



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager Rel. 6.3, Avaya Aura® Session Manager Rel. 6.3 and Avaya Session Border Controller for Enterprise Rel. 6.3 to support CenturyLink IQ® SIP Trunk Services – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking service for an enterprise solution consisting of Avaya Aura® Communication Manager Rel. 6.3, Avaya Aura® Session Manager Rel. 6.3, and Avaya Session Border Controller for Enterprise Rel. 6.3 to support CenturyLink IQ® SIP Trunk Services.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints.

CenturyLink IQ® SIP Trunk Services provides PSTN access via SIP trunks between the enterprise and CenturyLink'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.....	4
2.2.	Test Results	5
2.3.	Support	6
3.	Reference Configuration	7
4.	Equipment and Software Validated	9
5.	Configure Avaya Aura® Communication Manager.....	10
5.1.	Licensing and Capacity	11
5.2.	System Features.....	12
5.3.	IP Node Names.....	13
5.4.	Codecs	14
5.5.	IP Network Region.....	15
5.6.	Signaling Group	16
5.7.	Trunk Group.....	18
5.8.	Calling Party Information.....	22
5.9.	Inbound Routing.....	23
5.10.	Outbound Routing	24
6.	Configure Avaya Aura® Session Manager	27
6.1.	System Manager Login and Navigation.....	28
6.2.	Specify SIP Domain	29
6.3.	Add Location.....	30
6.4.	SIP Entities	33
6.5.	Entity Links	37
6.6.	Routing Policies	40
6.7.	Dial Patterns	41
6.8.	Add/View Avaya Aura® Session Manager	44
7.	Configure Avaya Session Border Controller for Enterprise	46
7.1.	Log in Avaya SBCE.....	46
7.2.	Global Profiles.....	48
7.2.1.	Server Interworking Avaya-SM.....	49
7.2.2.	Server Interworking SP-General.....	52
7.2.3.	Signaling Manipulation.....	54
7.2.4.	Server Configuration.....	57
7.2.5.	Routing Profiles	65
7.2.6.	Topology Hiding.....	68
7.3.	Domain Policies	72
7.3.1.	Application Rules.....	72
7.3.2.	Media Rules	74
7.3.3.	Signaling Rules	75
7.3.4.	End Point Policy Groups.....	82

7.4.	Device Specific Settings.....	85
7.4.1.	Network Management.....	85
7.4.2.	Media Interface	87
7.4.3.	Signaling Interface	89
7.4.4.	End Point Flows.....	92
8.	CenturyLink SIP Trunking Service Configuration	96
9.	Verification and Troubleshooting	97
9.1.	Troubleshooting	97
9.1.1.	Communication Manager.....	97
9.1.2.	Session Manager	97
9.1.3.	Avaya SBCE	98
10.	Conclusion	103
11.	References.....	104
12.	Appendix A: SigMa Script.....	106

1. Introduction

These Application Notes describe the steps required to configure Session Initiation Protocol (SIP) trunk service between the service provider CenturyLink and an Avaya SIP-enabled enterprise solution.

In the sample configuration, the Avaya SIP-enabled enterprise solution consists of an Avaya Aura® Communication Manager Rel. 6.3 (hereafter referred to as Communication Manager), Avaya Aura® Session Manager Rel. 6.3 (hereafter referred to as Session Manager), Avaya Session Border Controller for Enterprise Rel. 6.3 (hereafter referred to as Avaya SBCE), and various Avaya endpoints. This solution does not extend to configurations without the Avaya Session Border Controller for Enterprise or Avaya Aura® Session Manager.

During the interoperability testing, feature test cases were executed to ensure interoperability between CenturyLink and Communication Manager.

Customers using an Avaya SIP-enabled enterprise solution with CenturyLink IQ® SIP Trunk Services are able to place and receive PSTN calls via the SIP protocol. The converged network solution is an alternative to traditional analog trunks and/or PSTN trunks such as ISDN-PRI. This approach generally results in lower cost for the enterprise.

The terms “CenturyLink IQ® SIP Trunk Services”, “CenturyLink” and “Service Provider”, will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Avaya Solution & Interoperability Test Lab by connecting Communication Manager, Session Manager and the Avaya SBCE to CenturyLink IQ® SIP Trunk Services via the public internet, as depicted in **Figure 1**.

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 for 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 trunk interoperability, the following areas were tested for compliance:

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to DID numbers assigned by CenturyLink. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x0 Series IP Deskphones (H.323), Avaya 96x1 Series IP Deskphones (H.323 and SIP), Avaya 2420

Digital Deskphones, Avaya one-X® Communicator soft phone (H.323 and SIP), Avaya Communicator for Windows soft phone (SIP), analog Deskphones.

- Inbound and outbound PSTN calls to/from Remote Workers using Avaya 96x1 deskphones (SIP) and Avaya Communicator for Windows (SIP).
- Outgoing calls to the PSTN were routed via CenturyLink's network to the various PSTN destinations.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper codec negotiation and two way speech-path. Testing was performed with codecs: G.729A and G.711MU (CenturyLink's preferred codec order).
- No matching codecs.
- Voicemail and DTMF tone support (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular) calls.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.
- T.38 fax.

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. For Remote Worker configuration details, see Reference [12].

Items not tested included the following:

- Inbound toll-free calls, 911 calls (emergency).

2.2. Test Results

Interoperability testing of CenturyLink IQ® SIP Trunk Services with an Avaya SIP-enabled enterprise solution was completed successfully with the following observations/limitations.

- **Music on hold:** With Communication Manager configured to play music any time calls were placed on-hold by Communication Manager users, music was not played to PSTN users. The issue was related to the manner in which CenturyLink currently handles the SIP messages Communication Manager includes in the SDP of re-INVITES it sends when calls are placed on-hold. When a call from the PSTN is

placed on-hold by a Communication Manager user, Communication Manager sends a re-INVITE with “sendonly” in the SDP, in response, CenturyLink sends a 200 OK with “inactive” in the SDP. This response caused the audio path to be closed between Communication Manager and the PSTN user, thus resulting in the user not hearing music (only silence) while on hold. The issue was solved at the Avaya SBCE by removing the “sendonly” message Communication Manager includes in the SDP of re-INVITES, in response, CenturyLink sends a 200 OK with “sendrecv” in the SDP, opening the audio path in between Communication Manager and the PSTN user, thus resulting in the PSTN user hearing music while he/she is on hold. CenturyLink is currently investigating this issue (Refer to **Section 7.2.3**).

- **T.38 fax:** CenturyLink does not support ECM for T.38; ECM should be disabled in Communication Manager so the resulting call will negotiate to not use ECM. In addition, CenturyLink only supports T.38 fax version 0, Communication Manager supports version 0 and 1. Although Communication Manager supports T.38 fax versions 0 and 1, negotiation to version 0 was unsuccessful. The T.38 fax version mismatch was causing T.38 fax to fail in both directions (CM \leftarrow \rightarrow PSTN). The issue was solved at the Avaya SBCE by changing the value in the “T38FaxVersion” field received from Communication Manager from 1 to 0 before passing to CenturyLink. After this change was made T.38 fax was successfully tested in both directions (CM \leftarrow \rightarrow PSTN) (Refer to **Sections 5.4 and 7.2.3**).
- **Calls to Vectors using the SIP REFER method:** Calls from the PSTN to vectors configured for call re-direction using the SIP REFER method in Communication Manager were failing with a “403 Forbidden” response from CenturyLink. CenturyLink requires the domain name “voip.centurylink.com” to be included in the “host” part of the SIP URI Communication Manager sends in the “Refer-To” header of SIP REFER messages; Avaya was sending the IP address instead. This issue was solved at the Avaya SBCE by adding the domain name “voip.centurylink.com” to the host part of the SIP URI in the “Refer-To” header of SIP REFER messages before sending the REFER to CenturyLink (Refer to **Section 7.2.6**).
- **Network Call Redirection using 302 Moved Temporarily:** When a Communication Manager vector was programmed to redirect an inbound call to a PSTN number before answering the call in the vector, CenturyLink would send an ACK to the “302 Moved Temporarily” SIP message from the enterprise but would not redirect the call to the new PSTN party in the “Contact” header of the 302 message. The PSTN user initiating the call would hear a recorded announcement indicating that the call could not be completed as dialed, to check the number and to call again. CenturyLink indicated that Network Call Redirection using the 302 Moved Temporarily method is not currently supported.

2.3. Support

For support on CenturyLink systems visit the corporate Web page at:

<http://www.centurylink.com/business/voice/sip-trunk.html>

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 below illustrates the test configuration used. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the CenturyLink IQ® SIP Trunk Services through the public Internet.

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

- Avaya Aura® Communication Manager.
- Avaya G450 Media Gateway.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya 96x0-Series IP Deskphones (H.323).
- Avaya 96x1-Series IP Deskphones (H.323 and SIP).
- Avaya one-X® Communicator soft phones (H.323 and SIP).
- Avaya Communicator for Windows soft phone (SIP)
- Avaya 2420 Digital Deskphones.
- Analog Deskphones.
- Desktop PC running various administration interfaces.

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flow through the Avaya SBCE. This way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and CenturyLink across the public Internet is SIP over UDP. The transport protocol between the Avaya SBCE and Session Manager across the enterprise network is SIP over TCP. The transport protocol between Session Manager and Communication Manager across the enterprise network is SIP over TLS. Note that for ease of troubleshooting during the testing, the compliance test was conducted with the transport protocol set to **tcp** between Session Manager and Communication Manager.

A separate SIP trunk group was created between Communication Manager and Session Manager to carry the traffic to and from the service provider (two-way trunk group). To separate the codec settings required by the service provider from the codec used by the telephones, two IP network regions were used each with a dedicated signaling group.

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 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 translations and class of service restrictions are performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as Automatic Route Selection (ARS) and Class of Service restrictions. Once Communication Manager selected the proper SIP trunk; the call is routed to Session Manager. Session Manager once again used the configured dial patterns and routing policies to determine the route to the Avaya SBCE for egress to CenturyLink's network.

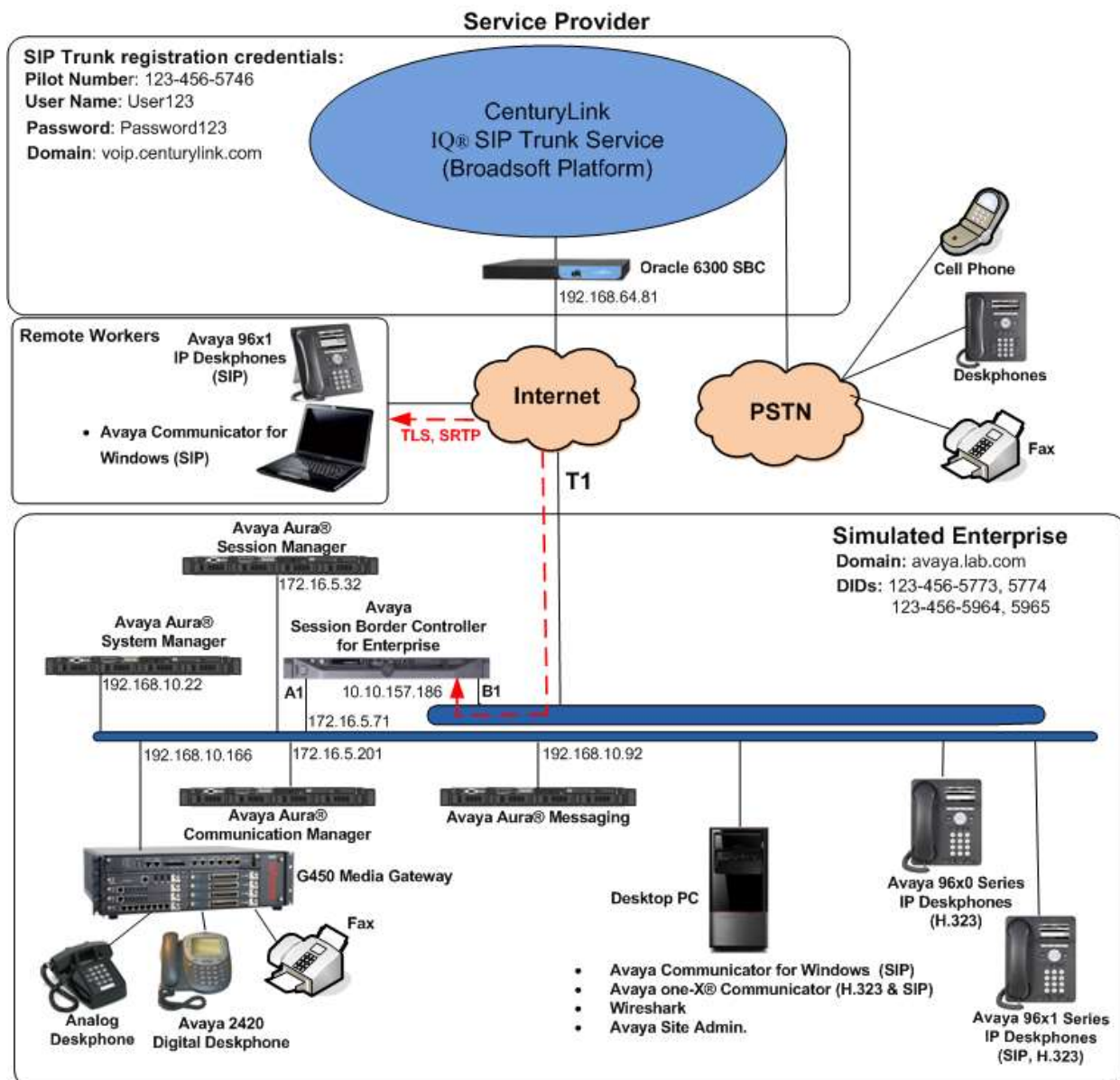


Figure 1: Avaya SIP-enabled Enterprise Solution and CenturyLink IQ® SIP Trunk Services.

4. Equipment and Software Validated

The following equipment and software were used for the compliance testing in the simulated enterprise:

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager	6.3.10 (Service Pack 10) (03.0.124.0-22147)
Avaya Aura® Session	6.3.13 (Service Pack 13) (6.3.13.0.631304)
Avaya Aura® System Manager	6.3.13 (Service Pack 13) Build No. 6.3.0.8.5682-6.3.8.5108 Software Update Rev. No. 6.3.13.10.3386
G450 Gateway	36.14.0
Avaya Session Border Controller for Enterprise	6.3.2-08-5478
Avaya Aura® Integrated Management Site Administrator	6.0.07
Avaya Aura® Messaging	6.3.2 Service Pack 2 Patch 3 (MSG-03.0.124.0-335_0217)
Avaya one-X® Communicator (SIP & H.323)	6.2.6.03-FP6
Avaya Communicator for Windows (SIP)	2.1.1.74
Avaya 96x0 Series IP Deskphones (H.323)	Avaya one-X® Deskphone Edition Version S3.242A
Avaya 96x1 Series IP Deskphones (H.323)	Avaya one-X® Deskphone Edition Version 6.6029
Avaya 96x1 Series IP Deskphones (SIP)	Avaya one-X® Deskphone SIP Version 6.5.0.17
Avaya 2420 Series Digital Deskphone	--
Lucent Analog Deskphone	--
CenturyLink	
BroadWorks Broadsoft	R20
Oracle 6300 Session Border Controller	7.1.2m3

Table 2 – Hardware and Software Components Tested

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from CenturyLink. It is assumed that the general installation of Communication Manager, the Avaya G450 Media Gateway and Session Manager has been previously completed.

In configuring Communication Manager, various components such as ip-network-regions, signaling groups, trunk groups, etc. need to be selected or created for use with the SIP connection to the Service Provider. Unless specifically stated otherwise, any unused ip-network-region, signaling group, trunk group, etc. can be used for this purpose.

