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. 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 toll-free, operator service, 911 and directory assistance.
- G.711MU and G.729A codecs.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.

- 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: http://support.avaya.com.

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

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.

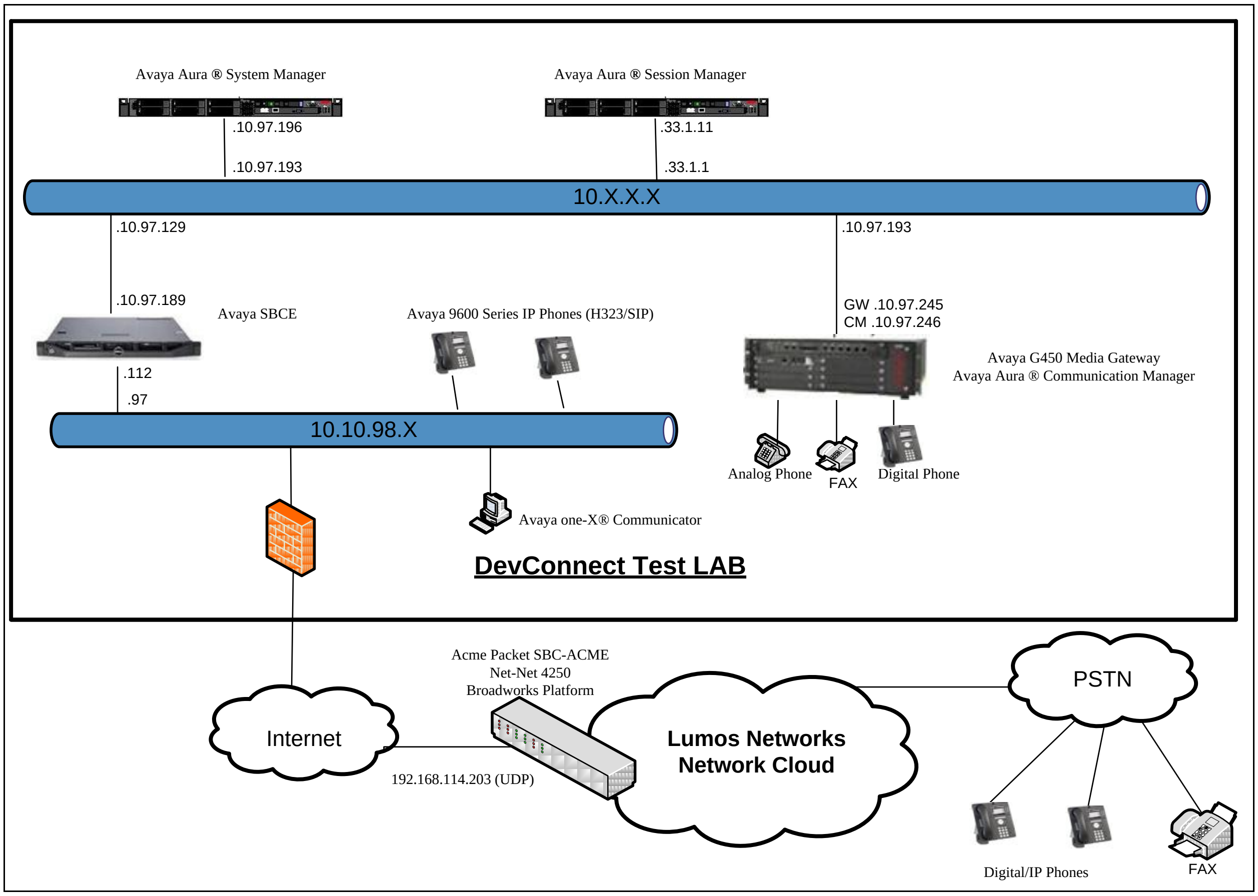


Figure 1: Avaya IP Telephony Network and Lumos Networks SIP Trunking

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 MM711 Analog MM712 Digital	HW01 FW001 HW31 FW087 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 Trunking 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 permission changes.)
```

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

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

    Abbreviated Dialing Enhanced List? n          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? n
        Analog Trunk Incoming Call ID? n                      CAS Branch? n
```

```
 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? y        Computer Telephony Adjunct 
Links? n
                 ARS/AAR Partitioning? y           Cvg Of Calls Redirected 
Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y           DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

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

```
display system-parameters customer-options                      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? y
                     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? y
                  Secondary Data Module? y
```

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
```

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.

```
change system-parameters features                                Page   9 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

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

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

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

SCCAN PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses 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**.

