



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

---

# **Application Notes for Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0 with Charter Spectrum Business SIP Trunk Service – Issue 1.0**

### **Abstract**

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

The Charter Spectrum Business SIP Trunking service provide customers with PSTN access via a SIP trunk between the enterprise and the service provider's network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

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

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results .....	6
2.3.	Support .....	6
3.	Reference Configuration .....	7
4.	Equipment and Software Validated .....	10
5.	Configure Avaya Aura® Communication Manager .....	11
5.1.	Licensing and Capacity .....	12
5.2.	System Features.....	13
5.3.	IP Node Names.....	15
5.4.	Codecs .....	16
5.5.	IP Network Regions .....	17
5.6.	Signaling Group .....	18
5.7.	Trunk Group.....	20
5.8.	Calling Party Information.....	24
5.9.	Inbound Routing.....	25
5.10.	Outbound Routing .....	26
6.	Configure Avaya Aura® Session Manager .....	30
6.1.	System Manager Login and Navigation.....	31
6.2.	SIP Domain .....	32
6.3.	Locations .....	32
6.4.	Adaptations.....	35
6.5.	SIP Entities .....	36
6.6.	Entity Links .....	40
6.7.	Routing Policies .....	42
6.8.	Dial Patterns .....	43
7.	Configure Avaya Session Border Controller for Enterprise .....	45
7.1.	System Access.....	45
7.2.	System Management .....	46
7.3.	Network Management .....	48
7.4.	Media Interfaces .....	49
7.5.	Signaling Interfaces.....	51
7.6.	Server Interworking.....	53
7.6.1.	Server Interworking Profile – Enterprise.....	53
7.6.2.	Server Interworking Profile – Service Provider.....	56
7.7.	Signaling Manipulation .....	58
7.8.	Server Configuration .....	59
7.8.1.	Server Configuration Profile – Enterprise .....	59
7.8.2.	Server Configuration Profile – Service Provider .....	61
7.9.	Routing .....	63
7.9.1.	Routing Profile – Enterprise .....	63

7.9.2.	Routing Profile – Service Provider .....	64
7.10.	Topology Hiding.....	65
7.10.1.	Topology Hiding Profile – Enterprise .....	65
7.10.2.	Topology Hiding Profile – Service Provider.....	66
7.11.	End Point Policy Groups .....	67
7.11.1.	End Point Policy Group – Enterprise .....	67
7.11.2.	End Point Policy Group – Service Provider.....	68
7.12.	End Point Flows.....	69
7.12.1.	End Point Flow – Enterprise .....	69
7.12.2.	End Point Flow – Service Provider .....	70
8.	Charter Spectrum Business SIP Trunking Service Configuration .....	71
9.	Verification and Troubleshooting .....	71
9.1.	General Verification Steps .....	71
9.2.	Communication Manager Verification.....	71
9.3.	Session Manager Verification .....	72
9.4.	Avaya SBCE Verification .....	74
10.	Conclusion .....	79
11.	References.....	79
12.	Appendix A: SigMa Script.....	80

# 1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between the Charter Spectrum Business SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.0 and various Avaya endpoints, listed in **Section 4**.

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

**Note** – As a required component of the Charter Spectrum Business SIP Trunking service offering, Charter will install a Customer Premises Equipment (CPE) device at the customer premises (enterprise site). Charter will perform the initial configuration and maintenance of this device as required. The Charter managed CPE device will constitute the service demarcation point between the service provider and the enterprise site.

Throughout these Application Notes, the terms “Service Provider”, “Charter Spectrum Business” and “Charter” will be used interchangeably throughout these Application Notes.

## 2. General Test Approach and Test Results

A simulated CPE site containing all the equipment for the Avaya SIP-enabled enterprise solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Charter Spectrum Business SIP Trunking service via the Charter’s managed CPE device, and a broadband connection to the public Internet.

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

## 2.1. Interoperability Compliance Testing

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

- SIP trunk static IP authentication.
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk via the service provider network.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones using “This Computer” and “Other Phone” modes. (H.323, SIP).
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows softphones (SIP).
- Inbound and outbound PSTN calls to/from SIP remote workers using Avaya 96x1 deskphones, Avaya one-X® Communicator and Avaya Communicator for Windows softphones.
- Various call types, including: local, long distance and local directory assistant (411).
- Codec G.711MU.
- Inbound and outbound PSTN calls using VoIP media resources in Avaya Media Gateways and the Avaya Aura® Media Server at the enterprise network.
- DTMF tones passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail redirection and navigation.
- User features such as hold and resume, transfer and conference.
- Off-net call transferring, call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Proper response/error treatment to different failure conditions.

**Note** – Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

The following items are not supported or were not tested:

- The use of the SIP REFER method for network call redirection is not currently supported by Charter.
- Inbound toll-free calls and 911 emergency calls are supported but were not tested as part of the compliance test.
- T.38 fax is not currently supported by Charter.

## 2.2. Test Results

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

- **No matching codec on outbound calls:** If an unsupported audio codec is received by Charter on the SIP Trunk (e.g., 722), Charter will respond with “480 Temporarily Unavailable” instead of “488 Not Acceptable Here”, the user will hear re-order. This issue does not have any user impact, and should not be seen since the codecs will be matched during the installation, it is listed here simply as an observation.
- **Inbound calls to an unassigned enterprise extension:** Communication Manager sends a “404 Not Found” message to Charter when it receives calls to an unassigned extension, the user hears re-order instead of the common announcement informing the user that he/she has reached a non-working number, to please check the number and to try again. This issue is considered non service affecting and it’s being investigated by Charter, in order to apply the correct announcement to the user.
- **Conference in Avaya Communicator softclients:** The Communication Manager conference feature is not supported in the Avaya Communicator current software release 2.1.3.80. An Avaya Aura® Conferencing server is required for ad-hoc conferences. This feature should be available in the upcoming release 3.0 of Avaya Communicator.
- **SIP header optimization:** There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider’s network. These headers were removed with the purposes of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider’s network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charging-Vector and P-Location (**Section 6.4**).

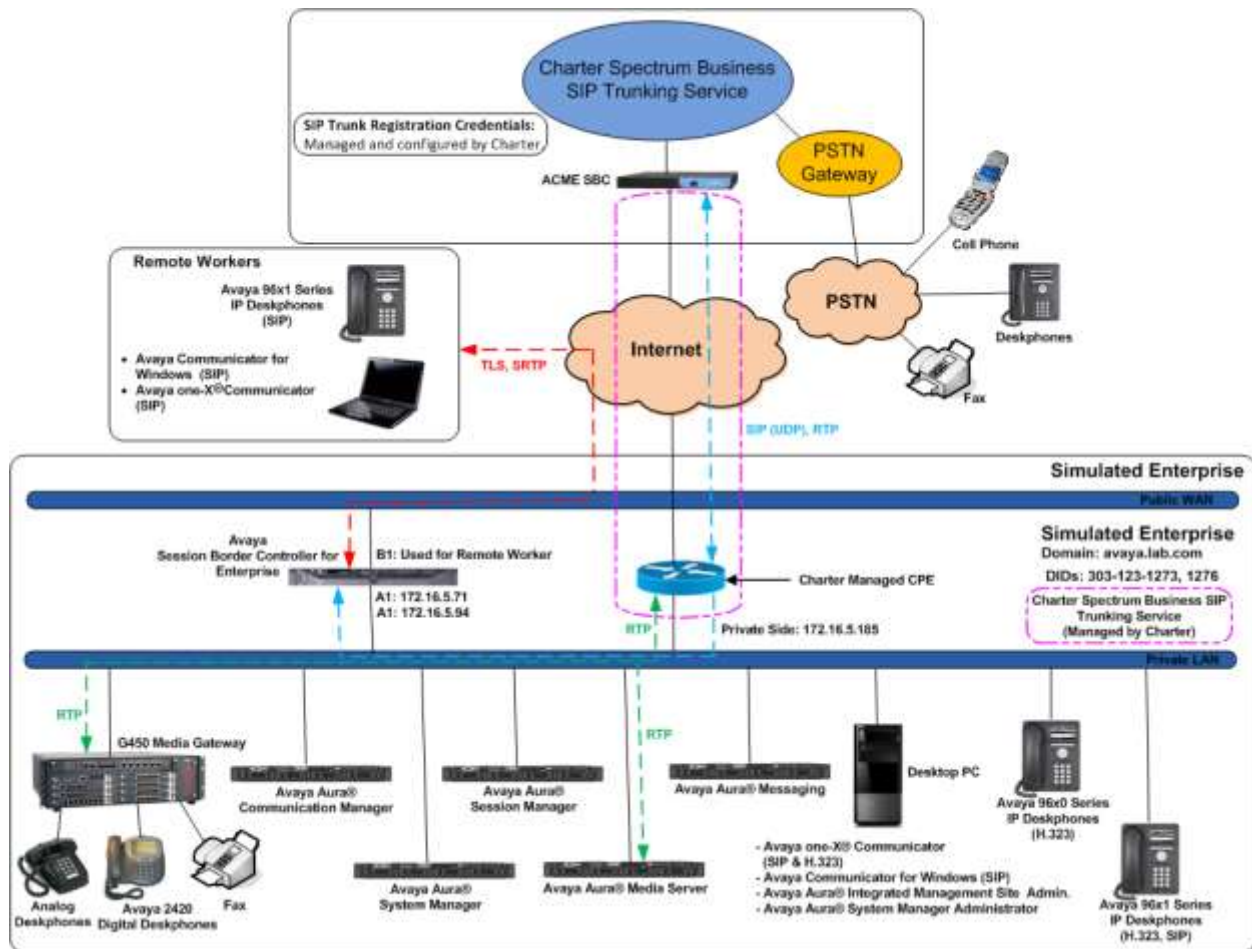
## 2.3. Support

For support on Charter Spectrum Business SIP Trunking service visit the corporate Web page at: <https://business.spectrum.com/> or call 800-314-7195.

### 3. Reference Configuration

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

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



**Figure 1: Avaya SIP Enterprise Solution connected to Charter Spectrum Business SIP Trunking Service**

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

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

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

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

For security reasons, TLS and SRTP are the recommended protocols to be used by all remote workers endpoints.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult [9] in the **References** section for additional information on this topic.