The Communication Manager configuration was performed using the Avaya Integrated Management Site Administrator. Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the public IP addresses shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements are not revealed. 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 SIP trunks to the Service Provider. The example below shows one license with a capacity of **24000** trunks is 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 to add additional capacity.

```
display system-parameters customer-options                               Page 2 of 11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 12000 10
      Maximum Concurrently Registered IP Stations: 18000 0
      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
      Maximum TN2501 VAL Boards: 128 0
      Maximum Media Gateway VAL Sources: 250 1
      Maximum TN2602 Boards with 80 VoIP Channels: 128 0
      Maximum TN2602 Boards with 320 VoIP Channels: 128 0
      Maximum Number of Expanded Meet-me Conference Ports: 300 0

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

On **Page 3**, verify that **ARS** is set to **y**.

```
display system-parameters customer-options                               Page 3 of 11
                                OPTIONAL FEATURES

Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
Access Security Gateway (ASG)? n          Authorization Codes? y
Analog Trunk Incoming Call ID? y          CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y   CAS Main? n
Answer Supervision by Call Classifier? y   Change COR by FAC? n
ARS? y Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y                  Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? n           DCS (Basic)? y
ASAI Link Core Capabilities? n           DCS Call Coverage? y
ASAI Link Plus Capabilities? n           DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n
Async. Transfer Mode (ATM) Trunking? n   Digital Loss Plan Modification? y
ATM WAN Spare Processor? n              DS1 MSP? y
ATMS? y                                DS1 Echo Cancellation? y
Attendant Vectoring? y

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

5.2. System Features

Use the **change system-parameters feature** 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 this field set to **none**.

```
change system-parameters features                               Page 1 of 20
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 20
      FEATURE-RELATED SYSTEM PARAMETERS

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

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

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

SCCAN PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

```

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the server running Communication Manager (*procr*), and for Session Manager (*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
HA-CM                     192.168.10.12
default                   0.0.0.0
msgserver                 172.16.5.12
procr                     172.16.5.201
procr6                    ::

      ( 7 of 7 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. CenturyLink SIP Trunking supports **G.729A** and **G.711MU**. Thus, these codecs were included in this set. Enter **G.729** and **G.711MU** in the **Audio Codec** column of the table; this is CenturyLink's preferred codec order. 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.729	n	2	20
2:	G.711MU	n	2	20
3:				
4:				
5:				
6:				
7:				

Media Encryption

1: none

2:

3:

On **Page 2**, set the **Fax Mode** to **t.38-standard** and disable **ECM** (T.38 fax is supported by CenturyLink, but ECM is not supported) (Refer to **Section 2.2**).

change ip-codec-set 2 Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? n

	Mode	Redundancy	Packet Size(ms)
FAX	t.38-standard	0	ECM: n
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

5.5. IP Network Region

Create a separate IP network region for the Service Provider trunk. 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**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

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

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1. 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 example below 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	BW-limits Units	Video	Intervening	Dyn CAC	A	G	L	A	G	L
1	2	y	NoLimit			n						
2	2									all		
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 SIP trunk. This signaling group is used for inbound and outbound calls between the Service Provider and the enterprise. For the compliance test, **signaling group 2** was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the recommended default value of *tls* (Transport Layer Security). Note that for ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to *tcp*. The transport method specified here is used between Communication Manager and Session Manager.
- 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 as Session Manager.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Server running 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**.

- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5070**. (For TCP, the well-known port value for SIP is 5060).
- Set the **Far-end Network Region** to the IP network region defined for the Service Provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **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 inside IP of the Avaya SBCE and the enterprise endpoint.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

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	

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 **Section 5.6**.
- 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 (sec)** 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. Note that the value assigned to the **Preferred Minimum Session Refresh Interval (sec)** field is doubled and assigned to the “Min-SE” Header Field in SIP INVITE messages for calls originating from Communication Manager. Using the default setting of **600** seconds as in the example, the “Min-SE” Header Field would be populated for 1200 seconds in SIP INVITE messages originating from Communication Manager.

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. Numbers in the “public” format are automatically preceded with a “+” sign when passed in the “From”, “Contact” and “P-Asserted Identity” (PAI) headers. The addition of the “+” sign impacted caller ID presentation on outbound calls sent to CenturyLink. Thus, the **Numbering Format** was set to *private* and the **Numbering Format** in the route pattern was set to *unk-unk* (Refer to **Section 5.10**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to *y*. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block.

Default values were used for all other fields.

```
change trunk-group 2                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                     Measured: none
                                                    Maintenance Tests? y

  Numbering Format: private
  UI Treatment: service-provider
  Replace Restricted Numbers? y
  Replace Unavailable Numbers? y

  Modify Tandem Calling Number: no

  Show ANSWERED BY on Display? y
```

Page 4 was configured using the parameters highlighted below.

- Set the **Network Call Redirection** field to **y**. This setting directs Communication Manager to use the SIP REFER method for transferring calls off-net to the PSTN.
- Set the **Send Diversion Header** field to **y**. When enabled, the Diversion Header (in the outbound INVITE message) provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.
- Set the **Support Request History** field to **n**.
- Set the **Telephone Event Payload Type** to **96**. The value preferred by CenturyLink.
- Set the **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
PROTOCOL VARIATIONS		
	Mark Users as Phone?	<u>n</u>
Prepend '+' to Calling/Alerting/Diverting/Connected Number?		<u>n</u>
	Send Transferring Party Information?	<u>n</u>
	Network Call Redirection?	<u>y</u>
Build Refer-To URI of REFER From Contact For NCR?		<u>n</u>
	Send Diversion Header?	<u>y</u>
	Support Request History?	<u>n</u>
	Telephone Event Payload Type:	<u>96</u>
	Convert 180 to 183 for Early Media?	<u>n</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>		

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. The DID numbers are assigned by the Service Provider. It is used to authenticate the caller. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs).

The screen below shows DID numbers assigned for testing. The DID numbers were mapped to enterprise extensions 3042, 3044 and 3045. These 10-digit numbers were used for the outbound calling party information on the Service Provider trunk when calls were originated from these extensions.

```
change private-numbering 1
```

```
Page    1 of   2
```

```
NUMBERING - PRIVATE FORMAT
```

Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len
4	3			4
4	5			4
4	3042	2	1234565773	10
4	3044	2	1234565964	10
4	3045	2	1234565774	10

Total Administered: 5
Maximum Entries: 540

5.9. Inbound Routing

DID numbers received from CenturyLink were mapped to extensions 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 number.

