



Application Notes for Configuring CenturyLink SIP Trunking (Sonus Platform) with Avaya Aura® Communication Manager R6.3, Avaya Aura® Session Manager R6.3, and Avaya Session Border Controller for Enterprise R6.2– Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunking (Sonus Platform) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager R6.3, Avaya Aura® Communication Manager R6.3.2, Avaya Session Border Controller for Enterprise R6.2 and various Avaya endpoints.

CenturyLink is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing 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.....	10
5. CONFIGURE AVAYA AURA® COMMUNICATION MANAGER.....	11
5.1. LICENSING AND CAPACITY	11
5.2. SYSTEM FEATURES.....	12
5.3. IP NODE NAMES.....	13
5.4. CODECS.....	13
5.5. IP NETWORK REGION	15
5.6. SIGNALING GROUP	16
5.7. TRUNK GROUP	18
5.8. CALLING PARTY INFORMATION.....	21
5.9. OUTBOUND ROUTING	22
6. CONFIGURE AVAYA AURA® SESSION MANAGER.....	25
6.1. SYSTEM MANAGER LOGIN AND NAVIGATION	26
6.2. SPECIFY SIP DOMAIN	28
6.3. ADD LOCATION	28
6.4. ADD ADAPTATION MODULE.....	31
6.5. ADD SIP ENTITIES	33
6.6. ADD ENTITY LINKS	37
6.7. ADD ROUTING POLICIES.....	40
6.8. ADD DIAL PATTERNS	42
6.9. ADD/VIEW SESSION MANAGER.....	45
7. CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	47
7.1. ACCESS MANAGEMENT INTERFACE	47
7.2. VERIFY NETWORK CONFIGURATION AND ENABLE INTERFACES	48
7.3. SIGNALING INTERFACE.....	51
7.4. MEDIA INTERFACE	52
7.5. SERVER INTERWORKING.....	53
7.5.1. Server Interworking: Session Manager.....	54
7.5.2. Server Interworking: CenturyLink	56
7.6. SERVER CONFIGURATION	58
7.6.1. Server Configuration: Session Manager.....	59
7.6.2. Server Configuration: CenturyLink.....	60
7.7. SIGNALING RULES	61
7.7.1. Signaling Rules: Session Manager.....	62
7.7.2. Signaling Rule: CenturyLink.....	65
7.8. MEDIA RULES	66
7.9. ENDPOINT POLICY GROUPS	67
7.9.1. Endpoint Policy Group: Session Manager.....	68
7.9.2. Endpoint Policy Group: CenturyLink	68
7.10. ROUTING	69
7.10.1. Routing: Session Manager	70

7.10.2. Routing: CenturyLink.....	71
7.11. TOPOLOGY HIDING.....	72
7.11.1. Topology Hiding: Session Manager.....	73
7.11.2. Topology Hiding: CenturyLink	74
7.12. END POINT FLOWS	75
7.12.1. End Point Flow: Session Manager.....	75
7.12.2. End Point Flow: CenturyLink	77
8. CENTURYLINK SIP TRUNKING CONFIGURATION	79
9. VERIFICATION AND TROUBLESHOOTING	79
10. CONCLUSION	81
11. REFERENCES	82

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunking (Sonus Platform) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager R6.3, Avaya Aura® Communication Manager R6.3, Avaya Session Border Controller for Enterprise (Avaya SBCE) R6.2 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with CenturyLink SIP Trunking service are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

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

A simulated enterprise site using Communication Manager, Session Manager and Avaya SBCE was connected to the public Internet using a broadband connection. The enterprise site was configured to connect to CenturyLink SIP Trunking service through the public IP network.

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to H.323 and SIP telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from H.323 and SIP telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from softphones. Two Avaya soft phones were used in testing: Avaya one-X® Communicator (1XC) and Avaya Flare® Experience for Windows. 1XC supports two work modes (Computer and Other Phone). Each supported mode was tested. 1XC also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. Both protocols were tested. Avaya Flare® Experience for Windows was used in testing as a simple SIP endpoint for basic inbound/outbound calls.
- SIP transport using UDP, TCP or TLS as supported.
- Direct IP-to-IP Media (also known as “Shuffling”) over a SIP Trunk. Direct IP-to-IP Media allows Communication Manager to reconfigure the RTP path after call establishment directly between the Avaya phones and the Avaya SBCE releasing media processing resources on the Avaya Media Gateway.

- Various call types including: local, long distance, inbound and outbound toll-free, international, Operator (0) and Operator-Assisted calls (0 + 10-digits), and local directory assistance (411).
- G.729A and G.711MU codecs.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail access and navigation using DTMF for inbound and outbound calls.
- Telephony supplementary features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call forwarding, transfer, conference and EC500 mobility (extension to cellular).
- Call Center scenarios.
- SIP REFER for call redirection and User-To-User Information (UII)
- T.38 faxing.
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones for calls to/from the PSTN via the CenturyLink SIP Trunking service.

Items not supported or not tested included the following:

- The emergency (911) call was not tested.

2.2. Test Results

Interoperability testing of CenturyLink SIP Trunking (Sonus Platform) was completed with successful results for all test cases with the exception of the observations/limitations noted below.

- **Transfer Inbound Calls To PSTN Using REFER** – Some scenarios of transferring inbound calls to the PSTN failed. The failures occurred with the following transfer scenarios:
 - Blind transfer of inbound call to the PSTN (termed as "Attended/Consultative Transfer with Early Completion" by CenturyLink) where the enterprise transfer initiator completes the transfer before the outbound call to the PSTN transfer destination is answered.
 - Consultative transfer of inbound call to the PSTN by the enterprise SIP hard phone where the enterprise transfer initiator completes the call transfer after the outbound call to the PSTN destination is answered.
 - Blind or consultative transfer of inbound call to the PSTN by the H.323 one-X® Communicator softphone.

In all the above transfer failures, CenturyLink sent a NOTIFY to the enterprise, after accepting the REFER message, indicating "481 Call Leg/Transaction Does Not Exist".

The above problem was reported to CenturyLink for investigation/resolution. CenturyLink advised that Attended/Consultative Transfer with Early Completion (1st transfer scenario above) is not yet supported on the SIP Trunking service (Sonus

Platform). Since transfer failures using REFER occurred with other transfer scenarios (2nd and 3rd scenarios above), it is recommended that use of REFER be turned off on Communication Manager (see **Section 5.7**) so that INVITE instead of REFER is used for call transfers until this problem is properly addressed (CenturyLink has opened a ticket with Sonus on this issue). In the compliance test, transfer of inbound calls to PSTN using INVITE was successfully verified.

- **SIP 1XC Conference with PSTN** – Using the Conference button on 1XC UI for conferencing existing PSTN call with another PSTN party might cause poor audio or audio loss. The safe operating procedure is to place the existing PSTN call on hold first, make a separate call to the PSTN, then connect the 2 calls into a conference.
- **Connected Party Display in PSTN Transfers** – After an existing call between a PSTN caller and an enterprise extension was transferred off-net to another PSTN party, the displayed connected party at both PSTN phones (the transferred party and the transfer-to party) showed the transferring party number (DID associated with the transferring extension) instead of the true connected-party number/ID. The true connected party information was conveyed by Communication Manager in SIP signaling messages (REFER, UPDATE) to the service provider, but this information was not used to update the true connected party number. The PSTN phone display is ultimately controlled by the PSTN carrier, thus this behavior is not necessarily indicative of a limitation of the CenturyLink SIP Trunking service. It is listed here simply as an observation.

2.3. Support

For technical support on CenturyLink SIP Trunk, contact CenturyLink using the Support link at <http://www.CenturyLink.com>

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to CenturyLink SIP Trunking through a public Internet WAN connection.

For security purposes, any actual public IP addresses used in the compliance test were changed to 192.168.x.x throughout these Application Notes where the 3rd and 4th octets were retained from the real addresses.

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

- Avaya S8800 Server running Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Session Manager
- Avaya S8800 Server running System Manager
- Avaya S8800 Server running voice messaging application (Avaya Aura® Messaging)
- Dell R210 V2 Server running Avaya SBCE
- Avaya 96x0-Series IP Telephones (H.323 and SIP)
- Avaya 96x1-Series IP Telephones (H.323 and SIP)
- Avaya 1600-Series IP Telephone (H.323)
- Avaya A175 Desktop Video Device a.k.a. Flare (used as a SIP voice endpoint)
- Avaya one-X® Communicator softphones (H.323 and SIP)
- Avaya Flare® Experience for Windows SIP softphone
- Windows HTTP server containing firmware for various Avaya IP phones to download

Located at the edge of the enterprise is the Avaya SBCE. It has a public interface that connects to the external network and a private interface that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through this enterprise SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The transport protocol between the enterprise SBC and CenturyLink across the public IP network is UDP; the transport protocol between the enterprise SBC and Session Manager across the enterprise IP network is TCP.