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

The transport protocol between the public interface of the Avaya SBCE and the Charter managed CPE device was UDP. The transport protocol between the private interface of the Avaya SBCE and the enterprise Session Manager across the enterprise IP network was TCP.



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

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

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

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

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

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
<b>Avaya</b>	
Avaya Aura® Communication Manager	7.0.0.2.0 (00.0.441.0-22684)
Avaya Aura® Session Manager	7.0.0.1 (7.0.0.1.700102)
Avaya Aura® System Manager	7.0.0.1 Build No. 7.0.0.0.16266-7.0.9.7001011 Software Update Rev. No. 7.0.0.1.4212
Avaya Session Border Controller for Enterprise	7.0.0-21-6602 Patch: sbc700-p001-20151005-7.0.0-1.x86_64.rpm
Avaya Aura® Messaging	6.3.3 Service Pack 3 (MSG-03.0.141.0-348_0304)
Avaya Aura® Media Server	7.7.0.236
Avaya G450 Media Gateway	37.20.0
Avaya 96x0 Series IP Deskphone (H.323)	Avaya one-X® Desk phone Edition Version S3.250A
Avaya 96x1 Series IP Deskphone (SIP)	Avaya one-X® Deskphone SIP Version 7.0.0.39
Avaya 96x1 Series IP Deskphone (H.323)	Avaya one-X® Deskphone H.323 Version 6.6029
Avaya one-X® Communicator (H.323, SIP)	6.2.10.03-FP10
Avaya Communicator for Windows (SIP)	2.1.3.80
Avaya 2420 Series Digital Deskphone	N/A
Avaya 6210 Analog Deskphone	N/A
<b>Charter Spectrum Business</b>	
Broadworks Broadsoft Application Server	AS_Rel_17.sp4_1.197
Acme Packet 4500 Series SBC	SCX6.2.0 MR-9 GA (Build 1014)
Adtran NetVanta 3430 Modular Access Router	R10.3.0.V

**Note** – The Adtran NetVanta 3430 Modular Access Router shown on the table above was installed at the enterprise site, and it is referenced throughout this document as “Charter managed CPE device”.

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

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

## 5. Configure Avaya Aura® Communication Manager

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

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Some screens captures will show the use of the **change** command instead of the **add** command, since the configuration used for the testing was previously added.

## 5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **122** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

display system-parameters customer-options		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	10
Maximum Concurrently Registered IP Stations:	18000	1
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	41000	1
Maximum Video Capable IP Softphones:	18000	7
Maximum Administered SIP Trunks:	24000	122
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
(NOTE: You must logoff & login to effect the permission changes.)		

## 5.2. System Features

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

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

  Music (or Silence) on Transferred Trunk Calls? all
  DID/Tie/ISDN/SIP Intercept Treatment: attendant
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
  Automatic Circuit Assurance (ACA) Enabled? n

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

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

change system-parameters features		Page 9 of 19
FEATURE-RELATED SYSTEM PARAMETERS		
CPN/ANI/ICLID PARAMETERS		
CPN/ANI/ICLID Replacement for Restricted Calls:	<u>restricted</u>	_____
CPN/ANI/ICLID Replacement for Unavailable Calls:	<u>unavailable</u>	_____
DISPLAY TEXT		
	Identity When Bridging:	<u>principal</u>
	User Guidance Display?	<u>n</u>
Extension only label for Team button on 96xx H.323 terminals? <u>n</u>		
INTERNATIONAL CALL ROUTING PARAMETERS		
	Local Country Code:	_____
	International Access Code:	_____
SCCAN PARAMETERS		
	Enable Enbloc Dialing without ARS FAC?	<u>n</u>
CALLER ID ON CALL WAITING PARAMETERS		
	Caller ID on Call Waiting Delay Timer (msec):	<u>200</u>

### 5.3. IP Node Names

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

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
ASBCE A1	172.16.5.71	
Lab-HG-SM	172.16.5.32	
MA-CM	192.168.10.12	
default	0.0.0.0	
media_server	192.168.10.46	
msqserver	172.16.5.12	
procr	172.16.5.201	
procr6	::	
( 8 of 8 administered node-names were displayed )		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

## 5.4. Codecs

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

change ip-codec-set 2 Page 1 of 2

IP CODEC SET

Codec Set: 2

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1:	G.711MU	n	2	20
2:		—	—	
3:		—	—	
4:		—	—	
5:		—	—	
6:		—	—	
7:		—	—	

On **Page 2**, set the **Fax Mode** to *off*. Charter does not support T.38 fax.

change ip-codec-set 2 Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? n

	Mode	Redundancy	Packet Size(ms)
FAX	off	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20



## 5.5. IP Network Regions

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

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

change ip-network-region 2		Page 1 of 20
IP NETWORK REGION		
Region: 2		
Location: 1	Authoritative Domain: <u>avaya.lab.com</u>	
Name: <u>SP Region</u>	Stub Network Region: <u>n</u>	
MEDIA PARAMETERS		
Codec Set: <u>2</u>	Intra-region IP-IP Direct Audio: <u>yes</u>	
UDP Port Min: <u>2048</u>	Inter-region IP-IP Direct Audio: <u>yes</u>	
UDP Port Max: <u>3349</u>	IP Audio Hairpinning? <u>n</u>	
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: <u>46</u>		
Audio PHB Value: <u>46</u>		
Video PHB Value: <u>26</u>		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: <u>6</u>		
Audio 802.1p Priority: <u>6</u>		
Video 802.1p Priority: <u>5</u>		
AUDIO RESOURCE RESERVATION PARAMETERS		
H.323 IP ENDPOINTS	RSVP Enabled? <u>n</u>	
H.323 Link Bounce Recovery? <u>y</u>		
Idle Traffic Interval (sec): <u>20</u>		
Keep-Alive Interval (sec): <u>5</u>		
Keep-Alive Count: <u>5</u>		

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

change ip-network-region 2										Page	4 of	20
Source Region: 2      Inter Network Region Connection Management										I		M
dst rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Intervening Prio Shr Regions	Dyn CAC	A	G		R	L	t
1	2	y	NoLimit				n					e
2	2										all	t
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												

## 5.6. Signaling Group

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

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

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

- **Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to *y*.

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

change signaling-group 2		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? <input type="checkbox"/>	Transport Method: tcp	
Q-SIP? <input type="checkbox"/>		
IP Video? <input type="checkbox"/>	Enforce SIPS URI for SRTP? <input type="checkbox"/>	
Peer Detection Enabled? <input type="checkbox"/>	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? <input type="checkbox"/>		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? <input type="checkbox"/>		
Alert Incoming SIP Crisis Calls? <input type="checkbox"/>		
Near-end Node Name: procr	Far-end Node Name: Lab-HG-SM	
Near-end Listen Port: 5070	Far-end Listen Port: 5070	
		Far-end Network Region: 2
Far-end Domain: avaya.lab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? <input type="checkbox"/>	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? <input type="checkbox"/>	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? <input type="checkbox"/>	
Enable Layer 3 Test? <input type="checkbox"/>	IP Audio Hairpinning? <input type="checkbox"/>	
H.323 Station Outgoing Direct Media? <input type="checkbox"/>	Initial IP-IP Direct Media? <input type="checkbox"/>	
	Alternate Route Timer(sec): 6	

- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TCP, the well-known port value is 5060). This is necessary so the SM can distinguish this trunk from the trunk used for other enterprise SIP traffic. For the compliance test both the **Near-end Listen Port** and **Far-end Listen Port** were set to *5070*.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to *y*. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to *n*, then the Avaya Media Gateway or Media Server will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and Media Server, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields.

## 5.7. Trunk Group

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

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

```
change trunk-group 2                                     Page 1 of 21
TRUNK GROUP
Group Number: 2      Group Type: sip      CDR Reports: y
Group Name: Service Provider      COR: 1      TN: 1      TAC: 602
Direction: two-way      Outgoing Display? n
Dial Access? n      Night Service:
Queue Length: 0
Service Type: public-ntwrk      Auth Code? n
Member Assignment Method: auto
Signaling Group: 2
Number of Members: 10
```

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

change trunk-group 2		Page 2 of 21
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: <u>auto</u>		
		Redirect On OPTIM Failure: <u>5000</u>
SCCAN? <u>n</u>	Digital Loss Group: <u>18</u>	
		Preferred Minimum Session Refresh Interval(sec): <u>600</u>
Disconnect Supervision - In? <u>y</u> Out? <u>y</u>		
XOIP Treatment: <u>auto</u>		Delay Call Setup When Accessed Via IGAR? <u>n</u>
Caller ID for Service Link Call to H.323 1xC: <u>station-extension</u>		

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

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

On **Page 4**, set the **Network Call Redirection** field to *n*. With this setting, Communication Manager will not use the REFER method, which is not supported by Charter, for the redirection of PSTN calls that are transferred back to the SIP trunk. Set the **Send Diversion Header** field to *y* and **Support Request History** to *n*. Set the **Telephone Event Payload Type** to **101**, the value preferred by Charter. Set **Identity for Calling Party Display** to *P-Asserted-Identity*. Default values were used for all other fields.

change trunk-group 2	Page 4 of 21
<b>PROTOCOL VARIATIONS</b>	
Mark Users as Phone? <u>n</u>	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? <u>n</u>	
Send Transferring Party Information? <u>n</u>	
Network Call Redirection? <u>n</u>	
Send Diversion Header? <u>y</u>	
Support Request History? <u>n</u>	
Telephone Event Payload Type: <u>101</u>	
Convert 180 to 183 for Early Media? <u>y</u>	
Always Use re-INVITE for Display Updates? <u>n</u>	
Identity for Calling Party Display: <u>P-Asserted-Identity</u>	
Block Sending Calling Party Location in INVITE? <u>n</u>	
Accept Redirect to Blank User Destination? <u>n</u>	
Enable Q-SIP? <u>n</u>	
Interworking of ISDN Clearing with In-Band Tones: <u>keep-channel-active</u>	
Request URI Contents: <u>may-have-extra-digits</u>	

