

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Lumos Networks SIP Trunking with Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2 and Avaya Session Border Controller for Enterprise 4.0.5 Q19 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Lumos Networks SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.2, Avaya Aura® Communication Manager 6.2, Avaya Session Border Controller for Enterprise (SBCE) 4.0.5 Q19 and various Avaya endpoints.

Lumos Networks is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Intr	oduction	4
2. Ger	neral Test Approach and Test Results	4
2.1. 2.2. 2.3.	Interoperability Compliance Testing Test Results Support	5
3. Ref	erence Configuration	6
4. Equ	ipment and Software Validated	7
5. Cor	nfigure Avaya Aura® Communication Manager	8
$5.1. \\ 5.2. \\ 5.3. \\ 5.4. \\ 5.5. \\ 5.6. \\ 5.7. \\ 5.8. \\ 5.9. \\ 5.10. \\ 5.11. \\ 5.12. \\ 5.13. $	Licensing and Capacity System Features IP Node Names Codecs IP Network Region Configure IP Interface for procr Signaling Group Trunk Group Calling Party Information Outbound Routing Incoming Call Handling Treatment Communication Manager Stations. Save Avaya Aura® Communication Manager Configuration Changes	9 10 10 12 13 13 15 18 19 21 22
6. Cor	nfigure Avaya Aura® Session Manager	22
6.1. 6.2. 6.3. 6.4.	Avaya Aura® System Manager Login and Navigation Specify SIP Domain Add Location Add SIP Entities	25 26 26
6.4. 6.4.	 Configure Session Manager SIP Entity	28 29
6.5. 6.6. 6.7. 6.8.	Add Entity Links Configure Time Ranges Add Routing Policies Add Dial Patterns	31 31
7. Cor	figure Avaya Session Border Controller for Enterprise	36
7.2.	Log in Avaya Session Border Controller for Enterprise Global Profiles 1. Configure Server Interworking - Avaya site 2. Configure Server Interworking – Lumos Networks site 3. Configure URI Groups	37 37 38

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	2 of 59
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LNCM62SM62SBCE

	7.2.4. Confi	gure Routing – Avaya site	39
		gure Routing – Lumos Networks site	
	7.2.6. Confi	gure Server – Avaya Aura® Session Manager	40
	7.2.7. Confi	gure Server – Lumos Networks ACME Packet SBC	41
	7.2.8. Confi	gure Topology Hiding – Avaya site	44
	7.2.9. Confi	gure Topology Hiding – Lumos Networks site	45
7.	3. Domai	n Policies	45
		e Application Rules	
	7.3.2. Creat	e Border Rules	46
	7.3.3. Creat	e Media Rules	47
	7.3.4. Creat	e Security Rules	48
		e Signaling Rules	
		e Time of Day Rules	
		e Endpoint Policy Groups	
7.		Specific Settings	
		ge Network Settings	
		e Media Interfaces	
		e Signaling Interfaces	
		guration Server Flows	
	7.4.4.1	Create End Point Flows - Session Manager	
	7.4.4.2	Create End Point Flows – Lumos Networks	56
8.	Lumos Netv	vorks SIP Trunking Configuration	56
9.	Verification	Steps	57
10.	Conclusion		57
11.	Additional I	References	58

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Lumos Networks SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.2, Avaya Aura® Communication Manager 6.2, Avaya Session Border Controller for Enterprise (SBCE) 4.0.5 Q19 and various Avaya endpoints.

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to Lumos Networks SIP Trunking 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 the Avaya SBCE with various types of Avaya phones.

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

2.1. Interoperability Compliance Testing

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

- Incoming PSTN calls to various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client). Avaya one-X® Communicator can place calls from the local computer or control a separate physical phone. Both of these modes were tested.
- Various call types including: local, long distance, international, outbound/inbound tollfree, operator service, 911 and directory assistance.
- G.711MU and G.729A codecs.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	4 of 59
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LNCM62SM62SBCE

- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call transfer, conference, forwarding and enterprise mobility (extension to cellular).
- Fax G.711 Pass Through.
- Contact Center.
- Registration and Authentication

Items not supported or not tested included the following:

• Network Call Redirection and User to User Information (NCR and UUI) are not tested because the functionality is not available at this time.

2.2. Test Results

Lumos Networks SIP Trunking passed compliance testing.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit: <u>http://support.avaya.com</u>.

For technical support on Lumos Networks service, visit: <u>http://www.lumosnetworks.com/support</u>

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to Lumos Networks SIP Trunking. This is the configuration used for compliance testing.

For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

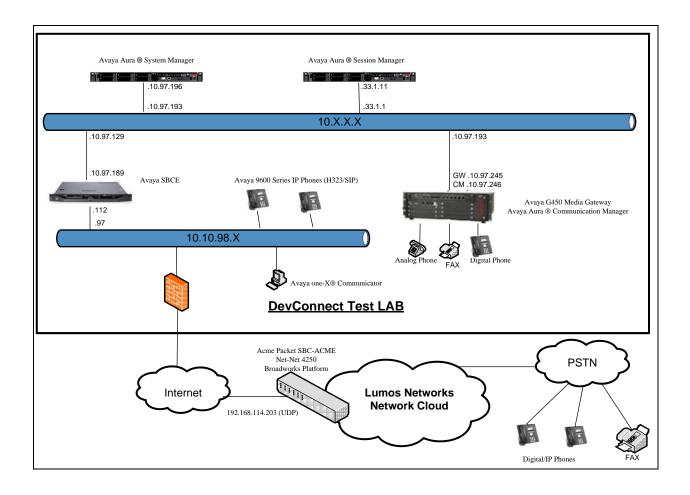


Figure 1: Avaya IP Telephony Network and Lumos Networks SIP Trunking

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components					
Equipment/Software	Release/Version				
Avaya S8300 Server	Avaya Aura® Communication Manager R6.2-				
	02.0.823.0 SP3				
Avaya G450 Media Gateway	HW01 FW001				
MM711 Analog	HW31 FW087				
MM712 Digital	HW05 FW009				
Avaya S8800 Server	Avaya Aura® Session Manager				
	R6.2.0.0.620103 - 6.2.1.621002				
Avaya S8800 Server	Avaya Aura ®System Manager R6.2.0 – SP1 –				
	6.2.0.0.15669 - 6.2.12.105				
Avaya Dell R210 V2 Server	Avaya Session Border Controller for				
	Enterprise R4.0.5 Q19				
Avaya 9640 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition S3.110b				
Avaya 96xx IP Phone (SIP)	6.0.3-120511				
Avaya Digital Telephones (1408D)	N/A				
Avaya Symphony 2000 Analog Telephone	N/A				
Avaya one-X® Communicator	3.2.3.15 64595				
Lumos Networks SIP Trun	king Solution Components				
Equipment/Software	Release/Version				
Acme Packet SBC-ACME Net-Net 4250	Firmware SC6.2.0 MR-3 Patch 1 (Build 642)				
	Build Date=06/29/10				
Broadworks Platform	R17 SP4				

Table 1: Equipment and Software Tested

The specific configuration above was 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 Lumos Networks SIP Trunking. It is assumed the general installation of Communication Manager, Avaya 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 and highlighted for brevity and clarity in presentation.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 4000 SIP trunks are available and 100 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES		_		
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:	4000	50		
Maximum Concurrently Registered IP Stations:	2400	2		
Maximum Administered Remote Office Trunks:	4000	0		
Maximum Concurrently Registered Remote Office Stations:	2400	0		
Maximum Concurrently Registered IP eCons:	68	0		
Max Concur Registered Unauthenticated H.323 Stations:	100	0		
Maximum Video Capable Stations:	2400	0		
Maximum Video Capable IP Softphones:	2400	2		
Maximum Administered SIP Trunks:	4000	100		
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0		
Maximum Number of DS1 Boards with Echo Cancellation:	80	0		
Maximum TN2501 VAL Boards:	10	0		
Maximum Media Gateway VAL Sources:	50	0		
Maximum TN2602 Boards with 80 VoIP Channels:	128	0		
Maximum TN2602 Boards with 320 VoIP Channels:	128	0		
Maximum Number of Expanded Meet-me Conference Ports:	300	0		
(NOTE: You must logoff & login to effect the per	rmissio	on change	s.)	

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

display system-parameters customer-options	Page 3 of 11
OPTIONAL FEATURES	
Abbreviated Dialing Enhanced List? n Access Security Gateway (ASG)? n	Audible Message Waiting? y Authorization Codes? n
Analog Trunk Incoming Call ID? n	CAS Branch? n

HV; Reviewed:
SPOC 1/28/2013

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

On Page 5, verify that Private Networking and Processor Ethernet are set to y.

display system-parameters customer-option	ns Page 5 of 11
OPTIONAL	FEATURES
Multinational Locations?	n Station and Trunk
MSP? n	
Multiple Level Precedence & Preemption?	n Station as Virtual Extension? n
Multiple Locations?	n
	System Management Data Transfer? n
Personal Station Access (PSA)?	y Tenant Partitioning? n
PNC Duplication?	n Terminal Trans. Init. (TTI)? y
Port Network Support?	n Time of Day Routing? n
Posted Messages?	n TN2501 VAL Maximum Capacity? y
Uniform Dialing Plan?	У
Private Networking?	y Usage Allocation Enhancements? y
Processor and System MSP?	n
Processor Ethernet?	y Wideband Switching? n
	Wireless? n
Remote Office?	n
Restrict Call Forward Off Net?	У
Secondary Data Module?	У

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** for allowing inbound calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to be transferred 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
```

HV; Reviewed: SPOC 1/28/2013

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.

```
9 of 19
change system-parameters features
                                                                Page
                        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 Communication Manager (**procr**) and Session Manager (**InteropSM**). These node names will be needed for defining the service provider signaling group in **Section 5.7**.

```
      Page 1 of 2

      IP NODE NAMES

      Name
      IP Address

      InteropSM
      10.33.1.11

      default
      0.0.0.0

      msgserver
      10.10.97.246

      procr
      10.10.97.246

      procr6
      ::
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 1 was used for this purpose. Lumos Networks SIP Trunking supports the **G.711MU** and **G.729**A codecs. Default values can be used for all other fields.

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

On **Page 2**, to enable G.711 Pass Through fax, set the **Fax Mode** to **pass-through**. Otherwise, set the Fax Mode to **off**.

change ip-codec-set	= 1		Page	2 of	2
	IP Codec S	et			
	Allow Direct-IP Multimedia? n				
	Mode	Redundancy			
FAX	pass-through	1			
Modem	off	0			
TDD/TTY	US	3			
Clear-channel	n	0			

5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP network region 1 was chosen for the service provider trunk. Use the **change ip-network-region** 1 command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **bvwdev7.com**. This name appears in the From header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 1
                                                               Page 1 of 20
                              IP NETWORK REGION
 Region: 1
                 Authoritative Domain: bvwdev7.com
Location:
   Name: procr
MEDIA PARAMETERS
                               Intra-region IP-IP Direct Audio: yes
     Codec Set: 1
                               Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048
                                          IP Audio Hairpinning? n
  UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
       Audio PHB Value: 46
       Video PHB Value: 26
802.1P/O 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
```

5.6. Configure IP Interface for procr

Use the **change ip-interface procr** command to change the Processor Ethernet (procr) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the procr for SIP Trunk signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones. Ensure **Enable Interface** is **y** and **Network Region** is **1**

```
change ip-interface procr

IP INTERFACES

Type: PROCR

Enable Interface? y

Network Region: 1

IPV4 PARAMETERS

Node Name: procr

Subnet Mask: /26
```

5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups between Communication Manager and Session Manager. The signaling groups are used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group **10** was used for outbound calls and signaling group **11** was used for inbound calls and they were configured using the parameters highlighted below.