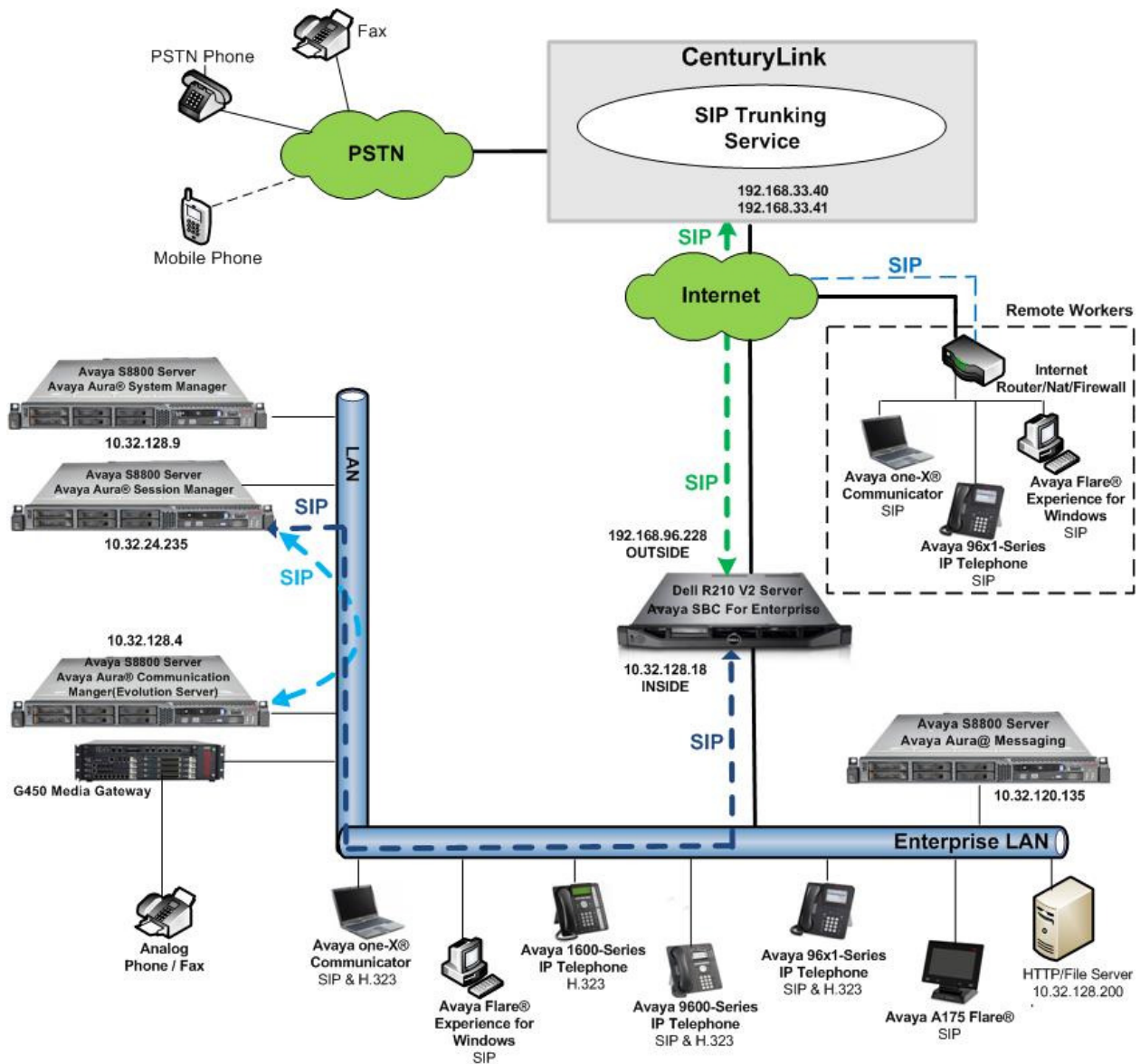


Figure 1: Avaya SIP Enterprise Solution Connecting To CenturyLink SIP Trunking

A separate trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec setting required by the service provider could be applied only to this specific trunk while not affecting other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

There are 2 SIP trunk groups from CenturyLink to the enterprise, therefore 2 access interfaces at CenturyLink SIP Trunking for the compliance test. CenturyLink SIP Trunking was configured to deliver TN (2-way DID numbers) calls to the enterprise from the interface at 192.168.33.40, and 8xx / RDID (1-way DID numbers) calls to the enterprise from the interface at 192.168.33.41. The enterprise was configured to send outbound calls to the CenturyLink SIP Trunking interface at 192.168.33.41.

Inbound calls flow from the service provider to Avaya SBCE then to Session Manager. Session Manager uses the configured Dial Patterns (or regular expressions) and Routing Policies to determine the recipient (in this case Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound feature treatment such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. Session Manager once again uses the configured Dial Patterns (or regular expressions) and Routing Policies to determine the route to Avaya SBCE. From the enterprise SBC, the call is sent to CenturyLink SIP Trunking through the public IP network.

The compliance test used Avaya Aura® Messaging for testing voice mail access/navigation and MWI (Messaging Wait Indicator) on Avaya enterprise phones. Other voice messaging applications such as Communication Manager Messaging could have been used to satisfy this test purpose.

The enterprise endpoints include both local extensions and Remote Worker phones that connect directly to the public Internet. The same Avaya SBCE was configured to connect to both the service provider network and Remote Worker using separate sets of public / private interfaces (**Figure 1** only shows the public / private interfaces used for connecting to the service provider network).

The administration of Avaya Aura® Messaging, Remote Worker via Avaya SBCE, and endpoints on Communication Manager and Session Manager are standard. Since these configuration tasks are not directly related to the inter-operation with CenturyLink SIP Trunking service, they are not included in these Application Notes.

4. Equipment and Software Validated

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	6.3 SP0 (R016x.03.0.124.0-20553)
Avaya G450 Media Gateway – ICC – ANA	31.20.0 /1 HW01 FW001 HW33 FW091
Avaya Aura® Session Manager running on Avaya S8800 Server	6.3 SP2 (6.3.2.0.632023)
Avaya Aura® System Manager running on Avaya S8800 Server	6.3.0 FP2 Build 6.3.0.8.5682-6.3.8.1627 Software Update Revision No: 6.3.2.4.1399
Avaya Aura® Messaging running on Avaya S8800 Server	6.2 SP2 Patch2 (MSG-02.0.823.0-19926)
Avaya Session Border Controller for Enterprise running on Dell R210 V2 Server	6.2.0.Q36
Avaya 9640 IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 2.6.10.1
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.2
Avaya 9611 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.2.4.08
Avaya 9621 IP Telephone (SIP)	Avaya one-X® Deskphone Edition 6.2.2
Avaya 1616 IP Telephone (H.323)	Avaya 1600 IP Deskphone Software Release 1.3 Maintenance Release 3
Avaya A175 Flare® Desktop Video Device (SIP telephone function)	Version 1.1.3 (SIP_A175_1_1_3_021913)
Avaya Flare® Experience for Windows	1.1 SP2 (1.1.2.11)
Avaya one-X Communicator (H.323 & SIP)	6.1.8.06-SP8-40314
Fax device	Ventafax Home Version 6.1.59.144
CenturyLink SIP Trunking Components	
Equipment/Software	Release/Version
CenturyLink iQ® SIP Trunk	7.3.7
Sonus NBS	7.3.7

The specific hardware and software listed in the table above were used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

5. Configure Avaya Aura® Communication Manager

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

The configuration of Communication Manager was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. After the completion of the configuration, perform a **save translation** command to make the changes permanent.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 4000 licenses are available and 60 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:		4000	36
Maximum Concurrently Registered IP Stations:		2400	10
Maximum Administered Remote Office Trunks:		4000	0
Maximum Concurrently Registered Remote Office Stations:		2400	0
Maximum Concurrently Registered IP eCons:		68	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		2400	0
Maximum Video Capable IP Softphones:		2400	2
Maximum Administered SIP Trunks:		4000	60
Maximum Administered Ad-hoc Video Conferencing Ports:		4000	0
Maximum Number of DS1 Boards with Echo Cancellation:		80	0
Maximum TN2501 VAL Boards:		10	0
Maximum Media Gateway VAL Sources:		50	0
Maximum TN2602 Boards with 80 VoIP Channels:		128	0
Maximum TN2602 Boards with 320 VoIP Channels:		128	0
Maximum Number of Expanded Meet-me Conference Ports:		300	0
(NOTE: You must logoff & login to effect the permission changes.)			

5.2. System Features

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

```
change system-parameters features                               Page 1 of 20
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? 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
```

On **Page 9** verify that a text string has been specified 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 **anonymous** for restricted and unavailable calls.

```
change system-parameters features                               Page 9 of 20
      FEATURE-RELATED SYSTEM PARAMETERS

      CPN/ANI/ICLID PARAMETERS
      CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
      CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

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

      INTERNATIONAL CALL ROUTING PARAMETERS
      Local Country Code:
      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 for Communication Manager (*procr*) and Session Manager (*sessionMgr*). These 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	10.32.128.18	
cmm	10.32.128.4	
default	0.0.0.0	
nwkSM	10.32.120.98	
procr	10.32.128.4	
procr6	::	
sessionMgr	10.32.24.235	

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.729A** and **G.711MU** in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

change ip-codec-set 2		Page 1 of 2
		IP Codec Set
Codec Set: 2		
Audio Codec	Silence Suppression	Frames Per Pkt Packet Size(ms)
1: G.729A	n	2 20
2: G.711MU	n	2 20
3:		

On **Page 2**, set the **Fax Mode** to *t.38-standard* since T.38 faxing is supported by CenturyLink SIP Trunking.

change ip-codec-set 2 Page 2 of 2

IP Codec Set

Allow Direct-IP Multimedia? n

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

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.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.com
Name: SP Region       Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 2          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048    IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS        RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5Keep-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
										G	A		t
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	c				
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	e			
1	2	y	NoLimit					n					t
2	2										all		
3													

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 5 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 that Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to *tcp*. The transport method specified here is used between Communication Manager and Session Manager. TCP was chosen for ease of tracing/debugging signaling between Communication Manager and Session Manager. In production environment, the default value of *tls* (Transport Layer Security) is recommended.
- 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 and for TCP the well-known port value is 5060). This is necessary for Session Manager to 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 **5068**.
- 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 a Session Manager.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *sessionMgr*. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- 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 SIP trunk and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completion.
- Set the **DTMF over IP** field to **rtp-payload**. This setting directs Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to **15**. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before canceling the call.
- Set **Initial IP-IP Direct Media** to **n**.
- Default values may be used for all other fields.