## 5.8. Calling Party Information

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

change private-numbering 1					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	3			4	Total Administered: 5 Maximum Entries: 540
4	5			4	
4	3042	2	3031231273	10	
4	3044	2	3031231275	10	
4	3047	2	3031231274	10	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	



## 5.9. Inbound Routing

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

change inc-call-handling-trmt trunk-group 2					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/ Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	10	3031231273	10	3042	
public-ntwrk	10	3031231274	10	3047	
public-ntwrk	10	3031231275	10	3044	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	

## 5.10. Outbound Routing

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

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all			Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	13	udp							
1	4	dac							
2	4	ext							
3	4	ext							
4	4	udp							
5	4	ext							
6	3	dac							
7	4	ext							
8	1	fac							
9	1	fac							
*	3	dac							
#	2	dac							

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

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:	8	
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code:	#7	
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code:	8	
Auto Route Selection (ARS) - Access Code 1:	9	Access Code 2: _____
Automatic Callback Activation:		Deactivation: _____
Call Forwarding Activation Busy/DA: _____	All: _____	Deactivation: _____
Call Forwarding Enhanced Status: _____	Act: _____	Deactivation: _____
Call Park Access Code:		
Call Pickup Access Code:	*44	
CAS Remote Hold/Answer Hold-Unhold Access Code:		
CDR Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation:		Deactivation: _____
Contact Closure Open Code:		Close Code: _____

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

change ars analysis 17							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
170	11	11	deny	fnpa	—	n	
1700	11	11	deny	fnpa	—	n	
171	11	11	deny	fnpa	—	n	
172	11	11	2	fnpa	—	n	
173	11	11	deny	fnpa	—	n	
174	11	11	deny	fnpa	—	n	
175	11	11	deny	fnpa	—	n	
176	11	11	deny	fnpa	—	n	
177	11	11	deny	fnpa	—	n	
178	11	11	deny	fnpa	—	n	
1786	11	11	2	fnpa	—	n	
179	11	11	deny	fnpa	—	n	
180	11	11	deny	fnpa	—	n	
1800	11	11	2	fnpa	—	n	
1800555	11	11	deny	fnpa	—	n	

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

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk:** Set to **1** to ensure 1 + 10 digits are sent to the service provider for long distance numbers in the North American Numbering Plan (NANP).
- **Numbering Format:** Set to **unk-unk**. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form in **Section 5.7**.

change route-pattern 2															Page 1 of 3	
Pattern Number: 2															Pattern Name: <u>Serv. Provider</u>	
SCCAN? <u>n</u> Secure SIP? <u>n</u> Used for SIP stations? <u>n</u>																
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Dgts					DCS/ QSIG Intw	IXC			
1:	<u>2</u>	<u>0</u>	<u>1</u>									<u>n</u>	<u>user</u>			
2:												<u>n</u>	<u>user</u>			
3:												<u>n</u>	<u>user</u>			
4:												<u>n</u>	<u>user</u>			
5:												<u>n</u>	<u>user</u>			
6:												<u>n</u>	<u>user</u>			

	BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	Sub	Numbering	LAR
	0	1	2	M	4	W	Request		Dgts	Format	
1:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>			<u>unk-unk</u>	<u>none</u>
2:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>				<u>none</u>
3:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>				<u>none</u>
4:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>				<u>none</u>
5:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>				<u>none</u>
6:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>				<u>none</u>

**Note** - Enter the **save translation** command (not shown) to save all the changes made to the Communication Manager configuration in the previous sections.

## 6. Configure Avaya Aura® Session Manager

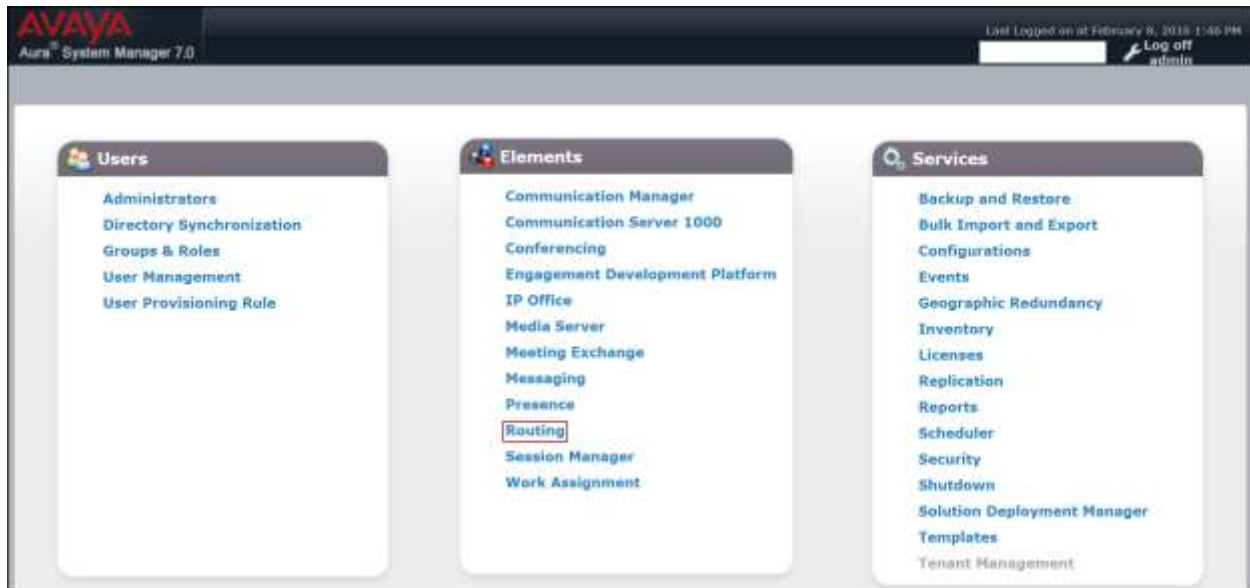
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

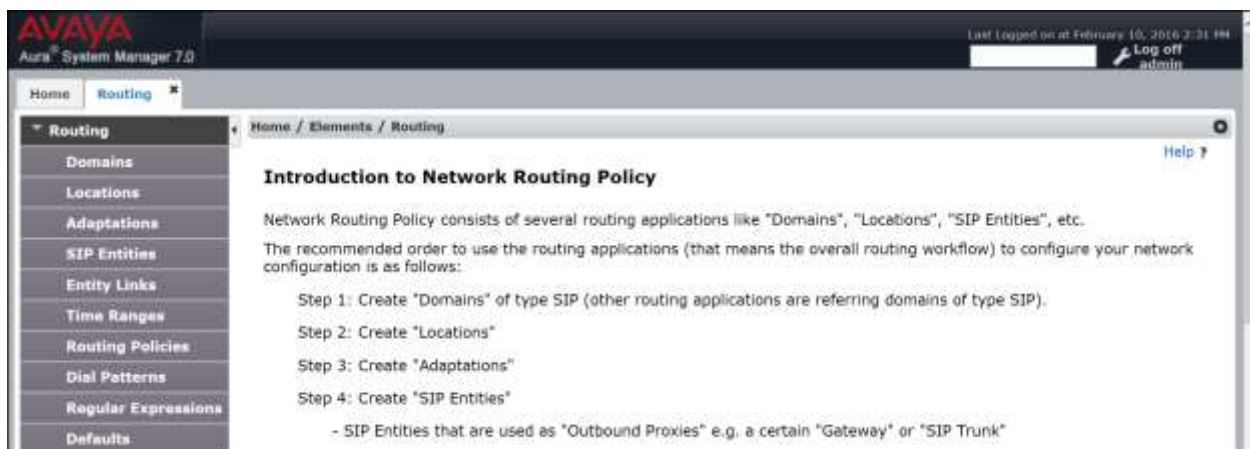
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

## 6.1. System Manager Login and Navigation

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



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



## 6.2. SIP Domain

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

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

The screen below shows the entry for the enterprise domain.

The screenshot displays the Avaya System Manager 7.0 interface. The left-hand navigation pane is expanded to show the 'Routing' section, with 'Domains' selected. The main content area is titled 'Domain Management' and shows a table with one item. The table has columns for 'Name', 'Type', and 'Notes'. The entry is 'avaya.lab.com' with Type 'sip' and Notes 'Enterprise Domain'. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the table area.

Name	Type	Notes
avaya.lab.com	sip	Enterprise Domain

## 6.3. Locations

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

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



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

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The left sidebar shows a navigation menu with 'Routing' selected, and sub-items like 'Domains', 'Locations', 'Adaptations', etc. The main content area is titled 'Location Details' and contains several sections for configuring the 'HG Session Manager' location.

**Location Details**

**General**

- Name:** HG Session Manager
- Notes:** (empty text area)

**Dial Plan Transparency in Survivable Mode**

- Enabled:** ☐
- Listed Directory Number:** (empty text field)
- Associated CM SIP Entity:** (empty text field)

**Overall Managed Bandwidth**

- Managed Bandwidth Units:** Kbit/sec
- Total Bandwidth:** (empty text field)
- Multimedia Bandwidth:** (empty text field)
- Audio Calls Can Take Multimedia Bandwidth:** ☒

**Per-Call Bandwidth Parameters**

- Maximum Multimedia Bandwidth (Intra-Location):** 1000 Kbit/Sec
- Maximum Multimedia Bandwidth (Inter-Location):** 1000 Kbit/Sec
- Minimum Multimedia Bandwidth:** 64 Kbit/Sec
- Default Audio Bandwidth:** 80 Kbit/sec

**Alarm Threshold**

- Overall Alarm Threshold:** 80 %
- Multimedia Alarm Threshold:** 80 %
- Latency before Overall Alarm Trigger:** 5 Minutes
- Latency before Multimedia Alarm Trigger:** 5 Minutes

**Location Pattern**

0 Items

☐ IP Address Pattern

Filter: Enable

Buttons: Commit, Cancel

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

The screenshot displays the Avaya Aura System Manager 7.0 interface. The left sidebar shows a navigation menu with 'Routing' selected, and 'Locations' highlighted under it. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' tab is active, showing the 'Name' field set to 'HG Communication Manager' and a 'Notes' field. Below this, the 'Dial Plan Transparency in Survivable Mode' section is visible, with an 'Enabled' checkbox and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'.