- Set the Group Type field to sip.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the value of **tcp** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as 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 **InteropSM.** 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 used port for TCP as 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 **bvwdev7.com** of the enterprise domain for signaling group **10** and blank value for signaling group **11**.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completion.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the Alternate Route Timer to 6. This defines the number of seconds the 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.
- Page 1 of add signaling-group 10 2 SIGNALING GROUP Group Number: 10 Group Type: sip IMS Enabled? n Transport Method: tcp Q-SIP? n IP Video? n Enforce SIPS URI for SRTP? y Peer Detection Enabled? y Peer Server: SM Near-end Node Name: procr Far-end Node Name: InteropSM Far-end Listen Port: 5060 Near-end Listen Port: 5060 Far-end Network Region: 1 Far-end Secondary Node Name: Far-end Domain: bvwdev7.com Bypass If IP Threshold Exceeded? n Incoming Dialog Loopbacks: eliminate RFC 3389 Comfort Noise? n DTMF over IP: rtp-payload Direct IP-IP Audio Connections? y Session Establishment Timer(min): 3 IP Audio Hairpinning? n Enable Layer 3 Test? y Initial IP-IP Direct Media? n H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
- Default values may be used for all other fields.

```
add signaling-group 11
                                                                        Page 1 of
                                                                                       2
                                   SIGNALING GROUP
 Group Number: 11
IMS Enabled? n
                                  Group Type: sip
                          Transport Method: tcp
        Q-SIP? n
     IP Video? n
                                                        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y Peer Server: SM
     Near-end Node Name: procr

--end Listen Port: 5060

Far-end Node Name:

Far-end Node Name:
                                                   Far-end Node Name: InteropSM
 Near-end Listen Port: 5060
                                              Far-end Listen Port: 5060
Far-end Domain:
                                                 Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks. Climin
DTMF over IP: rtp-payload
Session Establishment Timer(min): 3
Incoming Dialog Loopbacks: eliminate
                                                  RFC 3389 Comfort Noise? n
                                                 Direct IP-IP Audio Connections? y
                                                            IP Audio Hairpinning? n
                                                      Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n
                                                       Alternate Route Timer(sec): 6
```

5.8. Trunk Group

Use the **add trunk-group** command to create trunk groups for the signaling groups created in **Section 5.7**. For the compliance test, trunk group **10** was used for outbound calls and trunk group **11** was used for inbound calls and they were 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. (i.e. ***010**, ***011**).
- Set **Direction** to **outgoing** for trunk group **10** and **incoming** for trunk group **11**.
- Set the **Service Type** field to **public-ntwrk**.
- Set Member Assignment Method to auto.
- Set the **Signaling Group** to the signaling group configured in **Section 5.7**. Trunk group **10** was associated to signaling group **10** and trunk group **11** was associated to signaling group **11**.
- 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.

```
1 of 21
add trunk-group 10
                                                                          Page
                                    TRUNK GROUP
Group Number: 10 Group Type: sip CDR Reports: y
Group Name: LumosNetworks COR: 1 TN: 1 TAC: *010
Direction: outgoing Outgoing Display? n
 Dial Access? n
                                                          Night Service:
Queue Length: 0
Service Type: public-ntwrk Auth Code? n
                                                       Member Assignment Method: auto
                                                                  Signaling Group: 10
                                                               Number of Members: 50
                                                                                  1 of 21
add trunk-group 11
                                                                          Page
                                      TRUNK GROUP
  coup Number: 11Group Type: sipCDR Reports: yGroup Name: LumosNetworksCOR: 1TN: 1TAC: *011Direction: incomingOutpring Direction DirectionThe direction Direction Direction
Group Number: 11
   Direction: incoming Outgoing Display? n
                                                         Night Service:
 Dial Access? n
Queue Length: 0
Service Type: public-ntwrk Auth Code? n
                                                       Member Assignment Method: auto
```

Signaling Group: 11 Number of Members: 50

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. The compliance test used 10 digit numbering format. Thus, **Numbering Format** was set to **private** and the **Numbering Format** field in the route pattern was set to **unk-unk** (see **Section 5.10**).

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

```
add trunk-group 10

TRUNK FEATURES

ACA Assignment? n

Numbering Format: private

UUI Treatment: service-provider

Replace Restricted Numbers? y

Replace Unavailable Numbers? y

Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y

DSN Term? n
```

```
add trunk-group 11

TRUNK FEATURES

ACA Assignment? n

Numbering Format: private

UUI Treatment: service-provider

Replace Restricted Numbers? y

Replace Unavailable Numbers? y

Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y

DSN Term? n
```

On Page 4, set the Network Call Redirection field to y.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been re-directed. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to **101**.

```
add trunk-group 10
                                                                           4 of 21
                                                                    Page
                              PROTOCOL VARIATIONS
                          Mark Users as Phone? n
                 Prepend '+' to Calling Number? n
           Send Transferring Party Information? n
                      Network Call Redirection? y
                         Send Diversion Header? y
                       Support Request History? n
                  Telephone Event Payload Type: 101
           Convert 180 to 183 for Early Media? n
     Always Use re-INVITE for Display Updates? n
           Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
                                 Enable Q-SIP? n
```

5.9. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.8**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs). It is used to authenticate the caller.

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private-numbering entry can be applied for all extensions. In the example below, all stations with a 4-digit extension beginning with **7** will send the calling party number as the **Private Prefix** plus the extension number.

```
Page 1 of
                                                                            2
change private-numbering 0
                          NUMBERING - PRIVATE FORMAT
Ext Ext
                  Trk
                             Private
                                             Total
Len Code
                  Grp(s)
                            Prefix
                                             Len
 4 7
                  10
                             540941
                                             10
                                                    Total Administered: 21
                                                     Maximum Entries: 540
```

5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit **9** is used as the ARS access code. Enterprise callers will dial **9** to reach an "outside line". This common configuration is illustrated below. 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				NI ANATVET			Page	1 of	12
			DIAL PLAN ANALYSIS TABLE Location: all		Pe	rcent Fi	ıll: 2		
Dialed String		. Call h Type	Dialed String	Total Ca Length T		Dialed String	Total Length	Call Type	
40 6 7 9 *	4 4 1 4 4	udp ext ext fac dac dac							

Use the **change feature-access-codes** command to configure **9** as the **Auto Route Selection** (**ARS**) – **Access Code 2**.

change feature-access-codes	Page	1 of	11
FEATURE ACCESS CODE (F	AC)		
Abbreviated Dialing List1 Access Code:			
Abbreviated Dialing List2 Access Code:			
Abbreviated Dialing List3 Access Code:			
Abbreviated Dial - Prgm Group List Access Code:			
Announcement Access Code: *007			
Answer Back Access Code:			
Auto Alternate Routing (AAR) Access Code: *00			
Auto Route Selection (ARS) - Access Code 1:	Access Code 2: 9		
Automatic Callback Activation: *033	Deactivation:	#033	
Call Forwarding Activation Busy/DA: *30 All: *031	Deactivation:	#030	
Call Forwarding Enhanced Status: Act:	Deactivation:		
Call Park Access Code: *040			
Call Pickup Access Code: *041			
CAS Remote Hold/Answer Hold-Unhold Access Code: *042			
CDR Account Code Access Code:			
Change COR Access Code:			
Change Coverage Access Code:			
Conditional Call Extend Activation:	Deactivation:		
Contact Closure Open Code: *080		#080	
	51050 00de.		

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

change ars analysis O						Page	1 of	2
	P	-	GIT ANALY Location:		LE	Percent 1	Full: 1	
Dialed	Tot	al	Route	Call	Node	ANI		
String	Min	Max	Pattern	Type	Num	Reqd		
0	1	11	10	ор		n		
011	10	18	10	intl		n		
1613	11	11	10	pubu		n		
1800	11	11	10	pubu		n		
1877	11	11	10	pubu		n		
1908	11	11	10	pubu		n		
411	3	3	10	svcl		n		
911	3	3	10	svcl		n		

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used in route pattern 10 for the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **10** 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.
- **Numbering Format**: Set this field to **unk-unk** since private Numbering Format should be used for this route (see **Section 5.8**).

З change route-pattern 10 Page 1 of Pattern Number: 5 Pattern Name: LumosNetworks SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No.InsertedNoMrk Lmt List DelDigits DCS/ IXC QSIG Dqts Intw 1: 10 ٥ n user 2: n user 3: n user 4: n user 5: n user 6: user n BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 M 4 W Request Dgts Format Subaddress 1: yyyyyn n rest unk-unk none 2: yyyyyn n rest none 3: y y y y y n n rest none 4: yyyyyn n rest none 5: ууууул п rest none 6: yyyyyn n rest none

5.11. Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Service Provider is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group **11**. As an example, use the **change inc-call-handling-trmt trunk-group 11** to convert incoming DID numbers **540941**xxxx to 4 digit extension xxxx by deleting **6** of the incoming digits.

change inc-call-	handling-trm†	trunk-grou	ıp 11	Page	1 of	3
	INCOMJ	ING CALL HAN	NDLING TREATMENT			
Service/	Number	Number	Del Insert			
Feature	Len	Digits				
public-ntwrk	10	540941	6			

5.12. Communication Manager Stations

In the sample configuration, four digit station extensions were used with the format 7xxx. Use the **add station 7750** command to add an Avaya H.323 IP telephone

- Enter Type: 9640, Name: Ext_7750, Security Code: 1234, Coverage Path 1: 1
- Leave other values as default.

add station 7750	Page	1 of 5
	STATION	
Extension: 7750	Lock Messages? n	BCC: 0
Туре: 9640	Security Code: 1234	TN: 1
Port: S00008	Coverage Path 1: 1	COR: 1
Name: Ext 7750	Coverage Path 2:	COS: 1
-	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern:	1
-	Message Lamp Ext:	7750
Speakerphone: 2-way	Mute Button Enabled?	V
Display Language: english		-
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone?	n
barvivabie frame bebe. y		
	IP Video?	n
	II VIGEO:	11
	Customizable Labels?	Y

5.13. Save Avaya Aura® Communication Manager Configuration Changes

Use the **save translation** command to save the configuration.