```

add signaling-group 5                                     Page 1 of 2
                                                    SIGNALING GROUP

Group Number: 5                      Group Type: sip
IMS Enabled? n                      Transport Method: tcp
  Q-SIP? n
  IP Video? n                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

Near-end Node Name: procr                      Far-end Node Name: sessionMgr
Near-end Listen Port: 5068                      Far-end Listen Port: 5068
                                                Far-end Network Region: 2
                                                Far-end Secondary Node Name:

Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate                      Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                      RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
Enable Layer 3 Test? y                      Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n                      Alternate Route Timer(sec): 15

```

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 5 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 dialplan in the **TAC** field.
- Set the **Service Type** field to *public-ntwrk*.
- Set **Member Assignment Method** to *auto*.
- Set the **Signaling Group** to the signaling group created 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.

```
add trunk-group 5                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 5                                     Group Type: sip          CDR Reports: y
  Group Name: A-SP-Trunk                          COR: 1                TN: 1          TAC: 1005
  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: 5
                                                    Number of Members: 10
```

On **Page 2**, set the **Redirect On OPTIM Failure** timer to the same amount of time as the **Alternate Route Timer** on the signaling group form in **Section 5.6**. Note that the **Redirect On OPTIM Failure** timer is defined in milliseconds. Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

```
add trunk-group 5                                     Page 2 of 21
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                                    Redirect On OPTIM Failure: 15000
SCCAN? n                                           Digital Loss Group: 18
  Preferred Minimum Session Refresh Interval(sec): 600
  XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

On **Page 3**, set the **Numbering Format** field to *private*. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. The compliance test used 10 digit numbering format. Thus, **Numbering Format** was set to **private** and the **Numbering Format** field in the route pattern was set to *unk-unk* (see **Section 5.9**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on enterprise endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if an enterprise user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

add trunk-group 5		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		
DSN Term? n	SIP ANAT Supported? n	

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs). It is used to authenticate the caller.

The screen below shows a subset of the DID numbers assigned for testing. These 5 numbers were mapped to the 5 enterprise extensions 40000, 41011, 41012, 41014 and 41016. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 5 extensions.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5	3			5	Total Administered: 31
5	4			5	Maximum Entries: 540
5	40000	5	3036157106	10	
5	41011	5	3036157105	10	
5	41012	5	3036157107	10	
5	41014	5	3036157104	10	
5	41016	5	3036157108	10	

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 4 will send the calling party number as the **Private Prefix** plus the extension number.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5	8			5	Total Administered: 10
5	4	5	51675	10	Maximum Entries: 540

5.9. 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	
1	4	dac							
3	5	ext							
4	5	ext							
5	5	ext							
8	1	fac							
9	1	fac							
*	3	fac							
#	3	fac							

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

change feature-access-codes			FEATURE ACCESS CODE (FAC)						Page 1 of 11
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:									
Answer Back Access Code:									
Attendant Access Code:									
Auto Alternate Routing (AAR) Access Code: 8									
Auto Route Selection (ARS) – Access Code 1: 9			Access Code 2:						
Automatic Callback Activation:			Deactivation:						
Call Forwarding Activation Busy/DA: *01 All: *02			Deactivation: *03						
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 55 which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0						Page 1 of 2	
ARS DIGIT ANALYSIS TABLE						Percent Full: 3	
Location: all							
	Dialed String	Total		Route	Call	Node	ANI
		Min	Max	Pattern	Type	Num	Reqd
	0	1	1	55	op		n
	0	8	8	deny	op		n
	0	11	11	55	op		n
	00	2	2	2	op		n
	01	9	17	deny	iop		n
	011	10	18	55	intl		n
	1732	11	11	55	fnpa		n
	1800	11	11	55	fnpa		n
	1877	11	11	55	fnpa		n
	1908	11	11	55	fnpa		n
	411	3	3	55	svcl		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 55 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **5** 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:** The Prefix Mark of **1** 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:** Enter **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 55												Page 1 of 3		
Pattern Number: 55												Pattern Name: A-SP Route		
SCCAN? n												Secure SIP? n		
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits					QSIG		
Dgts												Intw		
1:	5	0	1								n	user		
2:											n	user		
3:											n	user		
4:											n	user		
5:											n	user		
6:											n	user		
		BCC VALUE		TSC	CA-TSC		ITC BCIE		Service/Feature		PARM	No.	Numbering	LAR
		0	1	2	M	4	W			Request		Dgts	Format	
												Subaddress		
1:	y	y	y	y	y	n	n	rest				unk-unk	none	
2:	y	y	y	y	y	n	n	rest					none	
3:	y	y	y	y	y	n	n	rest					none	
4:	y	y	y	y	y	n	n	rest					none	
5:	y	y	y	y	y	n	n	rest					none	
6:	y	y	y	y	y	n	n	rest					none	

6. Configure Avaya Aura® Session Manager

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

- Specify SIP Domain
- Add logical/physical Location that can be occupied by SIP Entities at the enterprise site
- Add Adaptation module to perform dial plan manipulation
- Add SIP Entities corresponding to Communication Manager, Avaya SBCE and Session Manager
- Add Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Add Routing Policies, which define route destinations and control call routing between the SIP Entities
- Add Dial Patterns, which specify dialed digits and govern to which SIP Entity a call is routed
- Add/View Session Manager, corresponding to the Session Manager 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, SIP Entities, and Session Manager itself. However, each item should be reviewed to verify proper configuration.

6.1. System Manager Login and Navigation

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



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

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top header features the Avaya logo, the product name 'Avaya Aura® System Manager 6.3', and user information: 'Last Logged on at June 10, 2013 11:12 AM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. A breadcrumb trail shows 'Home / Elements / Routing'. On the left, a navigation tree is expanded to 'Routing', listing sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Introduction to Network Routing Policy' and includes a 'Help ?' link. The text explains that Network Routing Policy consists of several applications like 'Domains', 'Locations', 'SIP Entities', etc., and provides a recommended order for configuration. The steps are: Step 1: Create 'Domains' of type SIP; Step 2: Create 'Locations'; Step 3: Create 'Adaptations'; Step 4: Create 'SIP Entities' (with sub-points: SIP Entities used as 'Outbound Proxies', create all 'other SIP Entities', and assign appropriate 'Locations', 'Adaptations', and 'Outbound Proxies'); Step 5: Create the 'Entity Links' (with sub-points: Between Session Managers and Between Session Managers and 'other SIP Entities'); Step 6: Create 'Time Ranges' (with sub-point: Align with the tariff information received from the Service Providers).

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at June 10, 2013 11:12 AM
Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing

Routing

- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

Introduction to Network Routing Policy [Help ?](#)

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 6: Create "Time Ranges"
 - Align with the tariff information received from the Service Providers

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, this includes the enterprise domain (*avaya.com*). Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name that matches the **Authoritative Domain** setting in **Section 5.5**.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the enterprise domain.

The screenshot shows a web interface for 'Domain Management'. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains'. Below this, the title 'Domain Management' is displayed. To the right of the title are two buttons: 'Commit' and 'Cancel'. Below the title bar, there is a table with one item. The table has three columns: 'Name', 'Type', and 'Notes'. The 'Name' column contains the text '* avaya.com'. The 'Type' column contains a dropdown menu with 'sip' selected. The 'Notes' column contains the text 'Enterprise Domain'. Above the table, there is a text '1 Item | Refresh' and a link 'Filter: Enable'. Below the table, there are two buttons: 'Commit' and 'Cancel'.

Name	Type	Notes
* avaya.com	sip	Enterprise Domain

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for 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).

In the **Location Pattern** section (see 2nd screen below), click **Add** and enter the following values:

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

Displayed below are the top and bottom halves of the screen for addition of the *Location 1* Location, which includes all equipment on the enterprise network. Click **Commit** to save.

[Home](#) / [Elements](#) / [Routing](#) / [Locations](#)

[Help ?](#)

Location Details

Commit

Cancel

General

* **Name:**

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): Kbit/Sec

* Minimum Multimedia Bandwidth: Kbit/Sec

* Default Audio Bandwidth:

Alarm Threshold

Overall Alarm Threshold: %

Multimedia Alarm Threshold: %

* Latency before Overall Alarm Trigger: Minutes

* Latency before Multimedia Alarm Trigger: Minutes

Location Pattern

5 Items | Filter:

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.1.2.*	Trenton CM 5.2.1 Environment
<input type="checkbox"/>	* 10.32.120.*	AAM and other CPE devices
<input type="checkbox"/>	* 10.32.128.*	Princeton CM and other CPE devices
<input type="checkbox"/>	* 10.32.24.235	SM (devcon-asm)
<input type="checkbox"/>	* 192.168.49.*	CPE endpoints

Note that call bandwidth management parameters should be set per customer requirement.

Also note that the “10.1.2.*” entry in the Location Pattern table above was not used by the compliance test. This entry was configured for other test projects.

6.4. Add Adaptation Module

Session Manager can be configured with Adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic Adaptation module

DigitConversionAdapter supports digit conversion of telephone numbers in specific headers of SIP messages. Other Adaptation modules are built on this generic, and can modify other headers to permit interoperability with third party SIP products.

For interoperability with CenturyLink SIP Trunking, one Adaptation is needed. This Adaptation is applied to the Communication Manager SIP Entity and maps inbound DID numbers from CenturyLink to local Communication Manager extensions.

To create an Adaptation, navigate to **Routing → Adaptations** 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:

- **Adaptation Name:** Enter a descriptive name for the Adaptation.
- **Module Name:** Enter *DigitConversionAdapter*

To map inbound DID numbers from CenturyLink to Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DID to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields:

- **Matching Pattern:** Enter a digit string used to match the inbound DID number.
- **Min:** Enter a minimum dialed number length used in the match criteria.
- **Max:** Enter a maximum dialed number length used in the match criteria.
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number.
- **Insert Digits:** Enter the number of digits to insert at the beginning of the received number.
- **Address to modify:** Select *destination*.

Click **Commit** to save.