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

The screenshot displays the Avaya Aura System Manager 7.0 interface, similar to the previous one. The left sidebar shows 'Routing' selected, and 'Locations' highlighted. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' tab is active, showing the 'Name' field set to 'HG ASBCE' and a 'Notes' field. Below this, the 'Dial Plan Transparency in Survivable Mode' section is visible, with an 'Enabled' checkbox and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'.

## 6.4. Adaptations

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

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

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

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

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

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

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

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Adaptations' selected. The main content area is titled 'Adaptation Details' and shows the 'General' tab. The 'Adaptation Name' is 'CM\_Outbound\_Header\_Removal', the 'Module Name' is 'DigitConversionAdapter', and the 'Module Parameter Type' is 'Name-Value Parameter'. Below this, there is a table with two columns: 'Name' and 'Value'. The first row has 'eRHdrs' in the 'Name' column and 'Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View' in the 'Value' column. At the bottom of the table, it says 'Select : All, None'. There are 'Commit' and 'Cancel' buttons at the top right of the form area.

## 6.5. SIP Entities

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

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

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

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.0', and a user login status 'Last Logged on at February 15, 2016 3:02 PM' with a 'Log off admin' link. The left sidebar contains a menu with 'Routing' selected, and sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes a breadcrumb trail 'Home / Elements / Routing / SIP Entities'. A 'Commit' button and a 'Cancel' button are located at the top right of the form area. The form is divided into two sections: 'General' and 'SIP Link Monitoring'. The 'General' section contains the following fields: 'Name' (HG Session Manager), 'FQDN or IP Address' (172.16.5.32), 'Type' (Session Manager), 'Notes' (Security Module), 'Location' (HG Session Manager), 'Outbound Proxy' (empty), 'Time Zone' (America/New\_York), and 'Credential name' (empty). The 'SIP Link Monitoring' section contains a single dropdown menu labeled 'SIP Link Monitoring' with the value 'Use Session Manager Configuration'.

AVAYA  
Aura System Manager 7.0

Last Logged on at February 15, 2016 3:02 PM  
Log off admin

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

Help

General

Name: HG Session Manager

FQDN or IP Address: 172.16.5.32

Type: Session Manager

Notes: Security Module

Location: HG Session Manager

Outbound Proxy:

Time Zone: America/New\_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the **HG CM Trunk 2** SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the “**procr**” interface in Communication Manager, as seen in **Section 5.3**.

AVAYA  
Aura System Manager 7.0

Last Logged on at February 11, 2016 7:44 AM  
Log off admin

Home Routing

Home / Elements / Routing / SIP Entities

**SIP Entity Details**

General

Commit Cancel

Name: HG CM Trunk 2

FQDN or IP Address: 172.16.5.201

Type: SIP

Notes: For Service Provider Calls

Adaptation: HG Communication Manager

Location: America/New\_York

Time Zone: America/New\_York

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

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.0', and a user login status 'Last logged on at February 11, 2016 2:44 AM' with a 'Log off admin' link. The left sidebar contains a menu with 'Routing' selected, and sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area shows the breadcrumb 'Home / Elements / Routing / SIP Entities' and the title 'SIP Entity Details' with 'General' selected. The form contains the following fields: 'Name' (HG ASBCE), 'FQDN or IP Address' (172.16.5.71), 'Type' (Other), 'Notes' (HG ASBCE), 'Adaptation' (CM\_Outbound\_Header\_Removal), 'Location' (HG ASBCE), and 'Time Zone' (America/New\_York). 'Commit' and 'Cancel' buttons are at the top right of the form area.

* Name:	HG ASBCE
* FQDN or IP Address:	172.16.5.71
Type:	Other
Notes:	HG ASBCE
Adaptation:	CM_Outbound_Header_Removal
Location:	HG ASBCE
Time Zone:	America/New_York

## 6.6. Entity Links

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

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

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

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left navigation pane has 'Entity Links' selected. The main area shows the 'Entity Links' configuration page. At the top, there are 'Commit' and 'Cancel' buttons. Below them is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, and a 'D' column. The table contains one row with the following values: Name: HG Session Manager, SIP Entity 1: HG Session Manager, Protocol: TCP, Port: 5070, SIP Entity 2: HG CM Trunk 2, DNS Override: (checkbox), Port: 5070, Connection Policy: trusted. Below the table, it says 'Select 1 of 1 None'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	D
HG Session Manager	HG Session Manager	TCP	5070	HG CM Trunk 2	<input type="checkbox"/>	5070	trusted	



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

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (highlighted), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and includes a breadcrumb trail: Home / Elements / Routing / Entity Links. At the top right of the main area are 'Commit' and 'Cancel' buttons. Below the title is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, and Connection Policy. A single row is displayed, showing a link between 'HG Session Manager' and 'HG ASBCE' using the 'TCP' protocol on port '5060'. The 'Connection Policy' is set to 'trunked'. A 'Filter: Enable' button is located at the top right of the table. Below the table is a 'Select: All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
* HG Session Manager	* HG Session Manager	TCP	* 5060	* HG ASBCE	<input type="checkbox"/>	* 5060	trunked

## 6.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added: an incoming policy with Communication Manager as the destination, and an outbound policy to the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).

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

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

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left navigation pane has 'Routing Policies' selected. The main area is titled 'Routing Policy Details' with 'General' and 'SIP Entity as Destination' sections. The 'General' section has fields for Name, Disabled, Retries, and Notes. The 'SIP Entity as Destination' section has a 'Select' button and a table of SIP entities.

Name	FQDN or IP Address	Type	Notes
HG CM Trunk 2	172.16.5.201	CM	For Service Provider Calls

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left navigation pane has 'Routing Policies' selected. The main area is titled 'Routing Policy Details' with 'General' and 'SIP Entity as Destination' sections. The 'General' section has fields for Name, Disabled, Retries, and Notes. The 'SIP Entity as Destination' section has a 'Select' button and a table of SIP entities.

Name	FQDN or IP Address	Type	Notes
HG ASBCE	172.16.5.71	Other	HG ASBCE

## 6.8. Dial Patterns

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

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

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

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** (not shown).

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 10 digit numbers starting with **303**, the area code assigned to the DID numbers provided by Charter, arriving from location **HG ASBCE**, used route policy **To HG CM trunk 2** to Communication Manager.

The screenshot shows the Avaya System Manager 7.0 interface. The left navigation pane has 'Routing' selected, and 'Dial Patterns' is highlighted. The main area is titled 'Dial Pattern Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following fields:

- Pattern:** 303
- Min:** 10
- Max:** 10
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:**
- SIP Domain:** avaya.lab.com (selected from a dropdown)
- Notes:**

Below the form is a section titled 'Originating Locations and Routing Policies' with 'Add' and 'Remove' buttons. It contains a table with one item:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> HG ASBCE		To HG CM Trunk 2	0	<input type="checkbox"/>	HG CM Trunk 2	Inbound calls to HG CM Trunk 2

At the bottom, it says 'Select: All, None'.

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

The example in this screen shows the 11 digit dialed numbers for outbound calls, beginning with **1**, arriving from the **HG Communication Manager** location, will use route policy **To HG ASBCE**, which sends the call out to the PSTN via Avaya SBCE and the service provider SIP Trunk. The SIP Domain was set to **-ALL-** since dial pattern 1 is shared among multiple SIP Domains in the Avaya lab, SIP Domain **Avaya.lab.com** could have been used instead.

**AVAYA**  
Aura® System Manager 7.0

Last Logged on at February 11, 2016 7:44 AM  
Log off admin

Item: Routing

Home / Elements / Routing / Dial Patterns

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

**General**

\* Pattern: 1  
 \* Min: 11  
 \* Max: 11

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

**Originating Locations and Routing Policies**

Add Remove

5 Items Filter: Enable

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> HG Communication Manager		To HG ASBCE	0	<input type="checkbox"/>	HG ASBCE	For outbound calls to Service Provider

Select: All, None

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

## 7. Configure Avaya Session Border Controller for Enterprise

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


### 7.1. System Access

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



The login page features the Avaya logo on the left. To the right, under the heading "Log In", are input fields for "Username" and "Password", followed by a "Log In" button. Below the login fields, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modification of this system is strictly prohibited. Unauthorized users are subject to corporate 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." A final line reads: "All users must comply with all corporate instructions regarding the protection of information assets." At the bottom, it says "© 2011 - 2013 Avaya Inc. All rights reserved."


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



The dashboard interface includes a top navigation bar with links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is titled "Session Border Controller for Enterprise" and features the Avaya logo. On the left is a navigation pane with the following menu items: Dashboard (highlighted), Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings). The main dashboard area is divided into several sections: "Information" (System Time: 12:11:53 AM CST, Version: 7.0.0-21-8802, Build Date: Sun Aug 9 21:08:40 EDT 2015, License State: OK, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0, Last Logged in at: 01/08/2016 23:16:05 CST, Failed Login Attempts: 0), "Installed Devices" (listing EMS and Avaya SBCE), "Alarms (past 24 hours)" (None found), and "Incidents (past 24 hours)" (Avaya SBCE: No Subscriber Flow Matched).

## 7.2. System Management

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



The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo. The left sidebar contains a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management (highlighted), Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled "System Management" and features four tabs: Devices (selected), Updates, SSL VPN, and Licensing. Below the tabs is a table listing installed devices.

Device Name	Management IP	Version	Status	Actions
Avaya SBCE	[Blurred]	7.0.0-21-6802	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

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

System Information: Avaya SBCE

General Configuration

Appliance Name

Avaya SBCE

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

License Allocation

Standard Sessions

Requested: 2000

2000

Advanced Sessions

Requested: 2000

2000

Scopia Video Sessions

Requested: 500

500

CES Sessions

Requested: 0

0

Encryption

☒

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
172.16.5.71	172.16.5.71	255.255.255.0	172.16.5.254	A1
172.16.5.94	172.16.5.94	255.255.255.0	172.16.5.254	A1
				B1
				B1
				B1

DNS Configuration

Primary DNS

Secondary DNS

DNS Location

DMZ

DNS Client IP

Management IP(s)

IP



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

In the reference configuration, the private interface of the Avaya SBCE (172.16.5.71) was used to connect to the enterprise network, while its public interface (174.16.5.94) was used to connect to the LAN interface of the Charter managed CPE device (172.16.5.185). The WAN interface of the Charter managed CPE device was used to connect to the public network. See **Figure 1**. Note that Charter is responsible for the configuration of the Charter managed CPE device; hence the configuration tasks for this device are not covered in these Application Notes.

