



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

---

# **Application Notes for Configuring EarthLink SIP Trunking with Avaya Aura® Communication Manager R6.2, Avaya Aura® Session Manager R6.2, and Avaya Session Border Controller for Enterprise R4.0.5 – Issue 1.0**

## **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between EarthLink SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager R6.2, Avaya Aura® Communication Manager R6.2, Avaya Session Border Controller for Enterprise R4.0.5 and various Avaya endpoints.

EarthLink 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

<b>1. INTRODUCTION.....</b>	<b>4</b>
<b>2. GENERAL TEST APPROACH AND TEST RESULTS .....</b>	<b>4</b>
2.1. INTEROPERABILITY COMPLIANCE TESTING .....	4
2.2. TEST RESULTS .....	5
2.3. SUPPORT.....	6
<b>3. REFERENCE CONFIGURATION .....</b>	<b>6</b>
<b>4. EQUIPMENT AND SOFTWARE VALIDATED.....</b>	<b>9</b>
<b>5. CONFIGURE AVAYA AURA® COMMUNICATION MANAGER.....</b>	<b>10</b>
5.1. LICENSING AND CAPACITY .....	10
5.2. SYSTEM FEATURES.....	11
5.3. IP NODE NAMES.....	12
5.4. CODECS.....	12
5.5. IP NETWORK REGION .....	13
5.6. SIGNALING GROUP .....	14
5.7. TRUNK GROUP .....	16
5.8. CALLING PARTY INFORMATION.....	19
5.9. OUTBOUND ROUTING .....	20
<b>6. CONFIGURE AVAYA AURA® SESSION MANAGER.....</b>	<b>23</b>
6.1. SYSTEM MANAGER LOGIN AND NAVIGATION .....	24
6.2. SPECIFY SIP DOMAIN .....	26
6.3. ADD LOCATION .....	26
6.4. ADD ADAPTATION MODULE.....	28
6.5. ADD SIP ENTITIES .....	30
6.6. ADD ENTITY LINKS .....	34
6.7. ADD ROUTING POLICIES .....	36
6.8. ADD DIAL PATTERNS .....	38
6.9. ADD/VIEW SESSION MANAGER.....	41
<b>7. CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE .....</b>	<b>43</b>
7.1. ACCESS MANAGEMENT INTERFACE .....	43
7.2. VERIFY NETWORK CONFIGURATION AND ENABLE INTERFACES .....	44
7.3. SIGNALING INTERFACE.....	46
7.4. MEDIA INTERFACE .....	47
7.5. SERVER INTERWORKING.....	48
7.5.1. Server Interworking: Session Manager.....	49
7.5.2. Server Interworking: EarthLink .....	51
7.6. SERVER CONFIGURATION .....	53
7.6.1. Server Configuration: Session Manager .....	54
7.6.2. Server Configuration: EarthLink .....	55
7.7. SIGNALING RULES AND MANIPULATION .....	56
7.7.1. Signaling Rules: Session Manager.....	57
7.7.2. Signaling Manipulation: EarthLink .....	59
7.8. MEDIA RULES .....	62
7.9. ENDPOINT POLICY GROUPS .....	63
7.9.1. Endpoint Policy Group: Session Manager.....	64
7.9.2. Endpoint Policy Group: EarthLink .....	64
7.10. ROUTING .....	65
7.10.1. Routing: Session Manager .....	66

7.10.2. Routing: <i>EarthLink</i> .....	66
7.11. TOPOLOGY HIDING.....	67
7.11.1. <i>Topology Hiding: Session Manager</i> .....	68
7.11.2. <i>Topology Hiding: EarthLink</i> .....	69
7.12. END POINT FLOWS .....	70
7.12.1. <i>End Point Flow: Session Manager</i> .....	71
7.12.2. <i>End Point Flow: EarthLink</i> .....	72
<b>8. EARTHLINK SIP TRUNKING CONFIGURATION.....</b>	<b>73</b>
<b>9. VERIFICATION AND TROUBLESHOOTING .....</b>	<b>73</b>
<b>10. CONCLUSION .....</b>	<b>75</b>
<b>11. REFERENCES .....</b>	<b>76</b>

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between EarthLink SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager R6.2, Avaya Aura® Communication Manager R6.2, Avaya Session Border Controller for Enterprise R4.0.5 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with EarthLink 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 EarthLink 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 Avaya one-X® Communicator (soft client). Avaya one-X® Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X® Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. Both protocols were tested.
- Various call types including: local, long distance, 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.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call forwarding, transfer, conference and mobility (extension to cellular).

Items not supported or not tested included the following:

- Inbound toll-free and emergency (911) calls were not tested.
- T.38 faxing is not supported by EarthLink SIP Trunking and therefore was not tested.

## 2.2. Test Results

Interoperability testing of EarthLink SIP Trunking was completed with successful results for all test cases with the exception of the observations/limitations noted below.

- **Contact Header "epv" Parameter** – The outbound call INVITE from enterprise SIP endpoints contained an "epv" parameter in the Contact header. EarthLink does not support this parameter in the Contact header: no "100 Trying" was returned to the enterprise and the call would eventually time out. During compliance testing, this interoperability issue was resolved by removing the "epv" parameter from the Contact header in the outbound call INVITE at the Avaya SBCE (See **Section 7.7.2**).
- **Packet Fragmentation** – When a call was re-directed off-net to a PSTN destination from the enterprise (transfer, forward, or EC500 redirection to a mobile phone), the outbound INVITE sometimes exceeded the Ethernet frame size and became fragmented. This fragmentation would cause failure of the re-directed calls. During compliance testing, a packet fragmentation workaround was implemented, by removing certain headers, as approved by Avaya product line management, in the outbound INVITE to reduce the message size. The problem was ultimately resolved when EarthLink upgraded the Acme Packet SBC to a new firmware release that handles packet fragmentation properly.
- **SilenceSupp versus Annexb for Silence Suppression** – EarthLink uses the SIP SDP parameter SilenceSupp to signal silence suppression. Communication Manager uses the annexb parameter for this purpose. As a result, neither side is able to signal this properly to the other side. G.729A codec was configured on Communication Manager during compliance test (therefore, annexb was turned off) to match the annexb setting in inbound call INVITE SDP. No user perceived problems were observed though silence suppression was most likely not achieved.
- **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 EarthLink SIP Trunking service. It is listed here simply as an observation.
- **Extra SIP Signaling** – After a call with PSTN was effectively transferred off-net to another PSTN party using REFER, a few extra signaling messages (INVITE and BYE)

from either side between the EarthLink network and enterprise were observed. These messages were limited in number and non-recurring. They would receive 481/491/487 responses and had no perceived negative impact on the transferred call, though the signaling was not completely clean. The extra INVITE from Communication Manager will be removed in Communications Manager Release 6.2 SP5 which is soon to be generally available. The extra INVITE and BYE messages from EarthLink will be addressed in a later release of the EarthLink SIP Trunking service.

- **302 SIP Message** – When a Communication Manager vector received an inbound call and the vector was programmed to re-direct the call to a PSTN number using the SIP 302 message, EarthLink ACKed the 302 message but the call was not delivered to the intended PSTN destination. The caller heard fast busy tones and/or an announcement that the call could not be completed as dialed. This problem has been under investigation by EarthLink.