Adaptation Details

General

* Adaptation name:

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

0 Items | Refresh
Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

Digit Conversion for Outgoing Calls from SM

8 Items | Refresh
Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
<input type="checkbox"/>	* 3036157104	* 10	* 10		* 10	41014	destination	
<input type="checkbox"/>	* 3036157105	* 10	* 10		* 10	41011	destination	
<input type="checkbox"/>	* 3036157106	* 10	* 10		* 10	40000	destination	
<input type="checkbox"/>	* 3036157107	* 10	* 10		* 10	41012	destination	
<input type="checkbox"/>	* 3036157108	* 10	* 10		* 10	41016	destination	

In the example shown above, if a user on the PSTN dials 303-615-7107, Session Manager will convert the number to 41012 in the Request URI before sending out the SIP INVITE to Communication Manager. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the DID number to its corresponding extension. For an outbound call, the Communication Manager private-numbering table was configured with an entry to convert the calling number from 41012 to 3036157107 in the From and other appropriate headers of outbound INVITE sent on the trunk group to Session Manager (as shown in **Section 5.8**).

During compliance testing, the digit conversions (or number mappings) in Session Manager Adaptation were varied to route inbound calls to various destinations (including access number to Avaya Aura® Messaging and Communication Manager Vector Directory Numbers) for different test cases.

6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes Communication Manager and Avaya SBCE. Navigate to **Routing → SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select *Session Manager* for Session Manager, *CM* for Communication Manager and *SIP Trunk* for Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to *Session Manager*. If applicable, select the Adaptation name created in **Section 6.4** that will be applied to this entity.
- **Location:** Select the Location defined previously.
- **Time Zone:** Select the time zone for the Location above.

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

Home / Elements / Routing / SIP Entities

SIP Entity Details [Help ?](#)

General

* Name: devcon-asm

* FQDN or IP Address: 10.32.24.235

Type: Session Manager

Notes: Session Manager for SP testing

Location: Location 1

Outbound Proxy:

Time Zone: America/New_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Commit Cancel

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

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

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

Defaults can be used for the remaining fields. Click **Commit** to save.

The compliance test used 2 **Port** entries:

- **5060** with **TCP** for connecting to Avaya SBCE
- **5068** with **TCP** for connecting to Communication Manager

In addition, port 5060 with TCP was also used by a separate SIP Link between Session Manager and Communication Manager for Avaya SIP telephones and SIP soft clients. This SIP Link was part of the standard configuration on Session Manager and was not directly relevant to the interoperability with CenturyLink SIP Trunking.

Other entries defined (for other projects) as shown in the screen were not used.

Port

TCP Failover port:

TLS Failover port:

Add Remove

7 Items Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	
<input type="checkbox"/>	5060	UDP	avaya.com	
<input type="checkbox"/>	5061	TLS	avaya.com	
<input type="checkbox"/>	5062	TCP	avaya.com	
<input type="checkbox"/>	5066	TCP	avaya.com	
<input type="checkbox"/>	5068	TCP	avaya.com	
<input type="checkbox"/>	5080	TCP	avaya.com	

Select : All, None

The following screen shows the addition of the Communication Manager SIP Entity. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created at Session Manager installation for use with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of Communication Manager. For the **Adaptation** field, select the Adaptation module previously defined for digit manipulation in **Section 6.4**.

The screenshot shows a web interface for configuring a SIP Entity. The breadcrumb trail at the top is "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details". There are "Commit" and "Cancel" buttons in the top right corner, along with a "Help ?" link. The "General" section contains the following fields: "Name" (sp5-cm), "FQDN or IP Address" (10.32.128.4), "Type" (CM), "Notes" (Princeton CM w/ trunk grp 5), "Adaptation" (CTL CM-ES), "Location" (Location 1), "Time Zone" (America/New_York), "Override Port & Transport with DNS SRV" (unchecked), "SIP Timer B/F (in seconds)" (4), "Credential name" (empty), and "Call Detail Recording" (none). The "Loop Detection" section has a "Loop Detection Mode" (Off). The "SIP Link Monitoring" section has a "SIP Link Monitoring" dropdown set to "Use Session Manager Configuration".

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel Help ?

General

* Name: sp5-cm

* FQDN or IP Address: 10.32.128.4

Type: CM

Notes: Princeton CM w/ trunk grp 5

Adaptation: CTL CM-ES

Location: Location 1

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the SIP Entity for Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the SBC's inside network interface (see **Figure 1**).

The screenshot displays the 'SIP Entity Details' configuration page. At the top, a breadcrumb trail reads 'Home / Elements / Routing / SIP Entities'. In the top right corner, there is a 'Help ?' link and two buttons: 'Commit' and 'Cancel'. The main section is titled 'SIP Entity Details' and contains a 'General' sub-section. The fields in the 'General' section are: 'Name' (ASBCE), 'FQDN or IP Address' (10.32.128.18), 'Type' (SIP Trunk), 'Notes' (Avaya SBCE), 'Adaptation' (empty dropdown), 'Location' (Location 1), 'Time Zone' (America/New_York), 'Override Port & Transport with DNS SRV' (unchecked checkbox), 'SIP Timer B/F (in seconds)' (4), 'Credential name' (empty text field), and 'Call Detail Recording' (egress). Below the 'General' section is the 'Loop Detection' section with 'Loop Detection Mode' set to 'Off'. At the bottom is the 'SIP Link Monitoring' section with 'SIP Link Monitoring' set to 'Use Session Manager Configuration'. All dropdown menus have a small downward arrow icon.

Home / Elements / Routing / SIP Entities

Help ?

Commit Cancel

SIP Entity Details

General

* Name: ASBCE

* FQDN or IP Address: 10.32.128.18

Type: SIP Trunk

Notes: Avaya SBCE

Adaptation:

Location: Location 1

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.6. Add 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 for use only by service provider traffic and the other to Avaya SBCE. 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 SIP Entity.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other SIP Entity as defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Connection Policy:** Select **Trusted**. *Note: If this selection is not made , calls from the associated SIP Entity specified in **Section 6.5** will be denied.*

Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and Avaya SBCE. It should be noted that in a customer environment the Entity Link to Communication Manager would normally use TLS. TCP, as was set for the compliance test, can be used to aid in troubleshooting since the signaling traffic would not be encrypted. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.

Entity Link to Communication Manager:

Home / Elements / Routing / Entity Links

Entity Links Commit Cancel Help ?

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* devcon-asm_sp5-c...	* devcon-asm	TCP	* 5068	* sp5-cm	* 5068	trusted

Select : All, None

Commit Cancel

Entity Link to Avaya SBC for Enterprise:

Home / Elements / Routing / Entity Links

Entity Links Commit Cancel Help ?

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* devcon-asm_ASBCe...	* devcon-asm	TCP	* 5060	* ASBCE	* 5060	trusted

Select : All, None

Commit Cancel

Note that a separate Entity Link existed between Communication Manager and Session Manager using port 5060 and TCP (not shown). This separate Entity Link carries SIP traffic between Session Manager and Communication Manager that is not necessarily related to calls to and from the service provider, such as traffic related to SIP endpoints registered to Session Manager, or traffic related to messaging application, which has SIP integration to Session Manager.

6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two Routing Policies must be added: one for Communication Manager and the other for 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.

Routing Policy for Communication Manager:

Home / Elements / Routing / Routing Policies

Help ?

Routing Policy Details

Commit

Cancel

General

* Name:

sp5-cm-route

Disabled:

☐

* Retries:

0

Notes:

Inbound SP DID to sp5-cm

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
sp5-cm	10.32.128.4	CM	Princeton CM w/ trunk grp 5

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item Refresh

Filter: Enable

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

Select : All, None

Routing Policy for Avaya SBCE:

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

Routing Policy Details

General

*

Name:

Disabled: ☐

*

Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
ASBCE	10.32.128.18	SIP Trunk	Avaya SBCE

Time of Day

1 Item

Filter:

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

Select : All, None

6.8. Add 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 specify which Routing Policy (that defines the route destination) will be selected for a particular call based on the dialed digits, destination SIP 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 SIP Domain used in the match criteria.
- **Notes:** Add a brief description (optional).

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

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other Dial Patterns (e.g., 411 directory assistance call, 011 international call, etc.) were similarly defined.

The first example shows that 11-digit dialed numbers that begin with *1* and have a destination SIP Domain of *avaya.com* use the *ASBCE-route* Routing Policy as defined in **Section 6.7**.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		ASBCE-route		<input type="checkbox"/>	ASBCE	Outbound to ASBCE for SP testing

Select : All, None

Note that the compliance test did not restrict outbound calls to specific US area codes. In real deployments, appropriate restriction can be exercised (e.g., use Dial Pattern 1908, 1732, etc. with 11 digits) per customer business policies.

Also note that *-ALL-* was selected for Originating Location. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed outbound back to the PSTN. For straight-forward outbound calls, like 411 local directory call, the enterprise Location *Location 1* could have been selected.

The second example shows that inbound 10-digit numbers that start with **303615710** use Routing Policy **sp5-cm-route** as defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by CenturyLink.

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

Dial Pattern Details
Commit Cancel

General

* Pattern: 303615710
* Min: 10
* Max: 10
Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: avaya.com
Notes: CTL inbound DID numbers

Originating Locations and Routing Policies
Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		sp5-cm-route		<input type="checkbox"/>	sp5-cm	Inbound SP DID to sp5-cm

Select : All, None

6.9. Add/View 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 a Session Manager Element, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager Element already exists, select the Session Manager of interest then click **View** (not shown) to view or **Edit** (not shown) to edit 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 FQDN of the Session Manager or the IP address of the Session Manager management interface.

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

The screenshot shows the 'View Session Manager' configuration page. The breadcrumb navigation at the top reads 'Home / Elements / Session Manager / Session Manager Administration'. A 'Return' button is located in the top right corner. Below the breadcrumb is a navigation menu with links: 'General', 'Security Module', 'NIC Bonding', 'Monitoring', 'CDR', 'Personal Profile Manager (PPM)', 'Connection Settings', and 'Event Server'. The 'General' link is selected and highlighted. Below the navigation menu, the configuration fields are displayed: 'SIP Entity Name' with the value 'devcon-asm', 'Description' (empty), 'Management Access Point Host Name/IP' with the value '10.32.24.233', 'Direct Routing to Endpoints' with a value of 'Enable', and 'VMware Virtual Machine' with an unchecked checkbox.