6. Configure Avaya Aura® Session Manager

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

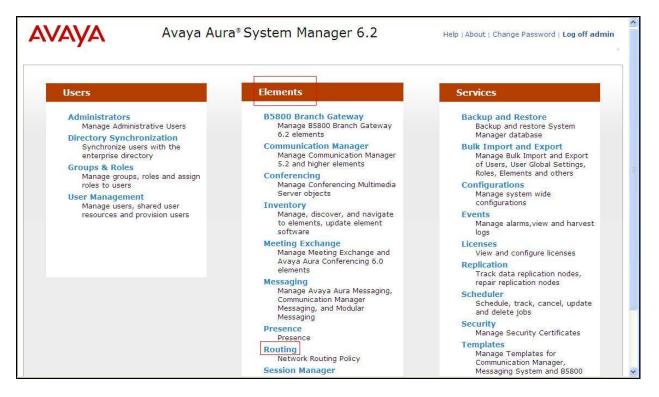
- SIP Domain.
- Logical/physical Location that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to Communication Manager, SBCE and Session Manager.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which define route destinations and control call routing between the SIP Entities.
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call.

HV; Reviewed:
SPOC 1/28/2013

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

6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL as https://<ip-address>/SMGR, where <ip-address> is the IP address of System Manager. At the System Manager Log On screen, enter appropriate User ID and Password and press the Log On button (not shown). The initial screen shown below is then displayed.



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

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

AVAYA	Avaya Aura® System Manager 6.2	Help About Change Password Log off admir
		Routing * Home
Routing	Home /Elements / Routing	
Domains		Help ?
Locations	Introduction to Network Routing Policy	
Adaptations	Network Routing Policy consists of several routing applications like "Domai	ins", "Locations", "SIP Entities", etc.
SIP Entities	The recommended order to use the routing applications (that means the	
Entity Links	configuration is as follows:	
Time Ranges	Step 1: Create "Domains" of type SIP (other routing applications are	referring domains of type SIP).
Routing Policies	Step 2: Create "Locations"	
Dial Patterns	Step 2: Cleate Locations	
Regular Expressions	Step 3: Create "Adaptations"	
Defaults	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	I Gateways, SIP Trunks)
	- Assign the appropriate "Locations", "Adaptations" and "Outbour	nd Proxies"
	Step 5: Create the "Entity Links"	
	- Between Session Managers	
	- Between Session Managers and "other SIP Entities"	
	Step 6: Create "Time Ranges"	

6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain **bvwdev7.com**. Navigate to **Routing** \rightarrow **Domains** in the left-hand navigation pane and click the **New** button in the right pane. In the new right pane that appears (not shown), 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) to save.

The screen below shows the entry for the enterprise domain.

Αναγα	Avaya Aura [®] System Manager 6.2				ed on at December 17, 2012 8:43 PM ange Password Log off admin		
							Routing * Home
Routing	↓ Hom	e /Elements / Routin	g / Domains				
Domains							Help ?
Locations	Doma	ain Management					
Adaptations	-	al New Developer	e Delete More Action				
SIP Entities	Edi	it New Duplication	e Delete More Action	5 *			
Entity Links		ems Refresh					Filter: Enable
Time Ranges		ems kerresn		1		character and	Filter: Enable
Routing Policies		Name		Туре	Default	Notes	
Dial Patterns		bvwdev7.com		sip		Lumos Networks	
Regular Expressions							
Defaults							
	Sele	ect : All <mark>,</mark> None					

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. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville**, which includes all equipment in the enterprise including Communication Manager, Session Manager and Avaya SBCE.

To add a Location, navigate to **Routing** \rightarrow **Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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

Click **Commit** to save.

AVAYA	Avaya Aura® System Manager 6.2	Last Logged on at November 19, 2012 2:27 PM Help About Change Password Log off admin
		Routing * Home
Routing	Home /Elements / Routing / Locations	
Domains		Help ?
Locations	Location Details	Commit Cancel
Adaptations		
SIP Entities	General	7
Entity Links	* Name: Belleville	
Time Ranges	Notes:	
Routing Policies		
Dial Patterns	Overall Managed Bandwidth	
Regular Expressions		
Defaults	Managed Bandwidth Units: Kbit/sec 💌	
	Total Bandwidth: 100000	
	Multimedia Bandwidth: 100000	
	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	

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

6.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and Avaya SBCE. Navigate to **Routing** \rightarrow **SIP Entities** 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.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	26 of 59
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LNCM62SM62SBCE

- Name: Enter a descriptive name.
- FQDN or IP Address: Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- Type: Select Session Manager for Session Manager, CM for Communication Manager and Other for Avaya SBCE.
 Adaptation: This field is only present if Type is not set to Session Manager. Adaptation module was not used in this configuration.
 Location: Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location Belleville.
- **Time Zone:** Select the time zone for the Location above.

In this configuration, there are three SIP Entities.

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Avaya Session Border Controller for Enterprise SIP Entity

6.4.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **InteropSM**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.1.11**

AVAVA	Avaya Aura® System Manager 6.2				on at November 19, 20 ge Password Log of	
					Routing *	Home
Routing	 Home / Elements / Routin 	g / SIP Entities				
Domains						Help ?
Locations	SIP Entity Details				Commit	Cancel
Adaptations	General					
SIP Entities		* Name:	InteropSM			
Entity Links		* FQDN or IP Address:	· · · · · · · · · · · · · · · · · · ·			
Time Ranges						
Routing Policies		Type:	Session Manager			
Dial Patterns		Notes:	Interop Session Manager			
Regular Expressions						
Defaults		Location:	Belleville 💌			
		Outbound Proxy:	×			
		Time Zone:	America/Toronto			
		Credential name:				
	SIP Link Monitoring	SIP Link Monitoring:	Use Session Manager Configuration 💌			

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 Session Manager listens for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain.

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

The compliance test used port **5060** with **TCP** for connecting to Communication Manager and port **5060** with **UDP** for connecting to Avaya SBCE.

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

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

Port						
TCP F	ailover port:					
TLS F	ailover port:					
Add	Remove					
	S					
1577-1078	ms Refresh					
5 Ite	ins Refresh					
5 Ite	Port	*	Protocol	Default Domain	Notes	
_			Protocol TCP 🗸	Default Domain bvwdev7.com	Notes	

6.4.2. Configure Communication Manager SIP Entity

The following screen shows the addition of the Communication Manager SIP Entity named G450_CM62. 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 during Session Manager installation for use with all other SIP traffic within the enterprise. The FQDN or IP Address field is set to the IP address of Communication Manager 10.10.97.246. The Location field is set to Belleville which is the Location that includes the subnet where Communication Manager resides. Note that CM was selected for Type.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	28 of 59
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LNCM62SM62SBCE

AVAYA		ogged on at November 19, 2012 2:27 Pl Change Password Log off admin
		Routing * Home
Routing	Home /Elements / Routing / SIP Entities	
Domains		Help ?
Locations	SIP Entity Details	Commit Cancel
Adaptations	General	
SIP Entities	* Name: G450_CM62	
Entity Links	* FQDN or IP Address: 10.10.97.246	
Time Ranges		
Routing Policies	Type: CM	
Dial Patterns	Notes: For CM6.2	
Regular Expressions		
Defaults	Adaptation:	
	Location: Belleville 💌	
	Time Zone: America/Toronto	
	Override Port & Transport with DNS SRV:	
	* SIP Timer B/F (in seconds): 4	
	Credential name:	
	Call Detail Recording: none	

6.4.3. Configure Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the addition of Avaya SBCE SIP entity named **AvayaSBCE_UDP**. The **FQDN or IP Address** field is set to the IP address of the SBC's private network interface **10.10.97.189**. The **Location** field is set to **Belleville** which includes the subnet where the Avaya SBCE resides. Note that **Other** was selected for **Type**.

AVAYA	Avaya Aura® System Manager	Last Logged on at November 19, 2012 2:27 PM Help About Change Password Log off admin	
			Routing * Home
Routing	 Home / Elements / Routing / SIP Entities 		
Domains			Help ?
Locations	SIP Entity Details		Commit Cancel
Adaptations	General		
SIP Entities	* Name:	AvayaSBCE UDP	
Entity Links	* FQDN or IP Address:	10 10 97 189	
Time Ranges			
Routing Policies		other	
Dial Patterns	Notes:	AvayaSBCE_UDP	
Regular Expressions			
Defaults	Adaptation:	:	
	Location:	: Belleville 🛩	
	Time Zone:	: America/Toronto	
	Override Port & Transport with DNS SRV:	:	
	* SIP Timer B/F (in seconds):	: 4	
	Credential name:	:	
	Call Detail Recording:	none 💙	

6.5. 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.

HV; Reviewed:
SPOC 1/28/2013

To add an Entity Link, navigate to **Routing** \rightarrow **Entity Links** 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:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager being used.
- **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 the Communication Manager Entity Link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **SIP Entity 2:** Select the name of the other system as defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager Entity Link, this must match the Near-end Listen Port defined on the Communication Manager signaling group in Section **5.7**.
- **Trusted:** Check this box. Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.4** will be denied.

Click **Commit** to save.

The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.7**.

AVAYA	Avaya Aura	System M	anager		Last Logged on at November 19, 2012 2:27 F Help About Change Password Log off admir					
								Routing * Home		
Routing	Home /Elements / Ro	uting / Entity Link	s							
Domains								Help ?		
Locations	Entity Links							Commit Cancel		
Adaptations										
SIP Entities	-									
Entity Links										
Time Ranges	1 Item Refresh							Filter: Enable		
Routing Policies	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes		
Dial Patterns	* InteropSM_G450_C	* InteropSM 💌	TCP 💙	* 5060	* G450_CM62	* 5060	Trusted 💌			
Regular Expressions										
Defaults										
	* Input Required							Commit Cancel		

The following screen illustrates the Entity Links to Avaya SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.2.4 and 7.2.6**.

AVAYA	Last Logged or Avaya Aura® System Manager 6.2 Help About Change									on at November 19, 2012 2:27 PM ge Password Log off admin				
									Routing	Home				
Routing	Home / Elements / Rome	uting / Entity Link	s											
Domains										Help ?				
Locations	Entity Links								Commit	Cancel				
Adaptations														
SIP Entities	r													
Entity Links														
Time Ranges	1 Item Refresh								Filter:	Enable				
Routing Policies	Name	SIP Entity 1	Protocol	Port	SIP Entity 2		Port	Connection Policy	Notes					
Dial Patterns	* InteropSM_AvayaSI	* InteropSM 💌	UDP 💌	* 5060	* AvayaSBCE_UDP	~	* 5060	Trusted 🔽	[
Regular Expressions														
Defaults	r.													
	* Input Required								Commit	Cancel				

6.6. Configure Time Ranges

Time Ranges is configured for time-based-routing. In order to add a Time Ranges, select **Routing** \rightarrow **Time Ranges** and then click **New** button. The Routing Policies shown subsequently will use the 24/7 range since time-based routing was not the focus of these Application Notes.