```
change node-names ip                                             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.

```
change ip-codec-set 1                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 1

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

                              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
Location:          Authoritative Domain: bvwdev7.com
    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/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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
                                                       Target socket load: 4800

      Enable Interface? y                           Allow H.323 Endpoints? y
                                                     Allow H.248 Gateways? y
        Network Region: 1                             Gatekeeper Priority: 5

                                 IPV4 PARAMETERS
             Node Name: procr                  IP Address: 10.10.97.246
           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.
- Default values may be used for all other fields.

```
add signaling-group 10                                          Page   1 of   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
 Near-end Listen Port: 5060                  Far-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
```

```
add signaling-group 11                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 11              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
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1
                                    Far-end Secondary Node Name:
Far-end Domain:
                                             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
```

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.

```
add trunk-group 10                                              Page   1 of  21
                                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
```

```
add trunk-group 11                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 11                    Group Type: sip            CDR Reports: y
  Group Name: LumosNetworks             COR: 1        TN: 1        TAC: *011
   Direction: incoming        Outgoing Display? n
 Dial Access? n                                    Night Service:
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                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     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                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     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                                              Page   4 of  21
                              PROTOCOL VARIATIONS

                           Mark Users as Phone? n
                 Prepend '+' to Calling Number? n
           Send Transferring Party Information? n
                      Network Call Redirection? y
                         Send Diversion Header? y
                       Support Request History? n
                  Telephone Event Payload Type: 101

            Convert 180 to 183 for Early Media? 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.

```
change private-numbering 0                                      Page   1 of   2
                           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                                       Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 2

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type

   40          4   udp
   6           4   ext
   7           4   ext
   9           1   fac
   *           4   dac
   #           4   dac
```

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

```
change feature-access-codes                                    Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *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      Close Code: #080
```

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 0                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 1