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	devcon-asm
Description	
Management Access Point Host Name/IP	10.32.24.233
Direct Routing to Endpoints	Enable
VMware Virtual Machine	<input type="checkbox"/>

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 Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

In the **Monitoring** section, enter a desired value for **Proactive cycle time (secs)** which determines the interval at which Session Manager sends out OPTIONS messages to the connected SIP Entities for checking reachability.

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

Security Module

SIP Entity IP Address10.32.24.235

Network Mask255.255.255.0

Default Gateway10.32.24.1

Call Control PHB46

QOS Priority6

Speed & DuplexAuto

VLAN ID

NIC Bonding

Enable Bonding☐

Driver Monitoring ModeARP

ARP Interval (msecs)100

ARP Target IP

ARP Target IP

ARP Target IP

Monitoring

Enable Monitoring☒

Proactive cycle time (secs)120

Reactive cycle time (secs)120

Number of Retries1

7. Configure Avaya Session Border Controller for Enterprise

Starting with Release 6.2, the Avaya SBCE supports both SIP Trunking to/from the service provider and Remote Worker. This section describes the configuration for SIP Trunking. Remote Worker configuration, not directly related to interoperability with the service provider, is not included. For Remote Worker configuration on Avaya SBCE, refer to the product documentation for the Avaya SBCE in **Section 11**. Note that Standard and Advanced Session Licenses are required for Remote Worker. Contact an authorized Avaya representative for assistance if additional licensing is required.

In the sample configuration, an Avaya SBCE is used as the CPE edge device between the Avaya enterprise site and CenturyLink SIP Trunking service.

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

7.1. Access Management Interface

Use a WEB browser to access the web management interface of Avaya SBCE by entering URL `https://<ip-addr>`, where `<ip-addr>` is the management LAN IP address assigned during installation. Log in as “ucsec” using proper login credentials.



The screenshot shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, under the heading "Log In", there are input fields for "Username:" and "Password:". Below these fields is a "Log In" button. A disclaimer text is present, stating that the system is restricted to authorized users and that unauthorized access is prohibited. It also mentions that system use may be monitored and recorded for administrative and security reasons. At the bottom, there is a copyright notice: "© 2011 - 2013 Avaya Inc. All rights reserved."

Once logged in, a Dashboard screen will be presented. The following image illustrates the menu items available on the left-side of the Dashboard screen.

7.2. Verify Network Configuration and Enable Interfaces

To view the network information provided during installation, navigate to **System Management**. In the right pane, click the **View** link for the Avaya SBCE device on the right.

A System Information page will appear showing the information provided during installation. In the **Appliance Name** field is the name of the device (**sp-ucsec1**). This name will be referenced in other configuration screens. The highlighted Interfaces **A1** and **B1** represent the private and public interfaces of the Avaya SBCE for SIP Trunking. Each of these interfaces must be enabled after installation. Note that the Management IP is in a different sub-net than the A1 private interface, as required by Avaya SBCE.

The other Interface entries in Network Configuration were configured for Remote Worker.

System Information: sp-ucsec1 X

General Configuration

Appliance Name	sp-ucsec1
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.32.128.18	10.32.128.18	255.255.255.0	10.32.128.254	A1
192.168.96.228	192.168.96.228	255.255.255.224	192.168.96.254	B1
192.168.96.228	192.168.96.228	255.255.255.224	192.168.96.254	B1
192.168.96.228	192.168.96.228	255.255.255.224	192.168.96.254	B1
10.32.128.19	10.32.128.19	255.255.255.0	10.32.128.254	A1

DNS Configuration

Primary DNS	10.32.128.200
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.32.128.18

Management IP(s)

IP	10.32.101.10
----	--------------

To enable the interfaces, first navigate to **Device Specific Settings** → **Network Management** in the left pane and select the device being managed in the center pane. The right pane will show the same **A1** and **B1** interfaces displayed in the previous screen. Click on the **Interface Configuration** tab.

Network Management: sp-ucsec1

Devices: **sp-ucsec1**

Interface Configuration

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

A1 Netmask: 255.255.255.0 A2 Netmask: B1 Netmask: 255.255.255.224 B2 Netmask:

Add Save Clear

IP Address	Public IP	Gateway	Interface	
10.32.128.18		10.32.128.254	A1	Delete
192.168.96.228		192.168.96.254	B1	Delete
		192.168.96.254	B1	Delete
		192.168.96.254	B1	Delete
10.32.128.19		10.32.128.254	A1	Delete

In the **Interface Configuration** tab, verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click the **Toggle State** button to enable the interface.

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

7.3. Signaling Interface

A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create separate signaling interfaces for the internal and external sides of the Avaya SBCE.

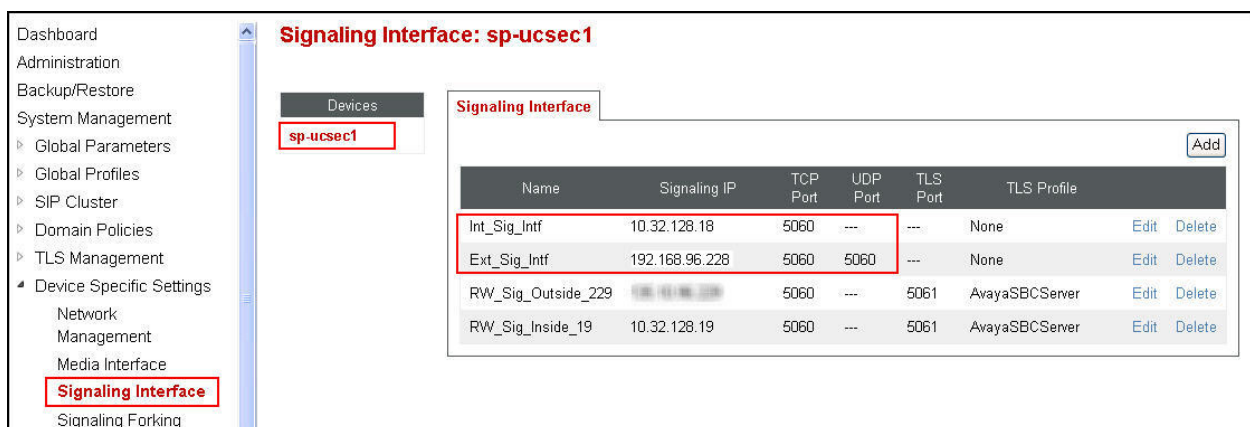
To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device to be managed (**sp-ucsec1**) and click the **Add** button in the right pane. A pop-up window (not shown) will appear requesting the name of the new interface, followed by a series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the right pane.

For the compliance test, the signaling interface **Int_Sig_Intf** was created for the Avaya SBCE internal interface for SIP Trunking. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Signaling IP** to the IP address associated with the private interface (A1) as shown in **Section 7.2**.
- Set **TCP port** to the port the Avaya SBCE will listen on for SIP requests from Session Manager.

The signaling interface **Ext_Sig_Intf** was created for the Avaya SBCE external interface for SIP Trunking. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Signaling IP** to the IP address associated with the public interface (B1) as shown in **Section 7.2**.
- Set **UDP port** to the port the Avaya SBCE will listen on for SIP requests from the service provider.



The screenshot shows the configuration page for the signaling interface of device **sp-ucsec1**. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. Under Device Specific Settings, the **Signaling Interface** option is selected. The main content area is titled **Signaling Interface: sp-ucsec1** and contains a table of configured interfaces. The table has columns for Name, Signaling IP, TCP Port, UDP Port, TLS Port, and TLS Profile. Two interfaces are listed: **Int_Sig_Intf** and **Ext_Sig_Intf**, both with a Signaling IP of 10.32.128.18 and 192.168.96.228 respectively, and a TCP Port of 5060. The **Ext_Sig_Intf** interface also has a UDP Port of 5060. Both interfaces have a TLS Port of 5061 and a TLS Profile of AvayaSBCServer. The **Int_Sig_Intf** interface has a TLS Profile of None. The **Ext_Sig_Intf** interface has a TLS Profile of None. The table also includes Edit and Delete links for each interface.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Int_Sig_Intf	10.32.128.18	5060	---	---	None	Edit	Delete
Ext_Sig_Intf	192.168.96.228	5060	5060	---	None	Edit	Delete
RW_Sig_Outside_229	10.32.128.19	5060	---	5061	AvayaSBCServer	Edit	Delete
RW_Sig_Inside_19	10.32.128.19	5060	---	5061	AvayaSBCServer	Edit	Delete

The other configuration entries shown in the screen are for Remote Worker.

7.4. Media Interface

A media interface defines an IP address and port range for transmitting media. Create separate media interfaces for the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Media Interface** in the left pane. In the center pane, select the Avaya SBCE device to be managed (**sp-ucsec1**). In the right pane, click the **Add** button. A pop-up window (not shown) will appear requesting the name of the new interface, followed by a series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the right pane.

For the compliance test, the media interface **Int_Media_Intf** was created for the Avaya SBCE internal interface for SIP Trunking. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Media IP** to the IP address associated with the private interface (A1) as shown in **Section 7.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and Session Manager. For the compliance test, the port range used was selected arbitrarily.

The media interface **Ext_Media_Intf** was created for the Avaya SBCE external interface for SIP Trunking. When configuring the interface, configure the parameters as follows:

- Set **Name** to a descriptive name.
- Set the **Media IP** to the IP address associated with the public interface (B1) as shown in **Section 7.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the service provider. For the compliance test, the port range used was selected arbitrarily.