## 2.3. Support

For technical support on the EarthLink SIP Trunking service, contact EarthLink Business Customer Care by using the support links provided at [www.earthlinkbusiness.com](http://www.earthlinkbusiness.com)

## 3. Reference Configuration

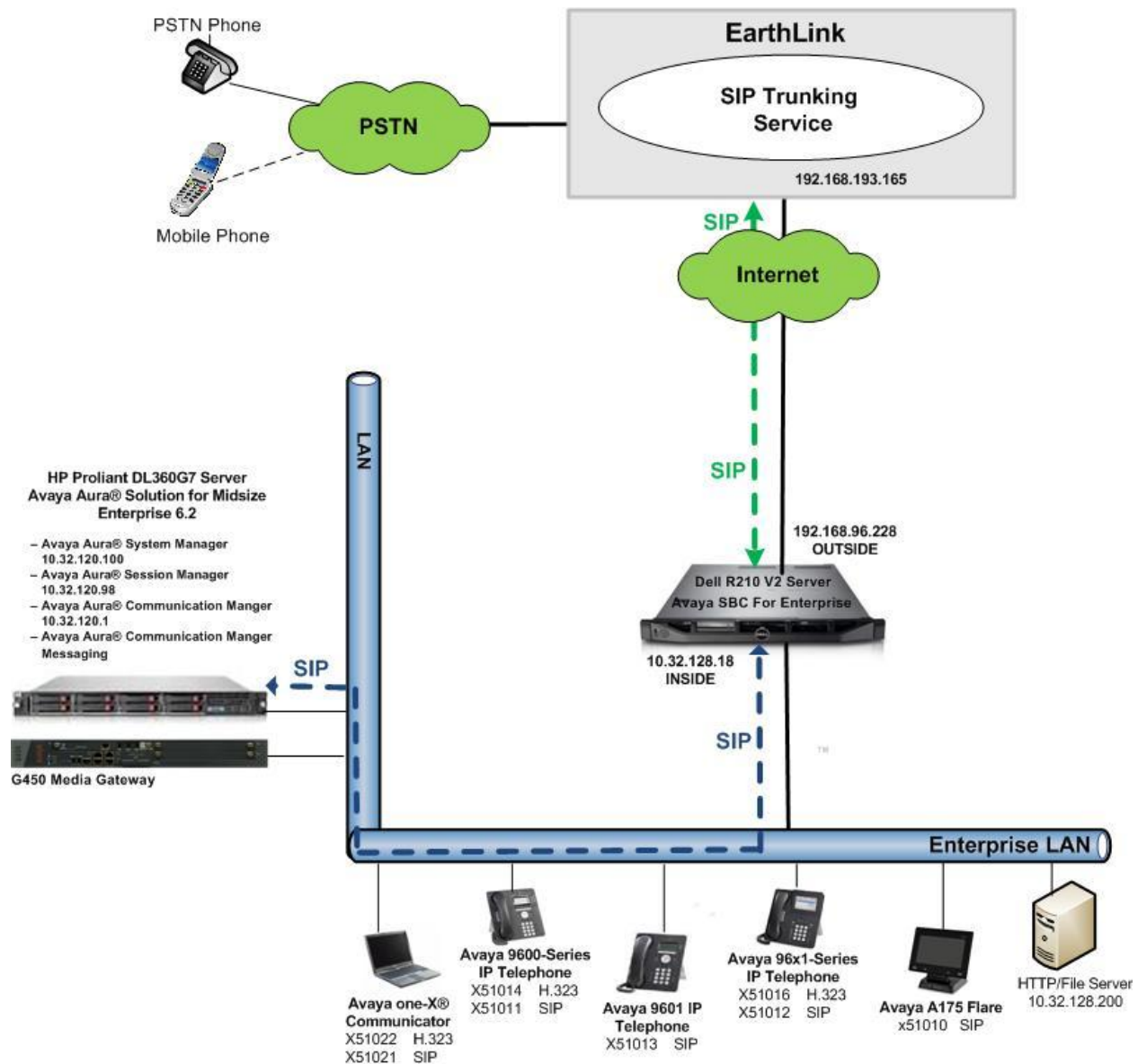
**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to EarthLink SIP Trunking through a public Internet WAN connection.

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 3<sup>rd</sup> and 4<sup>th</sup> octets were retained from the real addresses.

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

- HP Proliant DL360G7 Server running Avaya Aura® Solution for Midsize Enterprise 6.2 that includes
  - Communication Manager
  - Session Manager
  - System Manager
  - Communication Manager Messaging
- Avaya G450 Media Gateway
- Dell R210 V2 Server running Avaya SBCE
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya 96x1-Series IP Telephone (H.323 and SIP)
- Avaya 9601 IP Telephone (SIP)
- Avaya A175 Desktop Video Device a.k.a. Flare (used as a SIP voice endpoint)
- Avaya one-X® Communicator soft phones (H.323 and SIP)

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 EarthLink 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 EarthLink 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 and not affect other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

For inbound calls, the 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 EarthLink SIP Trunking through the public IP network.

The compliance test used Communication Manager Messaging for testing voice mail access/navigation and MWI (Messaging Wait Indicator) on Avaya enterprise phones. Communication Manager Messaging was chosen since Avaya Aura® Solution for Midsize Enterprise 6.2 includes this voice messaging component. Other voice messaging application such as Avaya Aura® Messaging could have been used to satisfy this test purpose.

The administration of Communication Manager Messaging and endpoints on Communication Manager are standard. Since the configuration tasks for Communication Manager Messaging and endpoints are not directly related to the inter-operation with EarthLink 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® Solution for Midsize Enterprise 6.2 running on HP Proliant DL360G7 Server <ul style="list-style-type: none"> <li>– Avaya Aura® Communication Manager</li> <li>– Avaya Aura® Communication Manager Messaging</li> <li>– Avaya Aura® Session Manager</li> <li>– Avaya Aura® System Manager</li> </ul>	6.2 SP3 (R016x.02.0.823.0-20199) 6.2 SP1 (CMM-02.0.823.0-0104) 6.2 SP4 (6.2.4.0.624005) 6.2.0-SP4 (6.2.16.1.1993)
Avaya G450 Media Gateway	31.22.0 /1
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1 SP5
Avaya 9640 IP Telephone (SIP)	Avaya one-X® Deskphone Edition SIP 2.6.9.1
Avaya 9611 IP Telephone (H.323)	Avaya one-X® Deskphone Edition H.323 6.2.2
Avaya 9621 IP Telephone (SIP)	Avaya one-X® Deskphone Edition SIP 6.2.1
Avaya 9601 IP Telephone (SIP)	Avaya one-X® Deskphone Edition SIP 6.1 SP5
Avaya A175 Flare™ Desktop Video Device (SIP telephone function)	SIP Version 1.1.2 (SIP_A175_1_1_2_020002)
Avaya one-X Communicator (H.323 & SIP)	6.1.7.04-SP7-39506
Avaya Session Border Controller for Enterprise running on Dell R210 V2 Server	4.0.5Q19
EarthLink SIP Trunking Components	
Equipment/Software	Release/Version
Acme Packet Net-Net 4500 Session Border Controller	SCX6.1.0 MR-7 Patch 5 (Build 861) <ul style="list-style-type: none"> <li>– Used for testing</li> </ul> SCX6.3.0 MR-4 Patch 1 <ul style="list-style-type: none"> <li>– Used to resolve packet fragmentation</li> </ul>
Metaswitch Softswitch	7.4