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

### 7.3. Network Management

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

Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, *Avaya\_SBCE* in the sample configuration. On the **Networks** tab, verify or enter the network information as needed.

Note that in the configuration used during the compliance test, the IP addresses assigned to the private (*172.16.5.71*) and public (*172.16.5.94*) sides of the Avaya SBCE were both assigned to interface **A1**.





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



## 7.4. Media Interfaces

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

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

**Add Media Interface**

Name: Private\_med

IP Address: Network\_A1 (A1, VLAN 0) | 172.16.5.71

Port Range: 35000 - 40000

Finish

A Media Interface facing the public side was similarly created with the name ***Public\_med***, as shown below. Under **IP Address**, the network and IP address to be associated with this interface was selected. The **Port Range** was left at the default values. Click **Finish**.

The screenshot shows a window titled "Add Media Interface" with a close button (X) in the top right corner. The window contains the following fields:

- Name:** A text box containing "Public\_med".
- IP Address:** A dropdown menu showing "Network\_A1 (A1, VLAN 0)" with a downward arrow. Below it, another dropdown menu shows "172.16.5.94" with a downward arrow.
- Port Range:** Two text boxes containing "35000" and "40000" separated by a hyphen.
- Finish:** A button at the bottom center of the window.

## 7.5. Signaling Interfaces

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

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

**Add Signaling Interface** X

Name: Private\_sig

IP Address: Network\_A1 (A1, VLAN 0) 172.16.5.71

TCP Port: Leave blank to disable 5060

UDP Port: Leave blank to disable

TLS Port: Leave blank to disable

TLS Profile: None

Enable Shared Control: ☐

Shared Control Port:

Finish

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

**Add Signaling Interface** X

Name

IP Address

TCP Port   
Leave blank to disable

UDP Port   
Leave blank to disable

TLS Port   
Leave blank to disable

TLS Profile

Enable Shared Control ☐

Shared Control Port

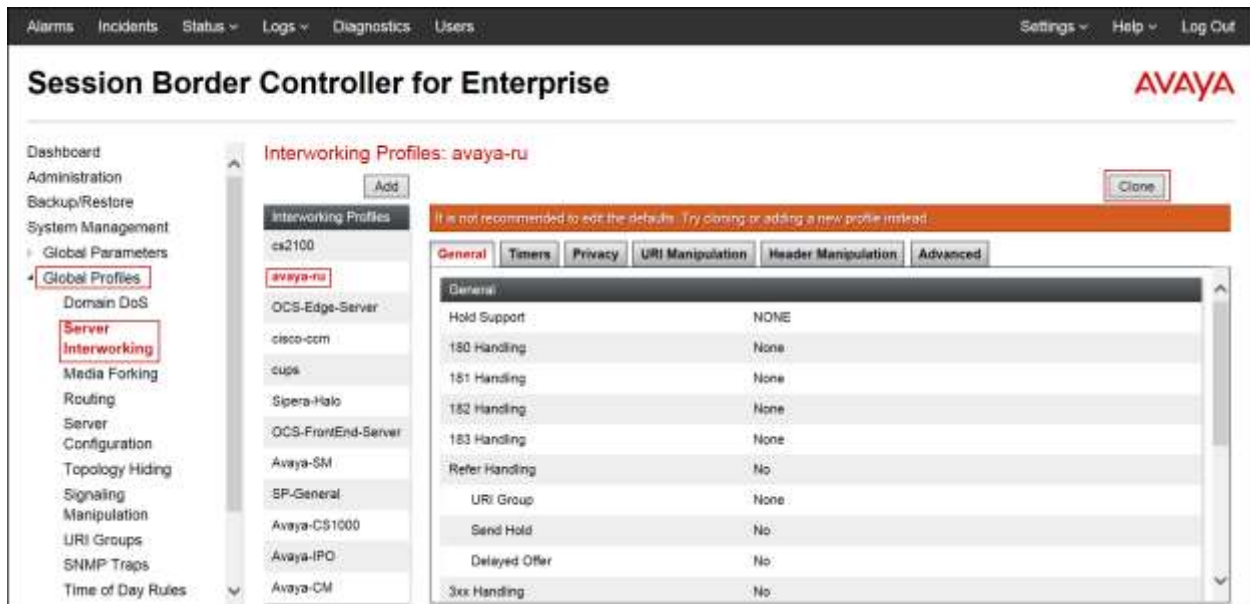
**Finish**

## 7.6. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

### 7.6.1. Server Interworking Profile – Enterprise

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



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



On the newly cloned **Avaya-SM** interworking profile, on the **General** tab all parameters retain their default values, as shown on the screen below.

Alarms Incidents Status ▾ Logs ▾ Diagnostics Users

## Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management
> Global Parameters
# Global Profiles
Domain DoS
**Server Interworking**
Media Forking
Routing
Server Configuration
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
> PPM Services
> Domain Policies
> TLS Management
> Device Specific Settings

### Interworking Profiles: Avaya-SM

Add

Interworking Profiles
cs2100
avaya-ru
OCS-Edge-Server
cisco-cdm
cups
Sipera-Halo
OCS-FrontEnd-Server
**Avaya-SM**
SP-General
Avaya-CS1000
Avaya-IPO
Avaya-CM

Click here to add a description

General Timers Privacy URI Manipulation Header Manipulation Advanced

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
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

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

The screenshot displays the 'Session Border Controller for Enterprise' configuration interface. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar lists various configuration categories, with 'Global Profiles' expanded to show 'Server Interworking'. The main content area is titled 'Interworking Profiles: Avaya-SM' and features a list of profiles on the left, including 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM' (highlighted), 'SP-General', 'Avaya-CS1000', 'Avaya-IPO', and 'Avaya-CM'. An 'Add' button is located above the list. The right pane shows the configuration for the 'Avaya-SM' profile, with tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced' (selected). The 'Advanced' tab contains settings for 'Record Routes' (Both Sides), 'Include End Point IP for Context Lookup' (Yes), 'Extensions' (Avaya), 'Diversion Manipulation' (No), 'Has Remote SBC' (Yes), 'Route Response on Via Port' (No), and 'DTMF Support' (None). An 'Edit' button is at the bottom right of the settings pane.

Alarms Incidents Status Logs Diagnostics Users

## Session Border Controller for Enterprise

Dashboard  
Administration  
Backup/Restore  
System Management  
    > Global Parameters  
    < Global Profiles  
        Domain DoS  
        Server Interworking  
        Media Forking  
        Routing  
        Server Configuration  
        Topology Hiding  
        Signaling Manipulation  
        URI Groups  
        SNMP Traps  
        Time of Day Rules  
    > PPM Services  
    > Domain Policies  
    > TLS Management  
    > Device Specific Settings

### Interworking Profiles: Avaya-SM

Add

Interworking Profiles

- cs2100
- avaya-ru
- OCS-Edge-Server
- cisco-ccm
- cups
- Sipera-Halo
- OCS-FrontEnd-Server
- Avaya-SM
- SP-General
- Avaya-CS1000
- Avaya-IPO
- Avaya-CM

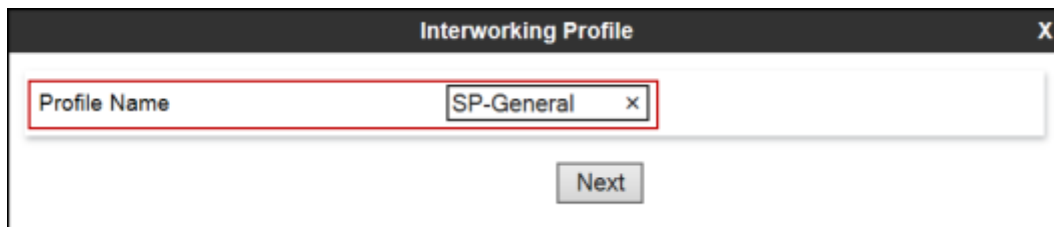
Click here to add a description.

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

Edit

## 7.6.2. Server Interworking Profile – Service Provider

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



The screenshot shows a dialog box titled "Interworking Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "SP-General". A red rectangular box highlights the "Profile Name" label and the input field. Below the input field, there is a "Next" button.

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



The screenshot shows the "General" tab of the "Interworking Profile" dialog box. The dialog has a title bar with "Interworking Profile" and a close button (X). The "General" tab is selected, showing a list of configuration options. The options are as follows:

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

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



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

Interworking Profile

X

Record Routes

☐ None

☐ Single Side

☒ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup

☐

Extensions

None

Diversion Manipulation

☐

Diversion Condition

None

Diversion Header URI

Has Remote SBC

☒

Route Response on Via Port

☐

DTMF

DTMF Support

☒ None

☐ SIP NOTIFY

☐ SIP INFO

Back

Finish

## 7.7. Signaling Manipulation

**Music on hold:** When calls from/to the PSTN were placed on-hold by Communication Manager users, the PSTN users did not hear Music while on-hold. A SigMa script was created to remove the “sendonly” message Communication Manager includes in the SDP of re-INVITEs when calls from/to the PSTN are placed on-hold, this allowed the PSTN users to hear Music while on-hold. The script was latter applied to the Service Provider side of the server configuration profile (refer to **Section 7.8.2**). The script was included under the **Remove\_Sendonly** script shown below.