The screenshot displays the Avaya SBCE configuration interface. On the left is a navigation pane with categories like Dashboard, Administration, System Management, and Device Specific Settings. Under Device Specific Settings, 'Media Interface' is selected. The main area is titled 'Media Interface: sp-ucsec1'. It features a 'Media Interface' tab and a table listing configured interfaces. A red box highlights the 'Int_Media_Intf' and 'Ext_Media_Intf' entries in the table. Above the table, a warning message states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' An 'Add' button is located to the right of the warning.

Name	Media IP	Port Range	Edit	Delete
Int_Media_Intf	10.32.128.18	35000 - 40000	Edit	Delete
Ext_Media_Intf	192.168.96.228	35000 - 40000	Edit	Delete
RW_Med_Outside_229		35000 - 40000	Edit	Delete
RW_Med_Inside_19	10.32.128.19	35000 - 40000	Edit	Delete

The other configuration entries shown in the screen are for Remote Worker.

7.5. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create a server interworking profile for Session Manager and a server interworking profile for the service provider SIP server. These profiles will be applied to the appropriate servers in **Section 7.6.1** and **7.6.2**.

To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, click **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the right pane. Alternatively, a new server interworking profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected server interworking profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screenshot displays the 'Interworking Profiles: Avaya-SM' configuration page. On the left is a navigation tree with categories like Dashboard, Administration, and System Management, with 'Global Profiles' expanded to show 'Server Interworking'. The center pane lists existing profiles: cs2100, avaya-ru, OCS-Edge-Ser..., cisco-ccm, cups, Sipera-Halo, OCS-FrontEnd..., **Avaya-SM** (selected), SP-General, CM, and default. An 'Add' button is at the top. The right pane shows the configuration for the selected 'Avaya-SM' profile, with tabs for General, Timers, URI Manipulation, Header Manipulation, and Advanced. The 'General' tab is active, showing a table of parameters.

General	
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No

7.5.1. Server Interworking: Session Manager

For the compliance test, a server interworking profile **Avaya-SM** was created for Session Manager. Shown below are the **General** and the **Advanced** tabs of the **Avaya-SM** server interworking profile. The parameters in all other tabs may retain default settings.

The **General** tab:

General	Timers	URI Manipulation	Header Manipulation	Advanced
General				
Hold Support	RFC2543			
180 Handling	None			
181 Handling	None			
182 Handling	None			
183 Handling	None			
Refer Handling	No			
3xx Handling	No			
Diversion Header Support	No			
Delayed SDP Handling	No			
T.38 Support	Yes			
URI Scheme	SIP			
Via Header Format	RFC3261			
Privacy				
Privacy Enabled	No			
User Name				
P-Asserted-Identity	No			
P-Preferred-Identity	No			
Privacy Header				
DTMF				
DTMF Support	None			
Edit				

The **Advanced** tab:

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

7.5.2. Server Interworking: CenturyLink

For the compliance test, the server interworking profile **SP-General** was similarly created for the CenturyLink SIP server. The **General** and **Advanced** tabs for this server interworking profile are shown below. The parameters in all other tabs may retain default settings.

The **General** tab:

General	Timers	URI Manipulation	Header Manipulation	Advanced
General				
Hold Support	NONE			
180 Handling	None			
181 Handling	None			
182 Handling	None			
183 Handling	None			
Refer Handling	No			
3xx Handling	No			
Diversion Header Support	No			
Delayed SDP Handling	No			
T.38 Support	Yes			
URI Scheme	SIP			
Via Header Format	RFC3261			
Privacy				
Privacy Enabled	No			
User Name				
P-Asserted-Identity	No			
P-Preferred-Identity	No			
Privacy Header				
DTMF				
DTMF Support	None			
Edit				

The **Advanced** tab:

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

7.6. Server Configuration

A server configuration profile defines the attributes of the physical server. Create a call server configuration profile for Session Manager and a trunk server configuration profile for the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Server Configuration** in the left pane. In the center pane, click **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the right pane. Alternatively, a new server profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected server profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screenshot displays the Avaya Server Configuration web interface. On the left, a navigation pane shows a tree structure with 'Server Configuration' highlighted. The main area is titled 'Server Configuration: Avaya-SM' and features an 'Add' button. Below this is a list of server profiles, with 'Avaya-SM' selected. To the right, the configuration details for the selected profile are shown in a tabbed format. The 'General' tab is active, displaying a table with the following information:

Property	Value
Server Type	Call Server
IP Addresses / FQDNs	10.32.24.235
Supported Transports	TCP
TCP Port	5060

Below the table is an 'Edit' button. At the top right of the configuration area, there are buttons for 'Rename', 'Clone', and 'Delete'.

7.6.1. Server Configuration: Session Manager

For the compliance test, the server configuration profile **Avaya-SM** was created for Session Manager. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to *Call Server*.
- Set **IP Addresses / FQDNs** to the IP address of the Session Manager signaling interface.
- Set **Supported Transports** to the transport protocol used for SIP signaling between Session Manager and the Avaya SBCE.
- Set **TCP Port** to the port Session Manager will listen on for SIP requests from the Avaya SBCE.

General	Authentication	Heartbeat	Advanced
Server Type			
		Call Server	
IP Addresses / FQDNs			
		10.32.24.235	
Supported Transports			
		TCP	
TCP Port			
		5060	
<div>Edit</div>			

On the **Advanced** tab, set **Interworking Profile** to the interworking profile for Session Manager defined in **Section 7.5.1**.

General	Authentication	Heartbeat	Advanced
Enable DoS Protection			
		<input type="checkbox"/>	
Enable Grooming			
		<input type="checkbox"/>	
Interworking Profile			
		Avaya-SM	
Signaling Manipulation Script			
		None	
TCP Connection Type			
		SUBID	
<div>Edit</div>			

7.6.2. Server Configuration: CenturyLink

For the compliance test, the server configuration profile **SP-CLink** was created for the service provider SIP server. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to *Trunk Server*.
- Set **IP Addresses / FQDNs** to the IP addresses of the 2 CenturyLink SIP Trunking access interfaces, separated by comma.
- Set **Supported Transports** to the transport protocol used for SIP signaling between CenturyLink and the Avaya SBCE.
- Set **UDP Port** to the port CenturyLink will listen on for SIP requests from the Avaya SBCE.

General	Authentication	Heartbeat	Advanced
Server Type			
Trunk Server			
IP Addresses / FQDNs			
67.148.33.40, 67.148.33.41			
Supported Transports			
UDP			
UDP Port			
5060			
Edit			

On the **Advanced** tab, set **Interworking Profile** to the interworking profile for CenturyLink defined in **Section 7.5.2**.

General	Authentication	Heartbeat	Advanced
Enable DoS Protection			
<input type="checkbox"/>			
Enable Grooming			
<input type="checkbox"/>			
Interworking Profile			
SP-General			
Signaling Manipulation Script			
None			
UDP Connection Type			
SUBID			
Edit			

7.7. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 7.9**.

To create a new signaling rule, navigate to **Domain Policies** → **Signaling Rules** in the left pane. In the center pane, click **Add**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by a series of pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the right pane. Alternatively, a new rule may be created by selecting an existing rule in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected rule which can then be edited as needed. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane.

Signaling Rules: SessMgr_SigRules

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

Click here to add a description.

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

Inbound

Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound

Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy

7.7.1. Signaling Rules: Session Manager

The proprietary AV-Correlation-ID and Endpoint-View headers are sent in various SIP messages from Session Manager. These headers contain the enterprise private network IP addresses and therefore should not be exposed external to the enterprise. For simplicity, these headers were simply removed (blocked) from both request and response messages originated from Session Manager.

Navigate to **Domain Policies** → **Signaling Rules** to configure Signaling Rules.

Click the **Add** button (not shown) to add a new signaling rule. In the **Rule Name** field, enter an appropriate name, such as *SessMgr_SigRules*.

A screenshot of a web-based configuration window titled "Signaling Rule" with a close button (X) in the top right corner. The window contains a text input field labeled "Rule Name" with the text "SessMgr_SigRules" entered. Below the input field is a button labeled "Next".

In the subsequent screen (not shown), click **Next** to accept defaults. In the Signaling QoS screen, click **Finish** (not shown).

After this configuration, the new “SessMgr_SigRules” rule will appear as follows in its **General** tab:

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS
Inbound					
Requests	Allow				
Non-2XX Final Responses	Allow				
Optional Request Headers	Allow				
Optional Response Headers	Allow				
Outbound					
Requests	Allow				
Non-2XX Final Responses	Allow				
Optional Request Headers	Allow				
Optional Response Headers	Allow				
Content-Type Policy					
Enable Content-Type Checks	<input checked="" type="checkbox"/>				
Action	Allow	Multipart Action		Allow	
Exception List	Exception List				
<input type="button" value="Edit"/>					

Select the **Request Headers** tab, and select the **Add In Header Control** button (not shown). In the displayed Add Header Control window, check the **Proprietary Request Header** checkbox. In the **Header Name** field, type *Endpoint-View*. Select *ALL* as the **Method Name**. For **Header Criteria**, select *Forbidden*. Retain the *Remove header* selection for **Presence Action**. The intent is to remove the Endpoint-View header which is inserted by Session Manager, but not needed by CenturyLink SIP Trunking service.

Similarly, configure an additional header control rule to remove the AV-Correlation-ID header in the inbound INVITE (coming from Session Manager).

Once complete, the **Request Headers** tab appears as follows.

General Requests Responses Request Headers Response Headers Signaling QoS								
<div>Add In Header Control Add Out Header Control</div>								
Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Correlation-ID	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Select the **Response Headers** tab and repeat the above configuration steps to

- Remove the Endpoint-View header in the 2XX response to ALL methods
- Remove the Endpoint-View header in the 1XX response to the INVITE method

Once configuration is completed, the **Response Headers** tab for the “SessMgr_SigRules” signaling rule appears as follows.