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 EarthLink 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 12000 licenses are available and 275 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	0
Maximum Concurrently Registered IP Stations:		18000	2
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		128	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		18000	0
Maximum Video Capable IP Softphones:		18000	2
<b>Maximum Administered SIP Trunks:</b>		<b>12000</b>	<b>275</b>
Maximum Administered Ad-hoc Video Conferencing Ports:		12000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
Maximum TN2501 VAL Boards:		10	0
Maximum Media Gateway VAL Sources:		250	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 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? y
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
```

On **Page 9** verify that a text string has been 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 19
      FEATURE-RELATED SYSTEM PARAMETERS

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

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

      INTERNATIONAL CALL ROUTING PARAMETERS
      Local Country Code: 1
      International Access Code: 011

      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 (*SM*). 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	
<b>SM</b>	<b>10.32.120.98</b>	
default	0.0.0.0	
nwk-aes1	10.32.120.3	
<b>procr</b>	<b>10.32.120.1</b>	
procr6	::	

### 5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 5 was used for this purpose. EarthLink 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 5		Page 1 of 2
		IP Codec Set
Codec Set: 5		
Audio Codec	Silence Suppression	Frames Per Pkt
Packet Size(ms)		
1: <b>G.729A</b>	n	2
2: <b>G.711MU</b>	n	2
3:		

On **Page 2**, set the **Fax Mode** to *off* since T.38 faxing is not supported by EarthLink SIP Trunking.

change ip-codec-set 5		Page 2 of 2
		IP Codec Set
Allow Direct-IP Multimedia? n		
	Mode	Redundancy
<b>FAX</b>	<b>off</b>	0
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 5 was chosen for the service provider trunk. Use the **change ip-network-region 5** command to configure region 5 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is *sip.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 5                                     Page 1 of 20

                                IP NETWORK REGION

Region: 5
Location:                Authoritative Domain: sip.avaya.com
      Name: SP Region
MEDIA PARAMETERS                                Intra-region IP-IP Direct Audio: yes
      Codec Set: 5                                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: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 5 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 5 will be used for calls between region 5 (the service provider region) and region 1 (the rest of the enterprise).

change ip-network-region 5										Page	4	of	20
Source Region: 5 Inter Network Region Connection Management										I			M
										G	A		t
<b>dst</b>	<b>codec</b>	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	c				
<b>rgn</b>	<b>set</b>	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	e			
1	5	y	NoLimit					n		t			
2													
3													
4													
5	5											all	

## 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 the recommended default value of *tls* (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to 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 **5261**.
- 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 *SM*. 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.

change signaling-group 5		Page 1 of 2
SIGNALING GROUP		
Group Number: 5	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5261	Far-end Listen Port: 5261	
	Far-end Network Region: 5	
	Far-end Secondary Node Name:	
Far-end Domain: sip.avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP 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 dial plan 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: AC SP Trunk                          COR: 1                 TN: 1             TAC: *05
  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 **900** 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): 900
```



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

On **Page 4**, the **Network Call Redirection** field can be set to **n** (default setting) or **y**. Setting the **Network Call Redirection** flag to **y** enables use of the SIP REFER message for call transfer as verified in the compliance test; otherwise the SIP INVITE message will be used for call transfer. Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to **101**, the value preferred by EarthLink.

add trunk-group 5	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? n	
Network Call Redirection? y	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? y	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Enable Q-SIP? 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 4 numbers were mapped to the 4 enterprise extensions 51011, 51012, 51014 and 51016. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 4 extensions.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
0	attd		0	1	Total Administered: 21
5	1			5	Maximum Entries: 540
5	2			5	
5	3			5	
5	4			5	
5	5			5	
5	6			5	
5	7			5	
5	8			5	
5	51011	5	9783781160	10	
5	51012	5	9783781161	10	
5	51014	5	9783781162	10	
5	51016	5	9783781163	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 8 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	8	5	97837	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: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	1	attd							
1	5	ext							
2	5	ext							
3	5	ext							
4	5	ext							
5	5	ext							
6	5	ext							
7	5	ext							
8	5	ext							
9	1	fac							
*	3	dac							
#	3	dac							

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

```

change feature-access-codes                                     Page 1 of 11
                                FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code: *10
Abbreviated Dialing List2 Access Code: *12
Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *14
Announcement Access Code: *19
Answer Back Access Code:

Auto Alternate Routing (AAR) Access Code: *00
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
Automatic Callback Activation: *33      Deactivation: #33
Call Forwarding Activation Busy/DA: *30    All: *31    Deactivation: #30
Call Forwarding Enhanced Status:      Act:      Deactivation:
Call Park Access Code: *40
Call Pickup Access Code: *41
CAS Remote Hold/Answer Hold-Unhold Access Code: *42
CDR Account Code Access Code:
Change COR Access Code:
Change Coverage Access Code:
Conditional Call Extend Activation:      Deactivation:
Contact Closure    Open Code: *80      Close Code: #80

```

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 5 which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
0	1	1	5	op		n	
0	8	8	deny	op		n	
0	11	11	5	op		n	
00	2	2	deny	op		n	
01	9	17	deny	iop		n	
011	10	18	5	intl		n	
1732	11	11	5	fnpa		n	
1800	11	11	5	fnpa		n	
1877	11	11	5	fnpa		n	
1908	11	11	5	fnpa		n	
411	3	3	5	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 5 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 (**Pfx Mrk**) 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 HNP 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 5													Page 1 of 3	
Pattern Number: 5													Pattern Name: AC SP Route	
SCCAN? n													Secure SIP? n	
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC
No			Mrk	Lmt	List	Del	Digits						QSIG	
													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

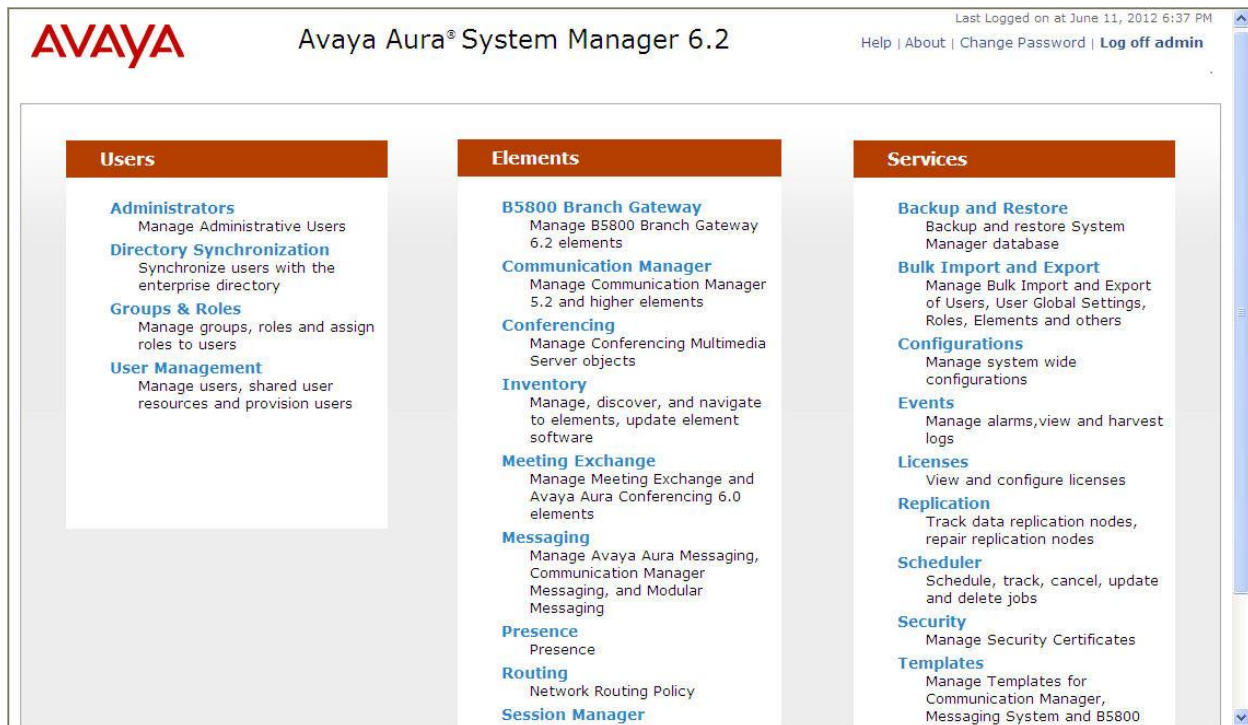
This section provides the procedures for configuring Session Manager. The procedures include the following items:

- 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 creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP Domains, Locations, SIP Entities, and Session Manager itself. However, each item should be reviewed to verify 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 6.2 web interface. The top header includes the Avaya logo, the product name "Avaya Aura® System Manager 6.2", and a user status bar indicating "Last Logged on at June 11, 2012 6:37 PM" with links for "Help", "About", "Change Password", and "Log off admin". Below the header, there are tabs for "Routing" and "Home". The left navigation pane shows a tree structure under "Routing" with 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 routing applications like "Domains", "Locations", "SIP Entities", etc., and provides a recommended order for configuration. The steps are 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"

## 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 (*sip.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 the 'Domain Management' interface. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains'. Below this, there is a 'Domain Management' section with a 'Help ?' link and 'Commit' and 'Cancel' buttons. A warning message states: 'Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset login credentials.' Below the warning, there is a table with one item. The table has columns: Name, Type, Default, and Notes. The entry is: Name: \* sip.avaya.com, Type: sip (dropdown), Default: ☐, Notes: Auto CS domain. At the bottom, there is a '\* Input Required' message and 'Commit' and 'Cancel' buttons.

Name	Type	Default	Notes
* sip.avaya.com	sip	<input type="checkbox"/>	Auto CS 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 2<sup>nd</sup> 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 **Belleville** Location, which includes all equipment on the enterprise network. Click **Commit** to save.

Home /Elements / Routing / Locations

Help ?
Commit
Cancel

Location Details

General

\* Name: Belleville
Notes: Enterprise Site for SP Testing

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec
Total Bandwidth:
Multimedia Bandwidth:
Audio Calls Can Take Multimedia Bandwidth:

Per-Call Bandwidth Parameters

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

Alarm Threshold

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

Location Pattern

Add Remove
2 Items Refresh Filter: Enable

	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.32.120.*	CPE CM, SM and other devices
<input type="checkbox"/>	* 10.32.128.*	SBCs

Select : All, None

\* Input Required
Commit
Cancel

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

## 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 EarthLink SIP Trunking, one Adaptation is needed. This Adaptation is applied to the Communication Manager SIP Entity and maps inbound DID numbers from EarthLink 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 EarthLink 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

CommitCancel

General

\* Adaptation name: NWK CM Adaptation

Module name: DigitConversionAdapter

Module parameter:

Egress URI Parameters:

Notes: Use with Avaya SBCE

Digit Conversion for Incoming Calls to SM

AddRemove

0 Items Refresh

Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

Digit Conversion for Outgoing Calls from SM

AddRemove

35 Items Refresh

Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
<input type="checkbox"/>	* 9783781160	* 10	* 10		* 10	51011	destination	
<input type="checkbox"/>	* 9783781161	* 10	* 10		* 10	51012	destination	
<input type="checkbox"/>	* 9783781162	* 10	* 10		* 10	51014	destination	
<input type="checkbox"/>	* 9783781163	* 10	* 10		* 10	51016	destination	

In the example shown above, if a user on the PSTN dials 978-378-1161, Session Manager will convert the number to 51012 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 51012 to 9783781161 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 Communication Manager 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:**

\* **FQDN or IP Address:**

**Type:**

**Notes:**

**Location:**

**Outbound Proxy:**

**Time Zone:**

**Credential name:**

**SIP Link Monitoring**

**SIP Link Monitoring:**

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
- **5261** with **TLS** for connecting to Communication Manager

In addition, port 5061 with TLS 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 EarthLink SIP Trunking.

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

**Port**

TCP Failover port:

TLS Failover port:

5 Items

Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP	sip.avaya.com	<input type="text" value="for ASBCE"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	UDP	sip.avaya.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	TLS	sip.avaya.com	<input type="text" value="for nwk-cm &amp; nwk-aes1"/>
<input type="checkbox"/>	<input type="text" value="5260"/>	TLS	sip.avaya.com	<input type="text" value="for nwk-cm-trk4"/>
<input type="checkbox"/>	<input type="text" value="5261"/>	TLS	sip.avaya.com	<input type="text" value="for nwk-cm-trk5"/>

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 SIP Entities. The breadcrumb trail at the top is "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details". In the top right corner, there is a "Help ?" link and two buttons: "Commit" and "Cancel".

The "General" section contains the following fields:

- Name:** nwk-cm-trk5
- FQDN or IP Address:** 10.32.120.1
- Type:** CM (dropdown menu)
- Notes:** AC SP Trunk
- Adaptation:** NWK CM Adaptation (dropdown menu)
- Location:** Belleville (dropdown menu)
- Time Zone:** America/New\_York (dropdown menu)
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (dropdown menu)

The "SIP Link Monitoring" section contains one field:

- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)



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 shows a web-based configuration interface for SIP Entities. The breadcrumb navigation at the top reads "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details". In the top right corner, there is a "Help ?" link and two buttons: "Commit" and "Cancel".

The "General" section contains the following fields:

- Name:** ASBCE
- FQDN or IP Address:** 10.32.128.18
- Type:** SIP Trunk (selected from a dropdown menu)
- Notes:** Avaya SBC for Enterprise
- Adaptation:** (empty dropdown menu)
- Location:** Belleville (selected from a dropdown menu)
- Time Zone:** America/New\_York (selected from a dropdown menu)
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (selected from a dropdown menu)

The "SIP Link Monitoring" section contains one field:

- SIP Link Monitoring:** Use Session Manager Configuration (selected from a dropdown menu)

## 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**.
- **Trusted:** Check this box. *Note: If this box is not checked, 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 as was set for the compliance test. TCP 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 Help ? Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM to CM TRK5	* nw-k-sm	TLS	* 5261	* nw-k-cm-trk5	* 5261	Trusted	

\* Input Required Commit Cancel

Entity Link to Avaya SBC for Enterprise:

Home /Elements / Routing / Entity Links

Entity Links Help ? Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM to ASBCE	* nw-k-sm	TCP	* 5060	* ASBCE	* 5060	Trusted	

\* Input Required Commit Cancel

Note that a separate Entity Link existed between Communication Manager and Session Manager using port 5061 and TLS (not shown) for carrying 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 Communication Manager Messaging, 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

Routing Policy Details [Help ?](#)

**General**

\* **Name:**

**Disabled:** ☐

\* **Retries:**

**Notes:**

**SIP Entity as Destination**

Name	FQDN or IP Address	Type	Notes
nwk-cm-trk5	10.32.120.1	CM	AC SP Trunk

**Time of Day**

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	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 SBC for Enterprise

**Time of Day**

1 Item | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	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 EarthLink and vice versa. Dial Patterns specifies 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 *sip.avaya.com* uses the **ASBCE Policy** Routing Policy as defined in **Section 6.7**.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Help ? Commit Cancel

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	ASBCE Policy	0	<input type="checkbox"/>	ASBCE	

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 **Belleville** could have been selected.