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	1234565773	10	3042	
public-ntwrk	10	1234565774	10	3045	
public-ntwrk	10	1234565964	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					
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: 3				
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	4	ext								
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: _____
    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: *01
    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: _____
    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 to the Service Provider (as defined next).

```

change ars analysis 1786                                     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
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
1809	11	11	2	hnpa	—	n
181	11	11	deny	fnpa	—	n
182	11	11	deny	fnpa	—	n
183	11	11	deny	fnpa	—	n
184	11	11	deny	fnpa	—	n
185	11	11	deny	fnpa	—	n
186	11	11	deny	fnpa	—	n
187	11	11	deny	fnpa	—	n
188	11	11	deny	fnpa	—	n
189	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 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the Service Provider. For the compliance test, trunk group **2** was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk:** **1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the Service Provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **Numbering Format:** Set to **unk-unk**. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

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

Note: To save all Communication Manager provisioning changes, enter the command **save translations**.

6. Configure Avaya Aura® Session Manager

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

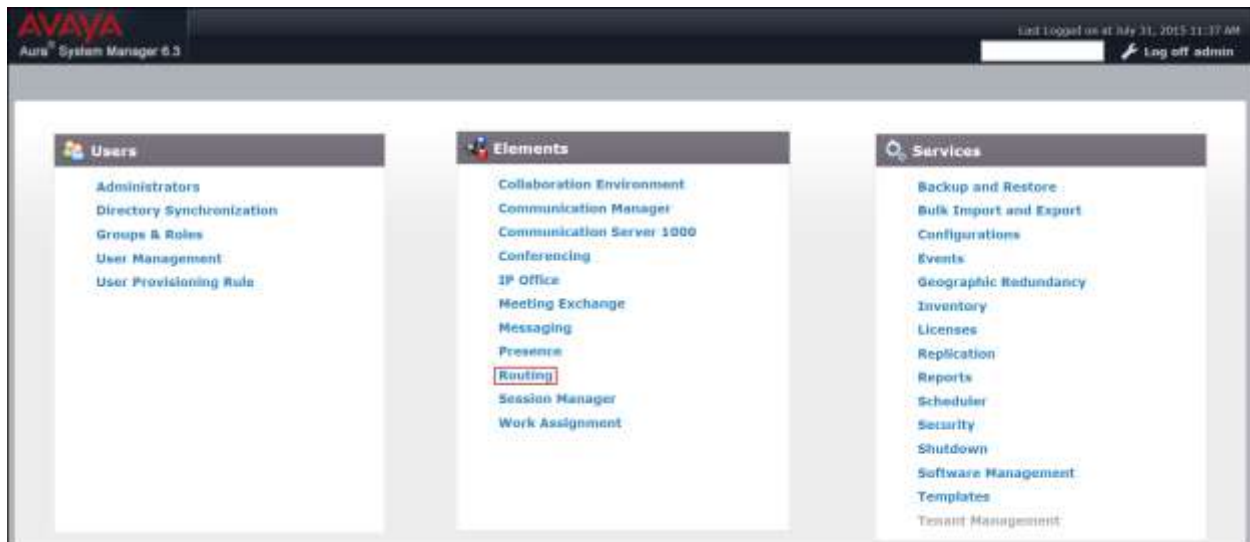
- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, the Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies,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

It may not be necessary to create all the items above when configuring a connection to the Service Provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, Locations, Adaptations, SIP Entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

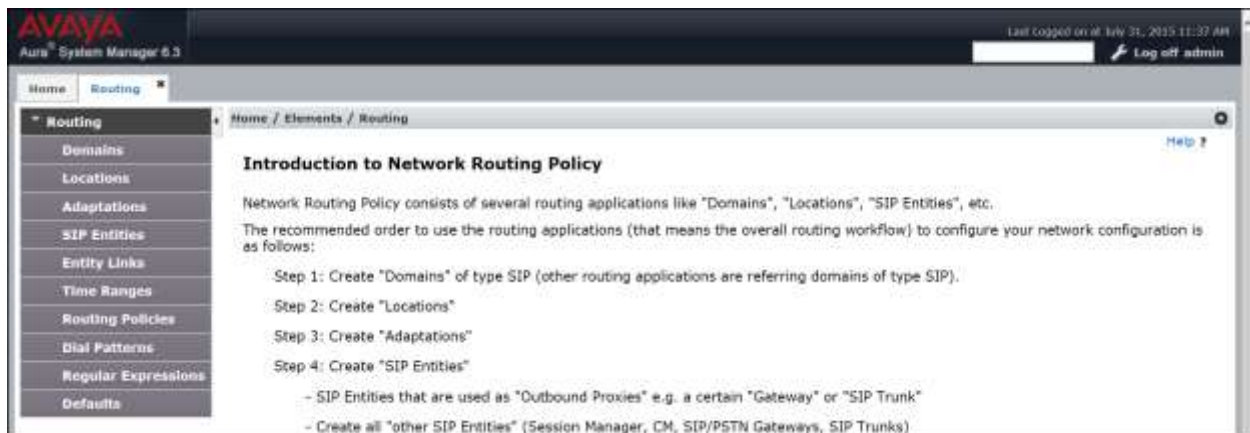
Note: Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

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 (not shown). The screen shown below is then displayed. Click on **Routing**.



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



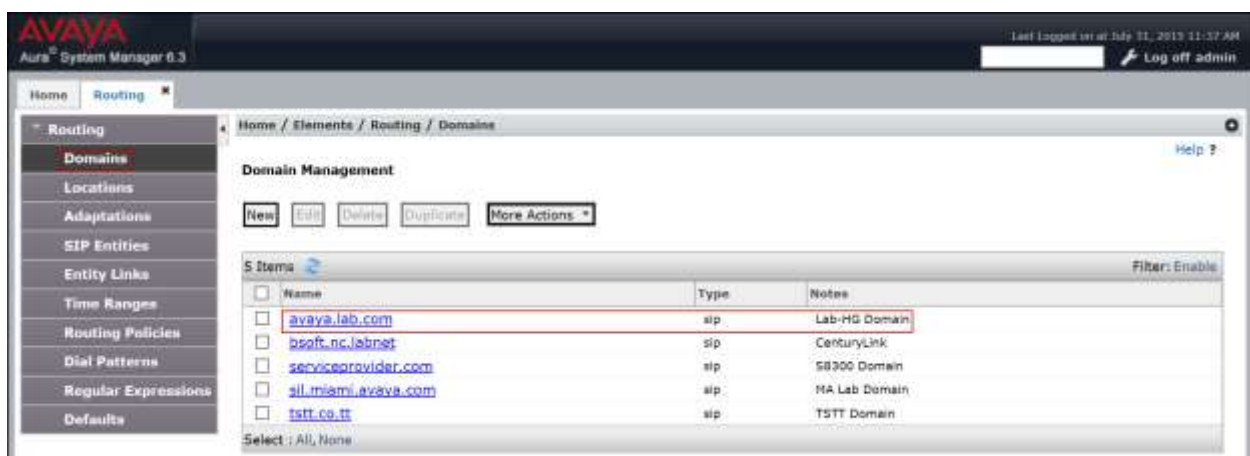
6.2. Specify SIP Domain

Create a SIP domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test the enterprise domain **avaya.lab.com** was used.

To add a domain 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 (not show).

The screen below shows the entry for the enterprise domain **avaya.lab.com**.



6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management and call admission control. 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).

Use default values for all remaining fields. Click **Commit** to save.

The screen below shows the **HG Session Manager** location. This location will be assigned later to the SIP Entity corresponding to Session Manager. Note that the “Overall Managed Bandwidth” section was removed for brevity, default values were used.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left navigation pane shows the 'Routing' menu expanded, with 'Locations' selected. The main content area is titled 'Home / Elements / Routing / Locations'. The 'Location Details' section includes a 'General' tab with the following fields: 'Name' (set to 'HG Session Manager'), 'Notes' (empty), 'Dial Plan Transparency in Survivable Mode' (Enabled: ☐, Listed Directory Numbers: empty, Associated CM SIP Entity: dropdown), '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), and 'Location Pattern' (Add, Remove buttons, 0 items, Filter: Enable, IP Address Pattern, Notes). The 'Commit' and 'Cancel' buttons are visible at the top right and bottom right of the form.

The following screen shows the **HG Communication Manager** location. This location will be assigned later to the SIP Entity corresponding to Communication Manager. Note that the “Overall Managed Bandwidth” section was removed for brevity, default values were used.

AVAYA
Aura System Manager 6.3

Last Logged in at July 11, 2015 11:37 AM
Log off admin

Home Routing

Home / Elements / Routing / Locations

Location Details Commit Cancel Help ?

General

* Name: HG Communication Manager
Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐
Listed Directory Number:
Associated CM SIP Entity:

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

Add Remove

0 Items Filter Enable

☐ IP Address Pattern Notes

Commit Cancel

The following screen shows the **HG ASBCE** location. This location will be assigned later to the SIP Entity corresponding to the Avaya SBCE. Note that the “Overall Managed Bandwidth” section was removed for brevity, default values were used.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The top navigation bar shows 'Home' and 'Routing'. The left sidebar lists various configuration options, with 'Locations' highlighted. The main content area is titled 'Home / Elements / Routing / Locations' and contains the following sections:

- Location Details:** Includes 'Name' (HG ASBCE) and 'Notes' (HG Avaya SBCE). Buttons for 'Commit' and 'Cancel' are present.
- General:** A section header.
- Dial Plan Transparency in Survivable Mode:** Includes an 'Enabled' checkbox, 'Listed Directory Numbers', and 'Associated CM SIP Entity'.
- Per-Call Bandwidth Parameters:** Includes fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth', and 'Default Audio Bandwidth'.
- Alarm Threshold:** Includes fields for 'Overall Alarm Threshold', 'Multimedia Alarm Threshold', 'Latency before Overall Alarm Trigger', and 'Latency before Multimedia Alarm Trigger'.
- Location Pattern:** Includes 'Add' and 'Remove' buttons, a table with 'IP Address Pattern' and 'Notes' columns, and a 'Filter: Enable' button.

Buttons for 'Commit' and 'Cancel' are also located at the bottom right of the page.

6.4. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand 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 interface that is used for SIP signaling.
- **Type:** Enter *Session Manager* for Session Manager, *CM* for Communication Manager and *Other* for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name**.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

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

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

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

For the compliance test, only two Ports were used:

- **5060** with **TCP** for connecting to the Avaya SBCE.
- **5070** with **TCP** for connecting to Communication Manager.

The following screen shows the addition of the Session Manager SIP entity. The name **HG Session Manager**, the IP address of the Session Manager signaling interface, the Location **HG Session Manager** created in **Section 6.3** and the corresponding Time Zone were used. Note that the “Entity Links” and “SIP Response to an OPTIONS Request” sections were removed for brevity.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left sidebar shows the navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The configuration fields are as follows:

- Name:** HG Session Manager
- FQDN or IP Address:** 172.16.5.32
- Type:** Session Manager
- Notes:** HG Session Manager
- Location:** HG Session Manager
- Outbound Proxy:** (empty)
- Time Zone:** America/New_York
- Credential name:** (empty)

Below the 'General' tab is the 'SIP Link Monitoring' section, which includes a 'Port' configuration area with 'TCP Failover port' and 'TLS Failover port' fields, and an 'Add' button. The 'SIP Link Monitoring' section also features a table with 10 items, showing a list of ports, protocols, and default domains. The table is filtered to show 'Enable' status.

Port	Protocol	Default Domain	Notes
5060	TCP	avaya.lab.com	
5060	UDP	avaya.lab.com	
5061	TLS	avaya.lab.com	
5062	TCP	avaya.lab.com	
5065	TLS	avaya.lab.com	
5070	TCP	avaya.lab.com	
5080	TCP	avaya.lab.com	
5081	TCP	avaya.lab.com	
5085	UDP	avaya.lab.com	
5086	TCP	avaya.lab.com	

At the bottom of the interface, there are 'Commit' and 'Cancel' buttons.

The following screen shows the addition of the Communication Manager SIP Entity.

A separate SIP entity for Communication Manager is required in order to route traffic from Communication Manager to the Service Provider.

The name ***HG CM Trunk 2***, the IP address of the server running Communication Manager created in **Section 5.3**, the Location ***HG Communication Manager*** created in **Section 6.3** and the corresponding Time Zone were used. Note that the “Entity Links” and “SIP Response to an OPTIONS Request” sections were removed for brevity.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left sidebar shows a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities (selected), 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. The 'General' tab is active. The configuration fields are as follows:

- Name:** HG CM Trunk 2
- FQDN or IP Address:** 172.16.5.201
- Type:** CM
- Notes:** CM SIP Trunk 2
- Adaptation:** (empty dropdown)
- Location:** HG Communication Manager
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Use Session Manager Configuration
- Supports Call Admission Control:** ☐
- Shared Bandwidth Manager:** ☐
- Primary Session Manager Bandwidth Association:** (empty dropdown)
- Backup Session Manager Bandwidth Association:** (empty dropdown)

Buttons for 'Commit' and 'Cancel' are located at the top right and bottom right of the form.

The following screen shows the addition of the SIP entity for the Avaya SBCE.

The name **HG ASBCE**, the inside IP address of the Avaya SBCE, the location **HG ASBCE** created in **Section 6.3** and the corresponding Time Zone were used. Note that the “Entity Links” and “SIP Response to an OPTIONS Request” sections were removed for brevity.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 6.3', and a user session summary showing 'Last Logged in at: July 11, 2015 11:37 AM' and a 'Log off admin' link. The left sidebar contains a menu with 'Routing' selected, and sub-items: Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / SIP Entities'. It features a 'SIP Entity Details' form with a 'General' tab. The form includes fields for 'Name' (HG ASBCE), 'FQDN or IP Address' (172.16.5.71), 'Type' (Other), and 'Notes' (HG ASBCE). Below these are 'Adaptation' and 'Location' (HG ASBCE) dropdowns, and a 'Time Zone' dropdown set to 'America/New_York'. Further down are fields for 'SIP Timer B/F (in seconds)' (4), 'Credential name', 'Call Detail Recording' (none), and 'CommProfile Type Preference'. A 'Loop Detection' section has a 'Loop Detection Mode' dropdown set to 'Off'. A 'SIP Link Monitoring' section has a 'SIP Link Monitoring' dropdown set to 'Use Session Manager Configuration'. At the bottom, there are checkboxes for 'Supports Call Admission Control' and 'Shared Bandwidth Managers', and dropdowns for 'Primary Session Manager Bandwidth Association' and 'Backup Session Manager Bandwidth Association'. 'Commit' and 'Cancel' buttons are located at the top right and bottom right of the form area.

6.5. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two entity links were created; one to Communication Manager and one to the Avaya SBCE, to be used only for Service Provider traffic. To add an entity link, navigate to **Routing → Entity Links** in the left-hand 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.
- **Protocol:** Select the transport protocol used for this link. For Communication Manager this was matched to the **Transport Method** defined on the Communication Manager signaling group in **Section 5.6**. For the Avaya SBCE, this was matched to the **Transport** defined on the **Server Configuration** for Session Manager (Call Server) in **Section 7.2.4**.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this was matched to the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**. For the Avaya SBCE, this was matched to the **Port** defined on the **Server Configuration** for Session Manager (Call Server) in **Section 7.2.4**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager or the Avaya SBCE select the respective SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system will receive SIP requests from Session Manager. For Communication Manager, this was matched to the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**. For the Avaya SBCE, this was matched to the **TCP Port** defined for the private **Signaling Interface** on the Avaya SBCE in **Section 7.4.3**.
- **Connection Policy:** Select *Trusted*.
- Click **Commit** to save.

The following screens illustrate the entity links to Communication Manager and to the Avaya SBCE. It should be noted that in a customer environment the entity link to Communication Manager would normally use TLS. For the compliance test, TCP was used to aid in troubleshooting since the signaling traffic is not encrypted.

The following screen shows the entity link to Communication Manager:

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a menu with options: 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 'Home / Elements / Routing / Entity Links'. It features a 'Commit' and 'Cancel' button at the top right. Below this 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 'HG Session Manager' as the Name, 'HG Session Manager' as SIP Entity 1, 'TCP' as Protocol, '5070' as Port, 'HG CM Trunk 2' as SIP Entity 2, '5070' as Port, and 'trusted' as Connection Policy. The table is filtered by 'Enable'. At the bottom, there are 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
