", and "Delete". The "Advanced" tab is active, showing "Enable DoS Protection" checked, "Enable Grooming" unchecked, "Interworking Profile" set to "SP-SI", "Signaling Manipulation Script" set to "None", and "Connection Type" set to "SUBID".

Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-SI
Signaling Manipulation Script	None
Connection Type	SUBID

## Server Configuration for EN

Server Configuration named **EN-SC** created for EN is discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from SP to EN to query the status of the SIP trunk.

In the **General** tab, click on the **Edit** button then specify **Server Type** for EN as **Call Server**. In the compliance testing, the link between the Avaya SBCE and EN was **TCP** and listened on port **5060**.

**Session Border Controller for Enterprise** AVAYA

Global Profiles

- Domain DoS
- Fingerprint
- Server Interworking
- Phone Interworking
- Media Forking
- Routing
- Server Configuration**

**Server Configuration: EN-SC**

Add Rename Clone Delete

Server Profiles

- EN-SC

**General** Authentication Heartbeat Advanced

Server Type: Call Server

IP Address / FQDN	Port	Transport
10.33.10.26	5060	TCP

Edit

Under **Advanced** tab, click on the **Edit** button, from the **Interworking Profile** drop down list select **EN-SI** as defined in **Section 7.2.4** and from the **Signaling Manipulation Script** drop down list select **None**. The other settings are kept as default.

**Session Border Controller for Enterprise** AVAYA

Dashboard

- Global Parameters
- Global Profiles
- Domain DoS
- Fingerprint
- Server Interworking
- Phone Interworking
- Media Forking
- Routing
- Server Configuration**

**Server Configuration: EN-SC**

Add Rename Clone Delete

Server Profiles

- SP-SC
- EN-SC

**General** Authentication Heartbeat **Advanced**

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile: EN-SI

Signaling Manipulation Script: None

TCP Connection Type: SUBID

Edit

## 7.3. Domain Policies

Domain Policies configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

### 7.3.1. Signaling Rules

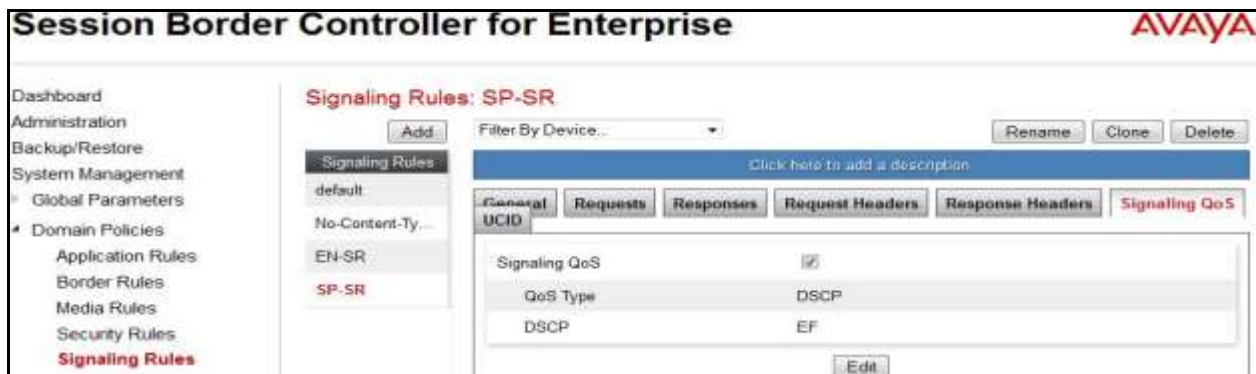
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

To clone a Signaling Rule, navigate to **Domain Policies → Signaling Rules**. With the **default** rule chosen, click on the **Clone** button.

#### Signaling Rules for SP

In the compliance testing, created signaling rule **SP-SR** is discussed below. All the tabs are kept as default values except **Signaling QoS** tab.

In **Signaling QoS** tab, click on **Edit** button and check **Signaling QoS**. Then select **EF** value for **DSCP** option.



## Signaling Rules for EN

In the compliance testing, created signaling rule **EN-SR** is discussed below. All the tabs are kept as default values except **Signaling QoS** tab.

In **Signaling QoS** tab, click on **Edit** button and check **Signaling QoS**. Then select **EF** value for **DSCP** option.



### 7.3.2. Endpoint Policy Groups

The rules created within the **Domain Policy** section are assigned to an **Endpoint Policy Group**. The **Endpoint Policy Group** is then applied to a **Server Flow** defined in the next section.

Endpoint Policy Groups were created for SP and EN.

To create a new policy group, navigate to **Domain Policies** → **End Point Policy Groups** and click on **Add**.

