



# **Configuring OneStream Networks' Global SIP Trunking with Avaya Aura® Communication Manager Evolution Server Release 6.2, Avaya Aura® Session Manager Release 6.2, and Avaya Session Border Controller for Enterprise Release 4.0.5 – Issue 1.0**

## **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between OneStream Networks' Global SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller For Enterprise 4.0.5 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Manager or Avaya Session Border Controller for Enterprise.

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

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing .....	4
2.2.	Test Results .....	5
2.3.	Support.....	7
3.	Reference Configuration .....	8
4.	Equipment and Software Validated .....	10
5.	Configure Avaya Aura® Communication Manager .....	11
5.1.	Licensing and Capacity .....	11
5.2.	System Features .....	12
5.3.	IP Node Names .....	13
5.4.	Codecs.....	13
5.5.	IP Network Region .....	14
	Signaling Group .....	16
5.6.	16	
5.7.	Trunk Group.....	17
5.8.	Calling Party Information .....	20
5.9.	Outbound Routing.....	21
5.10.	Saving Communication Manager Configuration Changes .....	23
6.	Configure Avaya Aura® Session Manager .....	24
6.1.	System Manager Login and Navigation .....	25
6.2.	Specify SIP Domain.....	26
6.3.	Add Location .....	27
6.4.	Add Adaptation Module .....	27
6.5.	Add SIP Entities.....	29
6.6.	Add Entity Links.....	32
6.7.	Add Routing Policies .....	33
6.8.	Add Dial Patterns.....	34
6.9.	Administer Application for Communication Manager .....	37
6.10.	Administer Application Sequence for Communication Manager.....	37
6.11.	Administer SIP Extensions .....	38
7.	Configure Avaya Session Border Controller for Enterprise .....	42
7.1.	Avaya Session Border Controller for Enterprise Login.....	43
7.2.	Global Profiles .....	45
7.2.1.	Routing Profiles .....	45
7.2.2.	Topology Hiding .....	47
7.2.3.	Server Interworking .....	50
7.2.4.	Signaling Manipulation.....	54
7.2.5.	Server Configuration.....	55
7.3.	Domain Policies .....	60
7.3.1.	Application Rules.....	60
7.3.2.	Media Rules .....	62
7.3.3.	Signaling Rules .....	64
7.3.4.	Endpoint Policy Groups .....	66

7.4.	Device Specific Settings .....	67
7.4.1.	Network Management.....	68
7.4.2.	Media Interface .....	68
7.4.3.	Signaling Interface .....	69
7.4.4.	End Point Flows - Server Flow .....	70
8.	OneStream Networks' Global SIP Trunking Configuration.....	72
9.	Verification and Troubleshooting .....	73
10.	Conclusion .....	76
11.	References .....	77

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between OneStream Networks' Global SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.2, Avaya Aura® Communication Manager 6.2 configured as an Evolution Server, Avaya SBC for Enterprise (Avaya SBCE) and various Avaya endpoints. This documented solution does not extend to configurations without Session Manager or Avaya SBCE.

Enterprise customers with an Avaya SIP-enabled solution can communicate with OneStream Networks' Global SIP Infrastructure over the public Internet, the private OneStream Networks MPLS network or via a third-party MPLS provider and access the PSTN by subscribing to OneStream Networks Global SIP Trunking.

OneStream Networks' Global SIP Trunking service helps businesses maximize their investment in their Avaya IP Telephony infrastructure by delivering reliable, scalable and cost-effective connections that provide global consolidation, redundancy and simplified management of voice traffic.

## 2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the OneStream Networks' Global SIP Trunking service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and Avaya SBCE.

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

### 2.1. Interoperability Compliance Testing

A simulated enterprise site comprised of 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 the OneStream Networks' Global SIP Trunking service Vendor Validation circuit through the public Internet.

**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 various phone types.

- Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types.
- Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phones.
- Various call types included: local, long distance, international, outbound toll-free, operator assisted calls, local directory assistance (411), etc.
- G.729A Codec, G.711A Codec and G.711MU Codec and proper codec negotiation.
- DTMF tone transmissions passed as out-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- Incoming and Outgoing fax over IP with t.38, G.711 Codec and G.729A Codec.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding with SIP Diversion method.
- EC500 mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues via vectors.
- Network Call Redirection using reINVITE for transfer of inbound call back to PSTN.
- Response to incomplete call attempts and trunk errors
- Session Timers implementation from both ends of enterprise and service provider.

**Items not supported by OneStream Networks or not tested as part of the compliance testing are listed as follows:**

- Inbound toll-free and outbound emergency calls (911) are supported but were not tested as part of the compliance testing.
- Vector call redirection before answering using “302 Moved Temporarily” method is not supported.
- Avaya one-X® Communicator Road Warrior with SIP is supported but was not tested as part of the compliance test.

## **2.2. Test Results**

The general test approach was to configure a simulated enterprise site using Communication Manager, Session Manager and Avaya SBCE to connect to the OneStream Networks’ Global SIP Trunking service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

Interoperability testing of OneStream Networks’ Global SIP Trunking service with the Avaya SIP-enabled enterprise solution was completed with successful results with the exception of the observations/limitations described below.

**01. Off-net blind transfer by a SIP phone:** Communication Manager SIP phone off-net blind transfers an inbound call back to PSTN. When Communication Manager sends REFER to complete the transfer after 200 OK received on the 2<sup>nd</sup> leg, the calling PSTN party does not hear the ring back tone. This issue is corrected by turning off the **Network Call Redirection** flag on outgoing trunk group setting, then Communication Manager successfully transferred the call with **reINVITE** method. Please refer to **Section 5.7** for configuration.

**02. Off-net blind transfer by one-X® Communicator SIP soft phone:** Communication Manager one-X® Communicator SIP soft phone off-net blind transfers an inbound call back to PSTN. When Communication Manager sends REFER to complete the transferring, OneStream Networks responds 404 Not Found. The transfer fails. This issue is corrected by turning off the **Network Call Redirection** flag on trunk group setting, then Communication Manager successfully transferred the call with **reINVITE** method. Please refer to **Section 5.7** for configuration.

**03. Network Call Redirection with “302 Moved Temporarily”:** A vector DN on Communication Manager is programmed to redirect an inbound call to PSTN before answering. When Communication Manager sends a “302 Moved Temporarily” SIP message to redirect the call, OneStream Networks responds with an ACK. However, the call is not redirected to the new PSTN party in the Contact header of the 302 message due to OneStream Networks not handling the 302 properly. There is no resolution currently available.

**04. No matching codec:** If the codec does not match any of the codec supported by OneStream Networks in an outbound from enterprise to PSTN, OneStream Networks responds with a “480 Temporary Unavailable”. The call is dropped as expected even when OneStream Networks does not respond with a proper “488 Not Acceptable Here”. This is listed here just simply as an observation.

**06. G.711 Fax over IP:** In inbound/outbound fax call scenarios with codec G.711 between enterprise and PSTN, the SIP call dialog looks identical to a regular G.711 voice call. The fax document is received in acceptable quality. Communication Manager does not officially support G.711 fax. However, incoming and outgoing G.711 fax calls appeared to work during testing when configuring fax = off. Communication Manager handles the call like a regular voice call and only supports G.711 fax in best effort.

**07. SigMa script FixPAI** was created to Update the P-Asserted Identity field with the value of FROM header to replace the unique IP Address received from OneStream Networks that caused the no talk path issue. Please refer to **Section 7.2.4** for configuration.

## 2.3. Support

For technical support on the OneStream Networks' Global SIP Trunking Service, contact OneStream Networks Business Customer Care via Email at [engineering@onestreamnetworks.com](mailto:engineering@onestreamnetworks.com) or by calling 877-877-1220 option 2.

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

### 3. Reference Configuration

**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to the OneStream Networks' Global SIP Trunking service (Vendor Validation circuit) through a public Internet WAN connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance test are masked in these Application Notes.

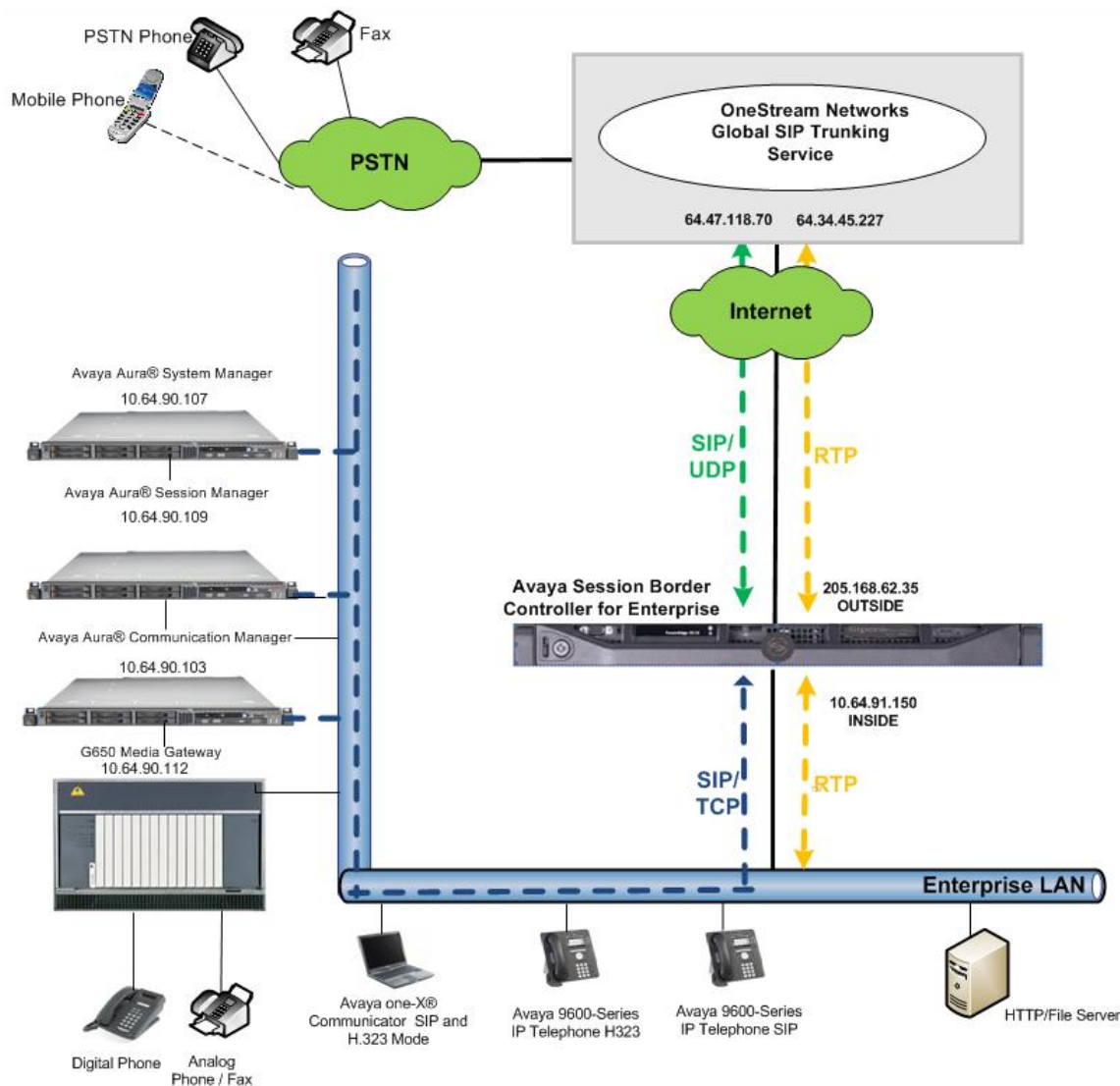
The Avaya components used to create the simulated customer site included:

- Avaya Aura® Communication Manager
- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya SBCE
- Avaya G450 Media Gateway
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator (H.323 and SIP)
- Avaya digital and analog telephones

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

For efficiency, a separate trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any setting or codec selection required by the service provider could be applied only to this trunk and will not affect other enterprise SIP traffic. In addition, this trunk carried both inbound and outbound traffic.