* HG Session Manager	* HG Session Manager	TCP	* 5070	* HG CM Trunk 2		* 5070	trusted

The following screen shows the entity link to the Avaya SBCE:

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a menu with options: 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 'Home / Elements / Routing / Entity Links'. It features a 'Commit' and 'Cancel' button at the top right. Below this 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 'HG Session Manager' as the Name, 'HG Session Manager' as SIP Entity 1, 'TCP' as Protocol, '5060' as Port, 'HG ASBCE' as SIP Entity 2, '5060' as Port, and 'trusted' as Connection Policy. The table is filtered by 'Enable'. At the bottom, there are 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
* HG Session Manager	* HG Session Manager	TCP	* 5060	* HG ASBCE		* 5060	trusted

The following screen shows the list of the newly added entity links. Note that only the highlighted entity links were created for the compliance test, and are the ones relevant to these Application Notes.

Avaya Aura System Manager 6.3

Last Logged in at: July 11, 2015 11:37 AM

Log off admin

Home Routing

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Entity Links

Entity Links

New Edit Delete Duplicate More Actions

23 Items Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	HG Session Manager AAC 5060 TCP	HG Session Manager	TCP	5060	AAC	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	AAC Entity Link
<input type="checkbox"/>	HG Session Manager Acme Packet sip1 5060 TCP	HG Session Manager	TCP	5060	Acme Packet sip1	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	HG Session Manager CS1K7.6 5085 UDP	HG Session Manager	UDP	5085	CS1K7.6	<input type="checkbox"/>	5085	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	HG Session Manager HG ASBCE 5060 TCP	HG Session Manager	TCP	5060	HG ASBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	HG Session Manager HG CM Trunk 1 5080 TCP	HG Session Manager	TLS	5061	HG CM Trunk 1	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	HG Session Manager HG CM Trunk 2 5070 TCP	HG Session Manager	TCP	5070	HG CM Trunk 2	<input type="checkbox"/>	5070	trusted	<input type="checkbox"/>	

Select : All, None

Page 1 of 2

6.6. Routing Policies

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

In the **General** section, enter the following values. Use default values for all remaining fields:

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

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

- Click **Commit** to save.

The following screen shows the routing policy for Communication Manager. Note that some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

The screenshot displays the Avaya Aura System Manager 6.3 interface for configuring a Routing Policy. The left navigation pane shows the 'Routing' menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a 'General' section with the following fields:

- Name:** To HG CM Trunk 2
- Disabled:** ☐
- Retries:** 0
- Notes:** Inbound calls to HG CM Trunk 2

Below the 'General' section is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table of available SIP entities:

Name	FQDN or IP Address	Type	Notes
HG CM Trunk 2	172.16.5.201	CM	CM SIP Trunk 2

The page includes 'Commit' and 'Cancel' buttons at the top right and bottom right.

The following screen shows the routing policy for the Avaya SBCE. Note that some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left-hand navigation pane is expanded to 'Routing', and the 'Routing Policies' sub-menu is selected. The main content area displays the 'Routing Policy Details' for a policy named 'To HG ASBCE'. The 'General' tab is active, showing fields for 'Name' (To HG ASBCE), 'Disabled' (unchecked), 'Retries' (0), and 'Notes' (Outbound calls via ASBCE). Below this, the 'SIP Entity as Destination' section is visible, featuring a 'Select' button and a table with one entry: 'HG ASBCE' with FQDN or IP Address '172.16.5.71', Type 'Other', and Notes 'HG ASBCE'. 'Commit' and 'Cancel' buttons are present at the top right and bottom right of the form.

6.7. Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to CenturyLink 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-hand 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. Use default values for all remaining fields:

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

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

- Click **Commit** to save.

Examples of dial patterns used for the compliance testing are shown below.

The first example shows dial pattern **1**, with destination SIP Domain of **-ALL-**, Originating Location Name **HG Communication Manager** and Routing Policy name **To HG ASBCE**. This dial pattern was used for outbound calls to the PSTN.

Note: 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 6.3

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

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

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

Originating Locations and Routing Policies

Add Remove

5 items

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	CSik Node	CSik7.6	To HG ASBCE	0	<input type="checkbox"/>	HG ASBCE	Outbound calls via ASBCE
<input type="checkbox"/>	HG Communication Manager		To HG ASBCE	0	<input type="checkbox"/>	HG ASBCE	Outbound calls via ASBCE

Select : All, None

The following dial pattern used for the compliance testing was for inbound calls to the enterprise. It uses dial pattern **123** matching the first three digits sent by CenturyLink on inbound calls to the enterprise. The pattern also matches the first three digits of DID numbers assigned to Communication Manager in **Section 5.9 Inbound Routing**. This dial pattern was configured with the destination SIP Domain of **avaya.lab.com**, Originating Location Name **HG ASBCE**, and Routing Policy name **To HG CM Trunk 2**.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, **Dial Patterns** (highlighted), Regular Expressions, and Defaults. The main content area is titled 'Dial Pattern Details' and includes a 'General' tab. The 'Pattern' field is set to '123', with 'Min' set to '3' and 'Max' set to '10'. The 'Emergency Call' checkbox is unchecked, 'Emergency Priority' is '1', and 'Emergency Type' is empty. The 'SIP Domain' dropdown is set to 'avaya.lab.com'. Below this is a table titled 'Originating Locations and Routing Policies' with one item listed. The table has columns: Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The row shows 'HG ASBCE' as the Originating Location Name, 'HG Avaya SBCE' as the Originating Location Notes, 'To HG CM Trunk 2' as the Routing Policy Name, Rank '0', 'Routing Policy Disabled' unchecked, 'HG CM Trunk 2' as the Routing Policy Destination, and 'Inbound calls to HG CM Trunk 2' as the Routing Policy Notes. The interface also includes 'Commit' and 'Cancel' buttons at the top and bottom right.

Note: The same procedure should be followed to add other required dial patterns.

6.8. Add/View Avaya Aura® Session Manager

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

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

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

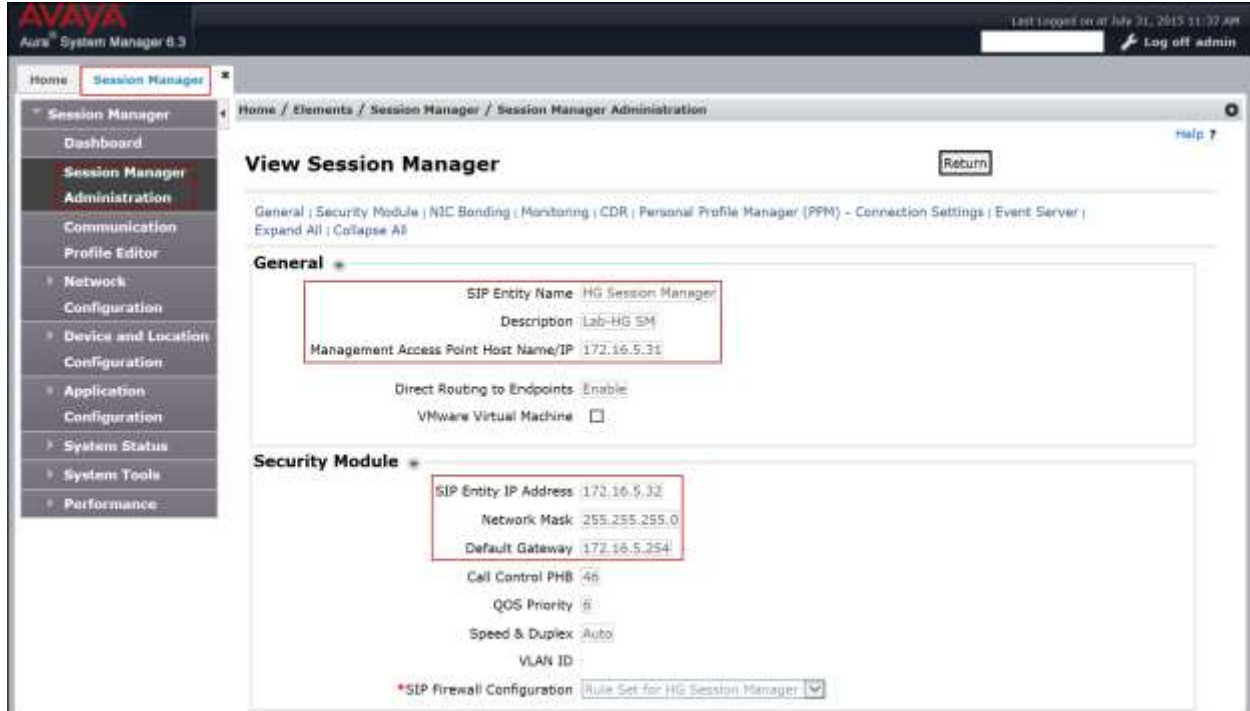
In the **Security Module** section, enter the following values:

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

Use default values for the remaining fields.

- Click **Save** (not shown).

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



AVAYA
Aura® System Manager 6.3

Last logged on at July 31, 2015 11:37 AM
Log off admin

Home Session Manager

Home / Elements / Session Manager / Session Manager Administration

View Session Manager

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

General

SIP Entity Name: HG Session Manager
Description: Lab-HG SM
Management Access Point Host Name/IP: 172.16.5.31

Direct Routing to Endpoints: Enable
VMware Virtual Machine: ☐

Security Module

SIP Entity IP Address: 172.16.5.32
Network Mask: 255.255.255.0
Default Gateway: 172.16.5.254

Call Control PHB: 46
QOS Priority: 8
Speed & Duplex: Auto
VLAN ID:

*SIP Firewall Configuration: Rule Set for HG Session Manager

7. Configure Avaya Session Border Controller for Enterprise

This section describes the required configuration of the Avaya SBCE to connect to CenturyLink's SIP Trunking service.

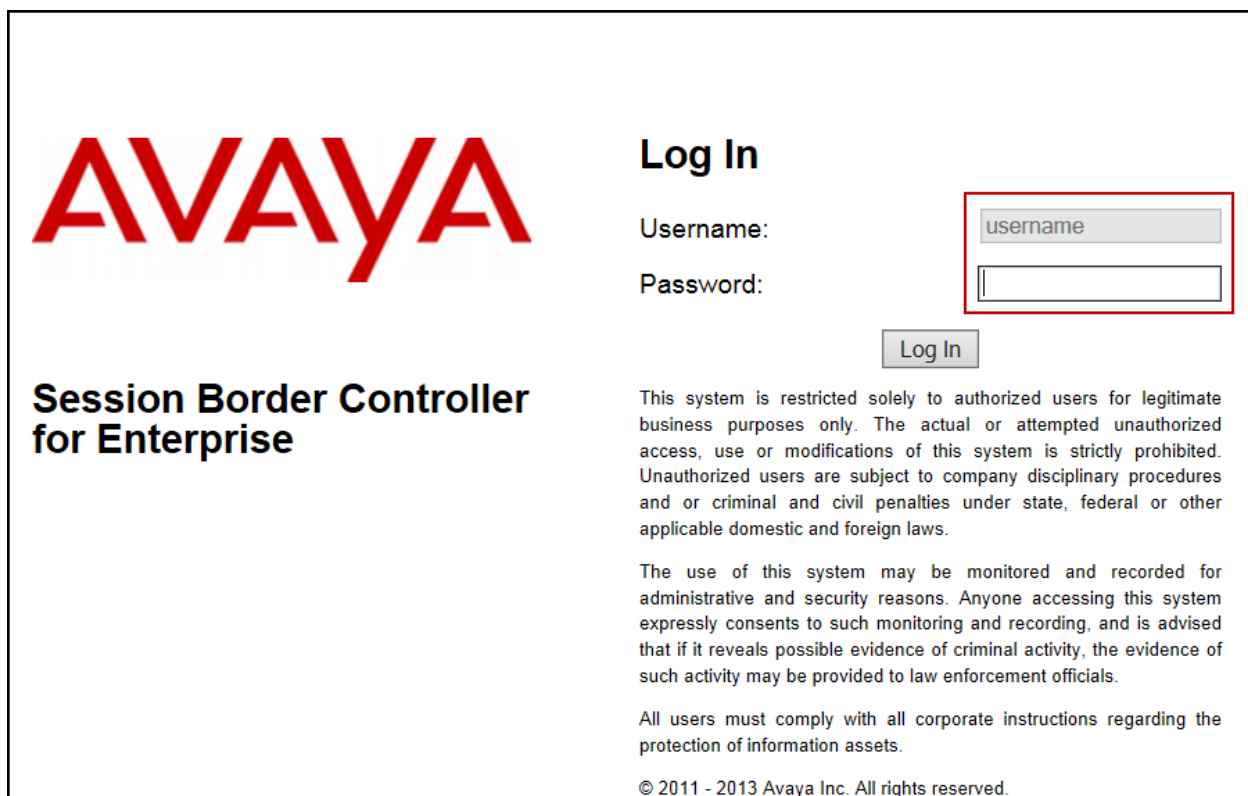
It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

Note: In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

7.1. Log in Avaya SBCE

Use a web browser to access the Avaya SBCE web interface, enter `https://<ip-addr>/sbc` in the address field of the web browser, where `<ip-addr>` is the management IP address of the Avaya SBCE.

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



The screenshot shows the Avaya Session Border Controller for Enterprise login page. On the left is the large red 'AVAYA' logo. Below it, the text 'Session Border Controller for Enterprise' is displayed. On the right, under the heading 'Log In', there are two input fields: 'Username:' and 'Password:'. The 'Username' field contains the text 'username'. Below these fields is a 'Log In' button. To the right of the login fields, there is a red rectangular box highlighting the input fields. Below the login fields, there is a paragraph of text: 'This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.' Below this paragraph is another paragraph: 'The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.' Below this paragraph is a third paragraph: 'All users must comply with all corporate instructions regarding the protection of information assets.' At the bottom of the page, there is a copyright notice: '© 2011 - 2013 Avaya Inc. All rights reserved.'

The **Dashboard** main page will appear as shown below.

The screenshot shows the Avaya Session Border Controller for Enterprise Dashboard. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various sections, with "Dashboard" highlighted. The main content area is titled "Dashboard" and features a warning message about application DEBUG level log messages. Below this, there are four panels: "Information" (showing system time, version, build date, license state, and licensing overages), "Installed Devices" (listing EMS and Avaya SBCE), "Alarms (past 24 hours)" (showing none found), and "Incidents (past 24 hours)" (showing none found). At the bottom, there is a "Notes" section with no notes found and an "Add" button.

Information	
System Time	11:22:50 PM GMT-08:00 Refresh
Version	6.3.2-08-5478
Build Date	Thu Apr 2 06:51:39 EDT 2015
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0

Installed Devices
EMS
Avaya SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

Notes
No notes found.

To view the system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Avaya SBCE** was already added.

The screenshot shows the Avaya Session Border Controller for Enterprise System Management page. The top navigation bar is the same as the dashboard. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, the sidebar menu lists various sections, with "System Management" highlighted. The main content area is titled "System Management" and features a tabbed interface with "Devices", "Updates", "SSL VPN", and "Licensing" tabs. The "Devices" tab is active, showing a table of installed devices. The table has columns for Device Name, Management IP, Version, and Status. The "Avaya SBCE" device is listed with a status of "Commissioned". Action buttons for "Reboot", "Shutdown", "Restart Application", "View", "Edit", and "Uninstall" are provided for each device.

Device Name	Management IP	Version	Status	Actions
Avaya SBCE	10.10.10.10	6.3.2-08-5478	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

To view the network configuration assigned to the Avaya SBCE, click **View** as shown on the previous screen. The **System Information** window is displayed as shown below.

The **System Information** screen shows **Network Configuration**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to *SIP* and the **Deployment Mode** was set to *Proxy*. Default values were used for all other fields.

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

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
10.10.157.186	10.10.157.186	255.255.255.0	10.10.157.129	B1
10.10.157.186	10.10.157.186	255.255.255.0	10.10.157.129	B1
10.10.157.186	10.10.157.186	255.255.255.0	10.10.157.129	A1
10.10.157.186	10.10.157.186	255.255.255.0	10.10.157.129	B1

DNS Configuration

Primary DNS

172.16.5.102

Secondary DNS

DNS Location

DMZ

DNS Client IP

172.16.5.71

Management IP(s)

IP

10.10.157.186

On the previous screen, note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces of the Avaya SBCE, respectively. The **A1** and **B1** interfaces and IP addresses shown are the ones relevant to the configuration of the SIP trunk to CenturyLink.

The management IP was blurred out for security reasons. The IP addresses used for the remote worker configuration was also blurred out since the remote worker configuration is beyond the scope of these Application Notes and is not discussed in these Application Notes.