          Dialed             Total      Route     Call    Node   ANI
          String            Min  Max   Pattern    Type    Num    Reqd
    0                       1    11     10        op             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**).

```
change route-pattern 10                                         Page   1 of   3
                    Pattern Number: 5   Pattern Name: LumosNetworks
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 10    0                                                              n   user
 2:                                                                      n   user
 3:                                                                      n   user
 4:                                                                      n   user
 5:                                                                      n   user
 6:                                                                      n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                               unk-unk   none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

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-trmt trunk-group 11                  Page   1 of   3
                       INCOMING CALL HANDLING 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
     Type: 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? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal             Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n

                                                         IP Video? n


                                             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

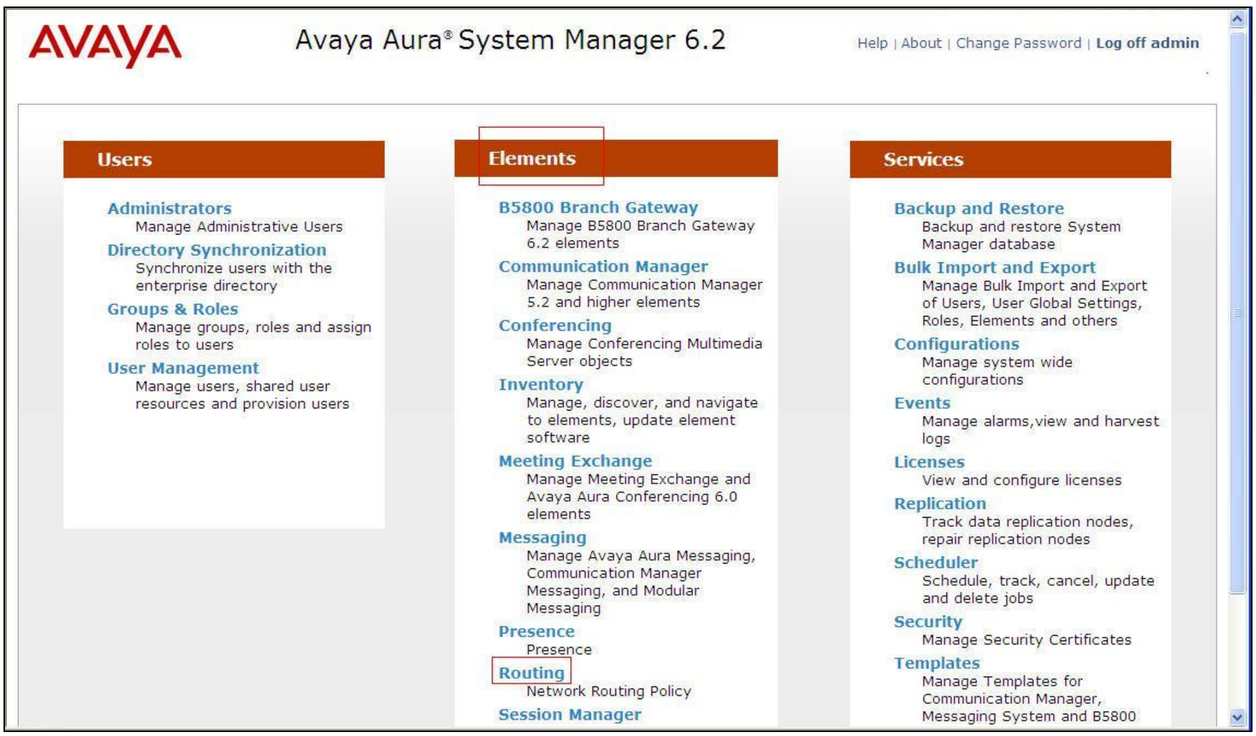
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- 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.