**Figure 1: Avaya IP Telephony Network Connecting to OneStream Networks' Complete Global SIP Trunking**

For inbound calls, the calls flow from the service provider to the 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 features 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. The Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the Avaya SBCE. From the Avaya SBCE, the call is sent to OneStream SIP Trunking.

For the compliance test, the enterprise sent 11 digits in the destination headers (e.g., Request-URI and to) and sent 10 digits in the source headers (e.g., From, Contact, and P-Asserted-Identity (PAI)) of the SIP messaging. OneStream sent 10 digits in both the source and destination headers.

## 4. Equipment and Software Validated

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

<b>Avaya IP Telephony Solution Components</b>	
Component	Release
Avaya Aura® System Manager	6.2.0 SP3 (Build 6.2.0.0.15669-6.2.12.307) (Software Update Revision 6.2.14.1.1959)
Avaya Aura® Session Manager	6.2.3.0.623006 (Build 6.2.0.0.15669-6.2.12.307) (Software Update Revision 6.2.14.1.1959)
Avaya Aura® Communication Manager	6.02.2.823.0
Avaya G450 Media Gateway	3.1.20.1
Avaya Session Border Controller for Enterprise	4.0.5 Q19
Avaya 9630G IP Telephone (H.323) running Avaya one-X® Deskphone Edition	R6_2_2_09-071012
Avaya 9641G IP Telephone (H.323) running Avaya one-X® Deskphone Edition	R6_2_2_09-071012
Avaya 9620 IP Telephone (SIP) running Avaya one-X® Deskphone SIP Edition	R6_2_0_082012
Avaya 96XX IP Telephone (SIP) running Avaya one-X® Deskphone SIP Edition	R6_2_0_082012
Avaya one-X® Communicator (H.323 or SIP)	6.1.3.08 (SP3-Patch2-35791)
Avaya 1408 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
<b>OneStream Networks' Global SIP Trunking Solution Components</b>	
Component	Release
Genband S3 Session Border Controller (SBC)	Release 8.0.3.

**Table 1: Equipment and Software Tested**

The specific equipment and software 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 OneStream Complete SIP Trunking. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from OneStream. 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 Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged for brevity and clarity in presentation. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements and public PSTN numbers are not revealed.

### 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** SIP trunks are available and **265** 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.

<b>display system-parameters customer-options</b>		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	1	
	<b>Maximum Administered SIP Trunks:</b>	<b>12000</b>	<b>265</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	1	
	Maximum TN2602 Boards with 80 VoIP Channels:	128	0	
	Maximum TN2602 Boards with 320 VoIP Channels:	128	0	

## 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 defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **Anonymous** for both.

```
display 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 of the server running Communication Manager (**procr**) and for Session Manager (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

change node-names ip		Page	1 of	2
		IP NODE NAMES		
Name	IP Address			
ACME	10.64.91.115			
GW	10.64.90.112			
SBCE-3	10.64.91.150			
SBCE-DT	10.64.19.100			
SM	10.64.90.109			
default	0.0.0.0			
procr	10.64.90.103	IP Address		
ACME	10.64.91.115			

### 5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. OneStream Networks' Global SIP Trunking service supports G.729A, and G.711MU. Enter the codec to be used in priority order in the **Audio Codec** column of the table. Default values can be used for all other fields. The following screen shows the codec set configuration at a certain time of the compliance test. During testing, the codec set specifications are varied to test for individual codec support as well as codec negotiation between the enterprise and the network at call setup time.

change ip-codec-set 2

Page 1 of 2

IP Codec Set

Codec Set: 2

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1:	G.711MU	n	2	20
2:	G.729A	n	2	20
3:				
4:				
5:				

On **Page 2**, set the **FAX Mode** to **t.38-standard**.

change ip-codec-set 2		Page 2 of 2
IP Codec Set		
Allow Direct-IP Multimedia? n		
	<b>Mode</b>	<b>Redundancy</b>
<b>FAX</b>	<b>t.38-standand</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 groups. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, **ip-network-region 2** was created for the service provider trunks. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

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

```

change ip-network-region 2                                     Page 1 of 20

                                IP NETWORK REGION

Region: 2
Location: 1      Authoritative Domain: avayalab.com
Name: SIP Trunks
MEDIA PARAMETERS
  Codec Set: 2      Intra-region IP-IP Direct Audio: yes
                   Inter-region IP-IP Direct Audio: yes
                   UDP Port Min: 16384      IP Audio Hairpinning? n
                   UDP Port Max: 40001
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 1 and region 2. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 2. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 2 will automatically create a complementary table entry on the IP network region 1 form for destination region 2. This complementary table entry can be viewed using the **display ip-network-region 2** command and navigating to **Page 4** (not shown).

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

Non-IP telephones (e.g., analog, digital) derive network region from the Avaya gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping. The following screen illustrates a subset of the IP network map configuration used to verify these Application Notes.

For the compliance test, devices with IP addresses in the 10.64.90.0/24 subnet are assigned to network region 1. These include Communication Manager, Session Manager and Avaya SBCE that were set up for shared test environment. IP telephones used for the compliance test, including both the Avaya 9600 IP Telephones and the Avaya one-X® Communicator soft

phones, are assigned to network region 1 with IP address in the 10.64.90.0/24 subnet. In production environments, different sites will typically be on different networks, and ranges of IP addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

change ip-network-map

Page 1 of 63

IP ADDRESS MAPPING

IP Address	Subnet Bits	Network Region	VLAN	Emergency Location	Ext
FROM: 10.64.90.50	/	1	n		
TO: 10.64.90.99					
FROM:	/		n		
TO:					
FROM:	/		n		
TO:					
FROM:	/		n		

## 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 1 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the recommended default value of **tcp**. For ease of troubleshooting during testing, part of the compliance test was conducted with the **Transport Method** set to **tcp**. The transport method specified here is used between Communication Manager and Session Manager.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as 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 **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). At the time of Session Manager installation, a SIP connection between Communication Manager and Session Manager would have been established for use by all Communication Manager SIP traffic using the well-known port value for TLS or TCP. By creating a new signaling group with a separate port value, a separate SIP connection is created between Communication Manager and Session



Manager for SIP traffic to the service provider. As a result, any signaling group or trunk group settings (**Section 5.7**) will only affect the service provider traffic and not other SIP traffic at the enterprise. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5060**.

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to **6**. This defines the number of seconds that Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

<b>add signaling-group 1</b>		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: <b>sip</b>	
IMS Enabled? <b>n</b>	Transport Method: <b>tcp</b>	
Q-SIP? <b>n</b>		
IP Video? <b>n</b>	Enforce SIPS URI for SRTP? <b>y</b>	
Peer Detection Enabled? <b>n</b>	Peer Server: Others	
Near-end Node Name: <b>procr</b>	Far-end Node Name: <b>SM</b>	
Near-end Listen Port: <b>5060</b>	Far-end Listen Port: <b>5060</b>	
	Far-end Network Region: <b>2</b>	
Far-end Domain: <b>avayalab.com</b>		
Incoming Dialog Loopbacks: <b>eliminate</b>	Bypass If IP Threshold Exceeded? <b>n</b>	
DTMF over IP: <b>rtp-payload</b>	RFC 3389 Comfort Noise? <b>n</b>	
Session Establishment Timer(min): <b>3</b>	Direct IP-IP Audio Connections? <b>y</b>	
Enable Layer 3 Test? <b>y</b>	IP Audio Hairpinning? <b>n</b>	
H.323 Station Outgoing Direct Media? <b>n</b>	Initial IP-IP Direct Media? <b>n</b>	
	Alternate Route Timer(sec): <b>6</b>	

## 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 1 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 shown in the previous step.
- 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 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: SIP Trunk to SP	COR: 1	TN: 1	TAC: *01
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 1	
		Number of Members: 10	

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value equal to the **Alternate Route Timer** on the signaling group form described in **Section 5.6**.

Verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **900** seconds was used.

Add trunk-group 1	Page 2 of 21
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
	Redirect On OPTIM Failure: 6000
SCCAN? n	Digital Loss Group: 18
	Preferred Minimum Session Refresh Interval(sec): 900
Disconnect Supervision - In? y Out? y	

On **Page 3**, set the **Numbering Format** field to **public**. Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

<b>add trunk-group 1</b>		<b>Page 3 of 21</b>
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
<b>Numbering Format: public</b>		
UI Treatment: service-provider		
<b>Replace Restricted Numbers? y</b>		
<b>Replace Unavailable Numbers? y</b>		
Modify Tandem Calling Number: no		

On **Page 4**, set the **Network Call Redirection** field to **y**. This setting enables the use of the SIP REFER message to transfer an incoming call to a vector number back to PSTN. Notes: the same outgoing trunk group in the later discussion will also have **Network Call Redirection** set to **y**, this setting is to use reINVITE to off-net transfer an incoming call back to PSTN. For more information, please refer to **Section 2.2**, observation 03.

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 some Extension to Cellular (EC500) call scenarios.

Set the **Support Request History** field to **y**. This parameter determines whether the SIP History-Info header will be included in the call-redirection INVITE from the enterprise.

Set the **Telephone Event Payload Type** to **101**, the value preferred by OneStream Networks. Set the **Convert 180 to 183 for Early Media** field to **y**.

Set the **Always Use re-INVITE for Display Updates** field to **y**. In SIP messages this field allows Communication Manager to send re-invite message to display update. The default value is n.

Set the **Identity for Calling Party Display** field to **P-Asserted-Identity**. This parameter determines which header to retrieve display information for the calling party when the From and

the P-Asserted Identity headers are available. The system displays this field, when the **Group Type** is SIP. P-Asserted-Identity is the default value.

```

add trunk-group 1
                                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? y
                                Telephone Event Payload Type: 101
                                Shuffling with SDP? n

                                Convert 180 to 183 for Early Media? y
                                Always Use re-INVITE for Display Updates? y
                                Identity for Calling Party Display: P-Asserted-Identity
                                Enable Q-SIP? n

```

## 5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, six DID numbers were assigned for testing. These six numbers were assigned to the six extensions 12001, 12006-12008, and 13001-02. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these six extensions.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
5	1			5	Total Administered: 14
5	2			5	Maximum Entries: 9999
5	3			5	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
5	4			5	
5	5			5	
5	6			5	
5	7			5	
5	8			5	
5	12001	1	5825551080	10	
5	12006	1	5625551085	10	
5	12007	1	5625551081	10	
5	12008	1	5625551082	10	
5	13001	1	5625551083	10	
5	13002	1	5625551084	10	

## 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						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
18	4	ext						
6	1	fac						
8	4	dac						
9	1	fac						
*	4	dac						
#	4	dac						

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

change feature-access-codes			Page 1 of 10	
FEATURE ACCESS CODE (FAC)				
Abbreviated Dialing List1 Access Code: *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				
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>			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:	
:				
Conditional Call Extend Activation:			Deactivation:	
Contact Closure Open Code:			Close Code:	

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 1 for outbound call and for vector call redirection which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all					Percent Full: 0		
	Dialed	Total		Route	Call	Node	ANI
	String	Min	Max	Pattern	Type	Num	Reqd
0		1	1	1	op		n
0		11	11	1	op		n
01		9	17	1	iop		n
011		8	18	1	intl		n
1		11	11	1	fnpa		n
1303		11	11	1	fnpa		n
562		10	10	1	natl		n
1720		11	11	1	fnpa		n
1800		11	11	1	fnpa		n

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

The example below shows the values used for route pattern 1 for outgoing calls.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 1 was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk:** **1** the prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for the long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.

change route-pattern 1													Page 1 of 3				
Pattern Number: 1													Pattern Name: SIP Trunk				
SCCAN? n													Secure SIP? n				
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC			
No			Mrk	Lmt	List	Del	Digits						QSIG				
													Intw				
1:	1	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					none				
2:	y	y	y	y	y	n	n	rest					none				
3:	v	v	v	v	v	n	n	rest					none				