The second example shows that inbound 10-digit numbers that start with **978378116** uses Routing Policy **CM TRK5 Policy** as defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by EarthLink.

[Help ?](#)

**Dial Pattern Details**

**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 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	CM TRK5 Policy	0	<input type="checkbox"/>	nwk-cm-trk5	AC SP Testing

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 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 'Help ?' link is in the top right corner. The page title is 'View Session Manager' with a 'Return' button. Below the title is a horizontal menu with links: 'General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |'. Below the menu are 'Expand All' and 'Collapse All' links. The 'General' section is expanded, showing the following fields: 'SIP Entity Name' with the value 'nwk-sm', 'Description' (empty), 'Management Access Point Host Name/IP' with the value 'nwk-sm.avaya.com', and 'Direct Routing to Endpoints' with the value 'Disable'.

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 message 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 Address10.32.120.98

Network Mask255.255.255.0

Default Gateway10.32.120.254

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)30

Reactive cycle time (secs)120

Number of Retries1

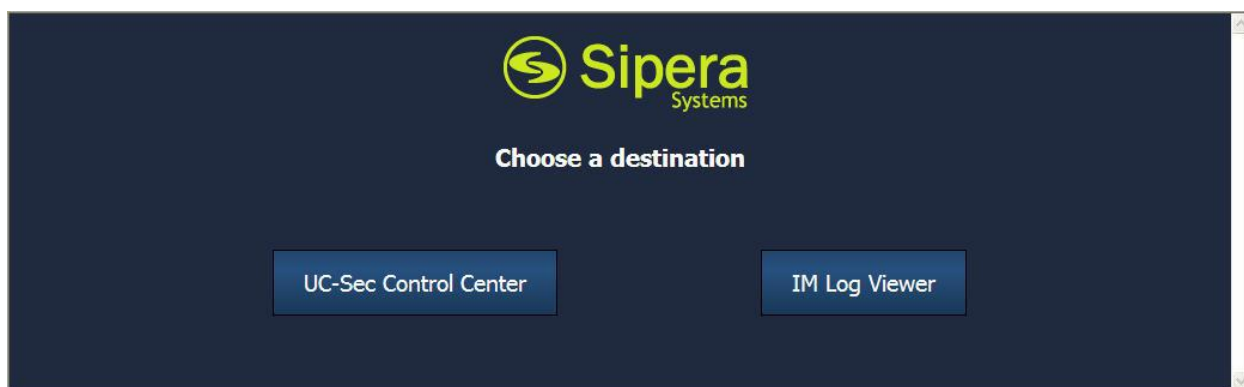
## 7. Configure Avaya Session Border Controller for Enterprise

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

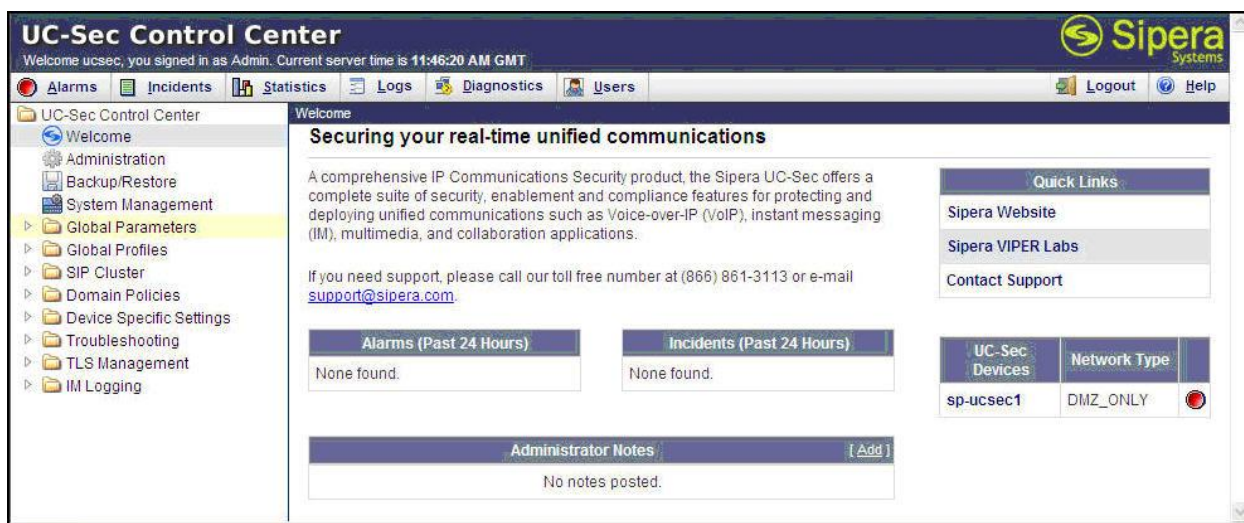
These Application Notes assume that the installation of the SBC and the assignment of a management IP Address have already been completed.

### 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. Select **UC-Sec Control Center** on the displayed web page, and log in using proper login credentials (not shown).



Once logged in, a Welcome screen will be presented. The following image illustrates the menu items available on the left-side of the UC-Sec Control Center 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 Config** icon highlighted below.



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. Interfaces **A1** and **B1** represent the private and public interfaces of the Avaya SBCE. 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.

System Information: sp-ucsec1

Network Configuration				
<b>General Settings</b>		<b>Device Settings</b>		
Appliance Name	sp-ucsec1	HA Mode	No	
Box Type	SIP	Secure Channel Mode	None	
Deployment Mode	Proxy	Two Bypass Mode	No	
<b>Network Settings</b>				
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
<b>DNS Configuration</b>		<b>Management IP(s)</b>		
Primary DNS	10.32.128.200	IP	10.32.101.10	
Secondary DNS				
DNS Location	DMZ			
DNS Client IP	10.32.128.18			

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.

The screenshot shows the UC-Sec Control Center interface. On the left, the 'Device Specific Settings' menu is expanded, and 'Network Management' is selected. In the center pane, 'sp-ucsec1' is selected under 'UC-Sec Devices'. The right pane shows the 'Interface Configuration' tab for 'sp-ucsec1'. A warning message states: '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.' Below this, there are fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask' (disabled), 'B1 Netmask' (255.255.255.224), and 'B2 Netmask' (disabled). There are 'Add IP', 'Save Changes', and 'Clear Changes' buttons. A table lists the IP addresses and their associated interfaces:

IP Address	Public IP	Gateway	Interface	
10.32.128.18		10.32.128.254	A1	✗
192.168.96.228		192.168.96.254	B1	✗

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.

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

### 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 (**sp-ucsec1**) to be managed. In the right pane, select **Add Signaling Interface**. 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 far right pane.

For the compliance test, the signaling interface **Int\_Sig\_Intf** was created for the Avaya SBCE internal interface. 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. 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 displays the UC-Sec Control Center interface. The left pane shows the navigation tree with 'Signaling Interface' selected under 'Device Specific Settings'. The center pane shows 'UC-Sec Devices' with 'sp-ucsec1' selected. The right pane shows the 'Signaling Interface' configuration table with two entries: 'Int\_Sig\_Intf' and 'Ext\_Sig\_Intf'. An 'Add Signaling Interface' button is visible in the top right of the right pane.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Int_Sig_Intf	10.32.128.18	5060	---	---	None		
Ext_Sig_Intf	192.168.96.228	---	5060	---	None		



## 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 (**sp-ucsec1**) to be managed. In the right pane, select **Add Media Interface**. 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 far right pane.