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.

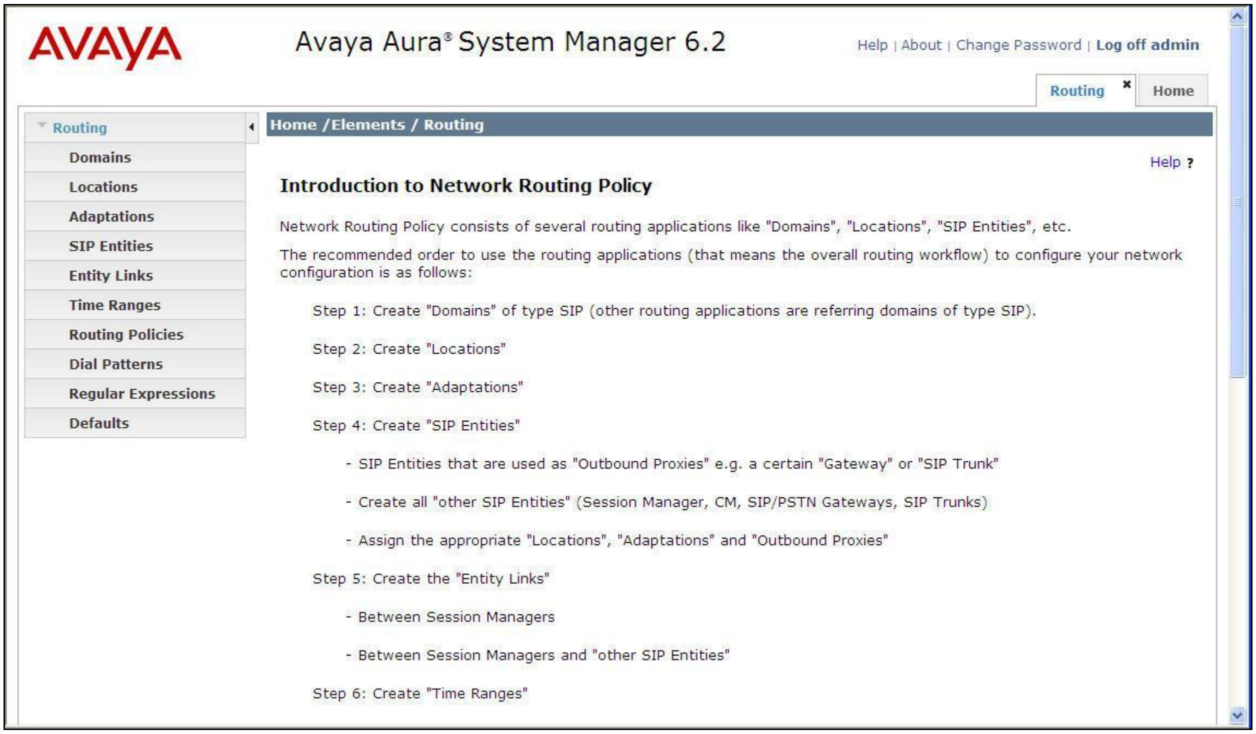
6.1. Avaya Aura® System Manager Login and Navigation

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.



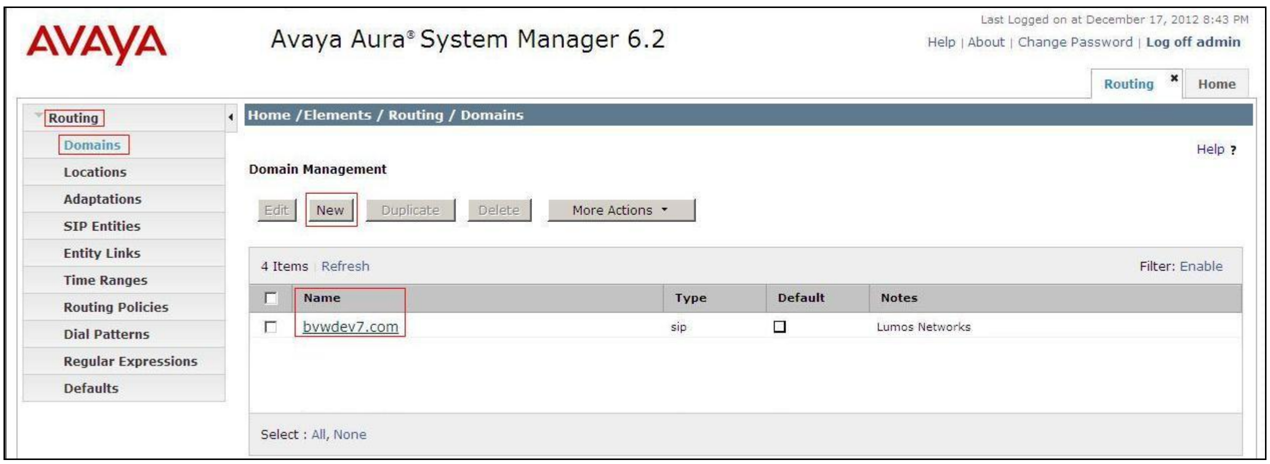
6.2. Specify SIP Domain

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 → 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.



6.3. Add Location

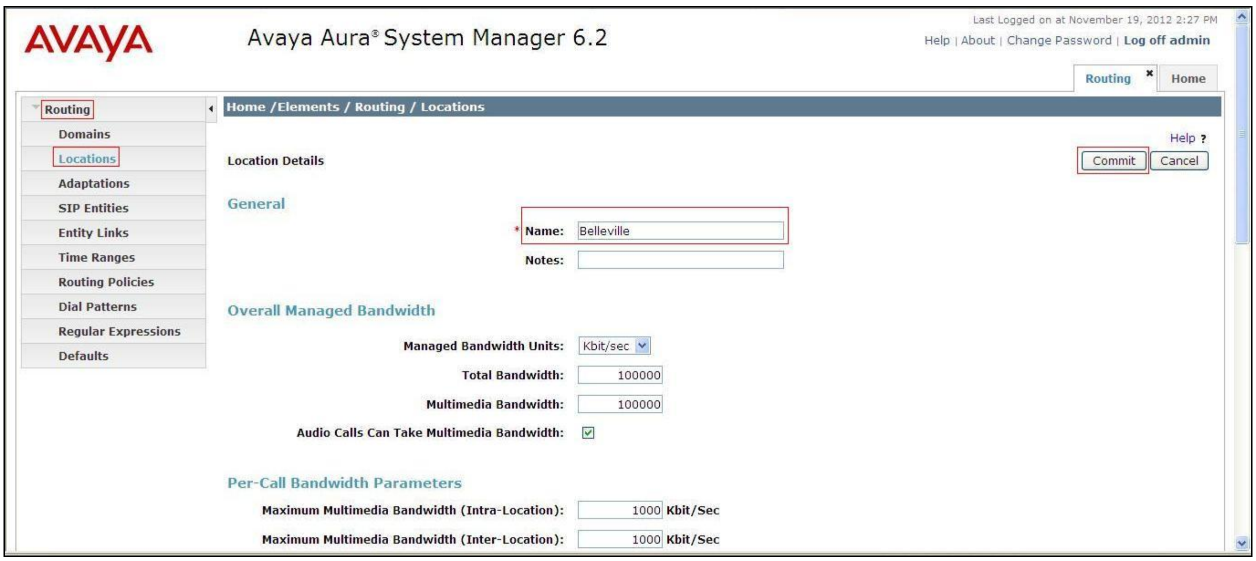
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville**, which includes all equipment in the enterprise including Communication Manager, Session Manager and Avaya SBCE.

To add a Location, navigate to **Routing →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.



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 → 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.