## 5.10. Saving Communication Manager Configuration Changes

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

## 6. Configure Avaya Aura® Session Manager

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

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

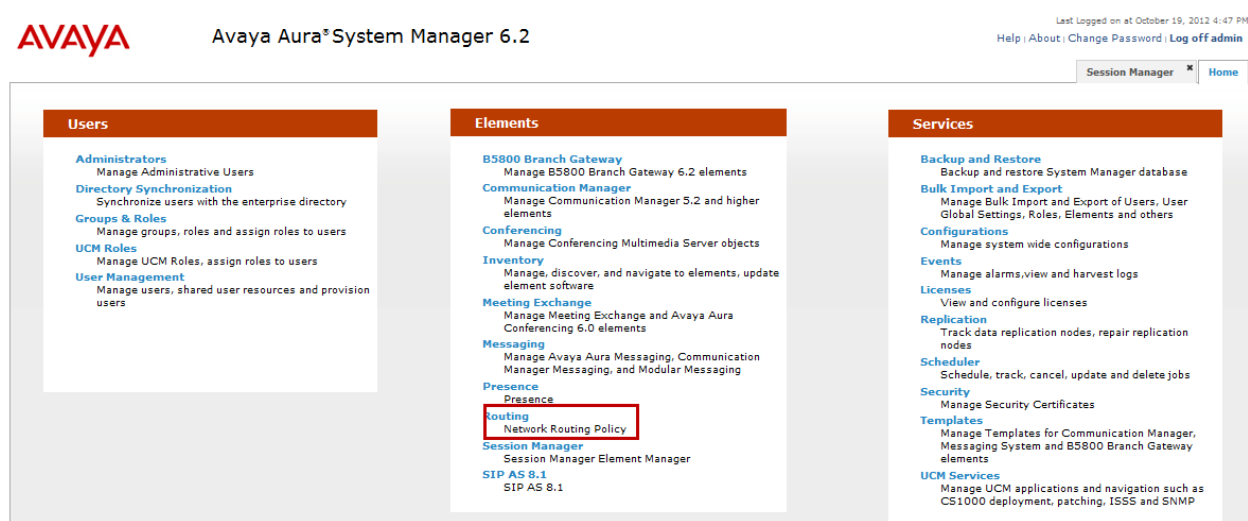
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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



## 6.1. System Manager Login and Navigation

Session Manager Configuration is accomplished by accessing the 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 **Home** page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Elements → Routing** link highlighted below.



Clicking the **Elements → Routing** link, displays the **Introduction to Network Routing Policy** page. The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing

Introduction to Network Routing Policy

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

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

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

## 6.2. Specify SIP Domain

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

The following screen shows the configured SIP domain. The Session Manager used in the verification of these Application Notes was shared among many Avaya interoperability test efforts. The domain **avayalab.com** was already being used for communication among a number of Avaya systems and applications, including an Avaya Aura® Messaging system with SIP integration to Session Manager. The domain **avayalab.com** is not known to the OneStream Networks' Global SIP Trunking service.

For a new domain fill in the following:

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

Click **Commit** (not shown). The screen below shows the entry for the enterprise domain

Home / Elements / Routing / Domains

Domain Management

Edit

New

Duplicate

Delete

More Actions

1 Item | Refresh

Filter: Enable

	Name	Type	Default	Notes
<input type="checkbox"/>	avayalab.com	sip	<input type="checkbox"/>	

## 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).

Click **Commit** to save.

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Locations

Location Details

Help ?

Commit Cancel

General

\* Name: Avaya SBCE-3

Notes: ASBCE-3

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

## 6.4. Add Adaptation Module

No adaptation was used for this compliance test. The mappings of internal extensions to OneStream DID numbers may be done in Session Manager (via Digit Conversion in adaptations) or in Communication Manager (via public-unknown-numbering, and incoming call handling treatment for the inbound trunk group) as set in **Section 5.8**.

The example below is the sample of the generic adaptation module **DigitConversionAdapter**.

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.

To create the adaptation that will be applied to the Communication Manager SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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**.
- **Module parameter:** Enter **fromto=true** to allow the From and To headers to be included in the digit conversion (i.e., in addition to other headers such as the P-Asserted-Identity and Request-URI headers).

The adaptation sample above can be applied to the Communication Manager SIP entity that supports digit conversion of telephone numbers in specific headers of SIP messages.

To map inbound DID numbers from OneStream to Communication Manager extensions in Session Manager, 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** since this digit conversion only applies to the destination number.

Click **Commit** to save.

#### Digit Conversion for Outgoing Calls from SM

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 5622961082	* 10	* 10		* 10	12008	destination		

Select : All, None

\* Input Required


## 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 the Avaya SBCE. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown).

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

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

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



Avaya Aura® System Manager 6.2

Last Logged on at December 21, 2012 11:51 AM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#)

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

Home / Elements / Routing / SIP Entities

**SIP Entity Details**

**General**

\* Name:

\* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

**SIP Link Monitoring**

SIP Link Monitoring:

[Help ?](#)

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 to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

The compliance test used **Port** entry **5060** with **UDP/TCP** and port **5061** for **TLS** for connecting to Communication Manager and Avaya SBCE.

**Port**

TCP Failover port:

TLS Failover port:

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avayaab.com	
<input type="checkbox"/>	5061	TLS	avayaab.com	

Select : All, None

The following screen shows the addition of 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. The **FQDN or IP Address** field is set to the IP address of Communication Manager. Select **Type** is **CM**. For the **Adaptation** field, select the adaptation module if **Adaptation** was previously defined for dial plan digit manipulation in **Section 6.4**. The **Location** field is set to **Location\_1** which is the location defined for the subnet where Communication Manager resides.

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

[Routing](#) \* [Home](#)

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit

Cancel

Help ?

General

\* Name:

CM62\_tg1

\* FQDN or IP Address:

10.64.90.103

Type:

CM

Notes:

CM62

Adaptation:

Location:

Location\_1

Time Zone:

America/Denver

Override Port & Transport with DNS SRV:

☐

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

4

Credential name:

Call Detail Recording:

none

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

The following screen shows the addition of the Avaya SBCE SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). **Link Monitoring Disabled** was selected for **SIP Link Monitoring**. If **Link Monitoring is Enabled** then the time settings should be adjusted or left at their default values per customer needs and requirements.

[Routing](#) x [Home](#)

Home / Elements / Routing / SIP Entities

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

SIP Entity Details

General

Name: ASBCE-3

FQDN or IP Address: 10.64.91.150

Type: SIP Trunk

Notes:

Adaptation:

Location: Avaya SBCE-3

Time Zone: America/Denver

Override Port & Transport with DNS SRV:

SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Disabled

Proactive Monitoring Interval (in seconds): 900

Reactive Monitoring Interval (in seconds): 120

Number of Retries: 1

Supports Call Admission Control:

Shared Bandwidth Manager:

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

[Help ?](#)
[Commit](#)
[Cancel](#)

## 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 one to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **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 system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.5**. For Avaya SBCE, select the Avaya SBCE SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the 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. Notes: 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. For the compliance test, TCP was 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:

The screenshot shows the Avaya Aura System Manager 6.2 interface. The left navigation pane is expanded to 'Routing' > 'Entity Links'. The main content area shows the 'Entity Links' configuration page. At the top, there is a breadcrumb 'Home / Elements / Routing / Entity Links' and a 'Help ?' link. Below this, there are 'Commit' and 'Cancel' buttons. A table with the following columns is displayed: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The table contains one item: Name: \*ASM62\_CM62\_tg1\_50, SIP Entity 1: \*ASM62, Protocol: TCP, Port: \*5060, SIP Entity 2: \*CM62\_tg1, Port: \*5060, Connection Policy: Trusted, Notes: . Below the table, there is a red asterisk and the text '\* Input Required', followed by 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
*ASM62_CM62_tg1_50	*ASM62	TCP	*5060	*CM62_tg1	*5060	Trusted	

### Entity Link to Avaya SBCE:

The screenshot shows the Avaya Aura System Manager 6.2 interface. The left navigation pane is expanded to 'Routing' > 'Entity Links'. The main content area shows the 'Entity Links' configuration page. At the top, there is a breadcrumb 'Home / Elements / Routing / Entity Links' and a 'Help ?' link. Below this, there are 'Commit' and 'Cancel' buttons. A table with the following columns is displayed: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The table contains one item: Name: \*ASM62\_ASBCE-3\_506, SIP Entity 1: \*ASM62, Protocol: TCP, Port: \*5060, SIP Entity 2: \*ASBCE-3, Port: \*5060, Connection Policy: Trusted, Notes: . Below the table, there is a red asterisk and the text '\* Input Required', followed by 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
*ASM62_ASBCE-3_506	*ASM62	TCP	*5060	*ASBCE-3	*5060	Trusted	

## 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 one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

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

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

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

The following screens show the Routing Policies **CM62\_tg1** for Communication Manager.

Avaya Aura® System Manager 6.2

Last Logged on at December 10, 2012 1:10 PM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

**Routing** x **Home**

Home / Elements / Routing / Routing Policies

**Routing Policy Details** [Help ?](#)

**General**

\* **Name:** To CM62\_tg1

**Disabled:** ☐

\* **Retries:** 0

**Notes:** CM TRK 1

**SIP Entity as Destination**

[Select](#)

Name	FQDN or IP Address	Type	Notes
CM62_tg1	10.64.90.103	CM	CM62

The following screens show the Routing Policies for Avaya SBCE.

Avaya Aura® System Manager 6.2

Last Logged on at December 10, 2012 1:10 PM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

**Routing** x **Home**

Home / Elements / Routing / Routing Policies

**Routing Policy Details** [Help ?](#)

**General**

\* **Name:** TO\_ASBCE-3

**Disabled:** ☐

\* **Retries:** 0

**Notes:**

**SIP Entity as Destination**

[Select](#)

Name	FQDN or IP Address	Type	Notes
ASBCE-3	10.64.91.150	SIP Trunk	

## 6.8. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to OneStream

Networks and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **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., 011 international calls, 411 directory assistance calls, etc.,) were similarly defined.

The first example shows that numbers that begin with **1** and have a destination domain of **ALL** from **Locations\_1** use route policy **To\_AS BCE-3**.

[Routing](#) \* [Home](#)

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](#)

<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"/>	Location_1		TO_ASBC-3	0	<input type="checkbox"/>	ASBC-3	

The second example shows that 10 digit numbers that start with **562** to domain **ALL** and originating from **Location\_1** and **ASBC-3** use route policy **CM62\_tg1** and **TO\_ASBC-3**. These are the DID numbers assigned to the enterprise from OneStream.

[Routing](#) \* [Home](#)

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](#)  
2 Items [Refresh](#)

<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"/>	Avaya SBCE-3	ASBC-3	To CM62_tg1	0	<input type="checkbox"/>	CM62_tg1	CM TRK 1
<input type="checkbox"/>	Location_1		TO_ASBC-3	0	<input type="checkbox"/>	ASBC-3	

The complete list of dial patterns defined for the compliance test is shown below.

Home / Elements / Routing / Dial Patterns

Help ?

Dial Patterns

EditNewDuplicateDeleteMore Actions ▾

7 Items Refresh

Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	011	10	15	<input type="checkbox"/>			-ALL-	International
<input type="checkbox"/>	1	5	5	<input type="checkbox"/>			-ALL-	VM 5 digits ext
<input type="checkbox"/>	1	11	11	<input type="checkbox"/>			-ALL-	Nation Wide 11 digits
<input type="checkbox"/>	11000	5	5	<input type="checkbox"/>			avaya@b.com	To VM
<input type="checkbox"/>	303	10	10	<input type="checkbox"/>			-ALL-	10 digits 303
<input type="checkbox"/>	411	3	3	<input type="checkbox"/>			-ALL-	Directory Assistance
<input type="checkbox"/>	562	10	10	<input type="checkbox"/>			-ALL-	OneStream DID

Select : All, None

## 6.9. Administer Application for Communication Manager

From the **Home** tab select **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration** → **Applications** and click **New** (not shown).

- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Communication Manager
- In the **CM System for SIP Entity** field select the SIP entity for the Communication Manager and select **Commit** to save the configuration.

Home / Elements / Session Manager / Application Configuration / Applications Help ?

**Application Editor** Commit Cancel

---

Application

\*Name

\*SIP Entity

\*CM System for SIP Entity  Refresh [View/Add CM Systems](#)

Description

## 6.10. Administer Application Sequence for Communication Manager

From the left panel navigate to **Session Manager** → **Application Configuration** → **Application Sequences** and click on **New** (not shown).

- In the **Name** field enter a descriptive name
- Under **Available Applications**, click the + sign (not shown) in front of the appropriate application instance. When the screen refreshes the application should be displayed under the **Applications in this Sequence** heading. Select **Commit**.

**Application Sequence Editor** 

## Application Sequence

\*Name

Description

## Applications in this Sequence




1 Item					
<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		<a href="#">Application to SIP TRK</a>	CM62_tg3	<input checked="" type="checkbox"/>	application to SIP TRK 3
Select : All, None					

## 6.11. Administer SIP Extensions

SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the **Home** tab select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of user@domain (e.g. 13001@avayalab.com) which is used to create the user's primary handle
- The **Authentication Type** should be **Basic**
- In the **Password/Confirm Password** fields enter an alphanumeric password

Identity *	Communication Profile *	Membership	Contacts
<b>Identity</b> ▼			
* <b>Last Name:</b> <input type="text" value="SIP CM62"/>			
* <b>First Name:</b> <input type="text" value="13001"/>			
<b>Middle Name:</b> <input type="text"/>			
<b>Description:</b> <input type="text"/>			
<b>Status:</b> <input type="text" value="Offline"/>			
<b>Update Time :</b> <input type="text" value="October 10, 2012 12:22"/>			
* <b>Login Name:</b> <input type="text" value="13001@avayalab.com"/>			
* <b>Authentication Type:</b> <input type="text" value="Basic"/>			
<a href="#">Change Password</a>			
<b>Source:</b> <input type="text" value="local"/>			
<b>Localized Display Name:</b> <input type="text" value="SIP CM62, 13001"/>			
<b>Endpoint Display Name:</b> <input type="text" value="SIP CM62, 13001"/>			
<b>Title:</b> <input type="text"/>			
<b>Language Preference:</b> <input type="text" value="English (United States)"/>			

On the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it, then expand the **Communication Address** section and click **New**. For the **Type** field select **Avaya SIP** from the drop-down menu (not shown). In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button (not shown).

Identity *	Communication Profile *	Membership	Contacts						
<b>Communication Profile</b> ▼									
<b>Communication Profile Password:</b> <input type="password" value="....."/> <a href="#">Edit</a>									
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Done"/> <input type="button" value="Cancel"/>									
<table border="1"> <thead> <tr> <th>Name</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/> Primary</td> </tr> </tbody> </table>				Name	<input checked="" type="radio"/> Primary				
Name									
<input checked="" type="radio"/> Primary									
Select : None									
* <b>Name:</b> <input type="text" value="Primary"/>									
<b>Default :</b> <input checked="" type="checkbox"/>									
<b>Communication Address</b> ▼									
<input type="button" value="New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>									
<table border="1"> <thead> <tr> <th>Type</th> <th>Handle</th> <th>Domain</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Avaya SIP</td> <td>13001</td> <td>avayalab.com</td> </tr> </tbody> </table>				Type	Handle	Domain	<input type="checkbox"/> Avaya SIP	13001	avayalab.com
Type	Handle	Domain							
<input type="checkbox"/> Avaya SIP	13001	avayalab.com							
Select : All, None									

Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** check box is checked
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field
- Select the appropriate application sequence from the drop-down menu in the **Origination Application Sequence** field configured in **Section 6.10**
- Select the appropriate application sequence from the drop-down menu in the **Termination Application Sequence** field configured in **Section 6.10**
- Select the appropriate location from the drop-down menu in the **Home Location** field

☒ **Session Manager Profile** ▼


<b>* Primary Session Manager</b>	ASM62 ▼	<table border="1"> <thead> <tr> <th>Primary</th> <th>Secondary</th> <th>Maximum</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>0</td> <td>2</td> </tr> </tbody> </table>	Primary	Secondary	Maximum	2	0	2
Primary	Secondary	Maximum						
2	0	2						
<b>Secondary Session Manager</b>	(None) ▼	<table border="1"> <thead> <tr> <th>Primary</th> <th>Secondary</th> <th>Maximum</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Primary	Secondary	Maximum			
Primary	Secondary	Maximum						
<b>Origination Application Sequence</b>	App_to_CM62 ▼							
<b>Termination Application Sequence</b>	App_to_CM62 ▼							
<b>Conference Factory Set</b>	(None) ▼							
<b>Survivability Server</b>	(None) ▼							
<b>* Home Location</b>	Location_1 ▼							



Expand the **CM Endpoint Profile** section.

- Select the Communication Manager SIP Entity from the **System** drop-down menu
- Select **Endpoint** from the drop-down menu for **Profile Type**
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- For the **Port** field select **IP** (not shown)
- Check the **Override Endpoint Name** box
- Select **Commit** (Not Shown) to save changes and the System Manager will add the Communication Manager user configuration automatically

---

☒ **CM Endpoint Profile** 

\* **System**

\* **Profile Type**

**Use Existing Endpoints** ☐

\* **Extension**

**Template**

**Set Type**

**Security Code**

\* **Port**

**Voice Mail Number**

**Preferred Handle**

**Delete Endpoint on Unassign of Endpoint from User or on Delete User.** ☐

**Override Endpoint Name** ☒

## 7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya Session Border Controller for Enterprise (Avaya SBCE). It is assumed that the software has already been installed. For additional information on these configuration tasks, see **Reference** [11] and [12].

This compliance test comprised the configuration for two major components, trunk server for service provider and call server for enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings, the configuration is defined in the Avaya SBCE web user interface as described in the following sections.

### Trunk server configuration elements for service provider OneStream Networks:

- Global Profiles:
  - o URI Groups
  - o Routing
  - o Topology Hiding
  - o Server Interworking
  - o Signaling Manipulation
  - o Server Configuration
- Domain Policies
  - o Application Rules
  - o Media Rules
  - o Signaling Rules
  - o Endpoint Policy Group
  - o Session Policy
- Device Specific Settings:
  - o Network Management
  - o Media Interface
  - o Signaling Interface
  - o End Point Flows → Server Flows
  - o Session Flows

### Call server configuration elements for enterprise Session Manager:

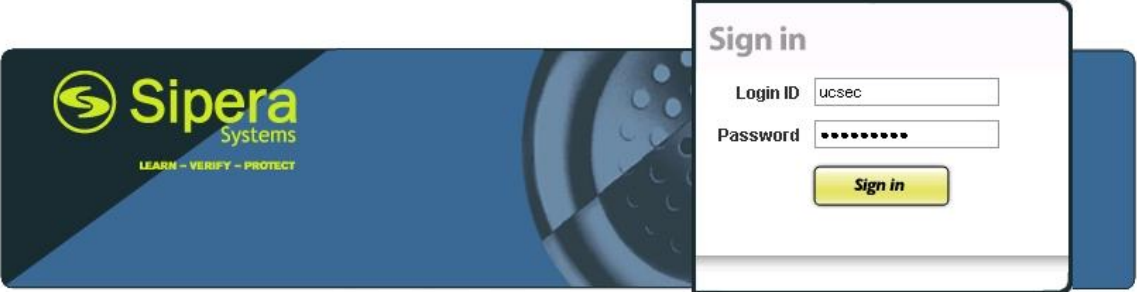
- Global Profiles:
  - o URI Groups
  - o Routing
  - o Topology Hiding
  - o Server Interworking
  - o Server Configuration
- Domain Policies
  - o Application Rules.
  - o Media Rules
  - o Signaling Rules
  - o Endpoint Policy Group
  - o Session Policy

- Device Specific Settings:
  - o Network Management
  - o Media Interface
  - o Signaling Interface
  - o End Point Flows → Server Flows
  - o Session Flows

## 7.1. Avaya Session Border Controller for Enterprise Login

Use a Web browser to access the Unify Communication Security (UC-Sec) web interface, enter `https://<ip-addr>/ucsec` in the address field of the web browser, where <ip-addr> is the management LAN IP address of UC-Sec.

Log in with appropriate credentials. Click **Sign In**.



The UC-Sec™ family of products from Siper Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

[Visit the Siper Systems website to learn more.](#)

**NOTICE TO USERS:** This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

The main page of the **UC-Sec Control Center** will appear.

**UC-Sec Control Center**  
Welcome ucsec, you signed in as Admin. Current server time is 1:25:08 PM GMT

**Securing your real-time unified communications**

A comprehensive IP Communications Security product, the Sipera UC-Sec offers a complete suite of security, enablement and compliance features for protecting and deploying unified communications such as Voice-over-IP (VoIP), instant messaging (IM), multimedia, and collaboration applications.

If you need support, please call our toll free number at (866) 861-3113 or e-mail [support@sipera.com](mailto:support@sipera.com).

Alarms (Past 24 Hours)	Incidents (Past 24 Hours)
None found.	ASBCE-3: No Subscriber Flow Matched
	ASBCE-3: No Subscriber Flow Matched
	ASBCE-3: No Subscriber Flow Matched
	ASBCE-3: No Subscriber Flow Matched
	ASBCE-3: No Subscriber Flow Matched

Administrator Notes	
No notes posted.	

**Quick Links**

- Sipera Website
- Sipera VIPER Labs
- Contact Support

UC-Sec Devices	Network Type
ASBCE-3	DMZ_ONLY

To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **sipera** is shown. To view the configuration of this device, click the **View Config** icon (the third icon from the right).

**UC-Sec Control Center**  
Welcome ucsec, you signed in as Admin. Current server time is 1:27:05 PM GMT

**System Management**

**Installed** **Updates**

Device Name	Serial Number	Version	Status
ASBCE-3	IPCS31030016	4.0.5.Q19	Commissioned

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

System Information: ASBCE-3																			
Network Configuration																			
<b>General Settings</b> <table border="1"> <tr> <td>Appliance Name</td> <td>ASBCE-3</td> </tr> <tr> <td>Box Type</td> <td>SIP</td> </tr> <tr> <td>Deployment Mode</td> <td>Proxy</td> </tr> </table>			Appliance Name	ASBCE-3	Box Type	SIP	Deployment Mode	Proxy	<b>Device Settings</b> <table border="1"> <tr> <td>HA Mode</td> <td>No</td> </tr> <tr> <td>Secure Channel Mode</td> <td>None</td> </tr> <tr> <td>Two Bypass Mode</td> <td>No</td> </tr> </table>		HA Mode	No	Secure Channel Mode	None	Two Bypass Mode	No			
Appliance Name	ASBCE-3																		
Box Type	SIP																		
Deployment Mode	Proxy																		
HA Mode	No																		
Secure Channel Mode	None																		
Two Bypass Mode	No																		
<b>Network Settings</b> <table border="1"> <thead> <tr> <th>IP</th> <th>Public IP</th> <th>Netmask</th> <th>Gateway</th> <th>Interface</th> </tr> </thead> <tbody> <tr> <td>10.64.91.150</td> <td>10.64.91.150</td> <td>255.255.255.0</td> <td>10.64.91.1</td> <td>A1</td> </tr> <tr> <td>205.168.62.35</td> <td>205.168.62.35</td> <td>255.255.255.0</td> <td>205.168.62.1</td> <td>B1</td> </tr> </tbody> </table>					IP	Public IP	Netmask	Gateway	Interface	10.64.91.150	10.64.91.150	255.255.255.0	10.64.91.1	A1	205.168.62.35	205.168.62.35	255.255.255.0	205.168.62.1	B1
IP	Public IP	Netmask	Gateway	Interface															
10.64.91.150	10.64.91.150	255.255.255.0	10.64.91.1	A1															
205.168.62.35	205.168.62.35	255.255.255.0	205.168.62.1	B1															
<b>DNS Configuration</b> <table border="1"> <tr> <td>Primary DNS</td> <td>10.80.150.201</td> </tr> <tr> <td>Secondary DNS</td> <td>4.2.2.2</td> </tr> <tr> <td>DNS Location</td> <td>DMZ</td> </tr> <tr> <td>DNS Client IP</td> <td>10.64.91.150</td> </tr> </table>			Primary DNS	10.80.150.201	Secondary DNS	4.2.2.2	DNS Location	DMZ	DNS Client IP	10.64.91.150	<b>Management IP(s)</b> <table border="1"> <tr> <td>IP</td> <td>10.64.90.150</td> </tr> </table>		IP	10.64.90.150					
Primary DNS	10.80.150.201																		
Secondary DNS	4.2.2.2																		
DNS Location	DMZ																		
DNS Client IP	10.64.91.150																		
IP	10.64.90.150																		

## 7.2. Global Profiles

Global Profiles allows for configuration of parameters across all UC-Sec appliances.