IMPORTANT! – During the Avaya SBCE installation, the Management interface, (labeled “M1”), of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to have this resolved.

7.2. Global Profiles

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

7.2.1. Server Interworking Avaya-SM

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk Service Providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or “cloned”. Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or “cloned”, and then modified to meet specific requirements for the enterprise SIP-enabled solution.

On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru**. Click **Clone** on top right of the screen.

Enter the new profile name in the **Clone Name** field, the name of **Avaya-SM** was chosen in this example. Click **Finish** (not shown).

For the newly created **Avaya-SM** profile, click **Edit** (not shown) at the bottom of the **General** tab:

- Check ***T.38 Support***.
- Leave other fields with their default values.
- Click **Finish** in the **Editing Profile** window.

The following screen capture shows the **General** tab of the newly created **Avaya-SM** Server Interworking Profile.

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 the product name and the Avaya logo.

On the left, a sidebar menu lists various configuration areas, with **Global Profiles** expanded to show **Server Interworking**.

The main content area is titled **Interworking Profiles: Avaya-SM**. It features a list of profiles on the left, including **cs2100**, **avaya-sm**, **OCS-Edge-Server**, **cisco-cm**, **csp**, **Sipera-Hub**, **OCS-FrontEnd-Server**, **Avaya-SM** (highlighted), **SP-General**, **Avaya-CS1000**, **Avaya-IP0**, and **Avaya-CM**. An **Add** button is located above the list.

The **Avaya-SM** profile is selected, and its configuration is shown in the **General** tab. The tab includes a description field and a list of settings:

Setting	Value
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.30 Support	Yes
URI Scheme	SIP
Via Header Format	RPC3201

The following screen capture shows the **Advanced** tab of the newly created **Avaya-SM** Server Interworking Profile.

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.

On the left, a sidebar menu lists various configuration areas, with "Global Profiles" and "Server Interworking" highlighted. The main content area is titled "Interworking Profiles: Avaya-SM" and features an "Add" button and "Rename", "Clone", and "Delete" options.

Below the title, there is a list of interworking profiles, including "cs2100", "avaya-ns", "OCS-Edge-Server", "cisco-com", "cups", "Sipera-Helo", "OCS-FrontEnd-Server", "Avaya-SM" (highlighted), "SP-General", "Avaya-CS1000", "Avaya-IPO", and "Avaya-CM".

The "Avaya-SM" profile is selected, and the "Advanced" tab is active. The "Advanced" tab shows a table of configuration settings:

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

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

7.2.2. Server Interworking SP-General

A second Server Interworking Profile named **SP-General** was created for the Service Provider.

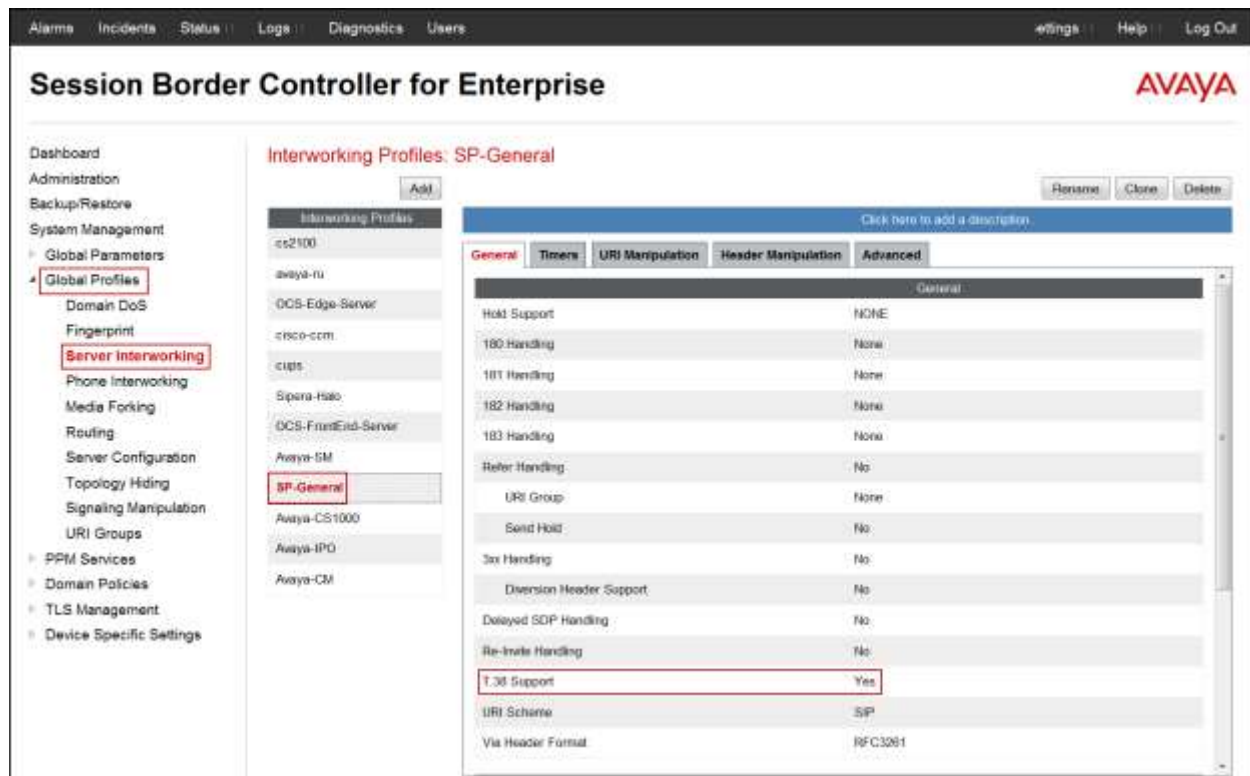
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add**.

Enter the new profile name (not shown), the name of **SP-General** was chosen in this example. Click **Next**:

On the **General** tab:

- Check **T.38 Support**.
- Leave other fields with their default values.
- Click **Next** until the Advanced tab is reached, then click **Finish** on the Advanced tab.

The following screen capture shows the **General** tab of the newly created **SP-General** Server Interworking Profile.



The following screen capture shows the **Advanced** tab of the newly created **SP-General** Server Interworking Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBC) 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.

On the left, a sidebar menu lists various configuration areas, with 'Global Profiles' expanded to show 'Server Interworking'.

The main content area is titled 'Interworking Profiles: SP-General'. It features a list of profiles on the left, including 'cs2100', 'avaya-ni', 'OCS-Edge-Server', 'cscc-com', 'oups', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General' (highlighted), 'Avaya-CS1000', 'Avaya-IPO', and 'Avaya-CM'. An 'Add' button is located above this list.

The 'SP-General' profile is selected, and its configuration is shown in the 'Advanced' tab. The configuration table lists various settings and their values:

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

Buttons for 'Rename', 'Clone', and 'Delete' are located at the top right of the profile configuration area. An 'Edit' button is at the bottom right.

7.2.3. Signaling Manipulation

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

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult [4] in the **References** section for more information on this topic.

Sigma scripts were created during the compliance test to correct the following interoperability issues (refer to **Section 2.2**):

- **T.38 fax support:** CenturyLink's Broadsoft soft switch only supports T.38 fax version 0, Communication Manager supports T.38 fax versions 0 and 1. Although Communication Manager supports fax versions 0 and 1, negotiation to version 0 was unsuccessful. The T.38 fax version mismatch was causing T.38 fax to fail in both directions (CM \leftarrow \rightarrow PSTN). A SigMa script was created to change the value in the "T38FaxVersion" field from 1 to 0 in re-INVITEs sent by Communication Manager before passing the re-INVITEs to CenturyLink. The script was latter applied to the Session Manager side of the server configuration profile (refer to **Section 7.2.4**). The name given to the script was **Chg fax version 1 to version 0**, as shown below.
- **Remove unwanted headers:** A Sigma script was created to remove headers that should not be exposed outside of the enterprise and to remove headers that have no value to the service provider, such as "Remote-Address". The script was latter applied to the Service Provider side of the server configuration profile (refer to **Section 7.2.4**). The script was included under the **CenturyLink_Sigma** script shown below.
- **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 7.2.4**). The script was included under the **CenturyLink_Sigma** script shown below.

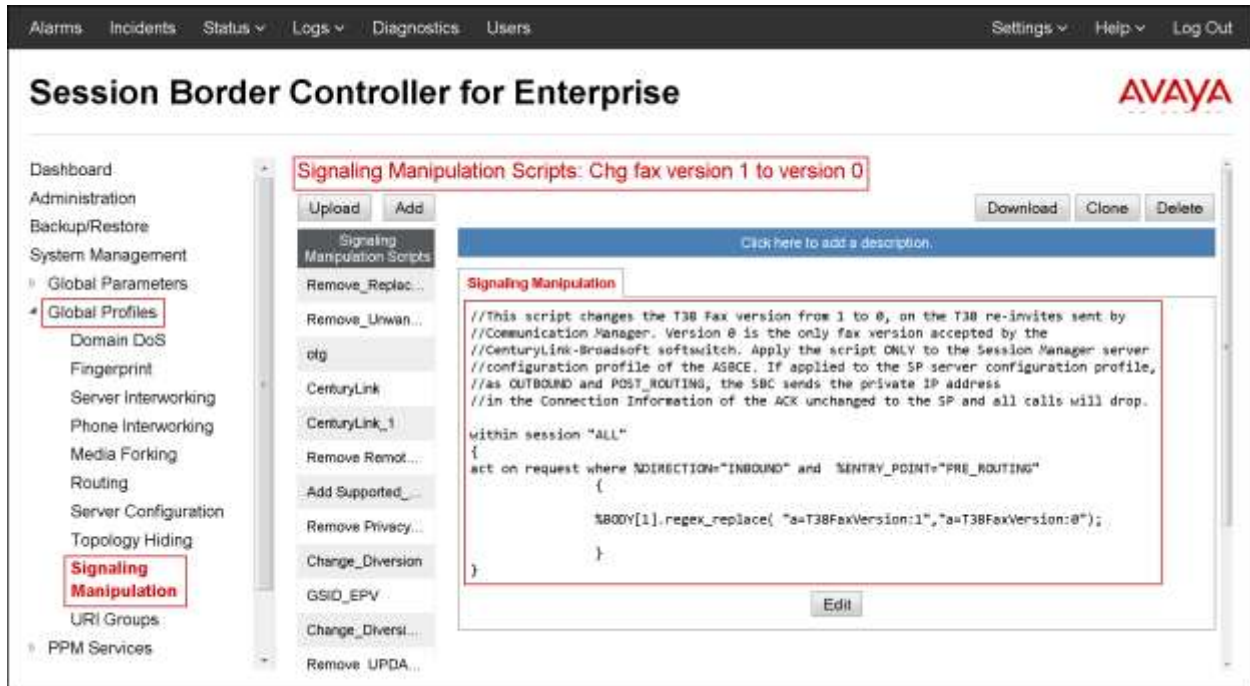
Note: Additional Avaya SBCE header manipulation will be performed by implementing Signaling Rules, in **Section 7.3.3** later in this document.

To create a SigMa script to change the **T38FaxVersion** value from 1 to 0 in the re-INVITEs sent by Communication Manager, on the left navigation pane, select **Global Profiles \rightarrow Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name, the name *Chg fax version 1 to version 0* was chosen in this example.

- Copy the complete script from **Appendix A**.
- Click **Save**.

The following screen capture shows the **Chg fax version 1 to version 0** SigMa script after it was added.



To create a SigMa script to remove the **Remote-Address** and the **a=sendonly** value from the SDP, on the left navigation pane, select **Global Profiles** → **Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name, the name *CenturyLink_Sigma* was chosen in this example.
- Copy the complete script from **Appendix A**.
- Click **Save**.

The following screen capture shows the **CenturyLink_Sigma** script after it was added.



7.2.4. Server Configuration

Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (Session Manager) and the Trunk Server which is the SIP Proxy at the Service Provider's network.

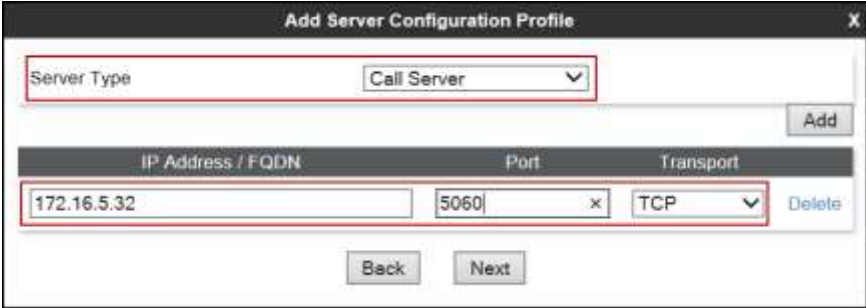
To add a server configuration profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration**. Click **Add** in the **Server Profiles** section and enter the profile name: *Session Manager*.



The screenshot shows a window titled "Add Server Configuration Profile". Inside, there is a text input field labeled "Profile Name" containing the text "Session Manager". To the right of the input field is a small "x" icon. Below the input field is a "Next" button.

In the **Add Server Configuration Profile** window:

- **Server Type:** select *Call Server*.
- **IP Address / FQDN:** *172.16.5.32* (IP Address of the Session Manager SIP entity).
- **Port:** *5060* (This port must match the port number defined in **Section 6.5**).
- **Transports:** Select *TCP*.
- Click **Next**.



The screenshot shows the "Add Server Configuration Profile" window with the following details:

- Server Type:** A dropdown menu set to "Call Server".
- Add:** A button to the right of the Server Type dropdown.
- Table:** A table with three columns: "IP Address / FQDN", "Port", and "Transport".

IP Address / FQDN	Port	Transport
172.16.5.32	5060	TCP
- Delete:** A button to the right of the table.
- Back:** A button below the table.
- Next:** A button below the table.

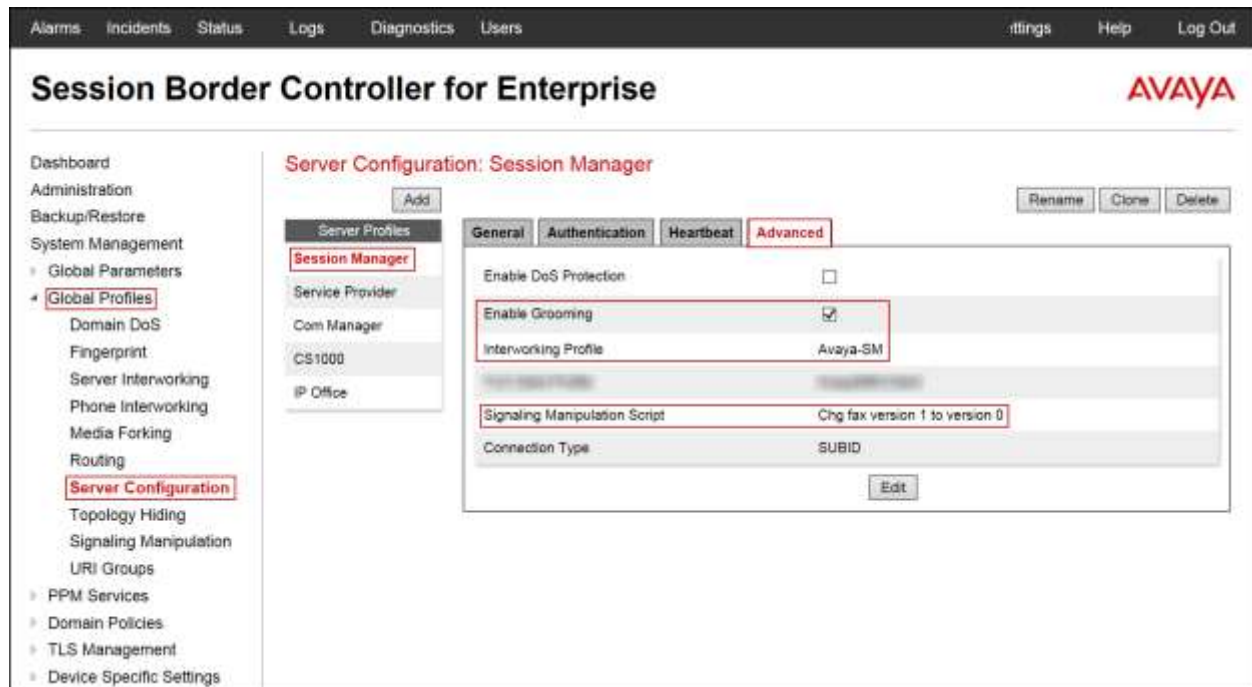
- Click **Next** in the **Add Server Configuration Profile - Authentication** window (not shown).
- Click **Next** in the **Add Server Configuration Profile - Heartbeat** window (not shown).

In the **Add Server Configuration Profile - Advanced** window:

- Check **Enable Grooming**.
- Select **Avaya-SM** from the **Interworking Profile** drop down menu, created in **Section 7.2.1**.
- Select **Chg fax version 1 to version 0** from the **Signaling Manipulation Script** drop down menu, created in **Section 7.2.3**.
- Click **Finish**.

The following screen capture shows the **General** tab of the newly created **Session Manager** Server Profile.

The following screen capture shows the **Advanced** tab of the newly created **Session Manager** Server Profile.



To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** section and enter the profile name: *Service Provider*.



In the **Add Server Configuration Profile** window

- **Server Type:** select *Trunk Server*.
- **IP Address/FQDN:** *192.168.64.81* (CenturyLink's SIP Proxy IP address).
- **Port:** *5100* (this port number was provided by CenturyLink. The port number may vary; this information should be provided by CenturyLink).
- **Transports:** Select *UDP*.
- Click **Next**.

IP Address / FQDN	Port	Transport
192.168.64.81	5100	UDP

On the **Authentication** tab:

- Check the *Enable Authentication* box.
- Enter the **User Name** credential provided by CenturyLink for SIP trunk registration.
- Leave the **Realm** blank.
- Enter **Password** credential provided by CenturyLink for SIP trunk registration.
- Click **Next**.

Enable Authentication	<input checked="" type="checkbox"/>
User Name	User123
Realm (Leave blank to detect from server challenge)	
Password
Confirm Password

On the **Heartbeat** tab:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider; **60** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
 - **From URI**: Use the **trunk pilot** number provided by the CenturyLink for SIP trunk registration (**1234565746**) and CenturyLink's domain name (**voip.centurylink.com**), as shown on the screen below.
 - **To URI**: Use the **trunk pilot** number provided by CenturyLink for SIP trunk registration (**1234565746**) and CenturyLink's domain name (**voip.centurylink.com**), as shown on the screen below.
- Click **Next**.

Add Server Configuration Profile - Heartbeat

Enable Heartbeat ☒

Method REGISTER ▾

Frequency 60 seconds

From URI 1234565746@voip.centurylink.com

To URI 1234565746@voip.cen

Back Next

In the **Add Server Configuration Profile - Advanced** window:

- Select **SP-General** from the **Interworking Profile**, created in **Section 7.2.2**.
- Select **CenturyLink_Sigma** from the **Signaling Manipulation Script**, created in **Section 7.2.3**.
- Click **Finish**.

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General

Signaling Manipulation Script CenturyLink_Sigma

Connection Type SUBID

Back Finish

The following screen capture shows the **General** tab of the newly created **Service Provider** Server Configuration Profile.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Server Configuration: Service Provider

Add Rename Clone Delete

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

Server Type Trunk Server

IP Address / FQDN	Port	Transport
192.168.64.81	5100	UDP

Edit

The following screen capture shows the **Authentication** tab of the newly created **Service Provider** Server Configuration Profile.

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 the product name and the Avaya logo. On the left, a sidebar menu lists various configuration categories, with 'Server Configuration' highlighted. The main content area is titled 'Server Configuration: Service Provider' and features a sub-menu with 'General', 'Authentication', 'Heartbeat', and 'Advanced' tabs. The 'Authentication' tab is active, showing a table with the following data:

Field	Value
Enable Authentication	<input checked="" type="checkbox"/>
User Name	User123
Realm	---

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible. The 'Edit' button is located at the bottom right of the table.

The following screen capture shows the **Heartbeat** tab of the newly created **Service Provider** Server Configuration Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface, showing the 'Heartbeat' tab of the 'Service Provider' configuration. The top navigation bar and sidebar menu are consistent with the previous screenshot. The main content area is titled 'Server Configuration: Service Provider' and features a sub-menu with 'General', 'Authentication', 'Heartbeat', and 'Advanced' tabs. The 'Heartbeat' tab is active, showing a table with the following data:

Field	Value
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	REGISTER
Frequency	60 seconds
From URI	123456746@voip.centurylink.com
To URI	123456746@voip.centurylink.com

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible. The 'Edit' button is located at the bottom right of the table.

The following screen capture shows the **Advanced** tab of the newly created **Service Provider** Server Configuration Profile.

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 the product name and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Server Configuration' highlighted. The main content area is titled 'Server Configuration: Service Provider' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. A list of server profiles is shown, with 'Service Provider' selected. The 'Advanced' tab is active, displaying configuration options: 'Enable DoS Protection' (unchecked), 'Enable Grooming' (unchecked), 'Interworking Profile' (set to 'SP-General'), 'Signaling Manipulation Script' (set to 'CenturyLink_Sigma'), and 'Connection Type' (set to 'SUBID'). An 'Edit' button is located at the bottom right of the configuration area.

General	Authentication	Heartbeat	Advanced
Enable DoS Protection <input type="checkbox"/>			
Enable Grooming <input type="checkbox"/>			
Interworking Profile		SP-General	
Signaling Manipulation Script		CenturyLink_Sigma	
Connection Type		SUBID	

7.2.5. Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing profiles were created; one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are sent to the service provider.

To create the inbound route, from the **Global Profiles** menu on the left-hand side:

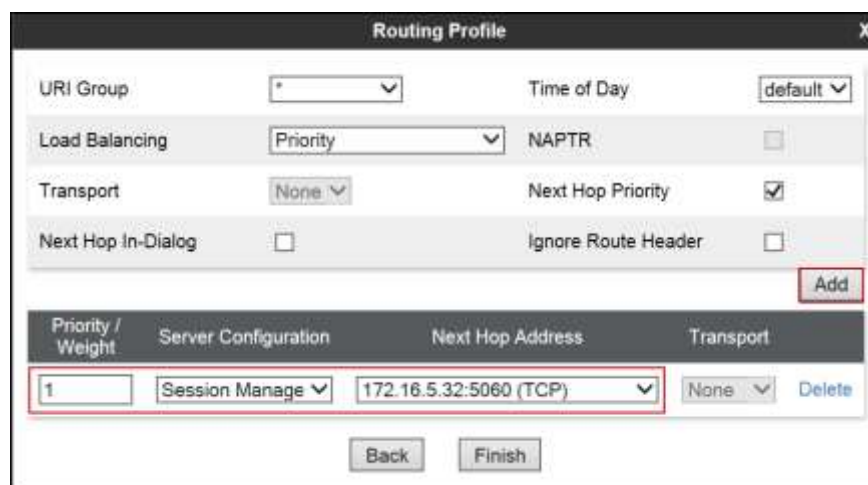
- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route_to_SM**.
- Click **Next**.



The image shows a 'Routing Profile' dialog box. It has a title bar with 'Routing Profile' and a close button. Inside, there is a text field labeled 'Profile Name' containing the text 'Route_to_SM'. To the right of the text field is a small 'x' icon. Below the text field is a 'Next' button.

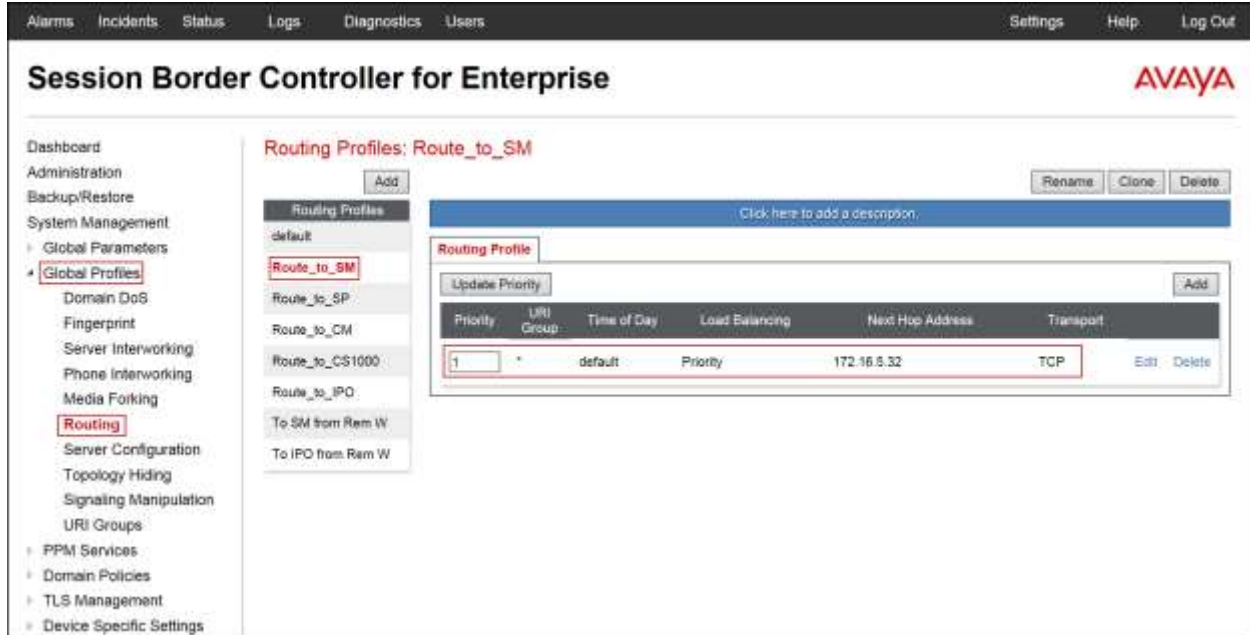
On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select **Session Manager**.
- Click **Finish**.



The image shows the 'Routing Profile' configuration screen. It has a title bar with 'Routing Profile' and a close button. The main area contains several settings: 'URI Group' (dropdown), 'Time of Day' (dropdown), 'Load Balancing' (dropdown), 'NAPTR' (checkbox), 'Transport' (dropdown), 'Next Hop Priority' (checkbox), 'Next Hop In-Dialog' (checkbox), and 'Ignore Route Header' (checkbox). There is an 'Add' button. Below these settings is a table with four columns: 'Priority / Weight', 'Server Configuration', 'Next Hop Address', and 'Transport'. The table has one row with the following values: '1', 'Session Manager', '172.16.5.32:5060 (TCP)', and 'None'. There is a 'Delete' button next to the 'Transport' column. At the bottom are 'Back' and 'Finish' buttons.

The following screen capture shows the newly created **Route_to_SM** Routing Profile.



Similarly, for the outbound route:

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route_to_SP**.
- Click **Next**.



On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select *Service Provider*.
- Click **Finish**.

Routing Profile

URI Group: * Time of Day: default

Load Balancing: Priority NAPTR: ☐

Transport: None Next Hop Priority: ☒

Next Hop In-Dialog: ☐ Ignore Route Header: ☐

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Service Provider	192.168.64.81:5100 (UDP)	None

Back Finish

The following screen capture shows the newly created **Route_to_SP** Routing Profile.

Session Border Controller for Enterprise

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Routing Profiles: Route_to_SP

Click here to add a description.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	192.168.64.81	UDP

7.2.6. Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, 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 SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Session Manager and the SIP trunk Service Provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

To add the Topology Hiding profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Select the **default** profile in the **Topology Hiding Profiles** list, then click **Clone** on top right of the screen.
- Enter the **Profile Name: *Session_Manager***.
- Click **Finish**.
- Click **Edit** on the newly added **Session_Manager** Topology Hiding profile.
- For **Request-Line** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the Enterprise (***avaya.lab.com***) under **Overwrite Value**.
- For **From** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the enterprise (***avaya.lab.com***) under **Overwrite Value**.
- For **To** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Enterprise (***avaya.lab.com***) under **Overwrite Value**.

The screenshot shows a window titled "Edit Topology Hiding Profile" with a table of configuration rules. The table has four columns: Header, Criteria, Replace Action, and Overwrite Value. The rules are as follows:

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

Each row has a "Delete" button to its right. A "Finish" button is located at the bottom center of the window.

The following screen capture shows the newly created **Session_Manager** Topology Hiding Profile.

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 the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Global Profiles' and 'Topology Hiding' highlighted. The main content area is titled 'Topology Hiding Profiles: Session_Manager' and features an 'Add' button. Below this, a list of profiles is shown, with 'Session_Manager' selected. The configuration details for 'Session_Manager' are displayed in a table with columns for Header, Criteria, Replace Action, and Overwrite Value. The table lists several SIP headers and their corresponding actions and values.

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

To add the Topology Hiding profile in the service provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Select the **default** profile in the **Topology Hiding Profiles** list, then click **Clone** on top right of the screen.
- Enter the **Profile Name: *Service_Provider***.
- Click **Finish**.
- Click **Edit** on the newly added **Service_Provider** Topology Hiding profile.
- For **Refer-To** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the service provider (***voip.centurylink.com***) under **Overwrite Value**.
- For **From** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (***voip.centurylink.com***) under **Overwrite Value**.
- For **Request-Line** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the service provider (***voip.centurylink.com***) under **Overwrite Value**.
- For **To** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (***voip.centurylink.com***) under **Overwrite Value**.

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

Finish

The following screen capture shows the newly created **Service_Provider** Topology Hiding Profile.

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.

The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (highlighted), Signaling Manipulation, URI Groups, PPM Services, Domain Policies, TLS Management, and Device Specific Settings.

The main content area is titled 'Topology Hiding Profiles: Service_Provider'. It features an 'Add' button and a list of profiles: default, disco_th_profile, Session_Manager, Service_Provider (highlighted), Com Manager, CS1000, and IP Office. Below the list is a table for the 'Service_Provider' profile.

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

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

7.3. Domain Policies

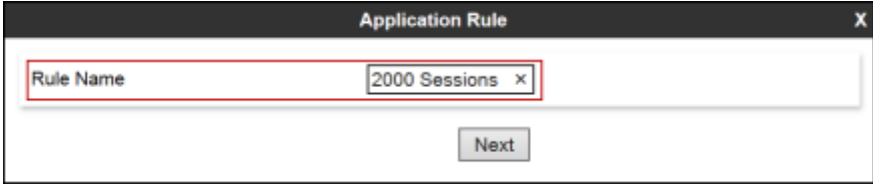
Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

Note: The **default-trunk** Application Rule could have been used instead of creating a new one, but a new Application Rule was created to allow changes in the future.

7.3.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies → Application Rules**.

- Click on the **Add** button to add a new rule.
- **Rule Name:** enter the name of the profile, e.g., *2000 Sessions*.
- Click **Next**.



- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **2000** was used in the sample configuration.
- Click **Finish**.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support: ☒ None, ☐ CDR w/ RTP, ☐ CDR w/o RTP

RTCP Keep-Alive: ☐

Back Finish

The following screen capture shows the newly created **2000 Sessions** Application Rule.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Application Rules: 2000 Sessions

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
Application Rules
Border Rules
Media Rules
Security Rules

Application Rules: default, default-trunk, default-subscriber-low, default-subscriber-high, default-server-low, default-server-high, **2000 Sessions**, 500 Sessions, Remote-Workers, test

Application Rule configuration:

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

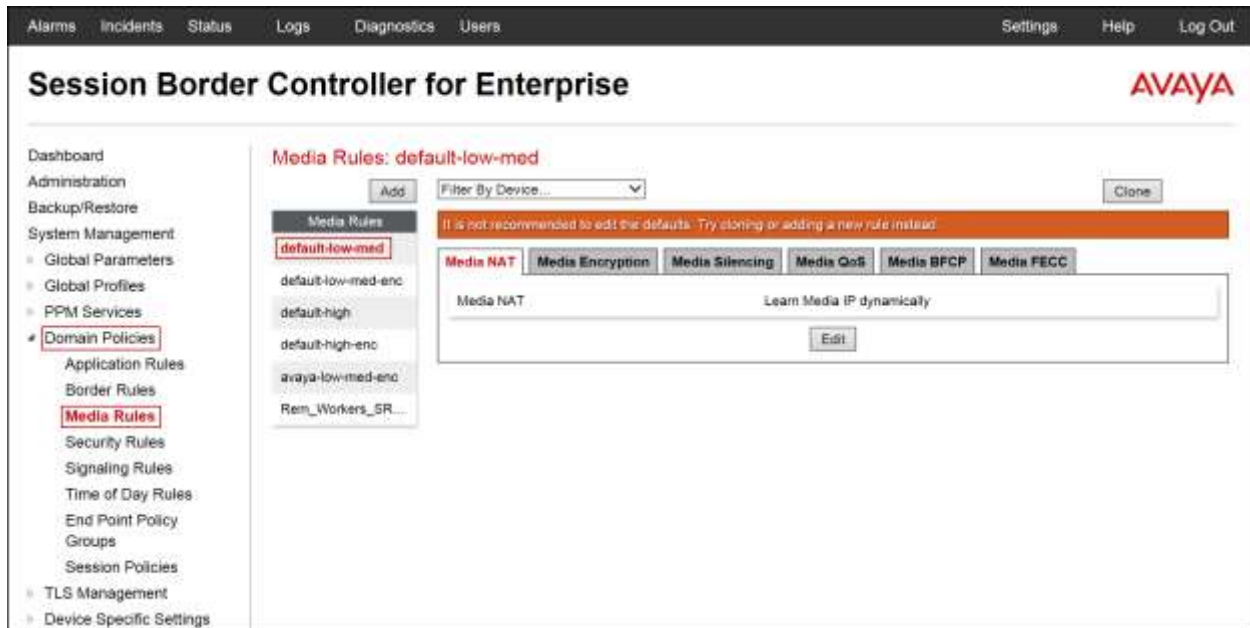
CDR Support: None

RTCP Keep-Alive: No

Edit

7.3.2. Media Rules

For the compliance test, the **default-low-med** Media Rule was used.



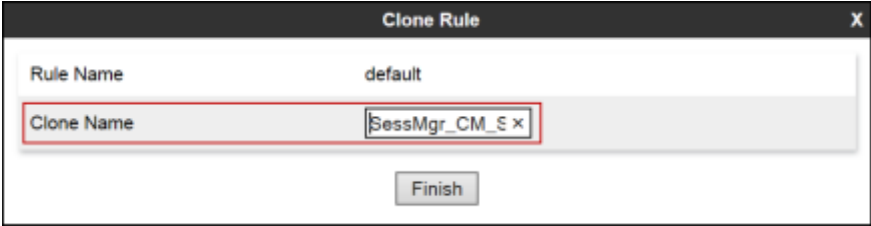
7.3.3. Signaling Rules

Signaling Rules define the actions to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. They also allow the control of the Quality of Service of the signaling packets.

Headers such as Alert-Info, P-Location, P-Charging-Vector and others are sent in SIP messages from Session Manager to the Avaya SBCE for egress to the service provider's network. These headers should not be exposed external to the enterprise. For simplicity, these headers were simply removed (blocked) from both requests and responses for both inbound and outbound calls.

A Signaling Rule was created, to later be applied in the direction of the enterprise to block unwanted headers coming from Session Manager from being propagated to CenturyLink's network. To add this header, in the **Domain Policies** menu, select **Signaling Rules**:

- Click on **default** in the **Signaling Rules** list.
- Click on **Clone** on top right of the screen.
- Enter a name: *SessMgr_CM_SigRule*.
- Click **Finish**.



Select the **Request Headers** tab of the newly created *SessMgr_CM_SigRule* Signaling Rule.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *AV-Global-Session-ID*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **Alert-Info** header:

- Select **Add in Header Control**.
- **Header Name:** *Alert-Info*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.

- Click **Finish**.

To add the **Endpoint-View** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *Endpoint-View*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **History-Info** header:

- Select **Add in Header Control**.
- **Header Name:** *History-Info*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-AV-Message-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-AV-Message-ID*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Charging-Vector** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Charging-Vector*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Location** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Location*.

- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

The following screen capture shows the **Request Headers** tab of the **SessMgr_CM_SigRule** Signaling Rule.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, System Management, and Signaling Rules. The 'Signaling Rules' category is expanded, and 'SessMgr_CM_SigRule' is selected. The main area displays the configuration for this rule, with the 'Request Headers' tab active. A table lists the configured headers, including AV-Global-Session-ID, Alert-Info, Endpoint-View, History-Info, P-AV-Message-ID, P-Charging-Vector, and P-Location. Each header is configured with Method Name: ALL, Header Criteria: Forbidden, and Action: Remove Header.

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
3	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	History-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
5	P-AV-Message-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Next, select the **Response Headers** tab of the newly created **SessMgr_CM_SigRule** Signaling Rule.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *AV-Global-Session-ID*.
- **Response Code:** *1XX*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *AV-Global-Session-ID*.

- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *AV-Global-Session-ID*.
- **Response Code:** *4XX*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *AV-Global-Session-ID*.
- **Response Code:** *5XX*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **Alert-Info** header:

- Select **Add in Header Control**.
- **Header Name:** *Alert-Info*.
- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **Endpoint-View** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *Endpoint-View*.
- **Response Code:** *1XX*.

- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **Endpoint-View** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *Endpoint-View*.
- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-AV-Message-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-AV-Message-ID*.