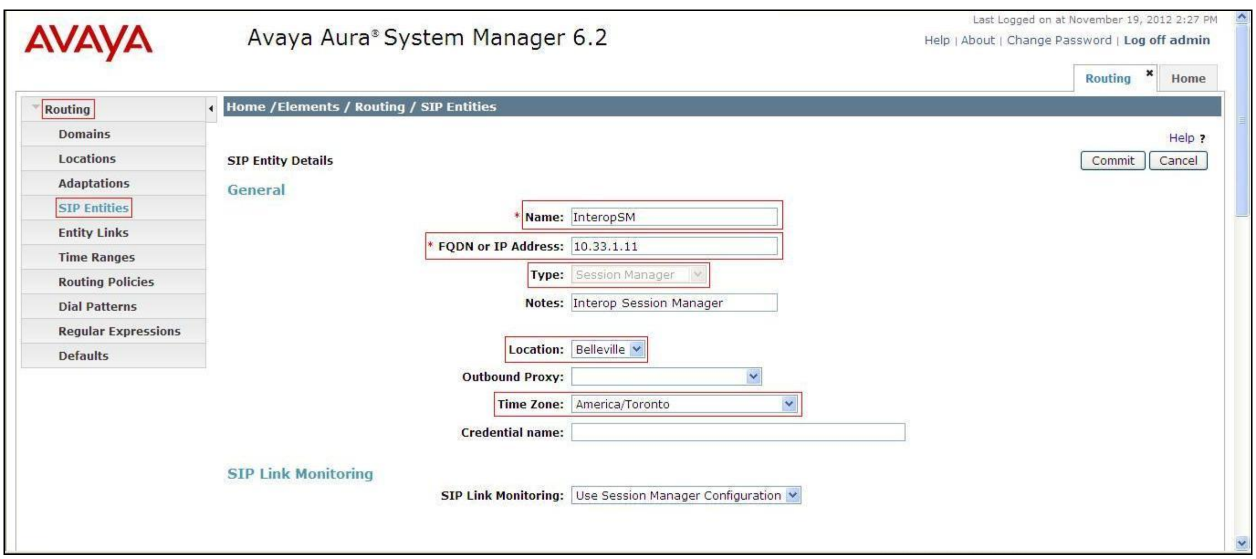
- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** for Avaya SBCE.
- **Adaptation:** This field is only 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**



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:

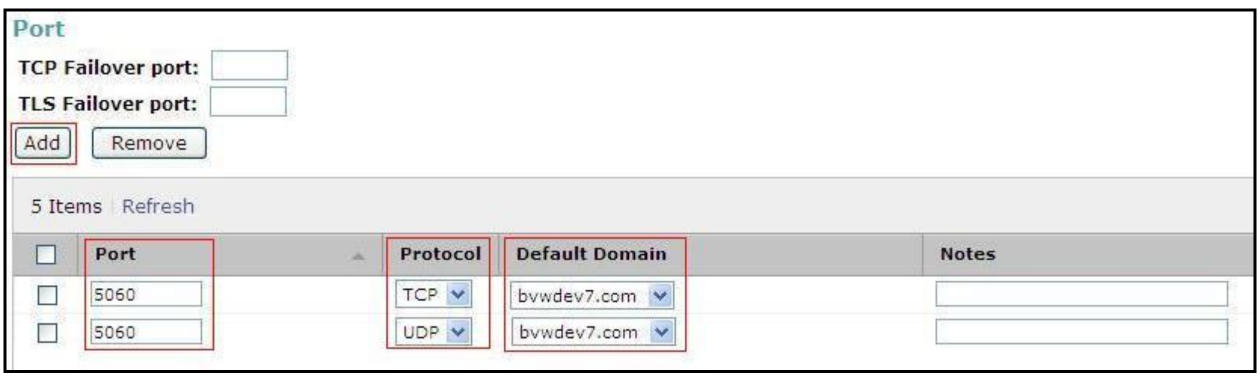
- **Port:** Port number on which Session Manager listens for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain.

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.

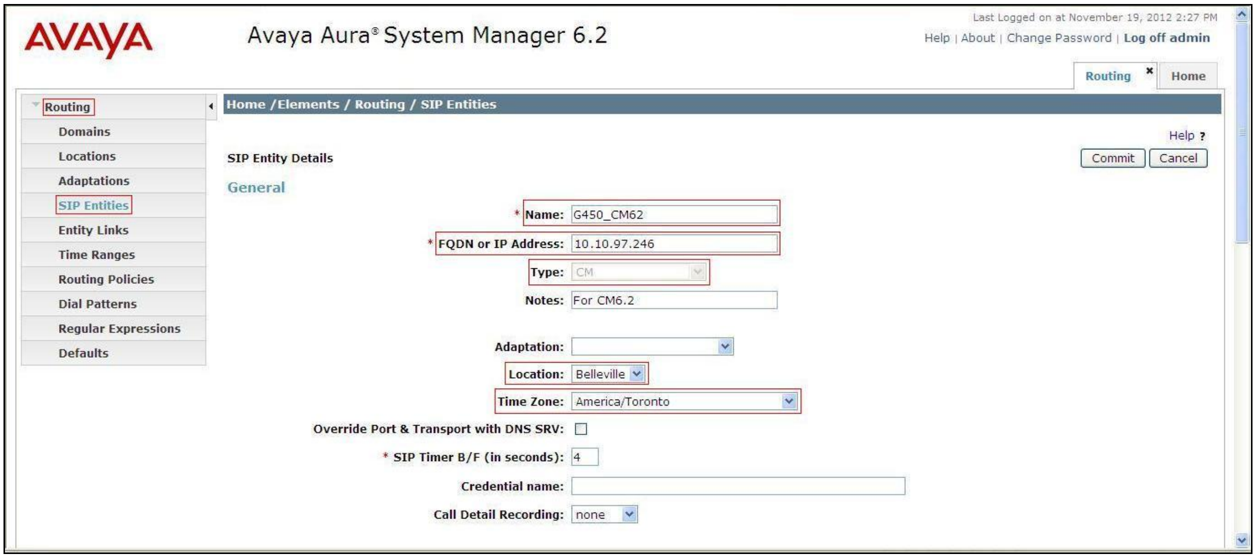
In addition, port 5060 with TCP was also used by a separate SIP Link between Session Manager and Communication Manager for Avaya SIP telephones and SIP soft clients. This SIP Link was part of the standard configuration on Session Manager and was not directly relevant to the inter-operability with Lumos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