### 7.2.1. Routing Profiles

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

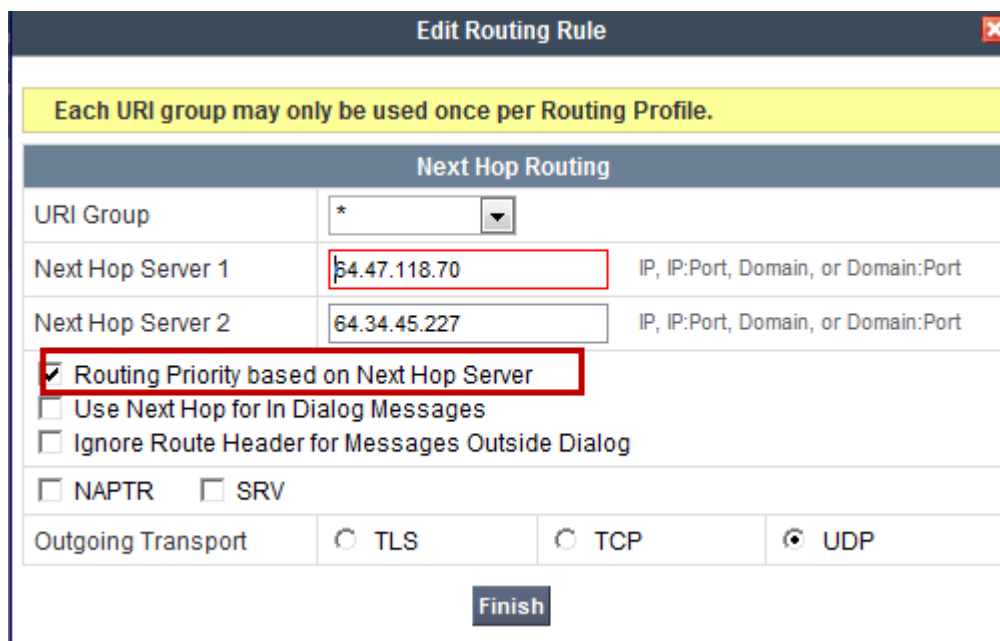
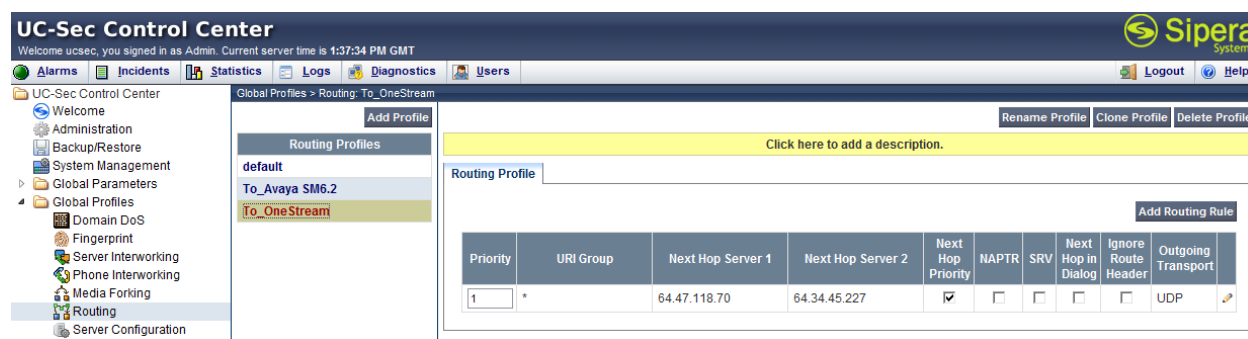
To create a **Routing Profile**, select **UC-Sec Control Center → Global Profiles → Routing**. Click on **Add Profile** (not shown).

In this compliance test, a **Routing Profile** named **To\_Avaya SM6.2** is created to be used in conjunction with the server flow defined for Session Manager. This entry is to route the outgoing enterprise SIP call to OneStream Networks destination. On the opposite direction, a **Routing Profile** named **To\_OneStream** is created to be used in conjunction with the server flow defined

for OneStream Networks. This entry is to route the incoming SIP call from OneStream Networks to enterprise as a destination.

### 7.2.1.1 Routing Profile for OneStream Networks

The screenshots below illustrate the **UC-Sec Control Center → Global Profiles → Routing: To\_OneStream**. As shown in **Figure 1**, OneStream Networks SIP Trunk is connected with transportation protocol UDP.



### 7.2.1.2 Routing Profile for Session Manager

The **Routing Profile** named **To\_Avaya SM6.2** is also defined to route the matching SIP call to **Next Hop Server 1** which is the IP address of Session Manager as a destination. As shown in **Figure 1**, Session Manager SIP entity is connected with transportation protocol TCP.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 1:40:54 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Routing: To\_Avaya SM6.2

Routing Profiles

default

To\_Avaya SM6.2

To\_OneStream

Click here to add a description.

Add Routing Rule

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	*	10.64.90.109	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

Edit Routing Rule

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group	<div style="border: 1px solid #ccc; background-color: #add8e6; padding: 2px;">*</div>		
Next Hop Server 1	<div style="border: 1px solid #ccc; padding: 2px;">10.64.90.109</div>	IP, IP:Port, Domain, or Domain:Port	
Next Hop Server 2	<div style="border: 1px solid #ccc; padding: 2px;"></div>	IP, IP:Port, Domain, or Domain:Port	

☒ Routing Priority based on Next Hop Server  
☐ Use Next Hop for In Dialog Messages  
☐ Ignore Route Header for Messages Outside Dialog  

☐ NAPTR    ☐ SRV

Outgoing Transport   
 ☐ TLS   
 ☒ TCP   
 ☐ UDP

Finish

## 7.2.2. Topology Hiding

**Topology Hiding** is an Avaya SBCE security feature which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**; this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from the Session Manager. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To create a **Topology Hiding** profile, select **UC-Sec Control Center** → **Global Profiles** → **Topology Hiding**. Click on **Add Profile** (not shown). In this compliance test, two **Topology Hiding** profiles were created, named **Avaya** and **OneStream**.

### 7.2.2.1 Topology Hiding Profile for OneStream Networks

The **OneStream** profile was defined to mask the enterprise SIP domain **avayalab.com** in Request-URI, From, and To headers towards OneStream Networks (the domain name defined here for Request-URI, From and To is to meet the SIP specification require by OneStream Networks); delete Record-Route and Via entries added by Session Manager and replace internal IP addresses in SDP by external IP address known to OneStream Networks. It secures the enterprise network topology and also meets the SIP requirement from service provider.

The screenshots below illustrate the **UC-Sec Control Center → Global Profiles → Topology Hiding: OneStream**

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

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

### 7.2.2.2 Topology Hiding Profile for Session Manager

The **Avaya** profile was defined to replace OneStream Networks SIP domain in the Request-Line, From, and To headers with the domain known to the enterprise. For compliance testing this was **avayalab.com**. The domain must match the domain set in Communication Manager's Signaling Group (**Section 5.6**) and in Session Manager (**Section 6.2**).



The screenshots below illustrate the **UC-Sec Control Center → Global Profiles → Topology Hiding: Avaya**.

UC-Sec Control Center  
Welcome ucsec, you signed in as Admin. Current server time is 1:55:03 PM GMT

Global Profiles > Topology Hiding: Avaya

Topology Hiding Profiles

- default
- cisco\_th\_profile
- Avaya**
- OneStream

Click here to add a description.

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

Edit

Edit Topology Hiding Profile

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

Finish

**Note:**

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in SIP URI-Host.
- The masking applied on From header also applies to Referred-By and P-Asserted-Identity headers.
- The masking applied on To header also applies to Refer-To header.

### 7.2.3. Server Interworking

Interworking Profile features are configured based on different Call and Trunk Servers.

To create a **Server Interworking** profile, select **UC-Sec Control Center → Global Profiles → Server Interworking**. Click on **Add Profile** (not shown).

In this compliance testing, two profiles were created; **OneStream** and **Avaya**.

#### 7.2.3.1 Server Interworking profile for OneStream Networks

Profile **OneStream** is defined to match the specification on OneStream Networks SIP Trunking. The General settings are configured with the following parameters while the other options for **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** are kept as default.

##### General settings:

- **Hold Support = None**. Avaya SBCE will not modify the hold/resume signaling for Communication Manager to send to OneStream Networks.
- **18X Handling = None**. Avaya SBCE will not handle 18X; it will keep the 18X messages from Communication Manager unchanged to send to OneStream Networks.
- **Refer Handling = unchecked**. Avaya SBCE will not handle Refer; it will keep the Refer messages from Communication Manager unchanged to send to OneStream Networks.
- **T.38 Support = checked**. OneStream Networks does support T.38 fax in this compliance testing.
- **Privacy Enabled = unchecked**. Avaya SBCE will not mask the FROM header with anonymous for outbound call to OneStream Networks. It depends on Communication Manager to enable/ disable privacy on individual call basis.
- **DTMF Support = None**. Avaya SBCE will send original DTMF supported by Communication Manager to OneStream Networks.

The screenshots below illustrate the **UC-Sec Control Center → Global Profiles → Server Interworking: OneStream**.

## Editing Profile: OneStream

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Next

## Editing Profile: OneStream

Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

Back Finish

### 7.2.3.2 Server Interworking profile for Session Manager

Profile **Avaya** is defined to match the specification on Communication Manager. The General settings are configured with the following parameters while the other options for **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** are kept as default.

#### General settings:

- **Hold Support** = **None**. Avaya SBCE will not modify the send message allowing Communication Manager to support hold/ resume for Music On Hold to play.
- **18X Handling** = **None**. Avaya SBCE will not handle 18X; it will keep the 18X messages from OneStream Networks unchanged to send to Communication Manager via Session Manager.
- **Refer Handling** = **unchecked**. Avaya SBCE will not handle Refer; it will keep the Refer messages from OneStream Networks unchanged to send to Communication Manager via Session Manager.
- **T.38 Support** = **checked**. OneStream Networks does support T.38 fax in this compliance testing.
- **Privacy Enabled** = **unchecked**. Avaya SBCE will not mask the From header with anonymous for inbound call from OneStream Networks. It depends on OneStream Networks to enable/disable privacy on individual call basis.
- **DTMF Support** = **None**. Avaya SBCE will send original DTMF supported by OneStream Networks to Communication Manager via Session Manager.

The screenshots below illustrate the **UC-Sec Control Center > Global Profiles > Server Interworking: SM**.