For the compliance test, the media interface **Int\_Media\_Intf** was created for the Avaya SBCE internal interface. 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. 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 UC-Sec Control Center interface. The left pane shows the navigation tree with 'Media Interface' selected under 'Device Specific Settings'. The center pane shows 'UC-Sec Devices' with 'sp-ucsec1' selected. The right pane shows the 'Media Interface' configuration page for 'sp-ucsec1'. It includes a warning message: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table listing existing media interfaces.

Name	Media IP	Port Range		
Int_Media_Intf	10.32.128.18	35000 - 40000		
Ext_Media_Intf	192.168.96.228	35000 - 40000		

## 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, select **Add Profile**. 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 far 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.

The screenshot displays the UC-Sec Control Center interface. The left pane shows the navigation tree with 'Server Interworking' selected under 'Global Profiles'. The center pane lists 'Interworking Profiles' with 'Avaya-SM' highlighted. The right pane shows the configuration for the 'Avaya-SM' profile, with the 'General' tab active. The configuration table is as follows:

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	No
URI Scheme	SIP
Via Header Format	RFC3261



### 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:

The screenshot shows the configuration page for the Avaya-SM server interworking profile. At the top, there are three buttons: "Rename Profile", "Clone Profile", and "Delete Profile". Below these is a yellow bar with the text "Click here to add a description." The main content area has five tabs: "General", "Timers", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is selected and displays the following settings:

General	
Hold Support	RFC 2543
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	No
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

Note that **T.38 Support** is disabled by default as shown in the preceding screenshot. This default setting is proper for Earthlink since T.38 Fax is not supported. This setting should be enabled if T.38 faxing is to be supported for the SIP Trunking service.

The **Advanced** tab:

General	Timers	URI Manipulation	Header Manipulation	Advanced
<b>Advanced Settings</b>				
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		
SLIC 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		
<a href="#">Edit</a>				

## 7.5.2. Server Interworking: EarthLink

For the compliance test, the server interworking profile **SP-General** was similarly created for the EarthLink 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
<b>General</b>				
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	No			
URI Scheme	SIP			
Via Header Format	RFC3261			
<b>Privacy</b>				
Privacy Enabled	No			
User Name				
P-Asserted-Identity	No			
P-Preferred-Identity	No			
Privacy Header				
<b>DTMF</b>				
DTMF Support	None			
<a href="#">Edit</a>				

Note that **T.38 Support** is disabled by default as shown in the preceding screenshot. This default setting is proper for Earthlink since T.38 Fax is not supported. This setting should be enabled if T.38 faxing is to be supported for the SIP Trunking service.

The **Advanced** tab:

General	Timers	URI Manipulation	Header Manipulation	Advanced
---------	--------	------------------	---------------------	----------

Advanced Settings	
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
SLIC 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 another 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, select **Add Profile**. 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 far 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.

The screenshot displays the UC-Sec Control Center interface. On the left, the 'Global Profiles' folder is expanded, and 'Server Configuration' is selected. The center pane shows a list of profiles, with 'NWK-SM' highlighted. The right pane shows the configuration details for the 'NWK-SM' profile, including the 'General' tab with the following settings:

General	
Server Type	Call Server
IP Addresses / FQDNs	10.32.120.98
Supported Transports	TCP
TCP Port	5060

An 'Edit' button is visible below the configuration table.

### 7.6.1. Server Configuration: Session Manager

For the compliance test, the server configuration profile **NWK-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.

The screenshot shows the configuration interface for a Session Manager profile. At the top, there are three buttons: "Rename Profile", "Clone Profile", and "Delete Profile". Below these are four tabs: "General", "Authentication", "Heartbeat", and "Advanced". The "General" tab is selected. The configuration table has the following data:

General	
Server Type	Call Server
IP Addresses / FQDNs	10.32.120.98
Supported Transports	TCP
TCP Port	5060

Below the table is an "Edit" button.

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

The screenshot shows the configuration interface for a Session Manager profile, with the "Advanced" tab selected. The configuration table has the following data:

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

Below the table is an "Edit" button.

## 7.6.2. Server Configuration: EarthLink

For the compliance test, the server configuration profile **SP-EarthLink** 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 address of the EarthLink SIP server.
- Set **Supported Transports** to the transport protocol used for SIP signaling between EarthLink and the Avaya SBCE.
- Set **UDP Port** to the port EarthLink will listen on for SIP requests from the Avaya SBCE.

The screenshot shows the configuration interface for the **SP-EarthLink** profile. At the top, there are three buttons: **Rename Profile**, **Clone Profile**, and **Delete Profile**. Below these are four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. The **General** tab is selected, displaying a table with the following configuration:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.193.165
Supported Transports	UDP
UDP Port	5060

Below the table is an **Edit** button.

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

The screenshot shows the configuration interface for the **SP-EarthLink** profile, specifically the **Advanced** tab. The tabs at the top are **General**, **Authentication**, **Heartbeat**, and **Advanced**. The **Advanced** tab is selected, displaying a table with the following configuration:

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

Below the table is an **Edit** button.



## 7.7. Signaling Rules and Manipulation

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, select **Add Rule**. 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 far right pane. Alternatively, a new rule may be created by selecting an existing rule in the center pane and clicking the **Clone Rule** 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.

The screenshot displays the UC-Sec Control Center interface. The left pane shows the navigation tree with 'Signaling Rules' selected under 'Domain Policies'. The center pane lists signaling rules, with 'SessMgr\_SigRules' highlighted. The right pane shows the configuration for 'SessMgr\_SigRules'.

**Domain Policies > Signaling Rules: SessMgr\_SigRules**

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

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**

Enable Content-Type Checks		<input checked="" type="checkbox"/>	
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

Edit




### 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 to the service provider network. 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.

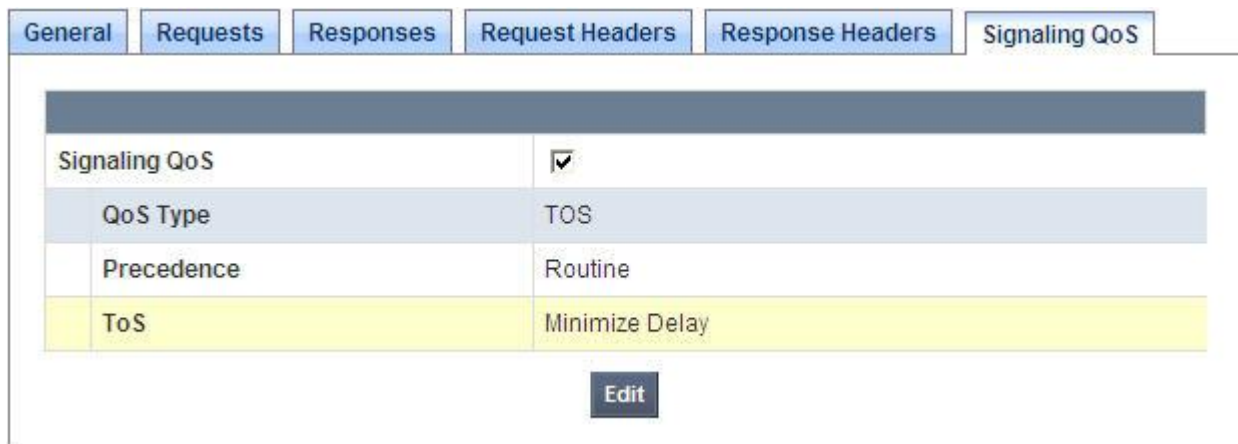
Click the **Add Rule** button (not shown) to add a new signaling rule. In the **Rule Name** field, enter an appropriate name, such as *SessMgr\_SigRules*.