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left, a navigation menu lists various sections, with 'Signaling Manipulation' highlighted under 'Global Profiles'. The main content area is titled 'Signaling Manipulation Scripts: Remove\_Sendonly'. It features an 'Add' button and a list of existing scripts, including 'Remove\_Sendonly' which is highlighted. The 'Remove\_Sendonly' script is shown in a text editor with the following content:

```
within session "INVITE" {  
  act on request where $DIRECTION="OUTBOUND" and $ENTRY_POINT="POST_ROUTING"  
  {  
    //Removes the a=sendonly from the re-INVITE messages..  
    $BODY[1].regex_replace("a=sendonly\r\n", "");  
  }  
}
```

An 'Edit' button is located at the bottom right of the script editor.

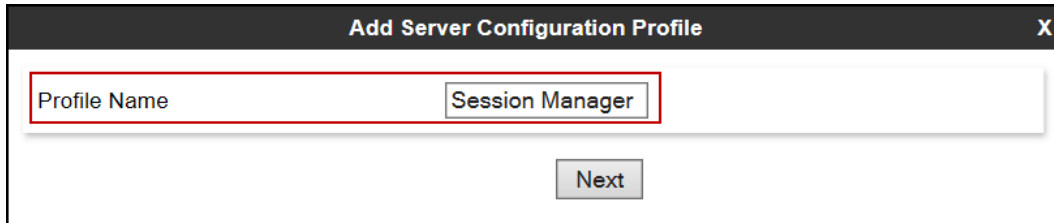
The details of the script used can be found in **Appendix A** in this document.

## 7.8. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and the Charter managed CPE device (Trunk Server).

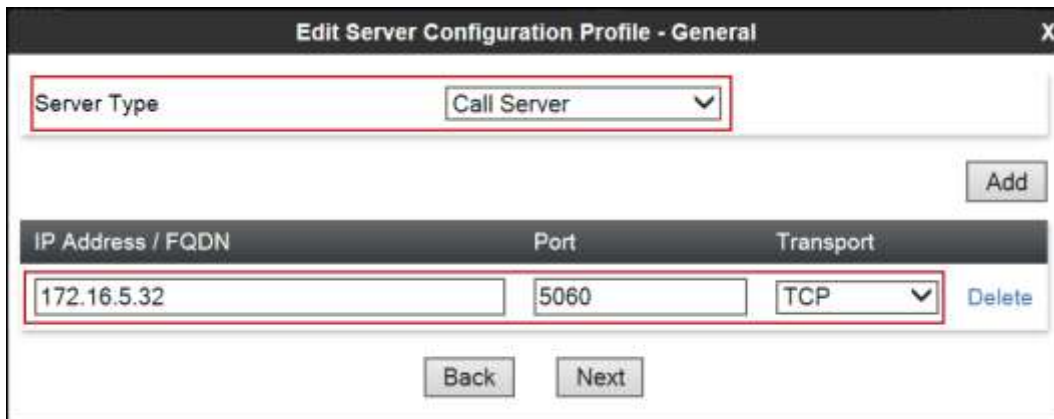
### 7.8.1. Server Configuration Profile – Enterprise

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



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

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



The screenshot shows a dialog box titled "Edit Server Configuration Profile - General" with a close button (X) in the top right corner. Inside the dialog, there is a "Server Type" dropdown menu set to "Call Server", which is highlighted with a red rectangular box. Below this, there is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The "IP Address / FQDN" field contains "172.16.5.32", the "Port" field contains "5060", and the "Transport" dropdown is set to "TCP". These three fields are highlighted with a red rectangular box. To the right of the table is a "Delete" button. Above the table is an "Add" button. At the bottom of the dialog are "Back" and "Next" buttons.

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

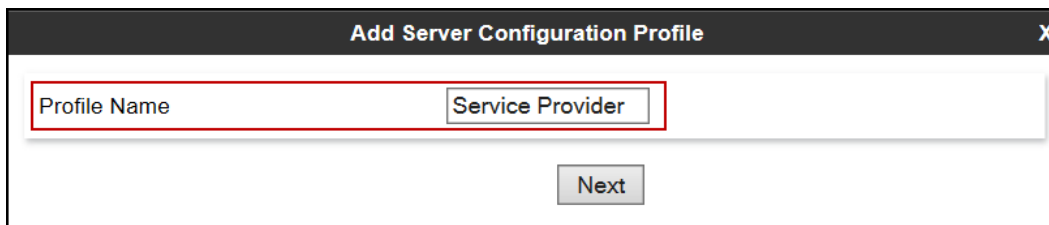
**Add Server Configuration Profile - Advanced** X

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-SM ▼
Signaling Manipulation Script	None ▼
Connection Type	SUBID ▼
Securable	<input type="checkbox"/>

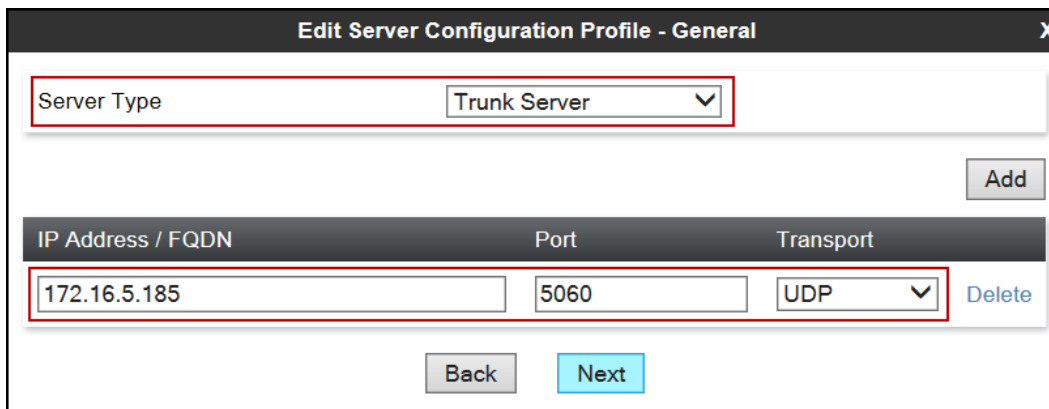
Back Finish

### 7.8.2. Server Configuration Profile – Service Provider

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



On the **Add Server Configuration Profile** Tab select **Trunk Server** from the drop down menu for the **Server Type**. On the **IP Addresses / FQDN** field, enter the IP address of the LAN interface of the Charter managed CPE device. Enter **5060** under **Port**, and select **UDP** for **Transport**. Click **Next**.



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

On the **Advanced** tab, select *SP-General* from the **Interworking Profile** drop down menu. Under **Signaling Manipulation Script**, select the *Remove\_Sendonly* script created in **Section 7.7**. Click **Finish**.

**Add Server Configuration Profile - Advanced** X

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General ▼
Signaling Manipulation Script	Remove_Sendonly ▼
Connection Type	SUBID ▼
Securable	<input type="checkbox"/>

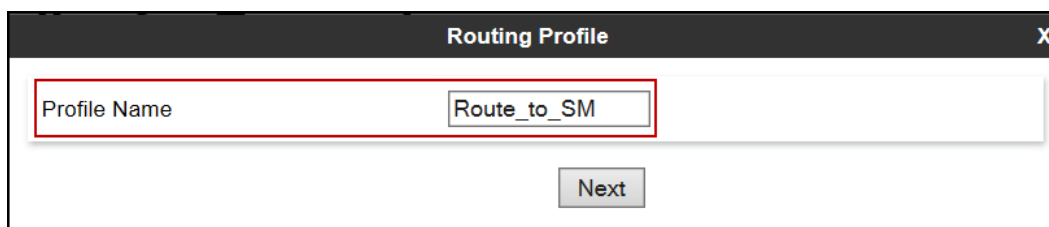
Back Finish

## 7.9. Routing

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

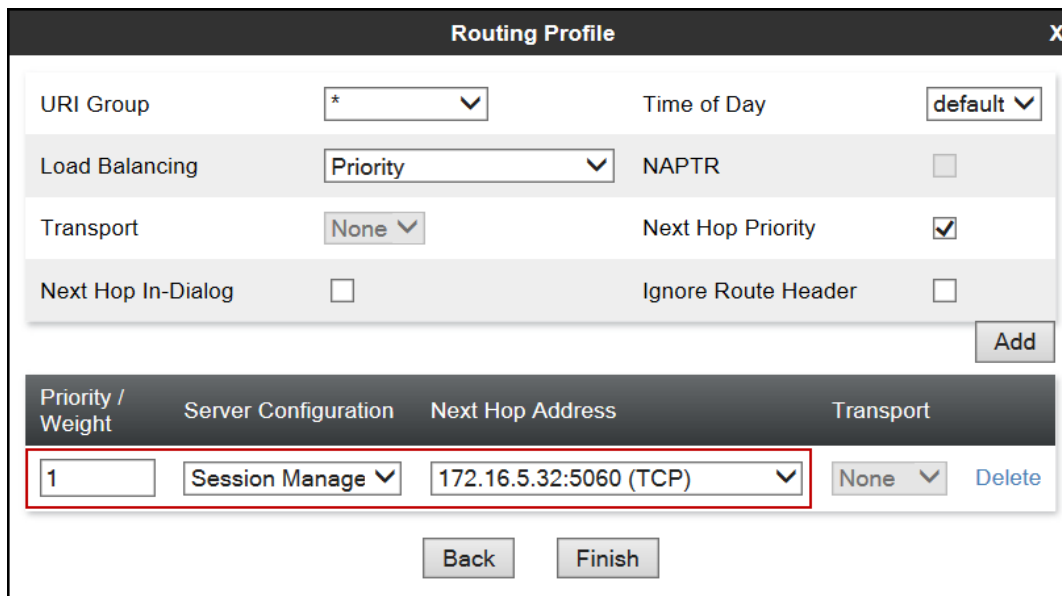
### 7.9.1. Routing Profile – Enterprise

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



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

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

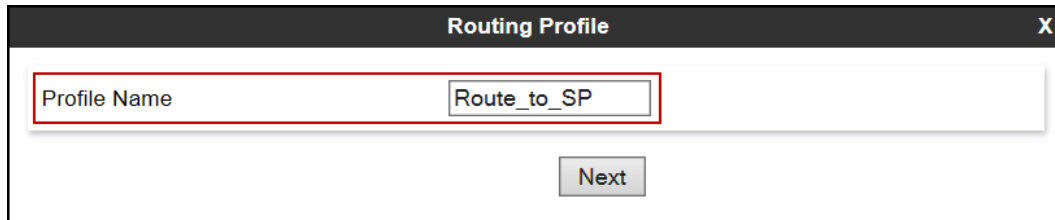


The screenshot shows the "Routing Profile" dialog box with various configuration options. The "URI Group" is set to "\*", "Time of Day" is "default", "Load Balancing" is "Priority", "NAPTR" is unchecked, "Transport" is "None", "Next Hop Priority" is checked, and "Next Hop In-Dialog" is unchecked. The "Add" button is visible. Below these options is a table with the following columns: "Priority / Weight", "Server Configuration", "Next Hop Address", and "Transport". The table contains one row with the following values: "1", "Session Manage", "172.16.5.32:5060 (TCP)", and "None". A "Delete" button is next to the "Transport" column. At the bottom of the dialog are "Back" and "Finish" buttons.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Session Manage	172.16.5.32:5060 (TCP)	None