Editing Profile: Avaya

General

Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Next

Editing Profile: Avaya

Privacy

Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

DTMF

DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
--------------	---

Back

Finish

## 7.2.4. Signaling Manipulation

The **Signaling Manipulation** feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE. Using this language, a script can be written and tied to a given **Server Configuration** which will be configured in the next steps through the UC-Sec GUI. The Avaya SBCE appliance then interprets this script at the given entry point or “hook point”.

These Application Notes will not discuss the full feature of the **Signaling Manipulation** but will show an example of a script created during compliance testing to normalize the incoming call information in the P-Asserted-Identity (PAI) Header. It is applied to OneStream Networks.

In this compliance testing, a SigMa script named **fixPAI** is created to apply to OneStream Networks Server Configuration.

Note: the SigMa script for Session Manager is unnecessary since the signaling has already been normalized on the OneStream Networks side.

To create a **Signaling Manipulation** script, select **UC-Sec Control Center → Global Profiles → Signaling Manipulation**. Click on **Add Script** (not shown).

The detail of SigMa script **fixPAI** is as following:

```
within session "ALL"
{
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    %HEADERS["P-Asserted-Identity"][1].URI.HOST = %HEADERS["FROM"][1].URI.HOST ;
  }
}
```

In the **Signaling Manipulation** script named **fixPAI** above, the statement **act on message where %DIRECTION="INBOUND" and %ENTRY\_POINT="PRE\_ROUTING"** is to specify the script will take effect on all type of SIP messages for inbound call and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement.

The script is to update PAI header's Host IP address with the IP address in the FROM header.

## 7.2.5. Server Configuration

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

To create a Server Configuration entry, select **UC-Sec Control Center** → **Global Profiles** → **Server Configuration**. Click on **Add Profile** (not shown).

In this compliance testing, two separate Server Configurations were created, server entry **OneStream\_SIP TRK** for OneStream Networks; and server entry **Avaya\_SM6.2 CM6.2** for Session Manager.

### 7.2.5.1 Server Configuration for OneStream Networks

The **Server Configuration** named **OneStream\_SIP TRK** was added for OneStream Networks and discussed in detail as below. The **General**, **Authentication**, **Heartbeat** and **Advanced** tabs will be provisioned.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a navigation tree with 'Global Profiles' expanded, leading to 'Server Configuration'. The main content area shows the configuration for the 'OneStream\_SIP TRK' profile. The 'General' tab is active, showing the following details:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	64.47.118.70, 64.34.45.227
Supported Transports	UDP
UDP Port	5060

Buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', 'Delete Profile', and 'Edit' are visible.

In the **General** tab, specify **Server Type** for OneStream Networks as a **Trunk Server**; the IP connectivity has also been defined here. In this compliance testing, OneStream Networks supports UDP and listens on port 5060.

Edit Server Configuration Profile - General	
Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma seperated list	64.47.118.70,64.34.45.227
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	
<input type="button" value="Finish"/>	

OneStream Networks does not support Digest Authentication on SIP Trunk. In this compliance testing, the authentication will not be implemented by Avaya SBCE. In **Authentication** tab, uncheck **Enable Authentication**.

Edit Server Configuration Profile - Authentication	
Enable Authentication	<input type="checkbox"/>
User Name	
Realm (Leave blank to detect from server challenge)	
Password	
Confirm Password	
<input type="button" value="Finish"/>	

In **Heartbeat** tab, **Enable Heartbeat** is checked to send OPTIONS in 60 seconds interval to check for the SIP trunk status, input From header as **PING@205.168.62.35** and To header as **PING@64.47.118.70** as expected by OneStream Networks. **TCP Probe** is kept unchecked as default.



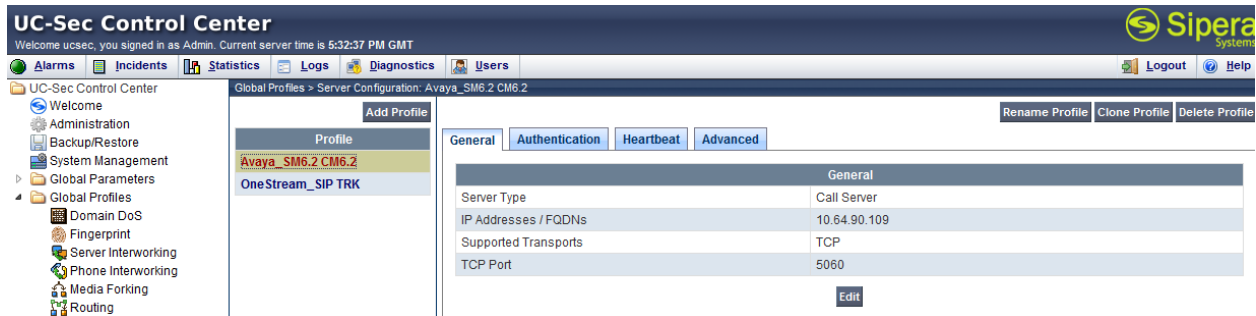
Edit Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	PING@205.168.62.35
To URI	PING@64.47.118.70
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds
<input type="button" value="Finish"/>	

Under **Advanced** tab, in **Interworking Profile** drop down list select entry **OneStream** as defined in **Section 7.2.3**, in **Signaling Manipulation Script** drop down list select entry **fixPAI** as defined in **Section 7.2.4**. This configuration is to apply the specific SIP profile and SigMa rules to the traffic from OneStream Networks. The other settings are kept as default.

Edit Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	OneStream
Signaling Manipulation Script	fixPAI
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
<input type="button" value="Finish"/>	

### 7.2.5.2 Server Configuration for Session Manager

The **Server Configuration** named **Avaya\_SM6.2 CM6.2** was added for Session Manager and discussed in detail below. The **General**, **Authentication**, **Heartbeat** and **Advanced** tabs will be provisioned.



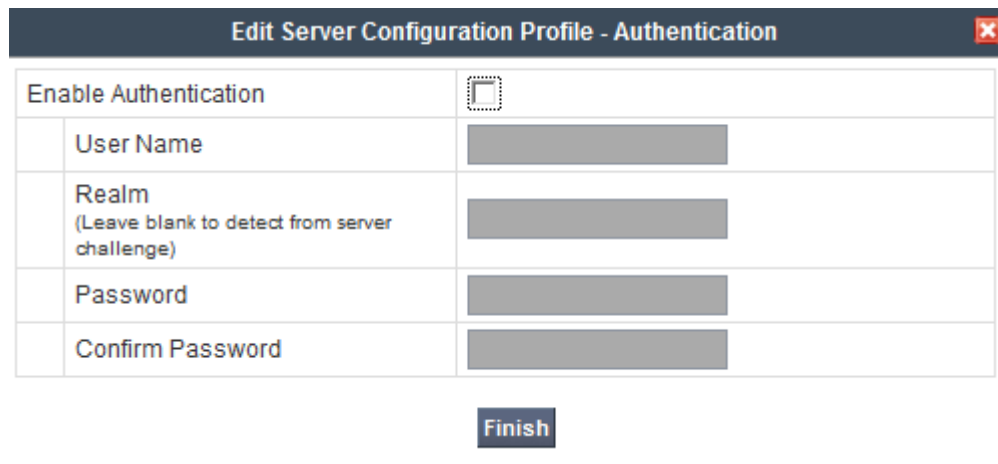
In the **General** tab, specify **Server Type** for Session Manager as a **Call Server**; the IP connectivity has also been defined here. In this compliance testing, Session Manager Link is TCP and listens on port 5060.

The screenshot shows the 'Edit Server Configuration Profile - General' dialog box. It contains the following fields and options:

Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.64.90.109
Supported Transports	<input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	
TLS Port	

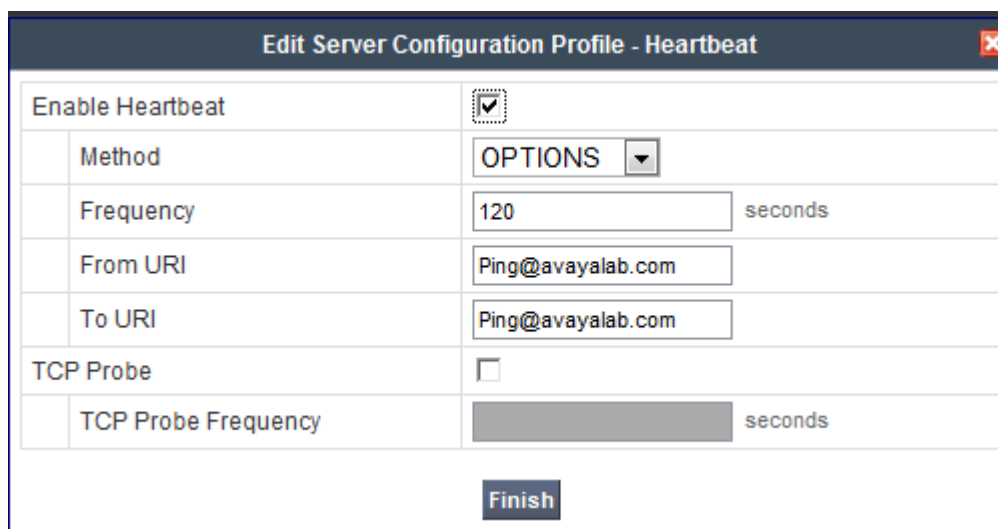
A 'Finish' button is located at the bottom of the dialog.

In **Authentication** tab, uncheck the checkbox **Enable Authentication**. Session Manager was configured as a trusted link in **Section 6.6**, and does not require authentication.



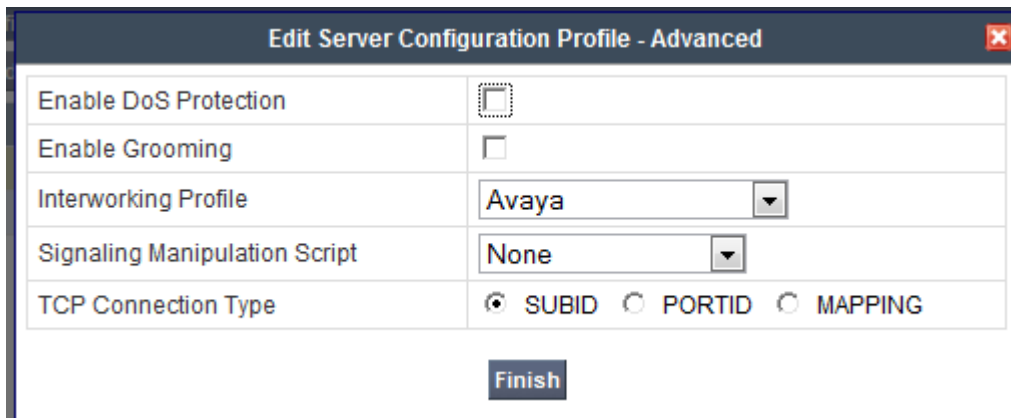
Edit Server Configuration Profile - Authentication	
Enable Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Realm (Leave blank to detect from server challenge)	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
<b>Finish</b>	

In **Heartbeat** tab, **Enable Heartbeat** is checked to send OPTIONS in 60 seconds interval to check for the SIP trunk status, input From header as **Ping@avayalab.com** and To header as **Ping@avayalab.com** as expected by Session Manager. **TCP Probe** is kept unchecked as default.



Edit Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	120 seconds
From URI	Ping@avayalab.com
To URI	Ping@avayalab.com
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	<input type="text"/> seconds
<b>Finish</b>	

Under **Advanced** tab, in **Interworking Profile** drop down list select entry **Avaya** as defined in **Section 7.2.4**, in **Signaling Manipulation Script** drop down list select **None** since there is no manipulation on Session Manager. The other settings are kept as default.



Edit Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
<b>Finish</b>	

## 7.3. Domain Policies

The **Domain Policies** feature configures, applies, and manages various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the UC-Sec security device to aggregate, monitor, control, and normalize call flows. There are default policies available to use, or a custom domain policy can be created.

### 7.3.1. Application Rules

**Application Rules** define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, it is possible to determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Create an **Application Rule** to set the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**.