## Endpoint Policy Group for SP

The following screen shows **SP-PG** created for SP:

- Set **Application** to *default-trunk*.
- Set **Border** to *default*.
- Set **Media** to *default-low-med*.
- Set **Security** to *default-high*.
- Set **Signaling** to *SP-SR* as created in **Section 7.3.1**.
- Set **Time of Day** to *default*.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Dashboard, Administration, Domain Policies (Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, Time of Day Rules, End Point Policy Groups, Session Policies), and Session Policies. The main content area is titled "Policy Groups: SP-PG". It includes an "Add" button, a "Filter By Device..." dropdown, and buttons for "Rename", "Clone", and "Delete". Below these are two blue bars with text: "Click here to add a description." and "Click here to add a row description.". A "Policy Group" section contains a table with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The table has one row with the following values: 1, default-trunk, default, default-low-med, default-high, SP-SR, and default. There are "Edit" and "Clone" links for this row. A "Summary" button and an "Add" button are also present.

## Endpoint Policy Group for EN

The following screen shows **EN-PG** created for EN:

- Set **Application** to *default-trunk*.
- Set **Border** to *default*.
- Set **Media** to *default-low-med*.
- Set **Security** to *default-high*.
- Set **Signaling** to *EN-SR* as created in **Section 7.3.1**.
- Set **Time of Day** to *default*.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Dashboard, Administration, Domain Policies (Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, Time of Day Rules, End Point Policy Groups, Session Policies), and Session Policies. The main content area is titled "Policy Groups: EN-PG". It includes an "Add" button, a "Filter By Device..." dropdown, and buttons for "Rename", "Clone", and "Delete". Below these are two blue bars with text: "Click here to add a description." and "Hover over a row to see its description.". A "Policy Group" section contains a table with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The table has one row with the following values: 1, default-trunk, default, default-low-med, default-high, EN-SR, and default. There are "Edit" and "Clone" links for this row. A "Summary" button and an "Add" button are also present.



## 7.4. Device Specific Settings

Device Specific Settings allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

### 7.4.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information was defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. This information populates the **Network Management** tab, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings** → **Network Management** and under the **Networks** tab verify the IP addresses assigned to the interfaces. The following screen shows the private interface is assigned to **A1** and the public interface is assigned to **B1**.

The screenshot shows the 'Network Management: SBCE62' page with the 'Networks' tab selected. A table lists two networks: Network\_A1 and Network\_B1. Network\_A1 has a gateway of 10.10.98.1, subnet mask of 255.255.255.192, and is assigned to interface A1 with IP address 10.10.98.22. Network\_B1 has a gateway of 10.10.98.97, subnet mask of 255.255.255.224, and is assigned to interface B1 with IP address 10.10.98.119. Both networks have 'Edit' and 'Delete' links.

Name	Gateway	Subnet Mask	Interface	IP Address	Edit	Delete
Network_A1	10.10.98.1	255.255.255.192	A1	10.10.98.22,	Edit	Delete
Network_B1	10.10.98.97	255.255.255.224	B1	10.10.98.119,	Edit	Delete

Enable the interfaces used to connect to the inside and outside networks on the **Interfaces** tab. The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface, click its **Toggle** button.

The screenshot shows the 'Network Management: SBCE62' page with the 'Interfaces' tab selected. A table lists two interfaces: A1 and B1. Both interfaces have a 'Status' of 'Enabled'. There is an 'Add VLAN' button in the top right corner.

Interface Name	VLAN Tag	Status
A1		Enabled
B1		Enabled

### 7.4.2. Media Interface

The Media Interface screen is where the media ports are defined. The Avaya SBCE will open a connection for RTP on the defined ports.

To create a new Media Interface, navigate to **Device Specific Settings → Media Interface** and click **Add**. Separate Media Interfaces were created for both inside and outside interfaces. The following screen shows the Media Interfaces created in the compliance testing.

**Note:** After the media interfaces are created, an application restart is necessary before the changes will take effect.

The screenshot shows the 'Media Interface: SBCE62' configuration page. On the left is a navigation menu with 'Media Interface' selected under 'Device Specific Settings'. The main area has a 'Media Interface' tab and a table of existing interfaces. A warning message states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' An 'Add' button is in the top right.

Name	Media IP	Port Range	Edit	Delete
InsideMedia	10.10.98.22	35000 - 40000		
OutsideMedia	10.10.98.119	35000 - 40000		

### 7.4.3. Signaling Interface

The Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP requests on the defined port.

To create a new Signaling Interface, navigate to **Device Specific → Settings → Signaling Interface** and click **Add**.

Separate Signaling Interfaces were created for both inside and outside interfaces. The following screen shows the Signaling Interfaces were created in the compliance testing with UDP/5060 for the outside interface to SP and TCP/5060 for the inside interface to EN.

The screenshot shows the 'Signaling Interface: SBCE62' configuration page. On the left is a navigation menu with 'Signaling Interface' selected under 'Device Specific Settings'. The main area has a 'Signaling Interface' tab and a table of existing interfaces. An 'Add' button is in the top right.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
InsideSignaling	10.10.98.22	5060	5060	---	None		
OutsideSignaling	10.10.98.119	5060	5060	---	None		

#### 7.4.4. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.

In the compliance testing, separate Server Flows were created for SP and EN. To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown). In the new window that appears, enter the following values. The other fields are kept default.