- **Response Code:** *1XX*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-AV-Message-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-AV-Message-ID*.
- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Charging-Vector** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Charging-Vector*.
- **Response Code:** *200*.

- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Conference** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Conference*.
- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Location** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Location*.
- **Response Code:** *1XX*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Location** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Location*.
- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Location** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Location*.
- **Response Code:** *4XX*.

- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Location** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Location*.
- **Response Code:** *5XX*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

The following screen capture shows the **Response Headers** tab of the **SessMgr_CM_SigRule** signaling rule.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
PPM Services
Domain Policies
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
Time of Day Rules
End Point Policy Groups
Session Policies
TLS Management
Device Specific Settings

Signaling Rules: SessMgr_CM_SigRule

Add Filter By Device... Rename Clone Delete

default
No-Content-Type-Checks
SessMgr_CS1K_SigRule
Remote Workers
Remove_headers
Remove_PAI
Remove_PAI_1
Contact
SessMgr_CM_SigRule
Remove_Update
OPTIONS

Click here to add a description...

General Requests Responses Request Headers **Response Headers** Signaling QoS UCID

Add In Header Control Add Out Header Control

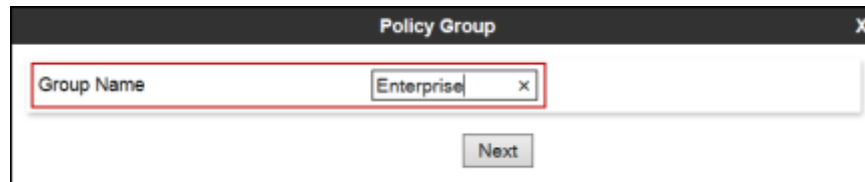
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	AV-Global-Session-ID	4XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	AV-Global-Session-ID	5XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	Alert-Info	200	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
6	Endpoint-View	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	Endpoint-View	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-AV-Message-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	P-AV-Message-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
10	P-Charging-Vector	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
11	P-Conference	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
12	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
13	P-Location	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
14	P-Location	4XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
15	P-Location	5XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.3.4. End Point Policy Groups

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

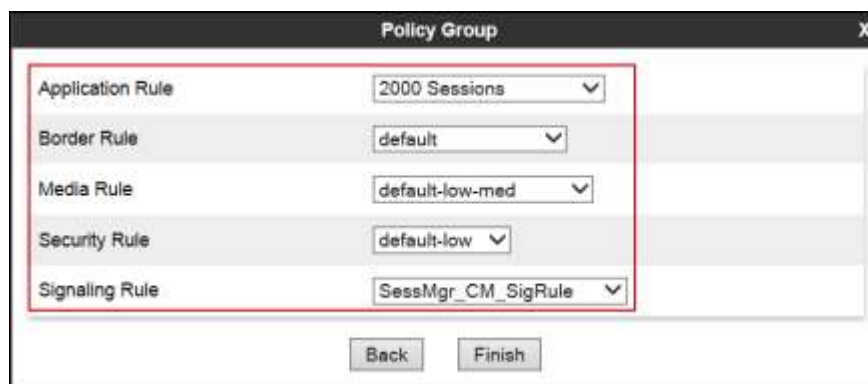
To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups**. Select **Add Group**:

- Under **Group Name** enter *Enterprise*.
- Click **Next**.



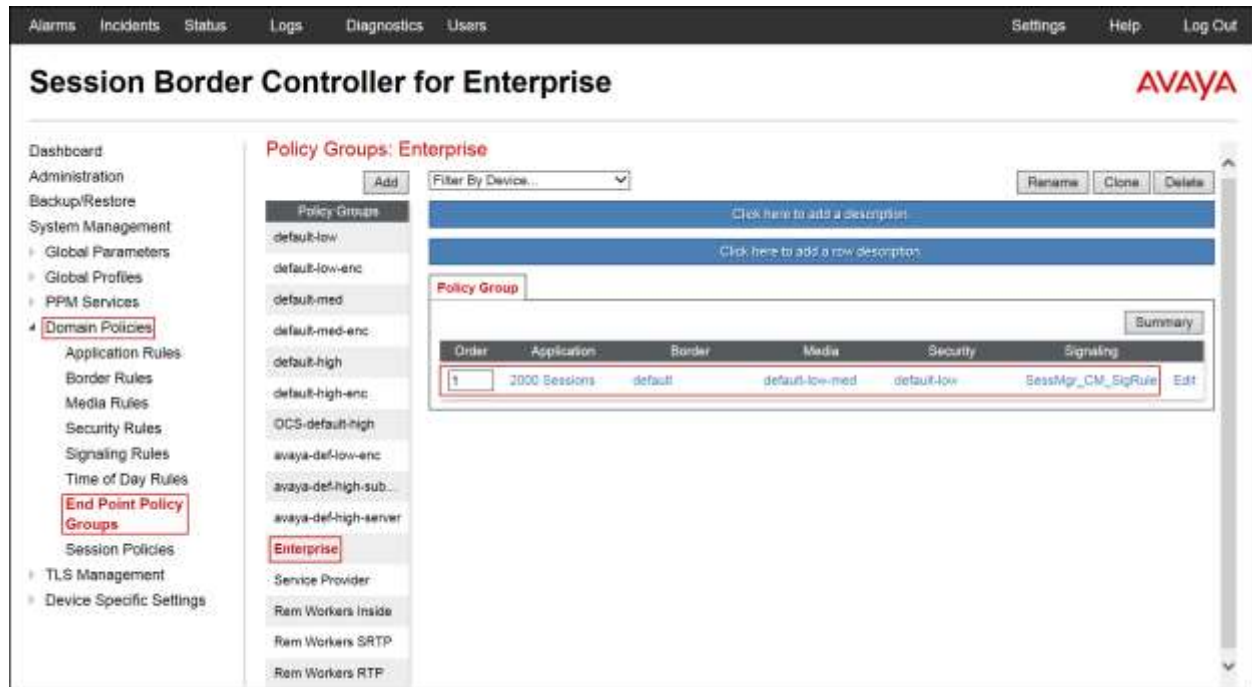
The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" which contains the text "Enterprise". A red rectangular box highlights this field. Below the input field, there is a "Next" button.

- **Application Rule:** *2000 Sessions*.
- **Border Rule:** *default*.
- **Media Rule:** *default-low-med*.
- **Security Rule:** *default-low*.
- **Signaling Rule:** *SessMgr_CM_SigRule*.
- Click **Finish**.



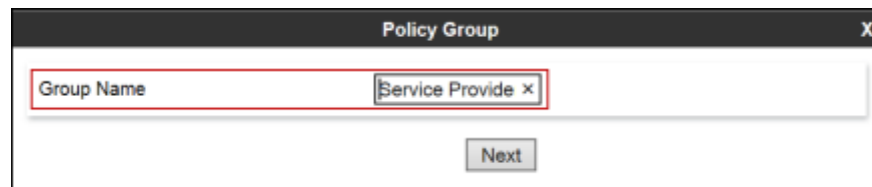
The screenshot shows the same "Policy Group" dialog box, but now it displays five dropdown menus. A red rectangular box highlights these five dropdowns. The values selected in the dropdowns are: "2000 Sessions" for Application Rule, "default" for Border Rule, "default-low-med" for Media Rule, "default-low" for Security Rule, and "SessMgr_CM_SigRule" for Signaling Rule. At the bottom of the dialog, there are two buttons: "Back" and "Finish".

The following screen capture shows the newly created **Enterprise** End Point Policy Group.



Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add Group**:

- Under **Group Name** enter *Service Provider*.
- Click **Next**.



- **Application Rule:** *2000 Sessions*.
- **Border Rule:** *default*.
- **Media Rule:** *default-low-med*.
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default*.
- Click **Finish**.

Policy Group

Application Rule: 2000 Sessions

Border Rule: default

Media Rule: default-low-med

Security Rule: default-low

Signaling Rule: default

Back Finish

The following screen capture shows the newly created **Service Provider** End Point Policy Group.

Session Border Controller for Enterprise

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Policy Groups: Service Provider

Policy Groups

Order	Application	Border	Media	Security	Signaling
1	2000 Sessions	default	default-low-med	default-low	default

7.4. Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

7.4.1. Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.

In the event that changes need to be made to the network configuration information, they can be entered here.

Use **Figure 1** as reference for IP address assignments.

Note: Only the highlighted entity items were created for the compliance test, and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in this Application Notes.



The screenshot shows 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. The left sidebar contains a tree view of the configuration menu, with "Device Specific Settings" expanded and "Network Management" selected. The main content area is titled "Network Management: Avaya SBCE" and has two tabs: "Interfaces" and "Networks". The "Networks" tab is active, displaying a table of network configurations. The table has columns for Name, Gateway, Subnet Mask, Interface, and IP Address. Two networks are listed: Network_A1 and Network_B1. The IP addresses 172.16.5.71 and 10.10.157.186 are highlighted with red boxes. There are "Edit" and "Delete" links for each network entry.

Name	Gateway	Subnet Mask	Interface	IP Address	
Network_A1	172.16.5.254	255.255.255.0	A1	172.16.5.71	Edit Delete
Network_B1	10.10.157.129	255.255.255.0	B1	10.10.157.186	Edit Delete

On the Interface Configuration tab, click the **Toggle** control for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **disabled**, so it is important to perform this step or the Avaya SBCE will not be able to communicate on any of its interfaces.

The screenshot displays the Avaya 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. A left sidebar contains a menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. The 'Device Specific Settings' category is expanded, showing 'Network Management' as a sub-option. The main content area is titled 'Network Management: Avaya SBCE' and features two tabs: 'Devices' and 'Networks'. The 'Networks' tab is active, showing a table with columns for Interface Name, VLAN Tag, and Status. The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Disabled). The 'Toggle' control for A1 and B1 is highlighted with a red box.

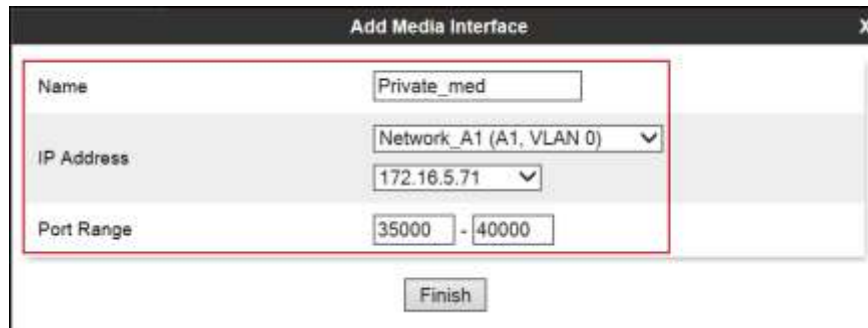
Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

7.4.2. Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the default port range 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**. Below is the configuration of the inside, private Media Interface of the Avaya SBCE.

- Select **Add** in the **Media Interface** area.
- **Name:** *Private_med*.
- **IP Address, Networks** pull down menu select *Network_A1 (A1, VLAN 0)*.
- **IP Address, IP Addresses** pull down menu select *172.16.5.71*.
- **Port Range:** *35000-40000*.
- Click **Finish**.

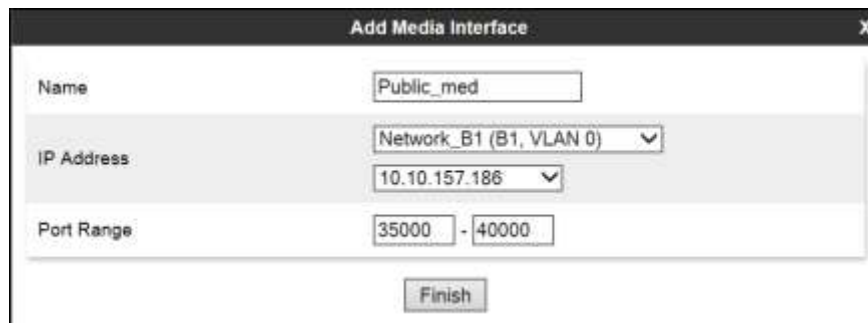


The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains the following fields:

- Name:** A text input field containing "Private_med".
- IP Address:** A section with two dropdown menus. The first dropdown is labeled "Networks" and contains "Network_A1 (A1, VLAN 0)". The second dropdown is labeled "IP Addresses" and contains "172.16.5.71".
- Port Range:** Two input fields containing "35000" and "40000" separated by a hyphen.
- Finish:** A button at the bottom right of the dialog.

Below is the configuration of the outside, public Media Interface of the Avaya SBCE.

- Select **Add** in the **Media Interface** area.
- **Name:** *Public_med*.
- **IP Address, Networks** pull down menu select *Network_B1 (B1, VLAN 0)*.
- **IP Address, IP Addresses** pull down menu select *10.10.157.186*.
- **Port Range:** *35000-40000*.
- Click **Finish**.



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

- Name:** A text input field containing "Public_med".
- IP Address:** A section with two dropdown menus. The first dropdown is labeled "Networks" and contains "Network_B1 (B1, VLAN 0)". The second dropdown is labeled "IP Addresses" and contains "10.10.157.186".
- Port Range:** Two input fields containing "35000" and "40000" separated by a hyphen.
- Finish:** A button at the bottom right of the dialog.

The following screen capture shows the newly created **Media Interfaces**.

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. A left-hand navigation menu lists various management sections, with "Device Specific Settings" and its sub-item "Media Interface" highlighted. The main content area is titled "Media Interface: Avaya SBCE" and contains a sub-tab "Media Interface". A red warning banner states: "Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management." Below this is a table of media interfaces with columns for Name, Media IP Network, Port Range, and actions (Edit, Delete). The table lists two interfaces: "Private_med" and "Public_med", both with port ranges of 35000 - 40000. Below the table, there are links to "Add", "Refresh", and "Reset".

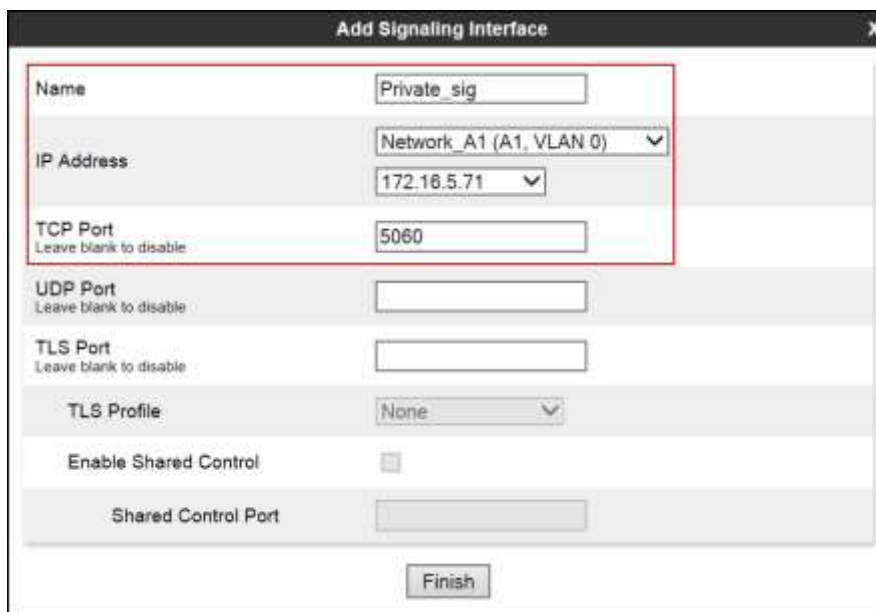
Name	Media IP Network	Port Range	Edit	Delete
Private_med	172.16.5.71 Network_A1 (AT_VLAN 5)	35000 - 40000	Edit	Delete
Public_med	10.10.157.186 Network_B1 (AT_VLAN 20)	35000 - 40000	Edit	Delete

7.4.3. Signaling Interface

To create the Signaling Interface toward Session Manager, from the **Device Specific** menu on the left hand side, select **Signaling Interface**.

Below is the configuration of the inside, private Signaling Interface of the Avaya SBCE.

- Select **Add** in the **Signaling Interface** area.
- **Name:** *Private_sig*.
- **IP Address, Networks** pull down menu select *Network_A1 (A1, VLAN 0)*.
- **IP Address, IP Addresses** pull down menu select *172.16.5.71*.
- **TCP Port:** *5060*.
- Click **Finish**.



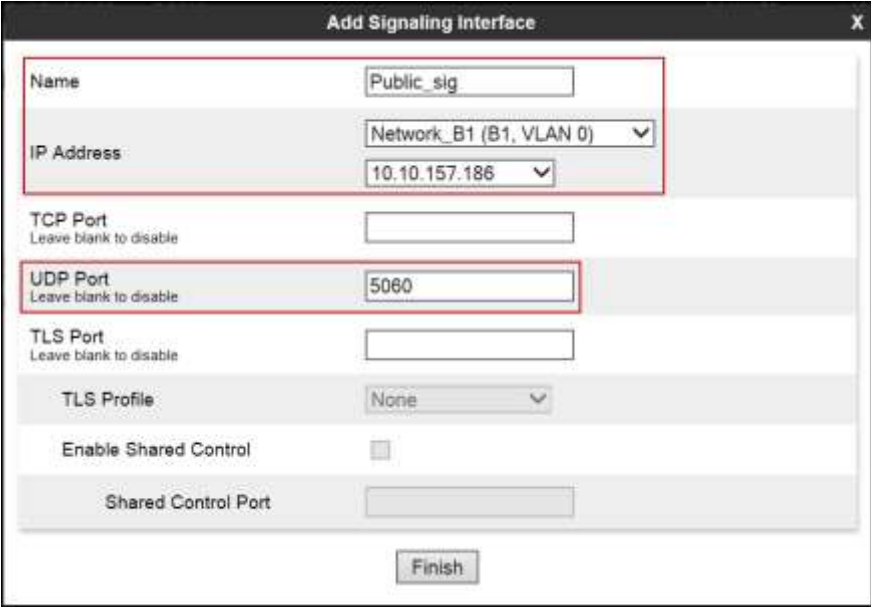
The screenshot shows a configuration window titled "Add Signaling Interface". The window contains several fields and a "Finish" button. A red rectangle highlights the "Name", "IP Address", and "TCP Port" fields. The "Name" field is set to "Private_sig". The "IP Address" field is a pull-down menu showing "Network_A1 (A1, VLAN 0)" and "172.16.5.71". The "TCP Port" field is set to "5060". Below these fields are "UDP Port", "TLS Port", "TLS Profile", "Enable Shared Control", and "Shared Control Port" fields. The "Finish" button is at the bottom right.

Name	Private_sig
IP Address	Network_A1 (A1, VLAN 0) 172.16.5.71
TCP Port	5060
UDP Port	
TLS Port	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

Below is the configuration of the outside, public signaling Interface of the Avaya SBCE.

- Select **Add** in the **Signaling Interface** area.
- **Name:** *Public_sig*.
- **IP Address, Networks** pull down menu select *Network_B1 (B1, VLAN 0)*.
- **IP Address, IP Addresses** pull down menu select *10.10.157.186*.
- **UDP Port:** *5060*.
- Click **Finish**.



The screenshot shows a web-based configuration window titled "Add Signaling Interface". The window contains several input fields and a "Finish" button. The "Name" field is set to "Public_sig". The "IP Address" section has a dropdown menu for "Networks" set to "Network_B1 (B1, VLAN 0)" and a dropdown menu for "IP Addresses" set to "10.10.157.186". The "UDP Port" field is set to "5060". The "TCP Port" field is empty. The "TLS Port" field is empty. The "TLS Profile" dropdown menu is set to "None". The "Enable Shared Control" checkbox is unchecked. The "Shared Control Port" field is empty. The "Finish" button is at the bottom right.

Name	Public_sig
IP Address	Network_B1 (B1, VLAN 0) 10.10.157.186
TCP Port	
UDP Port	5060
TLS Port	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

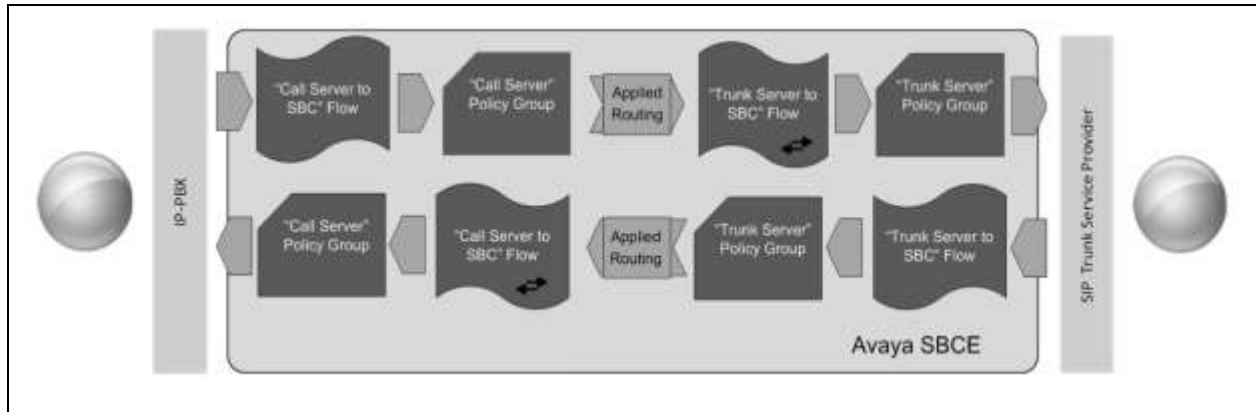
The following screen capture shows the newly created **Signaling Interfaces**.

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 shows "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with "Device Specific Settings" expanded and "Signaling Interface" selected. The main content area is titled "Signaling Interface: Avaya SBCE" and features a "Signaling interface" tab. A warning message states: "Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management." Below this, a table lists the configured signaling interfaces:

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	172.16.6.71 Network_A1 (A1, VLAN 5)	5060	5060	—	None	Edit Delete
Public_sig	10.10.157.186 Network_B1 (B1, VLAN 2)	—	5060	—	None	Edit Delete
...

7.4.4. End Point Flows

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



The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, and then the **Server Flows** tab. Click **Add** (not shown).