To clone an application rule, navigate to **UC-Sec Control Center → Domain Policies → Application Rules**. With the default rule chosen, click on **Clone Rule** as shown below.

**UC-Sec Control Center**  
Welcome ucsec, you signed in as Admin. Current server time is 5:46:55 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

Domain Policies > Application Rules: default

Add Rule Filter By Device... Clone Rule

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	5
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support	None		
IM Logging	No		
RTCP Keep-Alive	No		

Edit

Enter a descriptive name **OneStream\_App\_Rule** for the new rule and click **Finish**.

**Clone Rule**

Rule Name	default
Clone Name	OneStream_App_Rui

Finish

Modify the rule by clicking the **Edit** button. Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able to process. The following screen shows the modified **Application Rule** with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to **2000**. In the sample configuration, Communication Manager was programmed to control the concurrent sessions by setting the number of members in the trunk group (Section 5.7) to the allotted amount. Therefore, the values in the **Application Rule** named **OneStream\_App\_Rule** were set high enough to be considered non-blocking.

**Editing Rule: OneStream\_App\_Rule**

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

Miscellaneous

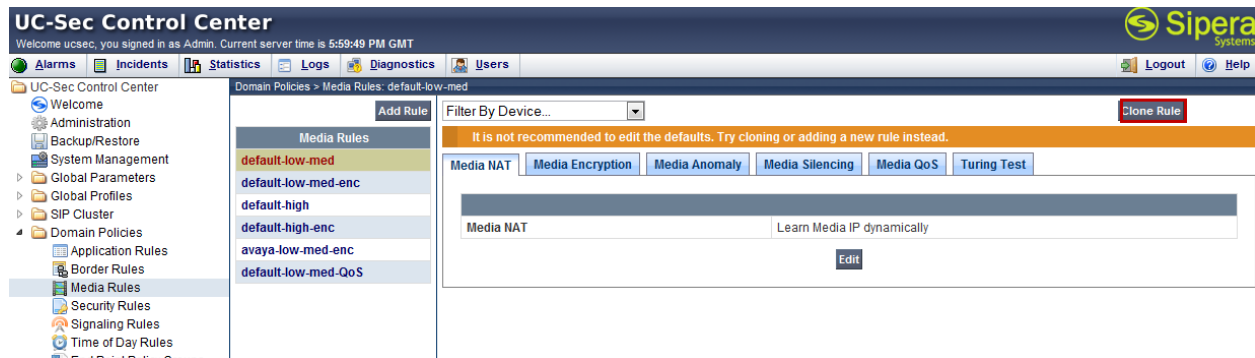
CDR Support	<input checked="" type="radio"/> None <input type="radio"/> CDR w/ RTP <input type="radio"/> CDR w/o RTP
IM Logging	<input type="checkbox"/>
RTCP Keep-Alive	<input type="checkbox"/>

Finish

### 7.3.2. Media Rules

**Media Rules** define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the UC-Sec security product.

Create a custom **Media Rule** to set the **Quality of Service** and **Media Anomaly Detection**. To create a custom **Media Rule**, navigate to **UC-Sec Control Center** → **Domain Policies** → **Media Rules**. With **default-low-med** selected, click **Clone Rule** as shown below.



Enter a descriptive name **default-low-med-QoS** for the new rule and click **Finish**.

Clone Rule	
Rule Name	default-low-med
Clone Name	default-low-med-QoS
<b>Finish</b>	

When the RTP packets of a call are shuffled from Communication Manager to an IP Phone, Avaya SBCE will interpret this as an anomaly and an alert will be created in the Incidents Log. Disabling **Media Anomaly Detection** prevents the **RTP Injection Attack** alerts from being created during an audio shuffle. The **default-low-med** rule was used for this compliance testing.

To modify the rule, select the **Media Anomaly** tab and click **Edit**, check **Media Anomaly Detection** and click **Finish**.

Media Anomaly	
Media Anomaly	
Media Anomaly Detection	<input checked="" type="checkbox"/>
Detect RTP Injection Attack	<input checked="" type="checkbox"/>
Asymmetric RTP	<input type="checkbox"/>
Action	Alert <span>▼</span>
<input type="button" value="Finish"/>	

The **Media Silencing** feature detects the silence when the call is in progress. If the silence is detected and exceeds the allowed duration, Avaya SBCE generates alert in Incidents Log. In this sample configuration, the Media Silencing detection is disabled due to the RTP packets could be lost in part on public WAN.

To modify the rule, select the **Media Silencing** tab and click **Edit**, uncheck **Media Silencing** and click **Finish**.

Media Silencing	
Media Silencing	
Media Silencing	<input type="checkbox"/>
Timeout (seconds)	<input type="text"/>
<input type="button" value="Finish"/>	

On the **Media QoS** tab select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for the media. The following screen shows the QoS values used for compliance testing.

Media QoS			
Media QoS Reporting			
RTCP Enabled		<input type="checkbox"/>	
Media QoS Marking			
Enabled		<input checked="" type="checkbox"/>	
<input type="radio"/> ToS			
	Audio Precedence	Routine	000
	Audio ToS	Minimize Delay	1000
	Video Precedence	Routine	000
	Video ToS	Minimize Delay	1000
<input checked="" type="radio"/> DSCP			
	Audio	EF	101110
	Video	EF	101110
<input type="button" value="Finish"/>			

### 7.3.3. Signaling Rules

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

Clone and modify the default signaling rule to apply for both enterprise and OneStream Networks. To clone a signaling rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** as shown below.



**UC-Sec Control Center**  
 Welcome ucsec, you signed in as Admin. Current server time is 6:06:04 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
  - Application Rules
  - Border Rules
  - Media Rules
  - Security Rules
  - Signaling Rules**
    - Time of Day Rules
    - End Point Policy Groups
    - Session Policies
    - Device Specific Settings
    - Troubleshooting
    - TLS Management
    - IM Logging

Domain Policies > Signaling Rules: default

Filter By Device... Clone Rule

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

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

Enter a descriptive name **Block\_Hdr\_Remark** for the new rule and click **Finish**.

**Clone Rule**

Rule Name	default
Clone Name	<b>Block_Hdr_Remark</b>

**Finish**

This rule was created to prevent certain headers in the SIP message from Session Manager from being propagated to OneStream Networks. Select this rule in the center pain, then select the **Request Headers** tab to view the manipulations performed on the request messages such as the initial INVITE. The following screen shows the **P-Location** and **Endpoint-View** headers removed during the compliance test.

Domain Policies > Signaling Rules: Block\_Hdr\_Remark

Add Rule Filter By Device... Rename Rule Clone Rule Delete Rule

Click here to add a description.

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	Endpoint-View	ALL	Forbidden	Remove Header	Yes	OUT		
2	P-location	ALL	Forbidden	Remove Header	Yes	OUT		

Similarly, manipulations can be performed on the SIP response messages. These can be viewed by selecting the **Response Headers** tab as shown below.

UC-Sec Control Center  
Welcome ucsec, you signed in as Admin. Current server time is 6:25:15 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Domain Policies > Signaling Rules: Block\_Hdr\_Remark

Filter By Device... [v] [Rename Rule] [Clone Rule] [Delete Rule]

Click here to add a description.

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	1XX	ALL	Forbidden	Remove Header	Yes	IN	[edit] [X]
2	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	[edit] [X]
3	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	[edit] [X]
4	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	[edit] [X]

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS values used for compliance testing.

Signaling QoS

Signaling QoS

Enabled

☒

ToS

Precedence

Routine

000

ToS

Minimize Delay

1000

DSCP

Value

AF32

011100

Finish

### 7.3.4. Endpoint Policy Groups

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

This sample configuration, create a separate **Endpoint Policy Group** for the enterprise and the OneStream Networks SIP Trunking.

To create a new policy group, navigate to **UC-Sec Control Center → Domain Policies → Endpoint Policy Groups** and click on **Add Group** (not shown).

### 7.3.4.1 Endpoint Policy Group for OneStream Networks

The following screen shows **default-low-remark** created for OneStream Networks SIP Trunking. Set the **Application**, **Media** and **Signaling** rules to the ones previously created. Set the **Border**, and **Time of Day** rules to **default** and set the **Security** rule to **default-low**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, Global Parameters, SIP Cluster, and Domain Policies. Under Domain Policies, 'End Point Policy Groups' is selected. The main area displays the configuration for the 'default-low-remark' policy group. It includes a 'Filter By Device...' dropdown, a 'Click here to add a description.' link, and a 'Hover over a row to see its description.' link. Below these is a table with columns: Order, Application, Border, Media, Security, Signaling, Time of Day, and an action column. The table contains one row with the following values: 1, OneStream\_App\_Rule, default, default-low-med-QoS, default-low, Block\_Hdr\_Remark, default, and an edit icon.

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	OneStream_App_Rule	default	default-low-med-QoS	default-low	Block_Hdr_Remark	default	

### 7.3.4.2 Endpoint Policy Group for Session Manager

The same **default-low-remark** created for OneStream Networks SIP Trunking was used for **Session Manager**. Set the **Application**, **Media** and **Signaling** rules to the ones previously created. Set the **Border**, and **Time of Day** rules to **default** and set the **Security** rule to **default-low**.

This screenshot is identical to the one above, showing the UC-Sec Control Center interface with the 'default-low-remark' policy group configuration. The table contains the same data: Order 1, Application OneStream\_App\_Rule, Border default, Media default-low-med-QoS, Security default-low, Signaling Block\_Hdr\_Remark, Time of Day default, and an edit icon.

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	OneStream_App_Rule	default	default-low-med-QoS	default-low	Block_Hdr_Remark	default	

## 7.4. Device Specific Settings

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

### 7.4.1. Network Management

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

Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the external interface is assigned to **B1**.

Device Specific Settings > Network Management: ASBCE-3

UC-Sec Devices

ASBCE-3

Network Configuration | Interface Configuration

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

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

Add IP    Save Changes    Clear Changes

IP Address	Public IP	Gateway	Interface	
10.64.91.150		10.64.91.1	A1	X
205.168.62.35		205.168.62.1	B1	X

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

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 2:52:49 AM EDT

Alarms Incidents Statistics Logs Diagnostics Users

UC-Sec Control Center

UC-Sec Devices

sipera

Network Configuration | Interface Configuration

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

### 7.4.2. Media Interface

The **Media Interface** screen is where the media ports are defined. Avaya SBCE will listen for RTP on the defined ports.

Create a **Media Interface** for both the inside and outside IP interfaces.

To create a new **Media Interface**, navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface** and click **Add Media Interface**.

The following screen shows the media interfaces created in the sample configuration for the inside and outside IP interfaces.

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

Device Specific Settings > Media Interface: ASBCE-3

UC-Sec Devices  
ASBCE-3

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add Media Interface

Name	Media IP	Port Range		
Avaya_Int_Media	10.64.91.150	35000 - 40000		
Ext_Media_to_OneStream	205.168.62.35	35000 - 40000		

### 7.4.3. Signaling Interface

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

Create a **Signaling Interface** for both the inside and outside IP interfaces. To create a new **Signaling Interface**, navigate to **UC-Sec Control Center → Device Specific → Settings → Signaling Interface** and click **Add Signaling Interface** (not shown).

The following screen shows the signaling interfaces created in the sample configuration with TCP and UDP ports 5060 used for the inside and outside IP interfaces.