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.5** to assign to the Flow.
- **URI Group:** Select the URI Group created in **Section 7.2.1** to assign to the Flow.  
**Note:** URI Group can be set to “\*” to match all calls.
- **Received Interface:** Select the Signaling Interface created in **Section 7.4.3** that the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 7.4.3** used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface created in **Section 7.4.2** used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 7.3.2** to assign to the Server Configuration.
- **Routing Profile:** Select the Routing Profile created in **Section 7.2.2** that the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the Topology-Hiding profile created in **Section 7.2.3** to apply to the Server Configuration.
- Click **Finish**.



The following screen shows the Server Flow **SP-SF** configured for SP.

The screenshot shows a configuration window titled "Edit Flow: SP-SF". It contains the following fields and values:

Field	Value
Flow Name	SP-SF
Server Configuration	SP-SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	InsideSignaling
Signaling Interface	OutsideSignaling
Media Interface	OutsideMedia
End Point Policy Group	SP-PG
Routing Profile	SP-to-EN
Topology Hiding Profile	EN-to-SP
File Transfer Profile	None

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

Similarly, the following screen shows the Server Flow **EN-SF** configured for EN.

The screenshot shows a configuration window titled "Edit Flow: EN-SF". It contains the following fields and values:

Field	Value
Flow Name	EN-SF
Server Configuration	EN-SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	OutsideSignaling
Signaling Interface	InsideSignaling
Media Interface	InsideMedia
End Point Policy Group	EN-PG
Routing Profile	EN-to-SP
Topology Hiding Profile	SP-to-EN
File Transfer Profile	None

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

## 8. Fibrenoire Service Configuration

Fibrenoire is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise side. Fibrenoire will provide the customer with the necessary information to configure the SIP connection from the enterprise to Fibrenoire. The information provided by Fibrenoire includes:

- IP address and port number used for signaling through security devices (if any).
- IP address and port number used for media through security devices (if any).
- Fibrenoire SIP domain. In the compliance testing, Fibrenoire preferred to use IP address as an URI-Host.
- CPE SIP domain. In the compliance testing, Fibrenoire preferred to use IP address of the Avaya SBCE as an URI-Host.
- Supported codecs.
- DID numbers.

The sample configuration between Fibrenoire and the enterprise for the compliance testing is a static configuration. There is no registration on the SIP trunk implemented on either Fibrenoire or enterprise side.

## 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.

### 9.1. Verification Steps

- Verify that endpoints at the enterprise site can place call to PSTN and that the call remains active for more than 35 seconds. This time period is included to satisfy SIP protocol timers.
- Verify that endpoints at the enterprise site can receive call from PSTN and that the call can remain active for more than 35 seconds. This time period is included satisfy SIP protocol timers.
- Verify that the user on 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. Protocol Traces

The following SIP headers are inspected using Wireshark trace analysis:

- Request-URI: verify the called party number and SIP domain.
- From: verify the calling party name and number.
- To: verify the called party name and number.
- P-Asserted-Identity: verify the calling party name and number.
- Privacy: verify the value “user” and/or “id” presents the private call scenario.

The following attributes in SIP message body are inspected using Wireshark trace analysis:

- Connection Information (c line): verify IP address of near end and far end endpoints.

- Time Description (t line): verify session timeout value of near end and far end endpoints.
- Media Description (m line): verify audio port, codec, DTMF event description.
- Media Attribute (a line): verify specific audio port, codec,ptime, send/ receive ability, DTMF event and fax attributes.

### 9.3. Troubleshooting

The followings are some tool and commands to debug/view the call progress and trunk status and activity.

#### 9.3.1. The Avaya SBCE

Use a network sniffing tool (e.g., Wireshark) to monitor the SIP signaling messages between Fibrenoire and the Avaya SBCE.

#### 9.3.2. Communication Manager

Below is a list of Communication Manager commands that can be run using SAT.

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

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise 6.3 to Fibrenoire Canada SIP Trunking Service. Fibrenoire SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large the enterprises. Fibrenoire provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The Fibrenoire SIP Trunking Service is considered **compliant** with Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.3.

## 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 6.3.4, July 2014.
- [2] *Administering Avaya Aura® System Platform*, Release 6.3.4, July 2014.
- [3] *Administering Avaya Aura® Session Manager*, Release 6.3, September 2014.
- [4] *Administering Avaya Aura® Communication Manager*, Release 6.3, Issue 7, September 2014.
- [5] *Programming Call Vectoring Features in Avaya Aura® Call Center Elite*, Release 6.3, May 2013.
- [6] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.2, January 2013.
- [7] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010.
- [8] *Administering Avaya one-X® Communicator*, July 2013.
- [9] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 5, October 2014.
- [10] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 6.3, Issue 3, October 2014.
- [11] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.
- [12] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communication Manager Rel. 6.3 and Avaya Aura® Session Managers Rel. 6.3*, Issue 1.0, October 2014.
- [13] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [14] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [15] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Product documentation for Fibrenoire Networks' SIP Trunking Solution is available from Fibrenoire.

---

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

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

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