- **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* (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** *Service_Provider*.
- **File Transfer Profile:** *None*.
- **Signaling Manipulation Script:** *None*.
- **Remote Branch Office:** *Any*.
- Click **Finish**.

The screenshot shows a configuration window titled "Edit Flow: SIP_Trunk_Flow". It contains a list of configuration fields with their respective values:

Field	Value
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
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

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

To create the call flow toward the Session Manager, click **Add**.

- **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* (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** *Session_Manager*.
- **File Transfer Profile:** *None*.
- **Signaling Manipulation Script:** *None*.
- **Remote Branch Office:** *Any*.
- Click **Finish**.

The screenshot shows a window titled "Edit Flow: Session_Manager_Flow". Inside, there is a list of configuration fields, each with a label and a value or a dropdown menu. The fields are: 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), File Transfer Profile (None), Signaling Manipulation Script (None), and Remote Branch Office (Any). A "Finish" button is located at the bottom right of the dialog.

Field	Value
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
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

The following screen capture shows the newly created **End Point Flows**.

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 shows the title "Session Border Controller for Enterprise" and the Avaya logo.

On the left sidebar, the "Device Specific Settings" menu is expanded, and "End Point Flows" is selected. The main content area is titled "End Point Flows: Avaya SBCE". It features two tabs: "Subscriber Flows" and "Server Flows", with "Server Flows" being the active tab.

Under the "Server Flows" tab, there are two sections for configuration:

- Server Configuration: Service Provider**: This section contains a table with the following data:

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SIP_Trunk_Flow	*	Private_sig	Public_sig	Service Provider	Route_to_SM	View Clone Edit Delete
- Server Configuration: Session Manager**: This section contains a table with the following data:

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
2	Session_Manager_Flow	*	Public_sig	Private_sig	Enterprise	Route_to_SP	View Clone Edit Delete

8. CenturyLink SIP Trunking Service Configuration

To use CenturyLink's SIP Trunking Service, a customer must request the service from CenturyLink using the established sales processes. The process can be started by contacting CenturyLink via the corporate web site at: <http://www.centurylink.com/business/voice/sip-trunk.html> and requesting information.

During the signup process, CenturyLink and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to CenturyLink's network. CenturyLink will provide SIP Trunk registration credentials, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, etc. This information is used to complete the Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise configuration discussed in the previous sections.

9. Verification and Troubleshooting

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

Verification Steps:

1. 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.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active with two-way audio for more than 35 seconds.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

9.1. Troubleshooting

9.1.1. Communication Manager

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

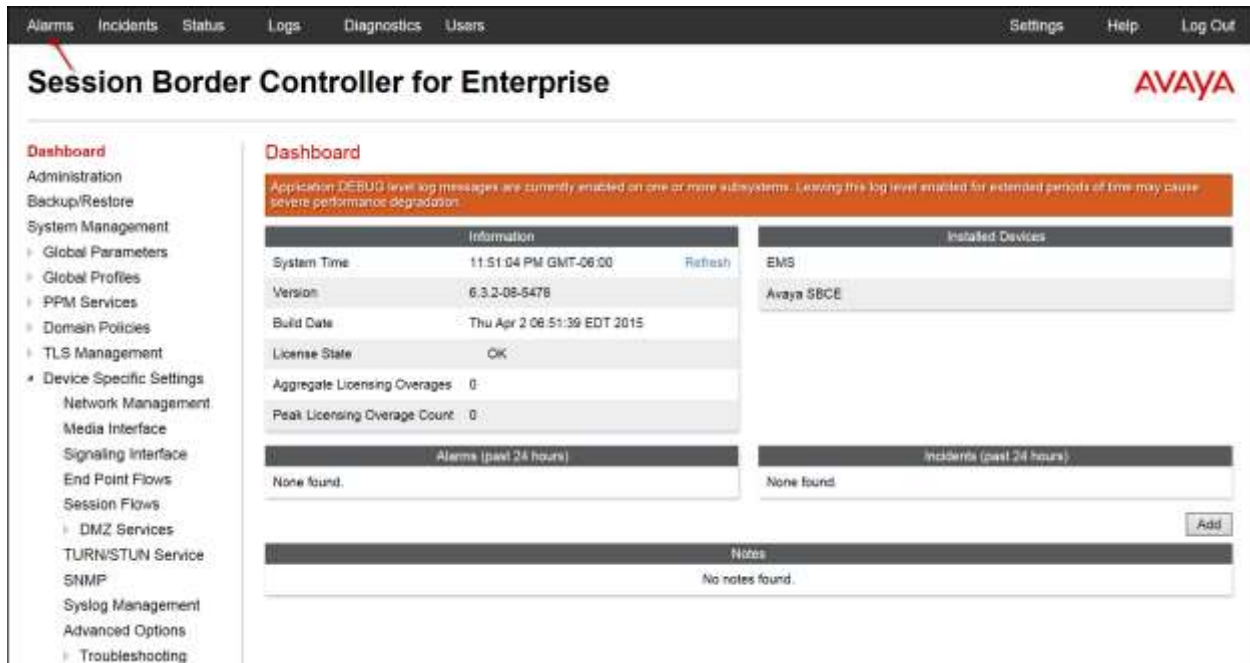
9.1.2. Session Manager

- **traceSM -x** – Session Manager command line tool for traffic analysis. Login to the Session Manager management CLI 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, navigate to **Home → Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

9.1.3. Avaya SBCE

There are several links and menus located on the taskbar at the top of the screen of the web interface that can be used for diagnostic and troubleshooting.

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



The screenshot shows the Avaya SBCE Dashboard. At the top, there is a navigation bar with links: Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left sidebar contains a "Dashboard" section and a list of menu items: Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings, Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, Advanced Options, and Troubleshooting. The main content area is titled "Dashboard" and features a warning banner about DEBUG log messages. Below this, there are four panels: "Information" (showing System Time, Version, Build Date, License State, and Licensing Overages), "Installed Devices" (listing EMS and Avaya SBCE), "Alarms (past 24 hours)" (showing "None found"), and "Incidents (past 24 hours)" (showing "None found"). A "Notes" section at the bottom indicates "No notes found."

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



The screenshot shows the Avaya Alarm Viewer page. The header includes the AVAYA logo and the title "Alarm Viewer". On the left, there is a "Devices" section with a list of devices: EMS and Avaya SBCE. The "Alarms" tab is selected, and the main content area displays a table with columns: ID, Details, State, Time, and Device. The table is currently empty, showing "No alarms found for this device." Below the table, there are "Clear Selected" and "Clear All" buttons.

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

Session Border Controller for Enterprise AVAYA

Dashboard

Application DEBUG level log messages are currently enabled on one or more subsystems. Leaving this log level enabled for extended periods of time may cause severe performance degradation.

Information	
System Time	11:51:04 PM GMT-06:00 Refresh
Version	6.3.2-08-5476
Build Date	Thu Apr 2 06:51:39 EDT 2015
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0

Installed Devices
EMS
Avaya SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

[Add](#)

Notes
No notes found.

The following screen shows the Incident Viewer page.

Incident Viewer AVAYA

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

Displaying results 0 to 0 out of 0.

Type	ID	Date	Time	Category	Device	Cause
No incidents found.						

[<<](#) [<](#) [1](#) [>](#) [>>](#)

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

Session Border Controller for Enterprise

Dashboard

Application DEBUG level log messages are currently enabled on one or more subsystems. Leaving this log level enabled for extended periods of time may cause severe performance degradation.

Information	
System Time	11:51:04 PM GMT-06:00 Refresh
Version	6.3.2-08-5478
Build Date	Thu Apr 2 06:51:39 EDT 2015
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	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 Diagnostics page with the results of a ping test.

Diagnostics

Pinging 172.16.5.201

Average ping from 172.16.5.71[A1] to 172.16.5.201 is 0.220ms.

Full Diagnostic | **Ping Test** | Appraisal | Protocol

Source Device / IP: Network_A1 (A1, VLAN 0)

Source Device / IP: 172.16.5.71

Destination IP: 172.16.5.201

Ping

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 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. A left-hand sidebar lists various configuration categories, with "Device Specific Settings" expanded to show "Troubleshooting" and "Trace" selected. The main content area is titled "Trace: Avaya SBCE" and features two tabs: "Packet Capture" (active) and "Captures". Below the tabs is a "Packet Capture Configuration" form with the following fields:

Packet Capture Configuration	
Status	Ready
Interface	Any
Local Address <small>(IP Port)</small>	All
Remote Address <small>* * Port, IP, IP Port</small>	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>(Using the name of an existing capture will overwrite it)</small>	Sample_Capture.pcap

At the bottom of the form are two buttons: "Start Capture" and "Clear".

Once the capture is stopped, click on 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. A left-hand navigation menu lists various configuration categories, with "Device Specific Settings" and "Troubleshooting" expanded. Under "Troubleshooting", the "Trace" option is selected. The main content area is titled "Trace: Avaya SBCE" and features a "Device" dropdown menu set to "Avaya SBCE". Two tabs, "Packet Capture" and "Captures", are visible, with "Captures" being the active tab. Below the tabs is a table of captured files. The table has columns for "File Name", "File Size (bytes)", and "Last Modified", along with a "Delete" button for each entry. The table contains two entries: "A1_Reverse_Proxy_20150707012015.pcap" (49,152 bytes, modified July 7, 2015 at 12:20:52 AM GMT-08:00) and "RWW1_20150707010500.pcap" (4,096 bytes, modified July 7, 2015 at 12:05:09 AM GMT-08:00). Above the table are controls for sorting (Last Modified, Descending) and buttons for Sort, Reset, and Refresh.

File Name	File Size (bytes)	Last Modified	
A1_Reverse_Proxy_20150707012015.pcap	49,152	July 7, 2015 12:20:52 AM GMT-08:00	Delete
RWW1_20150707010500.pcap	4,096	July 7, 2015 12:05:09 AM GMT-08:00	Delete

10.Conclusion

These Application Notes describe the procedures necessary for configuring Session Initiation Protocol (SIP) Trunk service for an enterprise solution consisting of Avaya Aura® Communication Manager Release 6.3, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.3 to support CenturyLink IQ® SIP Trunk Services, as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

11.References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya Aura® Communication Manager, including the following, is available at: <http://support.avaya.com/>

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.3 03-300509, Issue 10, June 2015.

Product documentation for Avaya Aura® System Manager, including the following, is available at: <http://support.avaya.com/>

- [2] *Administering Avaya Aura® System Manager for Release 6.3.13*, Release 6.3, Issue 8, July 2015.

Product documentation for Avaya Aura® Session Manager, including the following, is available at: <http://support.avaya.com/>

- [3] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 7, September 2014.

Product documentation for the Avaya Session Border Controller for Enterprise, including the following, is available at: <http://support.avaya.com/>

- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.
- [5] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 5, October 2014.

Product documentation for Avaya one-X® Communicator and Avaya Communicator for Windows, including the following, is available at: <http://support.avaya.com/>

- [6] *Administering Avaya one-X® Communicator*, Release 6.2 FP6, April 2015.
- [7] *Avaya one-X® Communicator Overview and Planning*, Release 6.2 FP6, April 2015.
- [8] *Implementing Avaya one-X® Communicator*, Release 6.2 FP6, April 2015.
- [9] *Using Avaya one-X® Communicator*, Release 6.2 FP6, April 2015.
- [10] *Using Avaya Communicator for Windows*, Release 2.1, Document Number: 18-604158, Issue 3, December 2014.
- [11] *Administering Avaya Communicator for Android, iPad, iPhone, and Windows*, Release 2.1, Issue 4, June 2015.

- [12] Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communication Manager Rel. 6.3 and Avaya Aura® Session Managers Rel. 6.3 - Issue 1.0

Product documentation for Remote Worker configuration is available at the following link:

<https://downloads.avaya.com/css/P8/documents/100183254>

Other resources:

- [13] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>.
[14] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

12. Appendix A: SigMa Script

Following are the Signaling Manipulation scripts that were used in the configuration of the Avaya SBCE, **Section 7.2.3**. When adding these scripts as instructed in **Section 7.2.3** enter a name for the script in the Title (e.g., **Chg fax version 1 to version 0** or **CenturyLink_Sigma**) and copy/paste the scripts as shown below.

Title: Chg fax version 1 to version 0

```
//This script changes the T38 Fax version from 1 to 0, on the T38 re-invites sent by
//Communication Manager. Version 0 is the only fax version accepted by the
//CenturyLink-Broadsoft softswitch. Apply the script ONLY to the Session Manager server
//configuration profile of the ASBCE. If applied to the SP server configuration profile,
//as OUTBOUND and POST_ROUTING, the SBC sends the private IP address
//in the Connection Information of the ACK unchanged to the SP and all calls will drop.
```

```
within session "ALL"
{
act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
{

    %BODY[1].regex_replace( "a=T38FaxVersion:1","a=T38FaxVersion:0");

}
}
```

Title: CenturyLink_Sigma

```
//The following script removes the Remote-Address header from outbound INVITEs and
//200 OK messages.
```

```
within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
    remove(%HEADERS["Remote-Address"])[1];
}
}
```

```
//The following script is required in order to play Music On Hold when a call is placed on
//hold at the PBX (CM). The script removes a=sendonly from the INVITE message sent by the
//PBX (CM) to CenturyLink.
```

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

©2015 Avaya Inc. All Rights Reserved.

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

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