GeneralRequestsResponsesRequest HeadersResponse HeadersSignaling QoS									
Add In Header ControlAdd Out Header Control									
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete

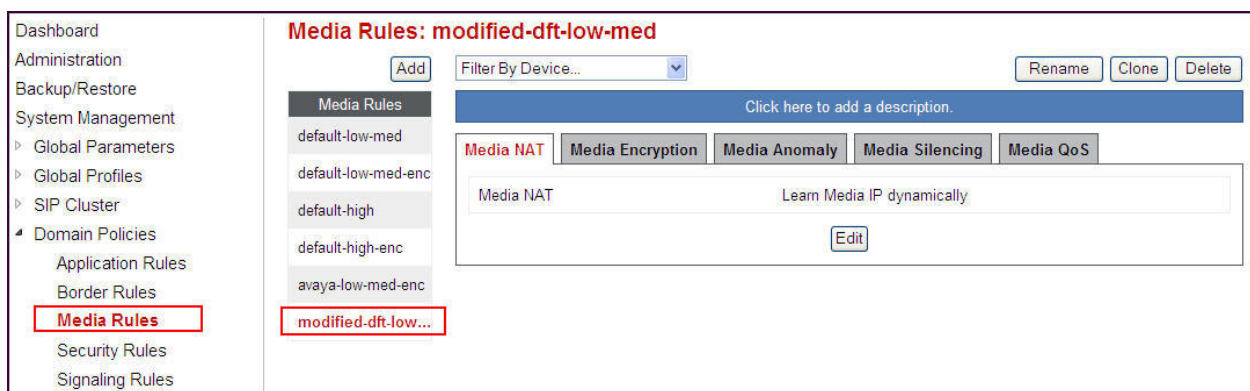
7.7.2. Signaling Rule: CenturyLink

The compliance test did not require creation of a new signaling rule specifically for CenturyLink.

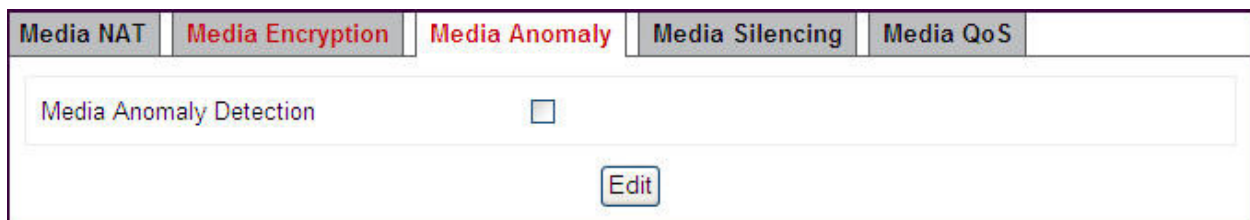
7.8. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 7.9**.

To create a new rule, navigate to **Domain Policies** → **Media Rules** in the left pane. In the center pane, click **Add**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by a series of pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the right pane. Alternatively, a new rule may be created by selecting an existing rule in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected rule which can then be edited as needed. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane.



For the compliance test, a single media rule **modified-dft-low-med** was created that was applied to both the Session Manager and the CenturyLink SIP servers. It was created by cloning the existing rule **default-low-med** which uses unencrypted media and then disabling **Media Anomaly Detection** on the Media Anomaly tab as shown below. This was done to prevent some false media errors from impacting the RTP media stream.



7.9. Endpoint Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, separate endpoint policy groups must be created for Session Manager and the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.12**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, click **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by a series of pop-up windows in which the group parameters can be configured. Once complete, the settings are shown in the right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane.

Policy Groups: SM

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- SM**
- Frontier
- General-SP
- SM-1

Policy Group

Order	Application	Border	Media	Security	Signaling	Time of Day
1	default	default	modified-dft-low-med	default-low	SessMgr_SigRules	default

For the compliance test, the endpoint policy group **SM** was created for Session Manager. Default values were used for each of the rules which comprise the group with the exception of **Media** and **Signaling**. For **Media**, select the media rule created in **Section 7.8**; for **Signaling**, select the signaling rule created in **Section 7.7**.

7.9.2. Endpoint Policy Group: CenturyLink

For the compliance test, the endpoint policy group **General-SP** was created for the CenturyLink SIP server. Default values were used for each of the rules which comprise the group with the exception of **Media**. For **Media**, select the media rule created in **Section 7.8**.

ACM; Reviewed:
SPOC 9/6/2013

7.10. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only after the traffic has matched an end point flow defined in **Section 7.12**. Create separate routing profiles for Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Routing** in the left pane. In the center pane, click **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the right pane. Alternatively, a new routing profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screenshot displays the Avaya Session Manager configuration interface. On the left is a navigation pane with the following menu items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, **Routing** (highlighted), Server Configuration, Topology Hiding, Signaling Manipulation, and URI Groups. The main content area is titled "Routing Profiles: To_SM" and includes an "Add" button at the top left and "Rename", "Clone", and "Delete" buttons at the top right. Below the title is a list of routing profiles: "default", "To_SM" (selected and highlighted in red), "To_Trunks", "To_WebCM", "To_Pstn", "To_Pstn2", "To_Pstn3", "To_Pstn4", "To_Pstn5", "To_Pstn6", and "default_Pstn". The right pane shows the configuration for the selected "To_SM" profile. It has a description field with the placeholder text "Click here to add a description." and an "Add" button. Below this is a table with the following columns: "Priority", "URI Group", "Next Hop Server 1", and "Next Hop Server 2". The table contains one row with the following values: "1" in the Priority column, "*" in the URI Group column, "10.32.24.235" in the Next Hop Server 1 column, and "---" in the Next Hop Server 2 column. At the bottom right of the table are "View" and "Edit" links.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	10.32.24.235	---

7.10.1. Routing: Session Manager

For the compliance test, the routing profile **To_SM** was created for Session Manager. When creating the profile, configure the parameters as follows:

- Set **URI Group** to the wild card * to match on any URI.
- Set **Next Hop Server 1** field to the IP address of the Session Manager signaling interface.
- Enable **Routing Priority based on Next Hop Priority**.
- Set **Outgoing Transport** to **TCP**.

Next Hop Routing

URI Group: *

Next Hop Server 1: 10.32.24.235

Next Hop Server 2:

Routing Priority based on Next Hop Server: ☒

Use Next Hop for In Dialog Messages: ☐

Ignore Route Header for Messages Outside Dialog: ☐

NAPTR: ☐

SRV: ☐

Outgoing Transport: ☐ TLS ☒ TCP ☐ UDP

Finish

Once complete, the **To_SM** routing profile appears as follows:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	10.32.24.235	---	View Edit

Add

7.10.2. Routing: CenturyLink

For the compliance test, the routing profile **To_Trunks** was created for CenturyLink. When creating the profile, configure the parameters as follows:

- Set **URI Group** to the wild card * to match on any URI.
- Set **Next Hop Server 1** field to the IP address of the CenturyLink SIP Trunking interface for receiving calls from the enterprise.
- Enable **Routing Priority based on Next Hop Priority**.
- Set **Outgoing Transport** field to **UDP**.

Next Hop Routing

URI Group: *

Next Hop Server 1: 192.168.33.41

Next Hop Server 2:

Routing Priority based on Next Hop Server: ☒

Use Next Hop for In Dialog Messages: ☐

Ignore Route Header for Messages Outside Dialog: ☐

NAPTR: ☐

SRV: ☐

Outgoing Transport: ☐ TLS ☐ TCP ☒ UDP

Finish

Once complete, the **To_Trunks** routing profile appears as follows:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	192.168.33.41	

View Edit

Add

7.11. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 7.12**.

To create a new profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, click **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a pop-up window in which a header can be selected and configured. Additional headers can be added in this window. Alternatively, a new topology hiding profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed. Once complete, the settings are shown in the right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

Topology Hiding Profiles: PRT-Domain

Buttons: Add, Rename, Clone, Delete

Click here to add a description.

Topology Hiding

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

Edit

7.11.1. Topology Hiding: Session Manager

For the compliance test, the topology hiding profile **PRT-Domain** was created for Session Manager. This profile was applied to traffic from the Avaya SBCE to Session Manager. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line**, **From** and **To** which should be set to **Overwrite**.
- For those headers to be overwritten, the **Overwrite Value** is set to the enterprise domain (**avaya.com**).

Topology Hiding			
Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	avaya.com
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	avaya.com
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	avaya.com
SDP	IP/Domain	Auto	---
<div>Edit</div>			

7.11.2. Topology Hiding: CenturyLink

For the compliance test, the topology hiding profile **SP-CLink** was created for CenturyLink. This profile was applied to traffic from the Avaya SBCE to the service provider network. When creating the profile, configure the parameters as follows:

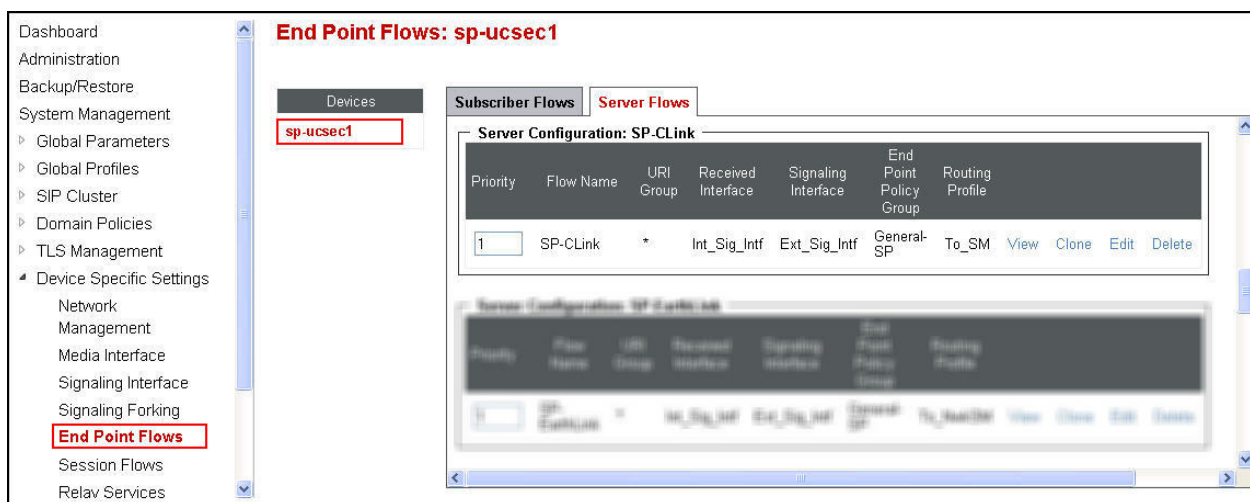
- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line** and **To** which should be set to **Overwrite**.
- For those headers to be overwritten, the **Overwrite Value** is set to the CenturyLink SIP Trunking access interface IP address (**192.168.33.41**) for receiving calls from the enterprise.