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



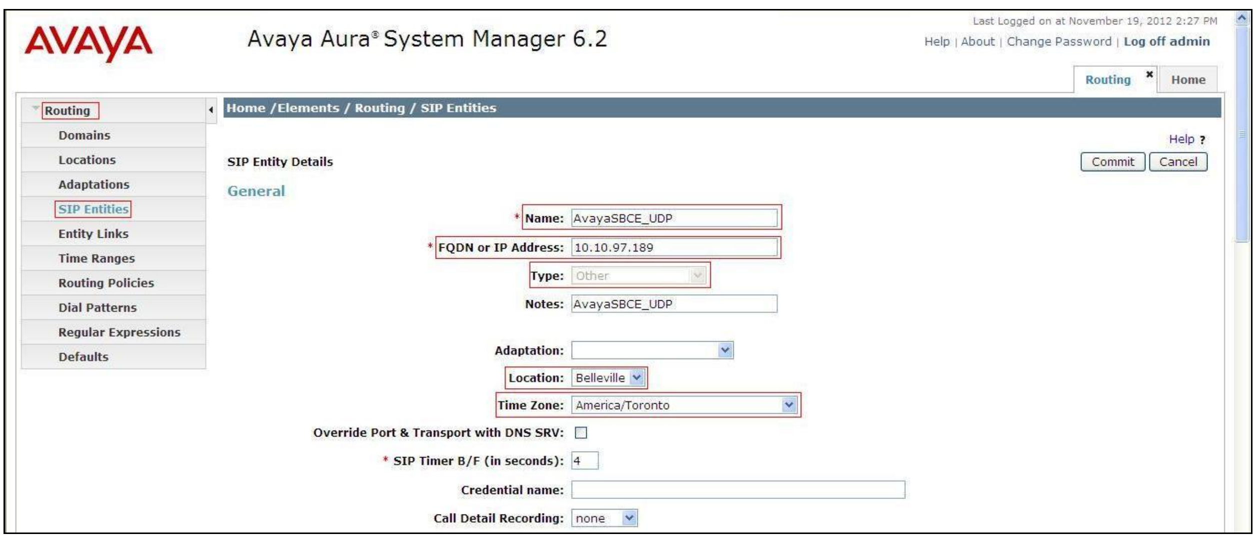
6.4.2. Configure Communication Manager SIP Entity

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**.



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**.



6.5. Add Entity Links

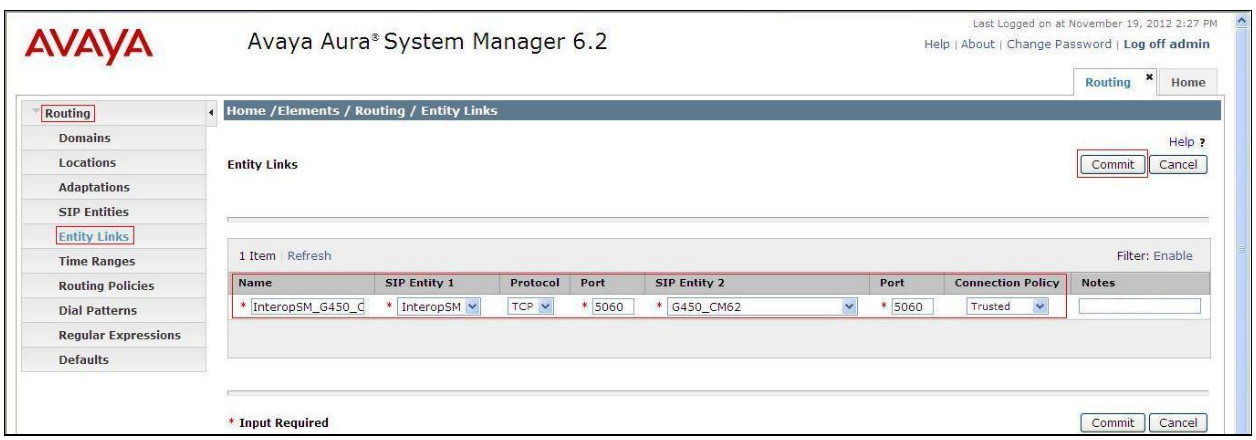
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by service provider traffic and one to the Avaya SBCE.

To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

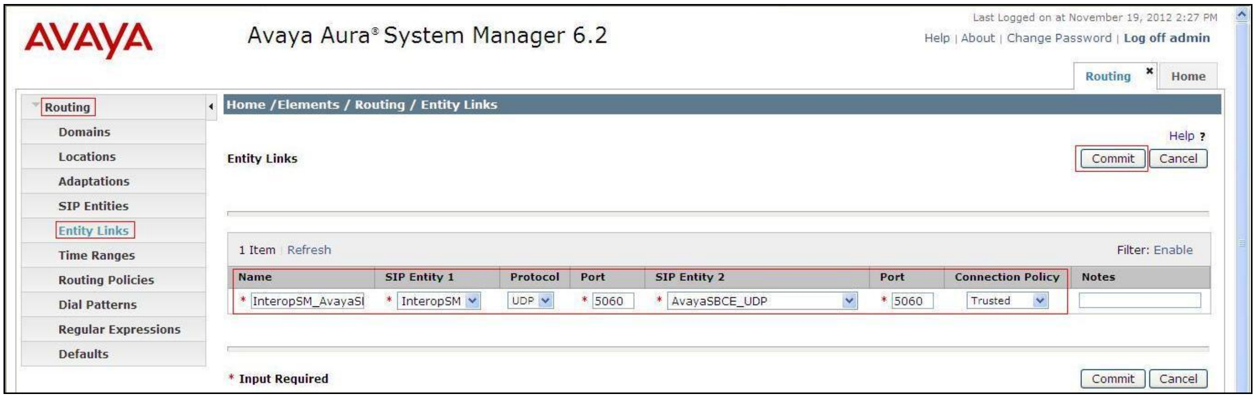
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager being used.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager Entity Link, this 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**.

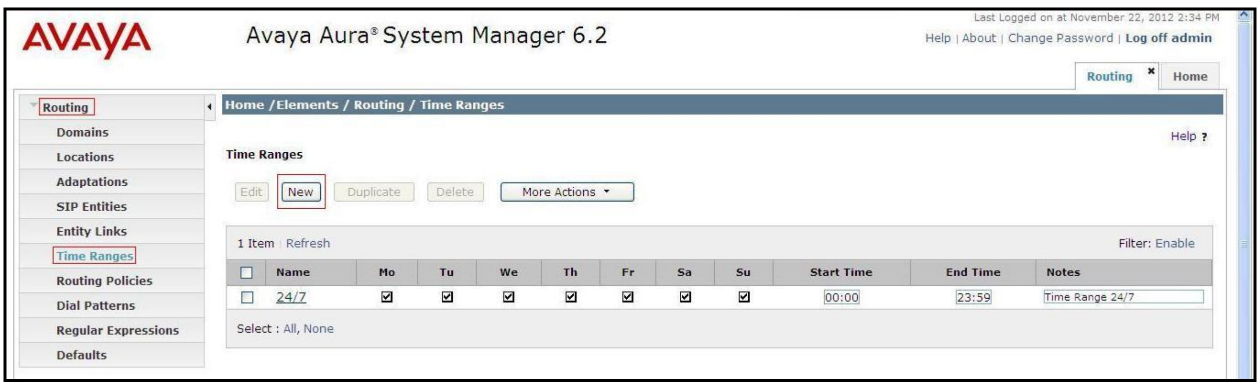


The following screen illustrates the Entity Links to Avaya SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.2.4 and 7.2.6**.