AVAYA	A	Avaya Aura® System Manager 6.2									Last Logged on at November 22, 2012 2:34 Help About Change Password Log off adm			
												Routing *	Home	
Routing	• Home	/Elements /	Routing /	Time Ra	nges									
Domains													Help ?	
Locations	Time R	Ranges												
Adaptations	Edit	New	Duplicate	Delete	M	ore Actions	- 1							
SIP Entities	Etait	[New]	Jupicace	Delere		Te Accions								
Entity Links		- Defeat										Filter: En	a shi s	
Time Ranges		m Refresh	_	_		_	_	_				Filter: En	lable	
Routing Policies		Name	Мо	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes		
Dial Patterns		<u>24/7</u>	2					V		00:00	23:59	Time Range 24/7		
Regular Expressions	Selec	ct : All, None												
Defaults														

6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two Routing Policies must be added: one for Communication Manager and one for Avaya SBCE. To add a Routing Policy, navigate to **Routing** \rightarrow **Routing Policies** 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.

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	31 of 59
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LNCM62SM62SBCE

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

The following screen shows the **Routing Policy Details** for the policy named **To_G450_CM62** associated with incoming PSTN calls from Lumos Networks to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **G450_CM62**

VAYA	Avaya Aura® Sys	stem Manager 6.2	Help A	Last Logged on at November 19, 2012 2:27 bout Change Password Log off admi
				Routing * Home
Routing	Home / Elements / Routing /	Routing Policies		
Domains				Help
Locations	Routing Policy Details			Commit Cancel
Adaptations				
SIP Entities	General			
Entity Links		* Name: To_G450_CM62		
Time Ranges		Disabled:		
Routing Policies		* Retries: 0		
Dial Patterns				
Regular Expressions		Notes:		
Defaults				
	SIP Entity as Destination	1		
	Select			
	Name	FQDN or IP Address	Туре	Notes
	G450_CM62	10.10.97.246	CM	For CM6.2

The following screen shows the **Routing Policy Details** for the policy named **To_Lumos_Networks** associated with outgoing calls from Communication Manager to the PSTN via Lumos Networks through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **AvayaSBCE_UDP**

AVAYA	Avaya Aura® Sy	stem Manager 6.2	He	Last Logged on at December 17, 2012 8:43 PM elp About Change Password Log off admin
	Home /Elements / Routing /	Pouting Policies		Routing * Home
Routing Domains Locations Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions Defaults	Routing Policy Details General SIP Entity as Destination Select	* Name: To_Lumos_Networks Disabled: * Retries: 0 Notes: For Lumos Networks		Help 7 Commit Cancel
	Name	FQDN or IP Address	Туре	Notes
	AvayaSBCE_UDP	10.10.97.189	Other	AvayaSBCE_UDP

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from Communication Manager to Lumos Networks through the Avaya SBCE and vice versa. Dial Patterns define which Route Policy will be selected as route destination for a particular call based on the dialed digits, destination Domain and originating Location.

To add a Dial Pattern, navigate to **Routing** \rightarrow **Dial Patterns** 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.

- **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., 1800 Toll free call, 011 international call, etc.) were similarly defined.

The first example shows that outbound 11-digit dialed numbers that begin with **1613** and have a destination SIP Domain of **bvwdev7.com** uses the **AvayaSBCE_UDP** Routing Policy as defined in **Section 6.7**.

NVAYA	Av	vaya Aura®Systen	Last Logged on at December 17, 2012 8:- Help About Change Password Log off adu						
Routing	• Home	/Elements / Routing / Dial P	atterns				-	Routing	Hom
Domains									Help
Locations	Dial Pa	attern Details						Commit	Cance
Adaptations									
SIP Entities	Gene	ral	0						
Entity Links			* Pattern: 1613						
Time Ranges			* Min: 11						
Routing Policies			* Max: 11	-					
Dial Patterns				-					
Regular Expressions			ergency Call: 🗌						
Defaults		Emerg	ency Priority: 1						
		Eme	ergency Type:						
			SIP Domain: bywe	dev7.com 💌					
			Notes: Lumo	s Networks Outbound Ca	alls				
	Add	Remove	ing Policies						
	1 Ite	m Refresh						Filter: I	Enable
		Originating Location Name 👻	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy	g Notes
		-ALL-	Any Locations	To Lumos Networks	D	Г	AvayaSBCE UDP	For Lum Network	

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

Also note that **-ALL-** was selected for **Originating Location Name**. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed outbound back to the PSTN.

The second example shows that inbound 10-digit numbers that start with **540** uses Routing Policy Destination **G450_CM62** as defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by Lumos Networks.

AVAYA	Avaya Aura [®] System Manager 6.2	Help /	Last Logged on at December 17, 2012 8:43 f Help About Change Password Log off admir				
				1	Routing *	Home	
Routing	Home /Elements / Routing / Dial Patterns					1	
Domains						Help	
Locations	Dial Pattern Details			1	Commit	Cancel	
Adaptations							
SIP Entities	General						
Entity Links	* Pattern: 540						
Time Ranges	* Min: 10						
Routing Policies	* Max: 10						
Dial Patterns	Emergency Call:						
Regular Expressions							
Defaults	Emergency Priority: 1						
	Emergency Type:						
	SIP Domain: bvwdev7.com						
	Notes: Lumos Networks Int	ound Calls					
	Originating Locations and Routing Policies						
	1 Item Refresh				Filter:	Enable	
	C Originating Location Name 1 A Originating Location Notes Name	Policy Rank 2 .*	Routing Policy Disabled	Routing Policy Destination	Routin Notes	g Policy	
	☐ Belleville To_G450_	CM62 0	Π	G450_CM62	For Lum Network		

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.

	A	vaya A	Aura	° Sys	stem Mana	ger 6.2		Help	Last Logged on at December 17, 2012 8:43 About Change Password Log off adm
									Routing * Hom
Routing	↓ Home	/Elemen	ts / Ro	uting /	Dial Patterns				
Domains									Help
Locations	Dial Pa	atterns							
Adaptations	Edit	New	Duo	licate	Delete	1ore Actions •			
SIP Entities	ECIL	INEW	μυυ	modue	Perece	IOLE ACCIONS .			
Entity Links	40.15	ems Refre	ada						Filter: Enable
Time Ranges	and the second							The second secon	Color States
Routing Policies		Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
Dial Patterns		0	1	11				bvwdev7.com	Lumos Networks Operator Outbound Calls
Regular Expressions		011	14	14				bvwdev7.com	Lumos Networks International Outbound Call
Defaults		<u>540</u>	10	10				bvwdev7.com	Lumos Networks Inbound Calls
		1613	11	11				bvwdev7.com	Lumos Networks Outbound Calls
		1800	11	11				bvwdev7.com	Lumos Networks Toll Free Outbound Calls
		<u>1877</u>	11	11				bvwdev7.com	Lumos Networks Toll Free Outbound Calls
		1908	11	11				bvwdev7.com	Lumos Networks Outbound Calls
		411	з	3				bvwdev7.com	Lumos Networks 411 Outbound Calls
		911	3	з				bywdev7.com	Lumos Networks 911 Outbound Calls

7. Configure Avaya Session Border Controller for Enterprise

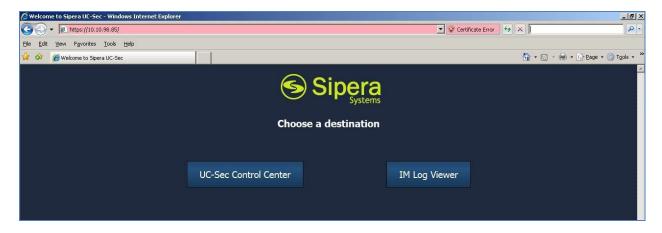
This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and Lumos Networks system.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Lumos Networks system resides on the Public side of the network.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see **Section 11** of these Application Notes.

7.1. Log in Avaya Session Border Controller for Enterprise

Access the web interface by typing "**https://x.x.x.x**" (where x.x.x.x is the management IP of the Avaya SBCE).



Select UC-Sec Control Center and enter the Login ID and Password.

Sipera Systems HARM-VERIFY-PROTECT	Sign in Login ID ucsec Password ••••••••••••••••••••••••••••••••••••
The UC-Sec [™] family of products from Sipera 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 Sipera Systems website to learn more.	
NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this	

HV; Reviewed: SPOC 1/28/2013 Solution & Interoperability Test Lab Application Notes ©2013 Avaya Inc. All Rights Reserved. 36 of 59 LNCM62SM62SBCE

7.2. Global Profiles

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

7.2.1. Configure Server Interworking - Avaya site

Server Interworking allows administrator to configure and manage various SIP call serverspecific capabilities such as call hold, 180 Handling, etc.

From the menu on the left-hand side, select **Global Profiles** \rightarrow **Server Interworking** \rightarrow **Add Profile**:

- Enter Profile name: **SM62**.
- Check Hold Support as RFC2543.
- Check **Diversion Header Support** as **Yes**.
- All other options on the General Tab can be left at default.

On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** Tabs: All options can be left at default. Click **Finish** (not shown).

The following screen shows a Session Manager server interworking profile (named: SM62) was added.

	atistics 🔄 Logs 👼 Diagnostics			Logout 🙆 Hel
UC-Sec Control Center SWelcome	Global Profiles > Server Interworking: SM	62		
Administration	Add Profile		Rename Profile	Clone Profile Delete Profile
Backup/Restore System Management	Showing page 2 of 2.		Click here to add a description.	
Global Parameters	<< < Interworking	General Timers URI Manipulation Heade	r Manipulation Advanced	
Global Profiles	Profiles		General	
Domain DoS	SM62	Hold Support	RFC2543	
Server Interworking		180 Handling	None	
Phone Interworking		181 Handling	None	
Routing		76		
Server Configuration	Skip to page	182 Handling	None	
Subscriber Profiles		183 Handling	None	
Signaling Manipulation		Refer Handling	No	
BURI Groups		3xx Handling	No	
SIP Cluster Domain Policies		Diversion Header Support	Yes	
Device Specific Settings		Delayed SDP Handling	No	
Troubleshooting		T.38 Support	No	
M Logging		URI Scheme	SIP	
		Via Header Format	RFC3261	
			Privacy	
		Privacy Enabled	No	
		User Name		
		P-Asserted-Identity	No	
		P-Preferred-Identity	No	
		Privacy Header		
			DTMF	
		DTMF Support	None	

7.2.2. Configure Server Interworking – Lumos Networks site

From the menu on the left-hand side, select Global Profiles \rightarrow Server Internetworking \rightarrow Add Profile

- Enter Profile name: Lumos.
- Check Hold Support as RFC2543.
- Check **Diversion Header Support** as **Yes**.
- All other options on the General Tab can be left at default.

On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** Tabs: All options can be left at default. Click **Finish** (not shown).

The following screen shows a Lumos Networks server interworking profile (named: Lumos) was added.