Device Specific Settings > Signaling Interface: ASBCE-3

UC-Sec Devices  
ASBCE-3

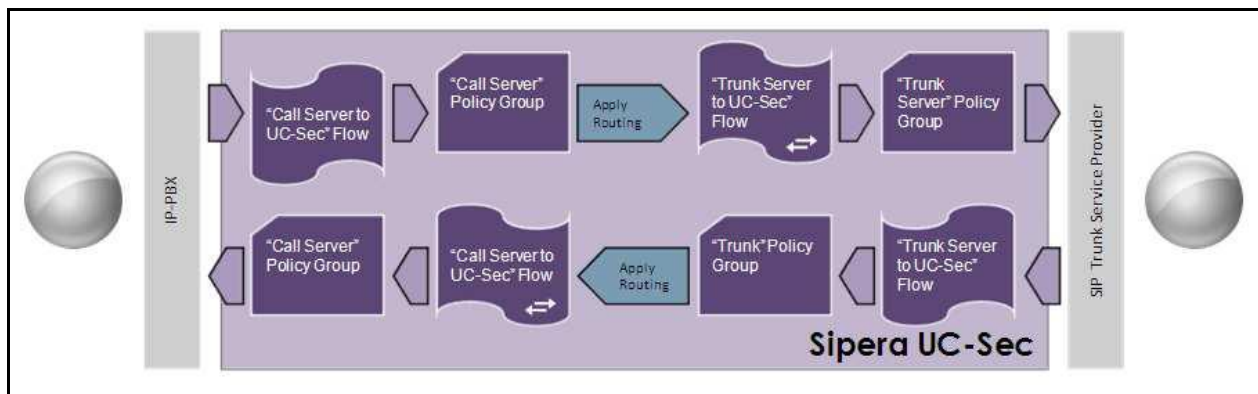
Signaling Interface

Add Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Sig_Inside_to_Avaya	10.64.91.150	5060	5060	---	None		
Sig_Outside_to_OneStream	205.168.62.35	---	5060	---	None		

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

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



Create a separate Server Flow for Session Manager and the OneStream Networks SIP Trunking.

To create a Server Flow, navigate to **UC-Sec Control Center → Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** (not shown).

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.5** to assign to the Flow.
- **URI Group:** Select the URI Group to assign to the Flow.
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy assigned to the Server Configuration.
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration.

Click **Finish** to save and exit.

The following screen shows the **Sever Flow** named **OneStream SIP\_Trunk** for OneStream Networks.

Edit Flow: OneStream SIP\_Trunk

Criteria	
Flow Name	OneStream SIP_Trunk
Server Configuration	OneStream_SIP TRK
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside_to_Avaya
Signaling Interface	Sig_Outside_to_OneStream
Media Interface	Ext_Media_to_OneStream
End Point Policy Group	default-low-remark
Routing Profile	To_Avaya SM6.2
Topology Hiding Profile	OneStream
File Transfer Profile	None

Finish

The following screen shows the **Sever Flow** named **Avaya\_SM** for Session Manager.



Criteria	
Flow Name	Avaya_SM
Server Configuration	Avaya_SM6.2 CM6.2
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside_to_OneStream
Signaling Interface	Sig_Inside_to_Avaya
Media Interface	Avaya_Int_Media
End Point Policy Group	default-low-remark
Routing Profile	To_OneStream
Topology Hiding Profile	Avaya
File Transfer Profile	None

Finish

## 8. OneStream Networks' Global SIP Trunking Configuration

OneStream Networks is responsible for the configuration of OneStream Networks' Global SIP Trunking service. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise. OneStream Networks will provide the customer with the necessary information to configure the SIP connection from the enterprise site to the OneStream Networks.

The provided information from OneStream Networks includes:

- IP address of the OneStream Networks SIP proxy.
- OneStream Networks SIP domain.
- Supported codecs.
- DID numbers.
- IP addresses and port numbers used for signaling or media through any security devices.
- A customized SIP signaling specification requirement for Call-ID, Contact headers.

The sample configuration between OneStream Networks and the enterprise for the compliance test is a static configuration. There is no registration of the SIP trunk or enterprise users to the OneStream Networks



## 9. Verification and Troubleshooting

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

### Verification Steps:

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

### Protocol Traces:

The following SIP headers are inspected using Wireshark traces:

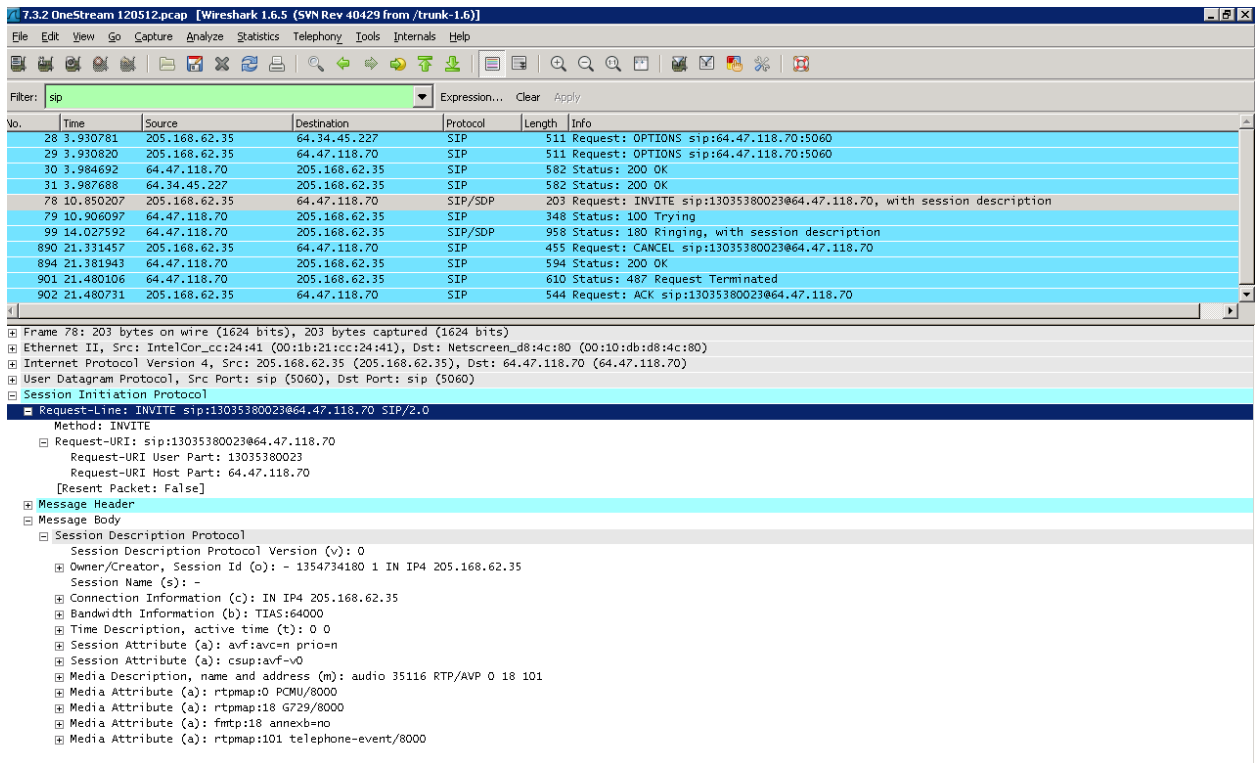
- Request URI: verify the request number and either SIP domain
- From: verify the display name and display number.
- To: verify the display name and display number.
- P-Assert-Identity: verify the display name and display number.
- Privacy: verify the “user, id” masking.

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

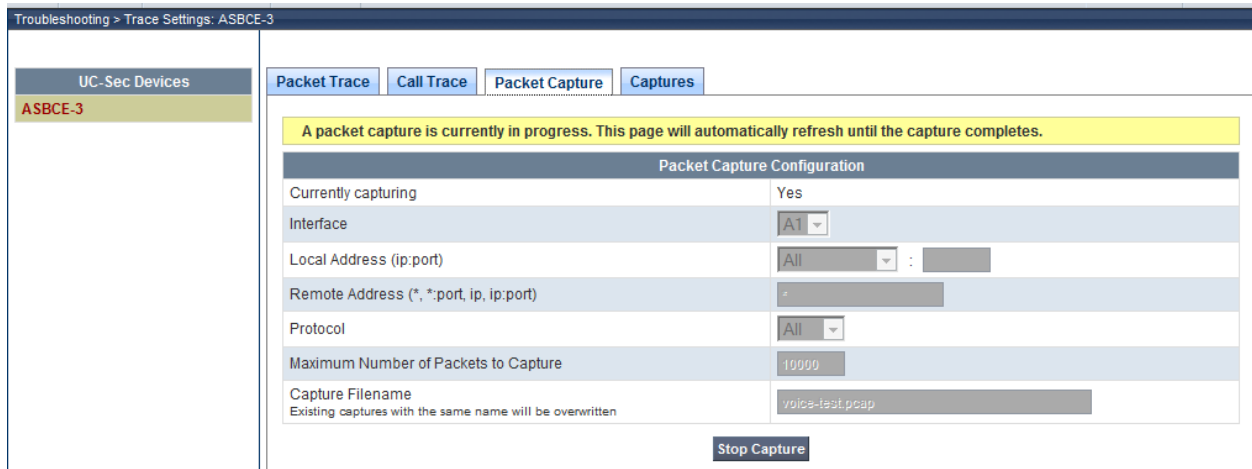
- Connection Information (c): verify IP address of far end endpoint
- Time Description (t): verify session timeout of far end endpoint
- Media Description (m): verify audio port, codec, DTMF event description
- Media Attribute (a): verify specific audio port, codec,ptime, send/ receive ability, DTMF event and fax attributes.

### Troubleshooting:

1. Avaya SBCE:
  - Using a network sniffing tool (e.g., Wireshark), monitor the SIP signaling messages between OneStream Networks and Avaya SBCE.
  - OneStream Networks SIP Trunking service returned 100 Trying and subsequent 18X call ringing or session progress messages signaling normal call progression.



- Using Avaya SBCE, navigate to **Troubleshooting** → **Trace Settings** in the **UC-Sec Control Center** menu on the left hand side and select the **Packet Capture** tab.
- Select the SIP Trunk interface from the **Interface** drop down menu
- Select the signaling interface IP address from the **Local Address** drop down menu
- Enter the IP address of the Service Provider’s SBC in the **Remote Address** field or enter a “\*” to capture all traffic
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example
- Specify the filename of the resultant pcap file in the **Capture Filename** field
- Click on **Start Capture** (not shown).



To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces (not shown).

## 2. Communication Manager:

- **list trace station** <extension number> - Trace 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.

## 3. Session Manager:

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

Avaya Aura® System Manager 6.2

Last Logged on at December 21, 2012 11:51 AM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

**Session Manager** x [Home](#)

**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 1:37 PM

Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	Version
ASM62	Core	0/0/0	✓	Up	Accept New Service	1/5	0	2/2	✗	6.2.3.0.623006

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 the test (not shown).

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2 and Avaya Session Border Controller For Enterprise 4.0.5 to OneStream Networks' Global SIP Trunking service. OneStream Networks' Global SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. OneStream Networks' Global SIP Trunking provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The OneStream Networks' Global SIP Trunking is considered compliant with Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2 and Avaya Session Border Controller For Enterprise 4.0.5.

## 11. References

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

- [1]*Installing and Configuring Avaya Aura® System Platform*, Release 6.2.1, July 2012.
- [2]*Administering Avaya Aura® System Platform*, Release 6.0.3, July 2012.
- [3]*Administering Avaya Aura® Communication Manager*, Issue 7.0, July 2012, Document Number 03-300509.
- [4]*Avaya Aura® Communication Manager Feature Description and Implementation*, Issue 9.0, July 2012, Document Number 555-245-205.
- [5]*Installing and Upgrading Avaya Aura® System Manager*, Release 6.2, July 2012.
- [6]*Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Number 03-603473.
- [7]*Administering Avaya Aura® Session Manager*, Release 6.2, July 2012, Document Number 03-603324.
- [8]*Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.
- [9]*Administering Avaya one-X® Communicator*, October 2011, Document Number 03-603324.
- [10]*Using Avaya one-X® Communicator*, April 2011.
- [11]*UC-Sec Install Guide (102-5224-400v1.01)*
- [12]*UC-Sec Administration Guide (010-5423-400v106)*
- [13]*RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [14]*RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [15]*RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>
- [16]*RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information*, <http://www.ietf.org/>

Product documentation for OneStream Networks' Global SIP Trunking is available from OneStream Networks.

---

**©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).