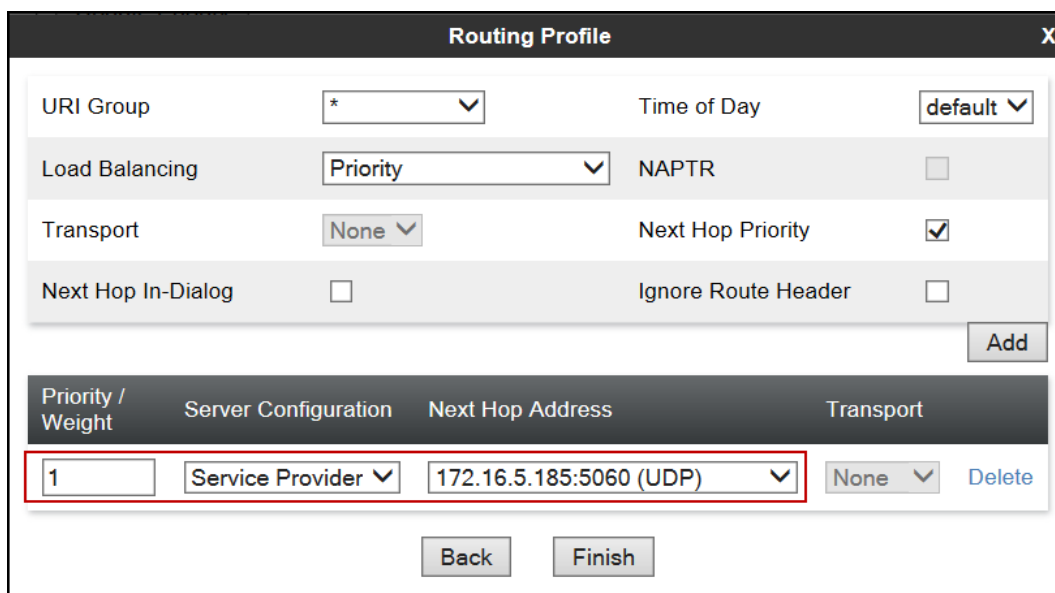
### 7.9.2. Routing Profile – Service Provider

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



The image shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Route\_to\_SP". Below the input field is a button labeled "Next".

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



The image shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. The dialog contains several configuration options and a table of entries.

Configuration options:

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

Buttons: Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Service Provider	172.16.5.185:5060 (UDP)	None	Delete

Buttons: Back, Finish



## 7.10. Topology Hiding

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

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

### 7.10.1. Topology Hiding Profile – Enterprise

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



The screenshot shows a 'Clone Profile' dialog box. It has a title bar with 'Clone Profile' and a close button (X). Inside, there are two text fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'Session\_Manager'. The 'Clone Name' field is highlighted with a red rectangular border. Below these fields is a 'Finish' button.

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

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

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

Finish

### 7.10.2. Topology Hiding Profile – Service Provider

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

Session Border Controller for Enterprise

Topology Hiding Profiles: Service\_Provider

Add

default

cisco\_ft\_profile

Session\_Manager

Service\_Provider

Com Manager

CS1000

IP Office

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

Edit

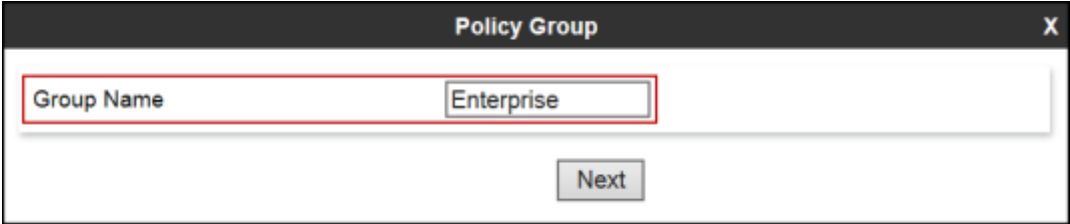
## 7.11. End Point Policy Groups

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

### 7.11.1. End Point Policy Group – Enterprise

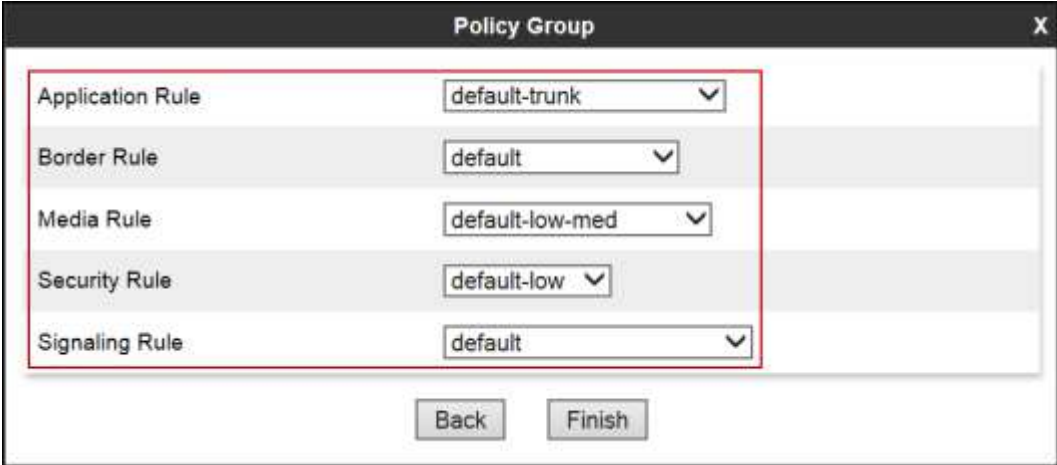
To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

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



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

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



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

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

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. A left-hand navigation menu lists various configuration areas, with 'End Point Policy Groups' highlighted under 'Domain Policies'. The main content area is titled 'Policy Groups: Service Provider' and features an 'Add' button, a 'Filter By Device' dropdown, and buttons for 'Rename', 'Clone', and 'Delete'. Below this, there are instructions to 'Click here to add a description...' and 'Hover over a row to see its description...'. A table titled 'Policy Group' is shown, with a 'Summary' button. The table has columns for Order, Application, Border, Media, Security, and Signaling. One row is visible with the following values: Order: 1, Application: default-trunk, Border: default, Media: default-low-med, Security: default-low, and Signaling: default. An 'Edit' button is located to the right of this row. At the bottom of the list, the 'Service Provider' policy group is highlighted.

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

## 7.12. End Point Flows

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

### 7.12.1. End Point Flow – Enterprise

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

Edit Flow: Session_Manager_Flow	
Flow Name	Session_Manager_Flow
Server Configuration	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
End Point Policy Group	Enterprise
Routing Profile	Route_to_SP
Topology Hiding Profile	Session_Manager
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

### 7.12.2. End Point Flow – Service Provider

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

Edit Flow: SIP_Trunk_Flow	
Flow Name	SIP_Trunk_Flow
Server Configuration	Service Provider
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
End Point Policy Group	Service Provider
Routing Profile	Route_to_SM
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

## 8. Charter Spectrum Business SIP Trunking Service Configuration

The service provider is responsible for the configuration of the SIP Trunking service, including the provisioning of the Charter managed CPE device in the customer's network. Charter will require from the customer the information needed to configure the service, which includes:

- IP addresses, subnet mask and default gateway to be assigned to the Charter managed CPE device interfaces (LAN and WAN), in order to be inserted at the edge of the enterprise site.
- IP address, protocol and port used to reach the Avaya SBCE at the enterprise.

Charter will provide the customer the necessary information to configure the SIP trunk connection from the enterprise site to the network, including:

- IP address, protocol and port used to reach the Charter managed CPE device.
- Supported codecs and order of preference.
- DID numbers.
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

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

## 9. Verification and Troubleshooting

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

### 9.1. General Verification Steps

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

### 9.2. Communication Manager Verification

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

- **list trace station** <extension number>  
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>

- Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>  
Displays signaling group service state.
- **status trunk** <trunk group number>  
Displays trunk group service state.
- **status station** <extension number>  
Displays signaling and media information for an active call on a specific station.

### 9.3. Session Manager Verification

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

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with categories like Session Manager, Network Configuration, Device and Location Configuration, Application Configuration, System Status, SIP Entity Monitoring, Managed, Bandwidth Usage, and Security Module Status. The main content area is titled "SIP Entity Link Monitoring Status Summary" and includes a "Run Monitor" button. Below this is a table showing the status of monitored entities for two Session Manager instances.