Alarms Incidents	tatistics 📃 Logs 👼 Diagnostics	Lusers	🛃 Lo	gout 🕜 <u>H</u> elp
UC-Sec Control Center	Global Profiles > Server Interworking: Lum	0S		
S Welcome	Add Profile		Rename Profile Clone Profile	Delete Profile
Backup/Restore	Showing page 2 of 2.	c	lick here to add a description.	
😫 System Management	<< < Interworking	General Timers URI Manipulation Header Manipu	lation Advanced	
Global Parameters	Profiles			
📓 Domain DoS	SM62		General	
Fingerprint Server Interworking	Lumos	Hold Support	RFC2543	
Phone Interworking		180 Handling	None	
Media Forking		181 Handling	None	
Routing		182 Handling	None	
📇 Subscriber Profiles		183 Handling	None	
Topology Hiding Signaling Manipulation	· · · · · · · · · · · · · · · · · · ·	Refer Handling	No	
Bighanny Manipulation	Skip to page	3xx Handling	Yes	
SIP Cluster		Diversion Header Support	Yes	
Domain Policies Device Specific Settings		Delayed SDP Handling	No	
Troubleshooting		T.38 Support	Yes	
TLS Management IM Logging		UBI Scheme	SIP	
		Via Header Format	RFC3261	
			RFC3201	
			Privacy	
		Privacy Enabled	No	
		User Name		
		P-Asserted-Identity	No	
		P-Preferred-Identity	No	
		Privacy Header		
			DTMF	
		DTME Support	DIMF	
		DTMF Support	INDIRE	

7.2.3. Configure URI Groups

The URI Group feature allows creation of any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group.

From the menu on the left-hand side, select **Global Profiles** \rightarrow **URI Groups**

- Select Add Groups, enter Group Name: Lumos Networks
- Edit the URI Type: **Plain** (not shown)
- Add URI: <u>*@10.10.98.112</u>, <u>*@10.200.100.10</u>, <u>*@192.168.114.203</u>, <u>*@anonymous.invalid</u>, <u>*@bvwdev7.com</u>, and <u>*@ia.ntelos.net</u>,

HV; Reviewed: SPOC 1/28/2013

• Click **Finish** (not shown).

Alarms 🔲 Incidents 🔢 Sta	atistics 📃 Logs 👼 Diagnostics	Users	🚮 Logout 🔞 H
C-Sec Control Center	Global Profiles > URI Groups: Lumos Netw	orks	
Welcome Administration	Add Group		Rename Group Delete Group
Backup/Restore	URI Groups		Click here to add a description.
System Management	Lumos Networks	URI Group	
Global Parameters Global Profiles			
Bomain DoS			Add URI
🏀 Fingerprint			
Server Interworking			URI Listing
Phone Interworking		*@10.10.98.112	0 X
Routing		*@10.200.100.10	2 X
Server Configuration		*@192.168.114.203	2 X
Subscriber Profiles		*@anonymous.invalid	2 X
Topology Hiding Signaling Manipulation		*@bvwdev7.com	0 X
URI Groups		*@ia.ntelos.net	2 X

7.2.4. Configure Routing – Avaya site

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.

From the menu on the left-hand side, select Global Profiles \rightarrow Routing \rightarrow Add Profile Enter Profile Name: Lumos_To_SM62

- URI Group: Lumos Networks
- Next Hop Server 1: 10.33.1.11 (Session Manager IP address)
- Check Next Hop Priority
- Outgoing Transport: UDP
- Click **Finish** (not shown).

🕘 Alarms 🔲 Incidents 🔢	Statistics 🔄 Logs	Diagnostics	Lsers								2 L	ogout 🕜
UC-Sec Control Center SWelcome	Global Profiles > Rou	ting: Lumos_To_SM6 Add Profile	2				Rename Pr	rofile	Ck	one Prof	ile	Delete Profil
Backup/Restore	Showing p	age 2 of 2			Cli	ck here to add a descripti	on.					
System Management Global Parameters	<< < Routing	CONTRACTOR OF THE OWNER OF	Routing Pro	file		10						
 Global Profiles Domain DoS 	Lumos_To_SM6	2									Add Ro	outing Rule
) Fingerprint Server Interworking Phone Interworking			Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR		Next Hop in Dialog	lgnore Route Header	Outgoing Transport
Media Forking	_	page	1	Lumos Networks	10.33.1.11	122	V					UDP .

7.2.5. Configure Routing – Lumos Networks site

The Routing Profile allows administrator to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select Global Profiles \rightarrow Routing \rightarrow Add Profile Enter Profile Name: SM62_To_Lumos

- URI Group: Lumos Networks
- Next Hop Server 1: 192.168.114.203 (IP Address provided by Customer)
- Check Next Hop Priority
- Outgoing Transport as UDP
- Click **Finish** (not shown).

Additional Incidentia	Statistics 📃 Logs 👼 Diagnostics	Lsers								9 L	ogout 🕜
UC-Sec Control Center S Welcome	Global Profiles > Routing: SM62_To_Lumo Add Profile	os				Rename Pi	rofile	Clo	ne Profil	le	Delete Prof
Backup/Restore	Showing page 2 of 2.			Cli	ck here to add a descripti	on.					
System Management Global Parameters Global Profiles Domain DoS	<< < Routing Profiles Lumos_To_SM62	Routing Prof	ile							Add Ro	outing Rule
Fingerprint Server Interworking Phone Interworking		Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV		Route	Outgoing Transport
Media Forking	Skip to page	1	Lumos Networks	192.168.114.203		V					UDP
Pro r		1	Lumos NetWorks	192.108.114.203		M	L			12	UDP

7.2.6. Configure Server – Avaya Aura® Session Manager

The Server Configuration screen contains four tabs: General, Authentication, Heartbeat, and Advanced. Together, these tabs allow configuration and management of various SIP call server-specific parameters such as UDP port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles** \rightarrow **Server Configuration** \rightarrow **Add Profile**.

Enter profile name: **SM62** On **General** tab:

- Server Type: Select Call Server
- IP Address/FQDNs: 10.33.1.11 (Session Manager IP Address)
- Supported Transports: UDP
- UDP Port: 5060

UC-Sec Control Cen Welcome ucsec, you signed in as Admin. Cu					Sipera Systems
Alarms Incidents K	stics 🗐 Logs 👼 Diagnostics 🚦	Users			Logout 🞯 Help
	Global Profiles > Server Configuration: SM62				
S Welcome	Add Profile			Rename Profile Clone Profile	Delete Profile
Backup/Restore	Profile	General Authentication Heartbeat Advanced			
System Management	SM62				
Global Parameters			General		
4 Global Profiles		Server Type	Call Server		
Domain DoS		IP Addresses / FQDNs	10.33.1.11		
Server Interworking		Supported Transports	UDP		
S Phone Interworking		UDP Port	5060		
Media Forking		OUPPon	5060		
Server Configuration			Edit		in the second

On the **Advanced** tab:

- Select SM62 for Interworking Profile
- Click **Finish** (not shown).

🕘 Alarms 🔲 Incidents 🏦 S	tatistics 📃 Logs 🗾 Diagnostics				2	Logout 🙆 Hel
UC-Sec Control Center Swelcome Administration	Global Profiles > Server Configuration: S Add Profile Profile	Me2 General Authentication Heartbeat Advanced		Rename Profile	Clone Profile	Delete Profile
System Management	SM62		Advanced			
 Global Profiles Domain DoS 		Enable DoS Protection				
Eingerprint		Enable Grooming	Г			
Server Interworking		Interworking Profile	SM62			
🚯 Phone Interworking 👔 Media Forking		Signaling Manipulation Script	None			
Routing		TCP Connection Type	SUBID			
Server Configuration		UDP Connection Type	SUBID			
 Topology Hiding Signaling Manipulation URI Groups 			Edit			

7.2.7. Configure Server – Lumos Networks ACME Packet SBC

From the menu on the left-hand side, select **Global Profiles** \rightarrow **Server Configuration** \rightarrow **Add Profile**

Enter profile name: Lumos

On General tab:

- Server Type: Select Trunk Server
- IP Address: 192.168.96.143 (Lumos Networks ACME Packet SBC IP Address)
- Supported Transports: UDP
- UDP Port: 5060

UC-Sec Control Co Welcome ucsec, you signed in as Admin		is 🚇 Users		Sipera Systems
UC-Sec Control Center Welcome Administration Backup/Restore	Global Profiles > Server Configuration : Add Profile Profile	umos General Authentication Heartbeat Advance	Rename Profile DoS Whitelist DoS Protection	Clone Profile Delete Profile
 System Management Global Parameters Global Profiles 	SM62 Lumos	Server Type	General Trunk Server	
📓 Domain DoS 🍥 Fingerprint 🗣 Server Interworking		IP Addresses / FQDNs Supported Transports	192.168.114.203 UDP	
Phone Interworking Media Forking Routing Server Configuration Subscriber Profiles		UDP Port	5060 Edit	

On the **Advanced** tab:

- Select Lumos for Interworking Profile
- Click **Finish** (not shown).

Alarms 🔲 Incidents 🔢	tatistics 🔄 Logs 👼 Diagnostics	Lusers		Logout 🕜 He
UC-Sec Control Center	Global Profiles > Server Configuration: Lu	mos		
S Welcome Administration	Add Profile		Rename Profile Clone Profil	e Delete Profile
Backup/Restore	Profile	General Authentication Heartbeat Adva	nced DoS Whitelist DoS Protection	
System Management	SM62		Advanced	
Global Parameters Global Profiles	Lumos	Enable DoS Protection		
📓 Domain DoS		Enable Grooming		
🎒 Fingerprint 🔩 Server Interworking		Interworking Profile	Lumos	
S Phone Interworking				
Routing		Signaling Manipulation Script	None	
Server Configuration		UDP Connection Type	SUBID	
Subscriber Profiles			Edit	
Topology Hiding Signaling Manipulation				

On the **Authentication** tab:

- Click **Edit** button.
- Check Enable Authentication and add appropriated User Name and Password.
- Click **Finish**.

Enable A	uthentication	v
U	ser Name	6409417760
R	ealm	
		Edit
	nable Authentication	5409417750
	User Name Realm (Leave blank to detect from server	5409417750
	challenge)	
	Password (Leave blank to keep existing password)	
	Confirm Password	
		11/5

- On the **Heartbeat** tab, click **Edit** button.
 - Check Enable Heartbeat.
 - Select Method: REGISTER
 - Add the value of **Frequency**: **60** seconds
 - Add From URI: 5409417750@ia.ntelos.net
 - Add To URI: 5409417750@ia.ntelos.net
 - Check TCP Probe
 - Add the value of **TCP Probe Frequency**: **10** seconds
- Click **Finish** (not shown)

🕘 Alarms 🔲 Incidents 🔢 S	tatistics 🔄 Logs 👼 Diagnostics	🚨 Users		🚮 Logout 🞯 🛛
UC-Sec Control Center SWelcome	Global Profiles > Server Configuration: Lu	imos	Rename Profile	e Clone Profile Delete Profil
📓 Backup/Restore	Profile	General Authentication Heartbeat	Advanced DoS Whitelist DoS Protection	
System Management	SM62		Heartbeat	
Global Profiles	Lumos	Enable Heartbeat	N	
Bomain DoS		Method	REGISTER	
😼 Server Interworking		Frequency	60 seconds	
Shone Interworking Addition Ad		From URI	5409417750@ia.ntelos.net	
Routing		To URI	5409417750@ia.ntelos.net	
Server Configuration		TCP Probe	N	
Signaling Manipulation		TCP Probe Frequency	10 seconds	
SIP Cluster			Edit	

7.2.8. Configure Topology Hiding – Avaya site

The Topology Hiding screen allows administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks

From the menu on the left-hand side, select **Global Profiles** → **Topology Hiding** Select **Add Profile**, enter Profile Name: **Lumos_To_SM62**

- For the Header **To**,
 - In the **Criteria** column select: **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column enter: **bvwdev7.com**
- For the Header **From**,
 - In the **Criteria** column, select: **IP/Domain**
 - In the **Replace Action** column, select: **Overwrite**
 - In the **Overwrite Value** column, enter: **bvwdev7.com**
- For the Header **Request-Line**,
 - In the **Criteria** column, select: **IP/Domain**
 - In the **Replace Action** column, select: **Overwrite**
 - In the **Overwrite Value** column, enter: **bvwdev7.com**

Alarms Incidents Incidents	tatistics 🔄 Logs 👼 Diagnostics	Lers			🛃 Logout 🔞 He
UC-Sec Control Center	Global Profiles > Topology Hiding: Lumos_T	o_SM62			
S Welcome	Add Profile			Rename Profile	Clone Profile Delete Profile
Backup/Restore	Showing page 1 of 2.		Click he	ere to add a description.	
System Management	Topology Hiding > >>	Topology Hiding			
Global Profiles	Profiles	Header	Criteria	Replace Action	Overwrite Value
Domain DoS Fingerprint	Lumos_To_SM62	Record-Route	IP/Domain	Auto	
Server Interworking		SDP	IP/Domain	Auto	
🔇 Phone Interworking		To	IP/Domain	Overwrite	bvwdev7.com
Routing		Via	IP/Domain	Auto	
log Server Configuration Subscriber Profiles		From	IP/Domain	Overwrite	bvwdev7.com
Topology Hiding	I 1	Request-Line	IP/Domain	Overwrite	bvwdev7.com

7.2.9. Configure Topology Hiding – Lumos Networks site

From the menu on the left-hand side, select **Global Profiles** → **Topology Hiding** Select **Add Profile**, enter Profile Name: **SM62_To_Lumos**

- For the Header **To**,
 - In the Criteria column, select: IP/Domain
 - In the **Replace Action** column, select: **Overwrite**
 - In the **Overwrite Value** column, enter: **ia.ntelos.net** (This domain is provided by Lumos Networks)
- For the Header **From**,
 - In the **Criteria** column select: **IP/Domain**
 - In the Replace Action column, select: Overwrite
 - In the Overwrite Value column, enter: ia.ntelos.net
- For the Header **Request-Line**,
 - In the Criteria column, select: IP/Domain
 - In the **Replace Action** column, select: **Overwrite**
 - In the Overwrite Value column, enter: ia.ntelos.net



7.3. Domain Policies

The Domain Policies feature allows administrator to configure, apply, and manage 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 different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or administrator can create a custom domain policy.

7.3.1. Create Application Rules

Application Rules allow administrator to 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, administrator can determine the maximum number of concurrent voice and video sessions so that the network will process to prevent resource exhaustion.

HV; Reviewed:	
SPOC 1/28/2013	

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Application Rules**

- Select the **default** Rule
- Select **Clone Rule** button
 - Enter Clone Name: SM62_Lumos_AppR
 - Click **Finish** (not shown).

🕘 Alarms 🔲 Incidents 👫 St	atistics 📃 Logs 👼 Diagnostics	Lusers				Logout 🛞 Hel
UC-Sec Control Center	Domain Policies > Application Rules: SM62 Add Rule Application Rules default SM62_Lumos_AppR	Lumos_AppR Filter By Device Application Rule Application Type Voice Video IM	지 고 고	Out I	Re Click here to add a description. Maximum Concurrent Sessions 1000	mame Rule Clone Rule Delete Rule Maximum Sessions Per Endpoint 1000
Indust Kules Scarth Rules Signaling Rules Time of Day Rules End Point Policy Groups Session Policies Device Specific Settings Troubleshooting Troubleshooting MLogging		CDR Support IM Logging RTCP Keep-Alive	None No No		Miscellaneous Edit	

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Application Rules**

- Select the **default** Rule
- Select **Clone Rule** button
 - Enter Clone Name: Lumos_AppR
 - Click **Finish** (not shown).

UC-Sec Control Ce Welcome ucsec, you signed in as Admin.					Sipera Sipera
Alarms Incidents	tatistics 📃 Logs 👼 Diagnostics	Lisers			🚮 Logout 🕜 Help
UC-Sec Control Center S Welcome Administration	Domain Policies > Application Rules: Lumo Add Rule	ss_AppR Filter By Device		Re	name Rule Clone Rule Delete Rule
 □ Backup/Restore □ System Management ▷ □ Global Parameters 	Application Rules default	Application Rule	CI	lick here to add a description.	
Global Profiles Global Profiles Global Profiles Global Policies	SM62_Lumos_AppR	Application Type	In Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Application Rules		Voice Video		000	1000
Media Rules		IM			
Signaling Rules			-	Miscellaneous	
Time of Day Rules End Point Policy Groups		CDR Support	None		
Session Policies		IM Logging	No		
 Device Specific Settings Troubleshooting 		RTCP Keep-Alive	No		
 TLS Management IM Logging 				Edit	

7.3.2. Create Border Rules

Border Rules allow administrator to control NAT Traversal. The NAT Traversal feature allows administrator to determine whether or not call flows through the DMZ need to traverse a firewall and the manner in which pinholes will be kept open in the firewall to accommodate traffic.

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Border Rules**

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	46 of 59
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LNCM62SM62SBCE

- Select the **default** Rule
- Select **Clone Rule** button
 - Enter Clone Name: SM62_Lumos_BorderR
 - Click **Finish** (not shown).

UC-Sec Control Ce Welcome ucsec, you signed in as Admin.			Siper
Alarms 🔲 Incidents 🌆 St	tatistics 📃 Logs 👼 Diagnostics	Lusers	Logout @ H
UC-Sec Control Center Welcome Administration Backup/Restore System Management	Domain Policies > Border Rules: SM62_Lu Add Rule Border Rules	Imos_BorderR	Rename Rule Clone Rule Delete Rule Click here to add a description. Click here to add a description. Click here to add a description.
Global Parameters Global Profiles Global Profiles SIP Cluster Domain Policies Application Rules	default No-Nat-Reg-Proxy SM62_Lumos_BorderR	NAT Traversal	ম
Media Rules		Refresh Interval Refresh For All Clients	80
Time of Day Rules Time of Day Rules Time of Day Rules Time of Day Rules Toubleshooting Toubleshooting Tusk Management Lis Management Mic.orgging		Use SIP Published IP Use SDP Published IP	전 전 Edit

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Border Rules**

- Select the **default** Rule
- Select **Clone Rule** button
 - Enter Clone Name: Lumos_BorderR
 - Click **Finish** (not shown).

🕽 Alarms 🔲 Incidents 👫 St	atistics 📃 Logs 👼 Diagnostics	L Users		🛃 Logout 🕜 Helj
UC-Sec Control Center	Domain Policies > Border Rules: Lumos_Bo	orderR		
S Welcome	Add Rule	Filter By Device	Renam	ne Rule Clone Rule Delete Rule
Backup/Restore	Border Rules		Click here to add a description.	
System Management	default	NAT Traversal		
Global Profiles	No-Nat-Reg-Proxy			
SIP Cluster	SM62_Lumos_BorderR		_	
Domain Policies	Lumos_BorderR	Enable Natting	N	
Border Rules		Refresh Interval	80	
Media Rules		Refresh For All Clients		
Security Rules				
🔯 Time of Day Rules		Use SIP Published IP	N	
End Point Policy Groups Session Policies		Use SDP Published IP		
Device Specific Settings			Edit	
Troubleshooting			Edit	
 Canadement Canadement Canada Management 		1		

7.3.3. Create Media Rules

Media Rules allow administrator to 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.

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Media Rules**

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	47 of 59
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LNCM62SM62SBCE

- Select the **default-low-med** Rule
- Select **Clone Rule** button
 - Enter Clone Name: SM62_Lumos_MediaR
 - Click **Finish** (not shown).

UC-Sec Control Ce Welcome ucsec, you signed in as Admin	9					
Alarms Incidents	Statistics 🔄 Logs 🛐 Diagnostics	S 🚨 Users			🔄 Lo	gout 🕜 Help
C-Sec Control Center	Domain Policies > Media Rules: SM62_Lu	imos_MediaR				
Welcome	Add Rule	Filter By Device		Rename Rule	Clone Rule	Delete Rule
📓 Backup/Restore	Media Rules		Click here to add	l a description.		
System Management	default-low-med	Media NAT Media Encryption M	edia Anomaly Media Silencing	Media QoS Turing Test		
Global Profiles	default-low-med-enc					
SIP Cluster	default-high					
 Domain Policies Application Rules 	default-high-enc	Media NAT	Learn Media IP	dynamically		
Border Rules	avaya-low-med-enc		Edit			
Security Rules	TurningTest					
Rignaling Rules	SM62_Lumos_MediaR					

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Media Rules**

- Select the **default-low-med** Rule
- Select Clone Rule button
 - Enter Clone Name: Lumos_MediaR
 - Click **Finish** (not shown)

	atistics 🔄 Logs 🗾 Diagnostics						Ø. L	ogout 🕜 <u>H</u> elj
UC-Sec Control Center SWelcome	Domain Policies > Media Rules: Lumos_M Add Rule	Filter By Device	-			Rename Rule	Clone Rule	Delete Rule
Backup/Restore	Media Rules			Click here to ad	d a description			
System Management	default-low-med	Media NAT Media Encryption	Media Anomaly M	Aedia Silencing	Media QoS	Turing Test		
Clobal Profiles	default-low-med-enc							24
SIP Cluster	default-high							
 Domain Policies Application Rules 	default-high-enc	Media NAT		Learn Media IF	o dynamically			
Border Rules	avaya-low-med-enc			Edi	t			
Media Rules	TurningTest	5						
Rignaling Rules	SM62 Lumos MediaR							
Time of Day Rules	Lumos_MediaR							
End Point Policy Groups Session Policies	procession and and a second se							

7.3.4. Create Security Rules

Security Rules allow administrator to define which enterprise-wide VoIP and Instant Message (IM) security features will be applied to a particular call flow. Security Rules allow administrator to configure Authentication, Compliance, Fingerprinting, Scrubber, and Domain DoS. In addition to determining which combination of security features are applied, administrator can also define the security feature profile, so that the feature is applied in a specific manner to a specific situation.

From the menu on the left-hand side, select **Domain Policies** → **Security Rules**

- Select the **default-med** Rule
- Select Clone Rule button
 - Enter Clone Name: SM62_Lumos_SecR
 - Click **Finish** (not shown)

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	48 of 59
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LNCM62SM62SBCE

	Center in. Current server time is 4:22:09 PM EST Statistics ELogs <u>Diagnostic</u>	s 🔯 Users		6	
UC-Sec Control Center	Domain Policies > Security Rules: SM62				godut 🕜 Hei
S Welcome	Add Rule	Filter By Device	Rename Rul	e Clone Rule	Delete Rule
Backup/Restore	Security Rules	Click here to	add a description.		
System Management	default-low	Authentication Compliance Fingerprint Scrubber Domain	DoS		
Global Profiles	default-med				
SIP Cluster	default-high	Autho	entication		
Domain Policies	SM62_Lumos_SecR	Enabled No			
Application Rules			Edit		
📕 Media Rules					
Security Rules		<u>k</u>			
Signaling Rules					

From the menu on the left-hand side, select **Domain Policies** → **Security Rules**

- Select the **default-med** Rule
- Select **Clone Rule** button
 - Enter Clone Name: Lumos_SecR
 - Click **Finish** (not shown).