The screenshot shows a dialog box titled "Signaling Rule" with a close button in the top right corner. Inside the dialog, there is a text input field labeled "Rule Name" which contains the text "SessMgr\_SigRules". 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.



The screenshot displays the "Signaling QoS" configuration screen. At the top, there are several tabs: "General", "Requests", "Responses", "Request Headers", "Response Headers", and "Signaling QoS". The "Signaling QoS" tab is selected. Below the tabs is a table with the following configuration:

Signaling QoS	<input checked="" type="checkbox"/>
QoS Type	TOS
Precedence	Routine
ToS	Minimize Delay

At the bottom of the table is an "Edit" button.

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 EarthLink 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								
Add In Header Control					Add Out Header Control			
Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Correlation-ID	INVITE	Forbidden	Remove Header	Yes	IN		
2	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN		

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 will appear as follows.

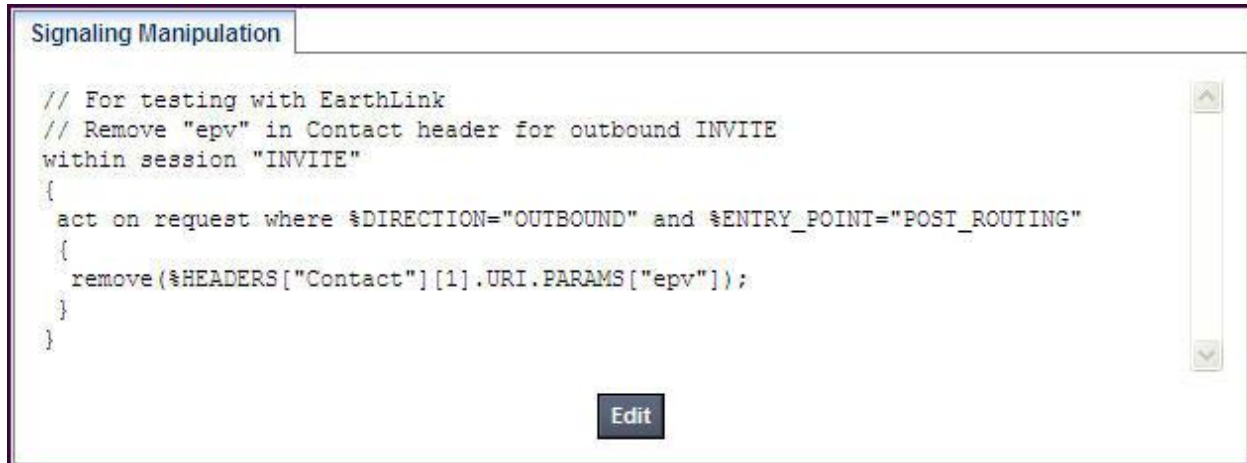
General	Requests	Responses	Request Headers	Response Headers	Signaling QoS				
			Add In Header Control	Add Out Header Control					
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN		
2	Endpoint-View	1XX	INVITE	Forbidden	Remove Header	Yes	IN		

### 7.7.2. Signaling Manipulation: EarthLink

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

However, for the reason cited in the observation/limitation list in **Section 2.2**, the “epv” parameter in the Contact header contained in the INVITE messages outbound to EarthLink was removed via the Avaya SBCE’s **Signaling Manipulation** feature using a proprietary scripting tool called SigMa.

To create a signaling manipulation script, navigate to **Global Profiles → Signaling Manipulation**. Click on **Add Script** (not shown), then type in a script title and enter the script statements/commands. Save the script by clicking on **Save** (not shown). For the compliance test, a script named “DelContactEPV” was created. The script is shown below.



```
// For testing with EarthLink
// Remove "epv" in Contact header for outbound INVITE
within session "INVITE"
{
  act on request where $DIRECTION="OUTBOUND" and $ENTRY_POINT="POST_ROUTING"
  {
    remove($HEADERS["Contact"][1].URI.PARAMS["epv"]);
  }
}
```

**Edit**

A script is tied to a server in **Global Profiles → Server Configuration**. For the compliance test, the above script was associated with the “SP-EarthLink” server. In the **Advanced** tab of the “SP-EarthLink” server, click **Edit**, then choose *DelContactEPV* for **Signaling Manipulation Script** as shown below. Click **Finish**.



Edit Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	DelContactEPV
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

**Finish**

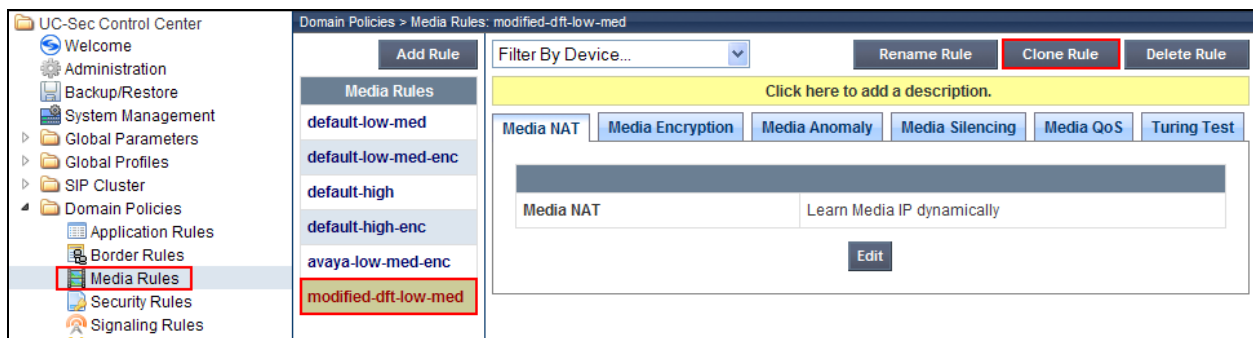
The screen below shows the **Advanced** tab of the “SP-EarthLink” server after the signaling manipulation script was added.

General	Authentication	Heartbeat	Advanced
<b>Advanced</b>			
Enable DoS Protection	<input type="checkbox"/>		
Enable Grooming	<input type="checkbox"/>		
Interworking Profile	SP-General		
Signaling Manipulation Script	DelContactEPV		
UDP Connection Type	SUBID		
<a href="#">Edit</a>			

## 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, select **Add Rule**. 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 far right pane. Alternatively, a new rule may be created by selecting an existing rule in the center pane and clicking the **Clone Rule** 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 used for both the Session Manager and the EarthLink 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, select **Add Group**. 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 far 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.

The screenshot displays the UC-Sec Control Center interface. The left pane shows the navigation tree with 'End Point Policy Groups' selected. The center pane lists various policy groups, with 'SM' selected. The right pane shows the configuration details for the 'SM' group, including a table of policy sets.

**Domain Policies > End Point 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**

**General-SP**

**Policy Group**

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





### 7.9.1. Endpoint Policy Group: Session Manager

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**.

Policy Group

View Summary

Add Policy Set

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



### 7.9.2. Endpoint Policy Group: EarthLink

For the compliance test, the endpoint policy group **General-SP** was created for the EarthLink 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**.