Topology Hiding			
Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	192.168.33.41
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	192.168.33.41
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
<div>Edit</div>			

7.12. End Point Flows

Endpoint flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at the 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 policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source end point flow and the destination end point flow. In the case of SIP trunking, the signaling endpoints are Session Manager and the service provider SIP server.

To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select the **Server Flows** tab and click the **Add** button in the upper portion of the screen (not shown). A pop-up window (not shown) will appear requesting the name of the new flow and the flow parameters. Once complete, the settings are shown in the right pane.



7.12.1. End Point Flow: Session Manager

For the compliance test, the end point flow **Avaya-SM** was created for Session Manager. All traffic from Session Manager will match this flow as the source flow and use the specified **Routing Profile** “To_Trunks” to determine the destination server and corresponding destination flow. The **End Point Policy Group** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Session Manager server created in **Section 7.6.1**.
- To match all traffic, set **URI Group**, **Transport** and **Remote Subnet** to *.
- Set **Received Interface** to the external signaling interface specified in **Section 7.3**.
- Set **Signaling Interface** to the internal signaling interface specified in **Section 7.3**.
- Set **Media Interface** to the internal media interface specified in **Section 7.4**.
- Set **End Point Policy Group** to the end point policy group defined for Session Manager in **Section 7.9.1**.
- Set **Routing Profile** to the routing profile defined in **Section 7.10.2** used to direct traffic to the CenturyLink SIP server.
- Set **Topology Hiding Profile** to the topology hiding profile defined for Session Manager in **Section 7.11.1**.

Edit Flow: Avaya-SM
X

Flow Name	<input style="width: 90%;" type="text" value="Avaya-SM"/>
Server Configuration	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">Avaya-SM ▼</div>
URI Group	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">* ▼</div>
Transport	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">* ▼</div>
Remote Subnet	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">* ▼</div>
Received Interface	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">Ext_Sig_Intf ▼</div>
Signaling Interface	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">Int_Sig_Intf ▼</div>
Media Interface	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">Int_Media_Intf ▼</div>
End Point Policy Group	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">SM ▼</div>
Routing Profile	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">To_Trunks ▼</div>
Topology Hiding Profile	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">PRT-Domain ▼</div>
File Transfer Profile	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">None ▼</div>

Finish

Once complete, the **Avaya-SM** end point flow appears as the highlighted entry in the screen below. The other flow entry was configured for Remote Worker.

Server Configuration: Avaya-SM						
<input type="button" value="Update"/>						
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	RW-Avaya-SM	*	RW_Sig_Outside_229	RW_Sig_Inside_19	Remote_User	default
2	Avaya-SM	*	Ext_Sig_Intf	Int_Sig_Intf	SM	To_Trunks

7.12.2. End Point Flow: CenturyLink

For the compliance test, the end point flow **SP-CLink** was created for the CenturyLink SIP server. All traffic from CenturyLink will match this flow as the source flow and use the specified **Routing Profile** “To_PrtSM” to determine the destination server and corresponding destination flow. The **End Point Policy Group** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For the **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the CenturyLink SIP server created in **Section 7.6.2**.
- To match all traffic, set **URI Group**, **Transport** and **Remote Subnet** to *.
- Set **Received Interface** to the internal signaling interface specified in **Section 7.3**.
- Set **Signaling Interface** to the external signaling interface specified in **Section 7.3**.
- Set **Media Interface** to the external media interface specified in **Section 7.4**.
- Set **End Point Policy Group** to the end point policy group defined for CenturyLink in **Section 7.9.2**.
- Set **Routing Profile** to the routing profile defined in **Section 7.10.1** used to direct traffic to Session Manager.
- Set **Topology Hiding Profile** to the topology hiding profile defined for CenturyLink in **Section 7.11.2**.

Edit Flow: SP-CLink
X

Flow Name	<input type="text" value="SP-CLink"/>
Server Configuration	<input type="text" value="SP-CLink"/> ▼
URI Group	<input type="text" value="*"/> ▼
Transport	<input type="text" value="*"/> ▼
Remote Subnet	<input type="text" value="*"/>
Received Interface	<input type="text" value="Int_Sig_Intf"/> ▼
Signaling Interface	<input type="text" value="Ext_Sig_Intf"/> ▼
Media Interface	<input type="text" value="Ext_Media_Intf"/> ▼
End Point Policy Group	<input type="text" value="General-SP"/> ▼
Routing Profile	<input type="text" value="To_SM"/> ▼
Topology Hiding Profile	<input type="text" value="SP-CLink"/> ▼
File Transfer Profile	<input type="text" value="None"/> ▼

Once complete, the **SP-CLink** end point flow appears as follows.

Server Configuration: SP-CLink										
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
<input type="text" value="1"/>	SP-CLink	*	Int_Sig_Intf	Ext_Sig_Intf	General-SP	To_SM	View	Clone	Edit	Delete

8. CenturyLink SIP Trunking Configuration

To use CenturyLink SIP Trunking, a customer must request the service from CenturyLink using the established sales and provisioning processes. The process can be started by contacting CenturyLink and requesting information via the online sales links or telephone numbers.

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

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

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

9. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands 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 with 2-way audio path.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active with 2-way audio path.
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.

Troubleshooting:

1. Communication Manager:
 - **list trace station** <extension number> - Traces calls to and from a specific station.
 - **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.

- **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
- **status trunk** <trunk group number> - Displays trunk group information.
- **status trunk** <trunk group number/channel number> - Displays signaling and media information for an active trunk channel.

2. Session Manager:

- **System State** – At System Manager, navigate to **Home** → **Elements** → **Session Manager**, as shown below. Verify that for the Session Manager of interest, a green check mark is placed under **Tests Pass** and the **Service State** is **Accept New Service**.

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State Shutdown System As of 3:21 PM

4 Items Refresh Show ALL Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication
<input type="checkbox"/>	devcon-asm	Core	✓	24/46/1429	Up	Accept New Service	4/15	0	6/6	✓
<input type="checkbox"/>	devcon-asm	Core	No Connection							
<input type="checkbox"/>	devcon-asm	Core	No Connection							
<input type="checkbox"/>	devcon-asm	Core	✓	0/0/0/0/0	Up	Accept New Service	0/0	0	0/0	✓

Select : All, None

- **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 tests.
- **traceSM -x** – Session Manager command line tool for traffic analysis. Log into an SSH or Telnet session with the Session Manager management interface to run this command.

3. Avaya SBCE

- **OPTIONS** - Use a network sniffer tool like Wireshark to verify that the service provider network will receive OPTIONS forwarded by the Avaya SBCE from the enterprise site as a result of the SIP Entity Monitoring configured for Session Manager. Reversely, when the service provider network responds to the OPTIONS from Session Manager, the Avaya SBCE will pass the response to Session Manager.

- **Incidents** – From the admin web interface of the Avaya SBCE, open the Incidents Viewer by clicking the **Incidents** menu button in the menu bar. Verify that no abnormal incidents are listed

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.3, Avaya Aura® Session Manager R6.3.2 and Avaya Session Border Controller for Enterprise R6.2 to CenturyLink SIP Trunking service (Sonus Platform). CenturyLink SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. CenturyLink SIP Trunking provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. References

The Avaya product documentation is available at <http://support.avaya.com> unless otherwise noted.

Avaya Aura® Session Manager/System Manager

- [1] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 2, June 2013
- [2] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Release 6.3, Issue 2, May 2013
- [3] *Administering Avaya Aura® System Manager*, Release 6.3, Issue 2, May 2013

Avaya Aura® Communication Manager

- [4] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509, Release 6.3, Issue 8, May 2013
- [5] *Programming Call Vectoring Features in Avaya Aura® Call Center Elite*, Release 6.3, Issue 1, May 2013

Avaya Endpoints

- [6] *Avaya one-X® Deskphone SIP 9621G/9641G User Guide for 9600 Series IP Telephones*, Document ID 16-603596, Issue 1, August 2012
- [7] *Avaya one-X® Deskphone H.323 9608 and 9611G User Guide*, Document ID 16-603593, Issue 3, February 2012
- [8] *Avaya one-X® Deskphone SIP for 9640/9640G IP Telephone User Guide Guide*, Document ID 16-602403, June 2013
- [9] *Avaya one-X® Deskphone H.323 for 9630 and 9630G IP Deskphone User Guide*, Document ID 16-300700, June 2013
- [10] *Avaya one-X® Deskphone Value Edition 1616 IP Deskphone User Guide*, Document ID 16-601448, June 2013
- [11] *Using the Avaya A175 Desktop Video Device with the Avaya Flare® Experience*, Document ID 16-603733, Issue 2, December 2011
- [12] *Using Avaya one-X® Communicator Release 6.1*, October 2011
- [13] *Using Avaya Flare® Experience for Windows*, Document ID 18-604158, Release 1.1, Issue 2, February 2013

Avaya Session Border Controller for Enterprise

- [1] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013
- [2] *Avaya Session Border Controller for Enterprise Overview and Specification*, Issue 2, March 2013

©2013 Avaya Inc. All Rights Reserved.

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

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