UC-Sec Control Center Welcome ucsec, you signed in as Admin. Current server time is 4:22:34 PM EST								
istics 🔄 Logs 👼 Diagnostics	Lusers		💆 Le	ogout 🕜 <u>H</u> elp				
Domain Policies > Security Rules: Lumos_t	iecR		-					
Add Rule	Filter By Device	Rename Rule	Clone Rule	Delete Rule				
Security Rules	Click here to add a description.							
default-low	Authentication Compliance Fingerprint Scrubber Domain DoS							
default-med								
default-high	Authentication							
	Enabled No							
	Edit							
Contraction of the Contraction of Co								
	rreni server time is 4:22:34 PM EST istics I Logs Diagnostics Donsin Policies > Security Rules Lumos - Add Rule Security Rules default-low	rrent server time is 4:22:34 PM EST istics I Logs S Diagnostics Users Donain Policies > Security Rules: Lumos_SecR Add Rule Filter By Device Security Rules Click here to add a description. default-low Authentication Compliance Fingerprint Scrubber Domain DoS (default-high SM62_Lumos_SecR	rrent server time is 4:22:34 PM EST istics Donain Policies > Security Rules: Lunos_SecR Add Rule Filter By Device Rename Rule Click here to add a description. default-low default-low default-high SM62_Lumos_SecR	Intent server time is 4:22:34 PM EST				

7.3.5. Create Signaling Rules

Signaling Rules allow administrator to 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 "patternmatched" against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

From the menu on the left-hand side, select **Domain Policies** → **Signaling Rules**

- Select the **default** Rule
- Select Clone Rule button
 - Enter Clone Name: SM62_Lumos_SigR
 - Click **Finish** (not shown).

	Current server time is 4:23:33 PM EST atistics 🔄 Logs 🗾 Diagnostic:	s 🔝 Users	5		_	_	_	Logout	<u>System</u>
UC-Sec Control Center	Domain Policies > Signaling Rules: SM62	_Lumos_SigR	- W						
S Welcome	Add Rule	Filter By Device Rename Rule Clone Rule Delete Ru						ete Rule	
Backup/Restore	Signaling Rules		Click here to add a description.						
System Management	default	General	Requests	Responses	Request Headers	Response Headers	Signaling QoS		
Global Profiles	No-Content-Type-Checks		Inbound						
Domain Policies	SM62_Lumos_SigR	Reques	sts			Allow			
Application Rules		Non-2X	X Final Respo	nses	,	Allow			
🔒 Border Rules 📕 Media Rules		Optiona	al Request He	aders		Allow			
Security Rules	Optiona	al Response F	leaders		Allow				
🔋 End Point Policy Groups						Outbound			
Session Policies		Reques				Allow			
Troubleshooting		a second second	X Final Respo			Allow			
TLS Management			al Request He			Allow			
III Logging		Optiona	al Response H	leaders	1	Allow			
		Content-Type Policy							
		Enable	Content-Type	Checks		ঘ			
		Action		A	llow	Multipart	Action	Allow	
		Except	ion List			Exception	List		
		1				Edit			

From the menu on the left-hand side, select **Domain Policies** → **Signaling Rules**

- Select the **default** Rule
- Select Clone Rule button
 - Enter Clone Name: Lumos_SigR
 - Click **Finish** (not shown).

Alarms 🔲 Incidents 👫 Sta	atistics 🔄 Logs 🗾 Diagnostics	Users						🛃 Logout 🞯	
UC-Sec Control Center	Domain Policies > Signaling Rules: Lumos_	SigR							
S Welcome	Add Rule	Filter By Dev	vice	-			Rename F	Rule Clone Rule Delete Ru	
Backup/Restore	Signaling Rules				C	lick here to add a desc	ription.		
System Management	default	General	Requests	Responses	Request Headers	Response Headers	Signaling QoS		
Global Profiles	No-Content-Type-Checks					Inbound			
 SIP Cluster Domain Policies 	SM62_Lumos_SigR	Requests				Allow			
Application Rules	Lumos_SigR		inal Respons	es		Allow			
 Border Rules Media Rules Security Rules Signaling Rules 			equest Heade			Allow			
		a the second second	esponse Hea			Allow			
		optional it	caponae neu	dera		741077			
Time of Day Rules End Point Policy Groups		Outbound							
Session Policies		Requests				Allow			
Device Specific Settings Troubleshooting		Non-2XX F	inal Respons	es		Allow			
E 🛅 TLS Management		Optional R	equest Heade	ers		Allow			
> 🛅 IM Logging		Optional R	esponse Hea	ders		Allow			
		5 11 0				Content-Type Polic	y		
			ntent-Type Ch			N			
		Action		A	llow	Multipar		Allow	
		Exception	List			Exceptio	on List		

7.3.6. Create Time of Day Rules

A Time-of-day (ToD) Rule allows administrator to determine when the domain policy, it is assigned to, will be in effect. ToD Rules provide complete flexibility to fully accommodate the

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LN

50 of 59 LNCM62SM62SBCE enterprise by, not only determining when a particular domain policy will be in effect, but also to whom it will apply, and for how long it will remain in effect.

From the menu on the left-hand side, select **Domain Policies** → **Time of Day Rules**

- Select the **default** Rule
- Select Clone Rule button
 - Enter Clone Name: SM62_Lumos_ToDR
 - Click **Finish** (not shown).

UC-Sec Control Ce Welcome ucsec, you signed in as Admin. C						
🕘 Alarms 📋 Incidents 🔢 Sta	tistics 🔄 Logs 👼 Diagnostics	Lusers			🛃 Logout 🞯 Help	
UC-Sec Control Center S Welcome Administration	Domain Policies > Time of Day Rules: SM	32_Lumos_ToDR Filter By Device	×	R	tename Rule Clone Rule Delete Rule	
Backup/Restore System Management Global Parameters	Time of Day Rules default SM62_Lumos_ToDR	Time of Day	Cli	ck here to add a description.		
 Global Profiles SIP Cluster 	Contraction of the Contraction of the Contraction of			Date		
Domain Policies Application Rules		Start Date	02/19/2007	End Date	Never	
Border Rules				Time		
📕 Media Rules 🈡 Security Rules		Start Time	12:00 AM	End Time	11:59 PM	
Signaling Rules				Recurrence		
		 Daily Weekly Monthly 	 Every Day Every Weekday Every Weekend 			
 TLS Management IM Logging 		Edit				

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Time of Day Rules**

- Select the **default** Rule
- Select Clone Rule button
 - Enter Clone Name: Lumos_ToDR
 - Click **Finish** (not shown).

UC-Sec Control Ce Welcome ucsec, you signed in as Admin.							
Alarms Incidents	atistics 📃 Logs 👼 Diagnostics	S 🞑 Users			Logout 🛞 Help		
UC-Sec Control Center SWelcome Administration	Domain Policies > Time of Day Rules: Lur Add Rule	nos_ToDR Filter By Device	-	5	Rename Rule Clone Rule Delete Rule		
📓 Backup/Restore	Time of Day Rules		Clic	k here to add a description.			
System Management	default	Time of Day					
Global Profiles	SM62_Lumos_ToDR			(UDD)			
SIP Cluster	Lumos_ToDR			Date			
 Domain Policies 		Start Date	02/19/2007	End Date	Never		
Application Rules				Time			
📕 Media Rules		Start Time	12:00 AM	End Time	11:59 PM		
Security Rules							
Time of Day Rules				Recurrence			
 End Point Policy Groups Session Policies Device Specific Settings Troubleshooting 		 Daily Weekly Monthly 	 Every Day Every Weekday Every Weekend 				
 TLS Management IM Logging 			Edit				

7.3.7. Create Endpoint Policy Groups

The End-Point Policy Group feature allows administrator to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD. (Each of which was created using the procedures contained in the previous sections.) A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of UC-Sec security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies** \rightarrow **End Point Policy Groups**

- Select Add Group
- Enter Group Name: SM62_Lumos_PolicyG
 - Select Application Rule: SM62_Lumos_AppR
 - Select Border Rule: SM62_Lumos_BorderR
 - Select Media Rule: SM62_Lumos_MediaR
 - Select Security Rule: SM62_Lumos_SecR
 - Select Signaling Rule: SM62 Lumos SigR
 - Select Time of Day: SM62_Lumos_ToDR
- Select **Finish** (not shown).

UC-Sec Control Ce Welcome ucsec, you signed in as Admin.		A EST						9	Sipera
Alarms 🔲 Incidents 👫 St	atistics 🔄 Logs 🗾 D	agnostics	Users					🔄 Lo	gout 🕜 <u>H</u> elp
UC-Sec Control Center	Domain Policies > End Point Pr	licy Groups: SM62	Lumos_PolicyG						
S Welcome	Add Group	Filter By Devi	ce]			Renam	e Group	Delete Group
Backup/Restore	Showing page 2 of 2.				Click here to add a	description.			
 Global Parameters Global Profiles SIP Cluster 	<< < Policy Groups SM62_Lumos_PolicyG	Policy Group			Hover over a row to se	e its description.			
 Domain Policies Application Rules 							View Summ	ary A	dd Policy Set
🔒 Border Rules 📕 Media Rules		Order	Application	Border	Media	Security	Signaling	Time of	Day
Security Rules	Skip to page	1 S	M62_Lumos_AppR	SM62_Lumos_BorderR	SM62_Lumos_MediaR	SM62_Lumos_SecR	SM62_Lumos_SigR	SM62_Lumo	IS_TODR 🥒 🕈
 Time of Day Rules End Point Policy Groups Session Policies 									

From the menu on the left-hand side, select **Domain Policies** \rightarrow **End Point Policy Groups**

- Select Add Group
- Enter Group Name: Lumos_PolicyG
 - Select Application Rule: Lumos_AppR
 - Select Border Rule: Lumos_BorderR
 - Select Media Rule: Lumos MediaR
 - Select Security Rule: Lumos SecR
 - Select Signaling Rule: Lumos_SigR
 - Select Time of Day: Lumos_ToDR
- Select **Finish** (not shown).