Session Manager	Type	Down	Partially Up	Monitored Entities			Total
				Up	Not Monitored	Deny	
HG Session Manager	Core	4	0	6	0	0	10
MA Session Manager	Core	5	0	9	0	0	14



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

**Session Manager Entity Link Connection Status**

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

All Entity Links for Session Manager: HG Session Manager

Summary View

10 Items · Refresh Filter: Stable

SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
CS1K7.6	172.16.20.40	5085	UDP	FALSE	UP	200 OK	UP
HG CM Trunk 98	172.16.5.201	5065	TLS	FALSE	UP	200 OK	UP
HG ASBCE	172.16.5.71	5060	TCP	FALSE	UP	200 OK	UP
HG AA Messaging	192.168.10.92	5060	TCP	FALSE	UP	200 OK	UP
HG CM Trunk 1	172.16.5.201	5061	TLS	FALSE	UP	200 OK	UP
HG CM Trunk 2	172.16.5.201	5070	TCP	FALSE	UP	200 OK	UP

Other Session Manager useful verification and troubleshooting tools include:

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

## 9.4. Avaya SBCE Verification

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

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

**Session Border Controller for Enterprise**

**Dashboard**

**Information**

System Time	12:30:50 AM CDT	<a href="#">Refresh</a>
Version	7.0.0-21-6602	
Build Date	Sun Aug 9 21:08:40 EDT 2015	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	10/08/2015 23:34:07 CDT	
Failed Login Attempts	0	

**Installed Devices**

- EMS
- Avaya SBCE

**Alarms (past 24 hours)**

None found.

**Incidents (past 24 hours)**

None found.

**Notes**

No notes found.

The following screen shows the **Alarm Viewer** page.

**Alarm Viewer**

**Devices**

- EMS
- Avaya SBCE

**Alarms**

<input checked="" type="checkbox"/>	ID	Details	State	Time	Device
No alarms found for this device.					

[Clear Selected](#) [Clear All](#)

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

**Session Border Controller for Enterprise** AVAYA

**Dashboard**

- Administration
- Backup/Restore
- System Management
  - Global Parameters
  - Global Profiles
  - PPM Services
  - Domain Policies
  - TLS Management
  - Device Specific Settings

**Information**

System Time	12:30:50 AM CDT	<a href="#">Refresh</a>
Version	7.0.0-21-0002	
Build Date	Sun Aug 9 21:08:40 EDT 2015	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	10/08/2015 23:34:07 CDT	
Failed Login Attempts	0	

**Installed Devices**

- EMS
- Avaya SBCE

**Alarms (past 24 hours)**  
None found.

**Incidents (past 24 hours)**  
None found.

**Notes**  
No notes found.

The following screen shows the **Incident Viewer** page.

**Incident Viewer** AVAYA

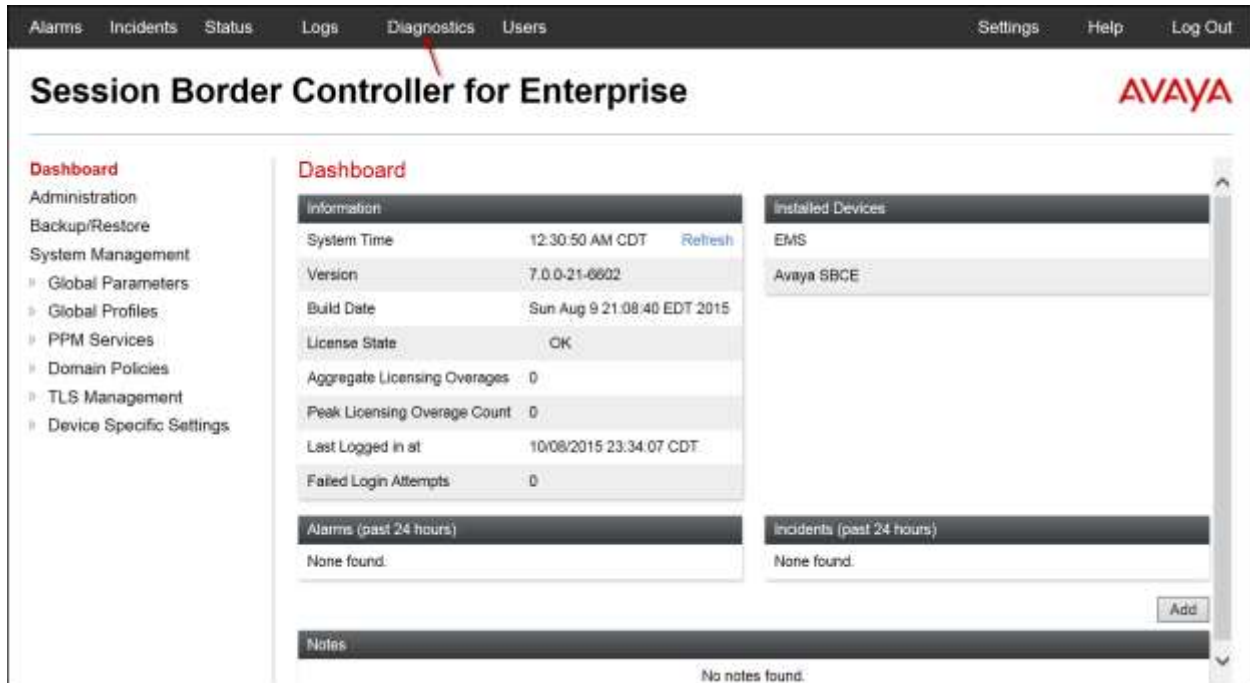
Device:  Category:  [Clear Filters](#) [Refresh](#) [Generate Report](#)

Displaying results 1 to 5 out of 5.

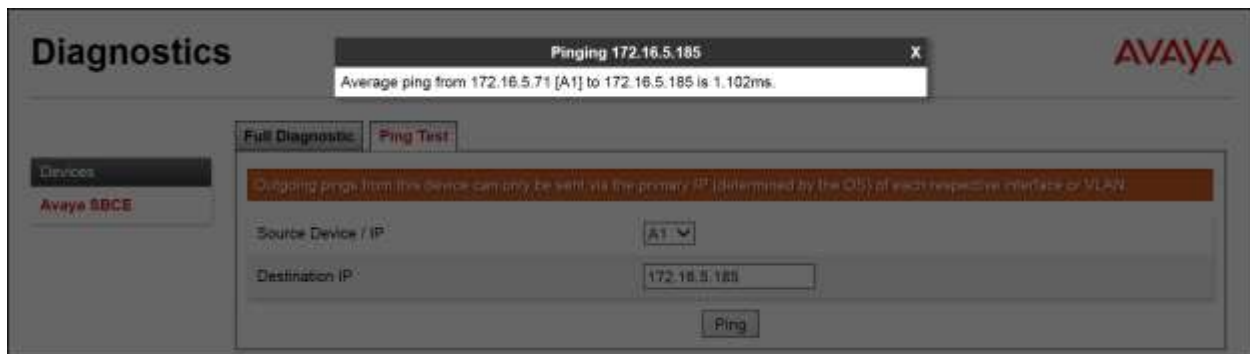
Type	ID	Date	Time	Category	Device	Cause
Message Dropped	722182809923738	10/8/15	11:40 PM	Policy	Avaya SBCE	No Subscriber Flow Matched
Server Heartbeat	721578865866258	9/24/15	10:55 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down
Server Heartbeat	720627871533350	9/2/15	11:49 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down
Server Heartbeat	720627092366599	9/2/15	11:23 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down
Server Heartbeat	720581909185100	9/1/15	10:16 PM	Policy	Avaya SBCE	Heartbeat Failed, Server is Down

<< < 1 > >>

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



The following screen shows the Diagnostics page with the results of a ping test.



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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. On the left sidebar, the navigation menu is expanded to "Device Specific Settings", which includes sub-items like Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, and Advanced Options. Under "Advanced Options", the "Troubleshooting" section is expanded, showing "Debugging", "Trace" (highlighted), "DoS", and "Learning". The main content area is titled "Trace: Avaya SBCE" and features two tabs: "Packet Capture" (active) and "Captures". The "Packet Capture Configuration" form includes the following fields: Status (Ready), Interface (A1), Local Address (IP:Port) (All), Remote Address (\*.\*.\*.\*:Port, IP, IP-Port), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (Test.pcap). A red box highlights the configuration fields. At the bottom of the form are "Start Capture" and "Clear" buttons.

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. On the left, a sidebar menu lists various configuration and management options, with "Troubleshooting" and its sub-item "Trace" highlighted. The main content area is titled "Trace: Avaya SBCE" and features two tabs: "Packet Capture" and "Captures". The "Captures" tab is active, showing a table of captured files. The table has columns for "File Name", "File Size (bytes)", and "Last Modified". A single entry is listed: "Test\_20151012004900.pcap" with a size of 12,288 bytes and a timestamp of "October 12, 2015 12:49:10 AM CDT". A "Delete" button is visible next to the entry. A "Refresh" button is located at the top right of the table area.

File Name	File Size (bytes)	Last Modified
Test_20151012004900.pcap	12,288	October 12, 2015 12:49:10 AM CDT

## 10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0, to connect to the Charter Spectrum Business SIP Trunking service, as shown in **Figure 1**.

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

## 11. References

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

- [1] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 7.0 August 2015.
- [2] *Administering Avaya Aura® Communication Manager*, Release 7.0, August 2015, Document Number 03-300509.
- [3] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, August 2015, Document Number 555-245-205.
- [4] *Deploying Avaya Aura® System Manager*, Release 7.0, November 2015.
- [5] *Deploying Avaya Aura® Session Manager on VMware®*, Release 7.0, August 2015.
- [6] *Administering Avaya Aura® Session Manager*, Release 7.0, August 2015.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
- [8] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.0, August 2015.
- [9] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, January 2016.
- [10] *Product Support Notice PSN004619u*, November 2015.  
<https://downloads.avaya.com/css/P8/documents/101015817>
- [11] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.7, August 2015.
- [12] *Implementing and Administering Avaya Aura® Media Server*, Release 7.7, August 2015.
- [13] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*, White Paper, August 2015.
- [14] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [15] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*,  
<http://www.ietf.org/>

## 12. Appendix A: SigMa Script

Following is the Signaling Manipulation scripts that was used in the configuration of the Avaya SBCE, **Section 7.8.2**. When adding these scripts as instructed in **Section 7.7** enter a name for the script in the Title (e.g., **Remove\_Sendonly**) and copy/paste the scripts as shown below.

```
within session "INVITE" {  
  act on request where %DIRECTION="OUTBOUND" and  
  %ENTRY_POINT="POST_ROUTING"  
  {  
  
    //Removes the a=sendonly from the re-INVITE messages.  
  
    %BODY[1].regex_replace("a=sendonly\r\n","");  
  
  }  
}
```



---

**©2016 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).