Policy Group

View Summary

Add Policy Set

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



## 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, select **Add Profile**. 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 far right pane. Alternatively, a new routing profile may be created by selecting an existing profile in the center pane and clicking the **Clone Profile** 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 UC-Sec Control Center interface. The left pane shows the navigation tree with 'Routing' selected. The center pane shows a list of routing profiles: 'default', 'To\_Trunks', 'To\_NwkSM', and 'To\_NwkSM'. The right pane shows the configuration for the 'To\_NwkSM' profile, including a table for routing rules.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.32.120.98	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

### 7.10.1. Routing: Session Manager

For the compliance test, the routing profile **To\_NwkSM** 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 **Next Hop Priority**.
- Set **Outgoing Transport** field to **TCP**.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.32.120.98	--	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

### 7.10.2. Routing: EarthLink

For the compliance test, the routing profile **To\_Trunks** was created for EarthLink. 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 EarthLink SIP server.
- Enable **Next Hop Priority**.
- Set **Outgoing Transport** field to **UDP**.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	192.168.193.165	--	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

## 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, select **Add Profile**. 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. Once complete, the settings are shown in the far 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.

The screenshot displays the UC-Sec Control Center interface. On the left, a tree view shows the navigation menu with 'Topology Hiding' selected. The main area is divided into three panes. The center pane, titled 'Global Profiles > Topology Hiding: NWK-Domain', contains a list of profiles: 'default', 'sipsec\_00\_profile', 'SP-General', 'NWK-Domain' (highlighted with a red box), and 'IPSec Domain'. Above this list are buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', and 'Delete Profile'. The right pane shows the configuration for the 'NWK-Domain' profile, featuring a table for 'Topology Hiding' settings.

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

An 'Edit' button is located below the table.

### 7.11.1. Topology Hiding: Session Manager

For the compliance test, the topology hiding profile **NWK-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 (**sip.avaya.com**).

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

### 7.11.2. Topology Hiding: EarthLink

For the compliance test, the topology hiding profile **SP-General** was created for EarthLink. 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.

Topology Hiding

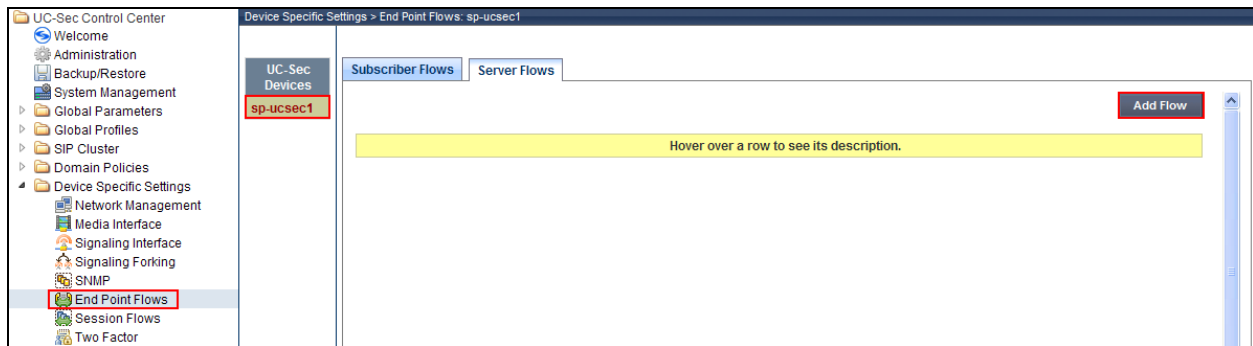
Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
To	IP/Domain	Auto	---

Edit

## 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 Flow** button. 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 far right pane.



### 7.12.1. End Point Flow: Session Manager

For the compliance test, the end point flow **NWK-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** (this setting is displayed as the flow heading in the screen shown below).
- 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 EarthLink SIP server.
- Set **Topology Hiding Profile** to the topology hiding profile defined for Session Manager in **Section 7.11.1**.

Subscriber Flows												
Server Flows												
Server Configuration: NWK-SM												
Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile	
1	NWK-SM	*	*	*	Ext_Sig_Intf	Int_Sig_Intf	Int_Media_Intf	SM	To_Trunks	NWK-Domain	None	  



## 7.12.2. End Point Flow: EarthLink




For the compliance test, the end point flow **SP-EarthLink** was created for the EarthLink SIP server. All traffic from EarthLink will match this flow as the source flow and use the specified **Routing Profile** “To\_NwkSM” 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 service provider SIP server created in **Section 7.6.2** (this setting is displayed as the flow heading in the screen shown below).
- 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 EarthLink 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 EarthLink in **Section 7.11.2**.

Subscriber Flows

Server Flows

Server Configuration: SP-EarthLink

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	SP-EarthLink	*	*	*	Int_Sig_Intf	Ext_Sig_Intf	Ext_Media_Intf	General-SP	To_NwkSM	SP-General	None			



## 8. EarthLink SIP Trunking Configuration

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

EarthLink 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. EarthLink will provide the customer with the necessary information to configure the SIP connection from enterprise to the EarthLink network. The information provided by EarthLink 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).
- EarthLink SIP domain. In the compliance test, EarthLink preferred to use IP address as URI-Host.
- CPE SIP domain. In the compliance testing, EarthLink preferred to use IP address of the Avaya SBCE as URI-Host.
- Supported codecs and order of preference.
- DID numbers.

The sample configuration between EarthLink and the enterprise for the compliance test is a static configuration. There is no registration on the SIP trunk implemented on either EarthLink 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** – 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 11:37 AM

2 Items

Refresh

Show ALL ▾

Filter: Enable

Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	Version
<a href="#">nw-sm</a>	Core	0/0/0		Up	Accept New Service	3/10	0	1/1		6.2.4.0.62
<a href="#">nw-sm</a>	Core	0/0/0		Up	Accept New Service	3/10	0	1/1		6.2.4.0.62

Select : All, None

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

## 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 report 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 R6.2, Avaya Aura® Session Manager R6.2 and Avaya Session Border Controller for Enterprise R4.0.5 to EarthLink SIP Trunking service. EarthLink SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. EarthLink 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® Solution for Midsize Enterprise**

- [1] *Avaya Aura® Solution for the Midsize Enterprise (ME) 6.2 Intelligent Workbook*, Workbook Version 2.2, November 2012
- [2] *Implementing Avaya Aura® Solution for Midsize Enterprise*, Release 6.2, July 2012

### **Avaya Aura® Session Manager/System Manager**

- [3] *Administering Avaya Aura® Session Manager*, Document ID 03-603324, Release 6.2, July 2012
- [4] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Doc ID 03-603325, Release 6.2, August 2012
- [5] *Administering Avaya Aura® System Manager*, Release 6.2, July 2012

### **Avaya Aura® Communication Manager**

- [6] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509, Release 6.2, December 2012
- [7] *Programming Call Vectoring Features in Avaya Aura® Call Center Elite*, Release 6.2, December 2012

### **Avaya one-X™ IP Phones**

- [8] *Avaya one-X™ Deskphone SIP for 9601 IP Telephone User Guide*, Document ID 16-603618, Issue 1, December 2010
- [9] *Avaya one-X™ Deskphone SIP 9621G/9641G User Guide for 9600 Series IP Telephones*, Document ID 16-603596, Issue 1, May 2011
- [10] *Avaya one-X™ Deskphone H.323 9608 and 9611G User Guide*, Document ID 16-603593, Issue 3, February 2012
- [11] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Document ID 16-601944, Release 2.6, June 2010
- [12] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Document ID 16-300698, Release 3.1, November 2009
- [13] *Administering Avaya one-X® Communicator*, October 2011
- [14] *Using Avaya one-X® Communicator Release 6.1*, October 2011

### **Avaya Session Border Controller for Enterprise**

- [1] *Sipera Systems E-SBC 1U Installation Guide*, Release 4.0.5, November 2011
- [2] *Sipera Systems E-SBC Administration Guide*, Release 4.0.5, November 2011

---

**©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](mailto:devconnect@avaya.com).