UC-Sec Control Ce Welcome ucsec, you signed in as Admin. (S S	
🕘 Alarms 🔲 Incidents 🍱 Sta	atistics 📃 Logs 👼 Diagnostics	Users						Logou	t 🕜 <u>H</u> elp
UC-Sec Control Center	Domain Policies > End Point Policy Groups	: Lumos_PolicyG		- 41					
S Welcome	Add Group	Filter By Device		-			Renan	ne Group Del	ete Group
📓 Backup/Restore	Showing page 2 of 2.				Click here to ac	ld a description.			
System Management	<< < Policy Groups				Hover over a row to	see its description	h.		
🖻 🛅 Global Profiles	SM62_Lumos_PolicyG	Policy Group							
 SIP Cluster Domain Policies Application Rules 	Lumos_PolicyG						View Summ	nary Add Poli	cy Set
🕵 Border Rules 📕 Media Rules		Order	Application	Border	Media	Security	Signaling	Time of Day	
Security Rules		1 L	umos_AppR	Lumos_BorderR	Lumos_MediaR	Lumos_SecR	Lumos_SigR	Lumos_ToDR	P 🕂
Signaling Rules Time of Day Rules End Point Policy Groups Session Policies	Skip to page								

7.4. Device Specific Settings

The Device Specific Settings feature for SIP allows administrator to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, administrator has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

7.4.1. Manage Network Settings

From the menu on the left-hand side, select **Device Specific Settings** → **Network Management**.

- Enter the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces:
 - IP Address for Inside interface: 10.10.97.189; Gateway: 10.10.97.129
 - IP Address for Outside interface: 10.10.98.112; Gateway: 10.10.98.97
- Select the physical interface used in the **Interface** column:
 - Inside Interface: A1
 - Outside Interface: B1

UC-Sec Control Ce Welcome ucsec, you signed in as Admin.					
Alarms Incidents	tatistics 🔄 Logs 🛃 Diagnosti	cs 📓 Users			Logout 🕢 He
UC-Sec Control Center SWelcome Administration	Device Specific Settings > Network Ma		Configuration		
System Management Global Parameters Global Profiles SIP Cluster Domain Policies Device Specific Settings Ketwork Management	sipera	Modifications or deletions of an restarts can be issued from Sy A1 Netmask 255.255.192		a require an application restart befor B1 Netmask 255,255,252	re taking effect. Application B2 Netmask
Hedia Interface Signaling Interface Signaling Forking		Add IP			Save Changes Clear Changes
SNMP		IP Address	Public IP	Gatew	vay Interface
Session Flows		10.10.97.189		10.10.97.129	A1 💌 🗙
Two Factor Relay Services Troubleshooting TLS Management M Logging		10.10.98.112		10.10.98.97	B1 🗹 X

• Select the Interface Configuration Tab.

HV; Reviewed: SPOC 1/28/2013

• Click **Toggle State** to toggle the State of the physical interfaces being used.

Alarma Incidente	Statistics 📃 Logs 👼 Diagnost	ics Ilears		Jegout 🕡 Help
UC-Sec Control Center	Device Specific Settings > Network M			Al Fodor . Teh
S Welcome Administration Backup/Restore System Management	UC-Sec Devices	Network Configuration Interface Configu	afion	
Global Parameters	sipera	Name	Administrative Status	
🚞 Global Profiles		A1	Enabled	Toggle State
🛅 SIP Cluster 🛅 Domain Policies		A2	Disabled	Toggle State
Device Specific Settings		B1	Enabled	Toggle State
Media Interface Signaling Interface Signaling Forking		82	Disabled	Toggle State

7.4.2. Create Media Interfaces

Media Interfaces define the type of signaling on the ports. The default media port range on the Avaya SBCE can be used for both inside and outside ports.

From the menu on the left-hand side, **Device Specific Settings** \rightarrow **Media Interface**

- Select Add Media Interface
 - Name: InsideMedia
 - Media IP: 10.10.97.189 (Internal IP Address toward Session Manager).
 - Port Range: 35000 40000
 - Click **Finish** (not shown).
- Select Add Media Interface
 - Name: OutsideMedia_Lumos
 - Media IP: 10.10.98.112 (External IP Address toward Lumos Networks trunk).
 - Port Range: 35000 40000
 - Click **Finish** (not shown).

UC-Sec Control C Welcome ucsec, you signed in as Admi	enter n. Current server time is 4:30:05 PM EST			6) Sipera
🕘 Alarms 🔲 Incidents 🔢	Statistics 📃 Logs 👼 Diagnos	stics 🔝 Users		S L	ogout 🕜 <u>H</u> el
UC-Sec Control Center Welcome Watministration Backup/Restore System Management Global Prameters Global Profiles Global Profiles Global Profiles Global Profiles Global Profiles Global Profiles Global Profiles Global Profiles Global Policies Global Policies Global Policies	Device Specific Settings > Media Int UC-Sec Devices sipera	Media Interface		estart before taking effect. Application resta	irts can be a Interface
Device Specific Settings		Name	Media IP	Port Range	
Network Management		InsideMedia	10.10.97.189	35000 - <mark>4</mark> 0000	2 X
Signaling Interface		OutsideMedia_Lumos	10.10.98.112	35000 - 40000	2 X

7.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select **Device Specific Settings** → **Signaling Interface**

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	54 of 59
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LNCM62SM62SBCE

- Select Add Signaling Interface
 - Name: InsideSIP_UDP
 - Media IP: 10.10.97.189 (Internal IP Address toward Session Manager).
 - UDP Port: 5060
 - Click **Finish** (not shown).

From the menu on the left-hand side, select **Device Specific Settings** → **Signaling Interface**

- Select Add Signaling Interface
 - Name: OutsideSIP_Lumos
 - Media IP: 10.10.98.112 (External IP Address toward Lumos Networks trunk).
 - UDP Port: 5060
 - Click **Finish** (not shown).

UC-Sec Control Ce Welcome ucsec, you signed in as Admin.							9	Sipera
Alarms Incidents	tatistics 🔄 Logs 👼 Diagnos	tics 🎑 Users					🛃 Logo	out 🕜 <u>H</u> elp
CO-Sec Control Center Welcome Administration Backup/Restore System Management Global Profiles Global Profiles	Device Specific Settings > Signaling I UC-Sec Devices Sipera	Interface: sipera	Signaling IP	TCP Port	UDP Port	TLS Port	Add Signaling In TLS Profile	terface
 SIP Cluster Domain Policies 		InsideSIP_UDP	10.10.97.189		5060		None	2 X
Device Specific Settings Network Management Media Interface Signaling Interface Signaling Forking		OutsideSIP_Lumos	10.10.98.112	-	5060		None	X

7.4.4. Configuration Server Flows

Server Flows allow administrator to categorize trunk-side signaling and apply a policy.

7.4.4.1 Create End Point Flows - Session Manager

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**

- Select the **Server Flows** Tab.
- Select Add Flow, enter Flow Name: To Lumos Networks
 - Server Configuration: SM62
 - URI Group: Lumos Networks
 - Transport: *
 - Remote Subnet: *
 - Received Interface: OutsideSIP_Lumos
 - Signaling Interface: InsideSIP_UDP
 - Media Interface: InsideMedia
 - End Point Policy Group: SM62_Lumos_PolicyG
 - Routing Profile: SM62_To_Lumos
 - Topology Hiding Profile: Lumos_To_SM62
 - File Transfer Profile: None
 - Click **Finish** (not shown).

7.4.4.2 Create End Point Flows – Lumos Networks

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**

- Select the Server Flows Tab
- Select Add Flow, enter Flow Name: From Lumos Networks
 - Server Configuration: Lumos
 - URI Group: Lumos Networks
 - Transport: *
 - Remote Subnet: *
 - Received Interface: InsideSIP_UDP
 - Signaling Interface: OutsideSIP_Lumos
 - Media Interface: OutsideMedia_Lumos
 - End Point Policy Group: Lumos_PolicyG
 - Routing Profile: Lumos_To_SM62
 - Topology Hiding Profile: SM62_To_Lumos
 - File Transfer Profile: None
 - Click **Finish** (not shown).

UC-Sec Control Ce Welcome ucsec, you signed in as Admin.		time is 4:36:40 PM EST									S (S	ipera Systems
🕘 Alarms 🔲 Incidents 🍱 St	tatistics 📃	Logs 👼 Diagnostics 🎑	<u>U</u> sers								🛃 Logou	t 🕜 <u>H</u> elp
UC-Sec Control Center Welcome Administration Backup/Restore System Management Global Praneters Global Profiles	Subscribe	ific Settings > End Point Flows: siper	a									
Global Promes Global	Priority	Flow Name	URI Grou	p Tra	insport	Remote Subnet		Interface	Signal Interfa		End Point Policy Group	Routing P
 Device Specific Settings Network Management 	1	To Lumos Networks	Lumos Netwo	rks *	*		OutsideSIP	_Lumos	InsideSIP	_UDP InsideMedia	SM62_Lumos_Policy	G SM62_To_I
📕 Media Interface 😤 Signaling Interface 🏠 Signaling Forking	Server Co	onfiguration: Lumos										
SNMP	Priority	Flow Name	URI Group	Transpor	t Remo Subn		Received Interface	Signaling	Interface	Media Interface	End Point Policy Group	Routing Prof
Session Flows Two Factor Relay Services	1	From Lumos Networks	Lumos Networks	*	*	In	nsideSIP_UDP	OutsideSIF	_Lumos	OutsideMedia_Lumo	s Lumos_PolicyG	Lumos_To_S

8. Lumos Networks SIP Trunking Configuration

Lumos Networks is responsible for the network configuration of the Lumos Networks SIP Trunking service. Lumos Networks will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. Lumos Networks will provide the IP address of the Lumos Networks SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete configurations for Communication Manager, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between Lumos Networks and the enterprise is a static configuration. There is a registration of the SIP trunk or enterprise users to the Lumos Networks network.

9. Verification Steps

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.

Troubleshooting:

- 1. Enter the following commands using Communication Manager System Access Terminal (SAT) interface:
 - **list trace station** <extension number> Traces calls to and from a specific station.
 - **list trace tac** <trunk access code number> Trace calls over a specific trunk group.
 - **status station** <extension number> Displays signaling and media information for an active call on a specific station.
 - **status trunk-group** <trunk-group number> Displays trunk-group state information.
 - **status signaling-group** <signaling-group number> Displays signaling-group state information.
- 2. Session Manager:
 - Call Routing Test The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to Elements → Session Manager → System Tools → Call Routing Test. Enter the requested data to run the test.
 - **traceSM** -**x** Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to Lumos Networks SIP Trunking. This solution successfully passed compliance testing via the Avaya DevConnect Program. Please refer to **Section 2.2** for any exceptions or workarounds.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	57 of 59
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LNCM62SM62SBCE

11. Additional References

This section references the documentation relevant to these Application Notes.

Product services for Avaya SBCE may be found at: http://www.sipera.com/products-services/esbc

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

Avaya Aura® Session Manager/System Manager

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

Avaya Aura® Communication Manager

- [4] Administering Avaya Aura® Communication Manager, Document ID 03-300509, Release 6.2, July 2012
- [5] Programming Call Vectors in Avaya Aura® Call Center, 6.0, June 2010

Avaya one-X® IP Phones

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

IETF (Internet Engineering Task Force) SIP Stnadards Specifications

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	
SPOC 1/28/2013	©2013 Avaya Inc. All Rights Reserved.	LN

©2013 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and TM 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 <u>devconnect@avaya.com</u>.