6.6. Configure Time Ranges

Time Ranges is configured for time-based-routing. In order to add a Time Ranges, select **Routing → 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.



6.7. Add Routing Policies

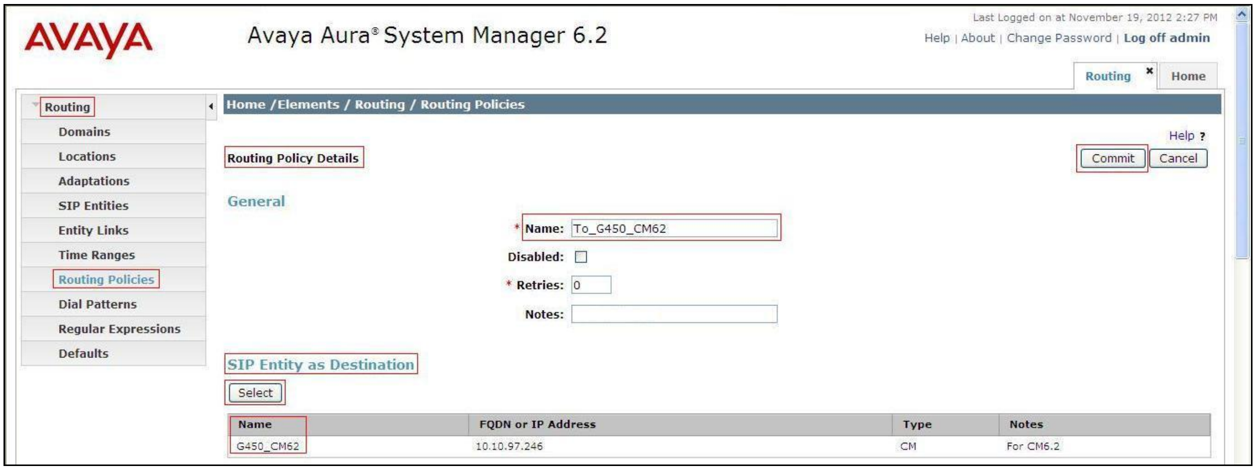
Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two Routing Policies must be added: one for Communication Manager and one for Avaya SBCE. To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand navigation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

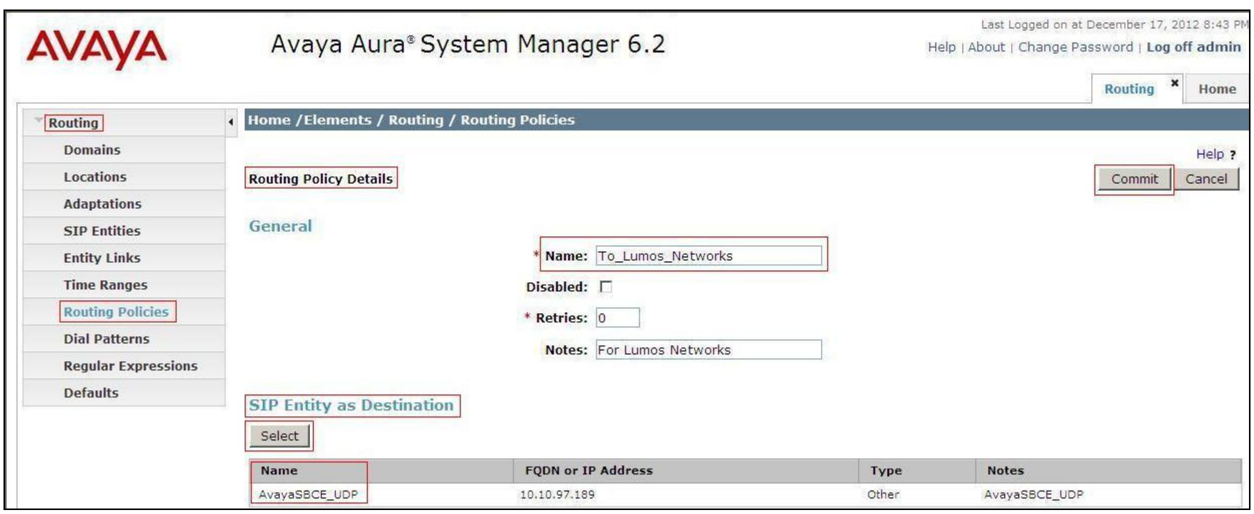
- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

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**



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**



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 → 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.

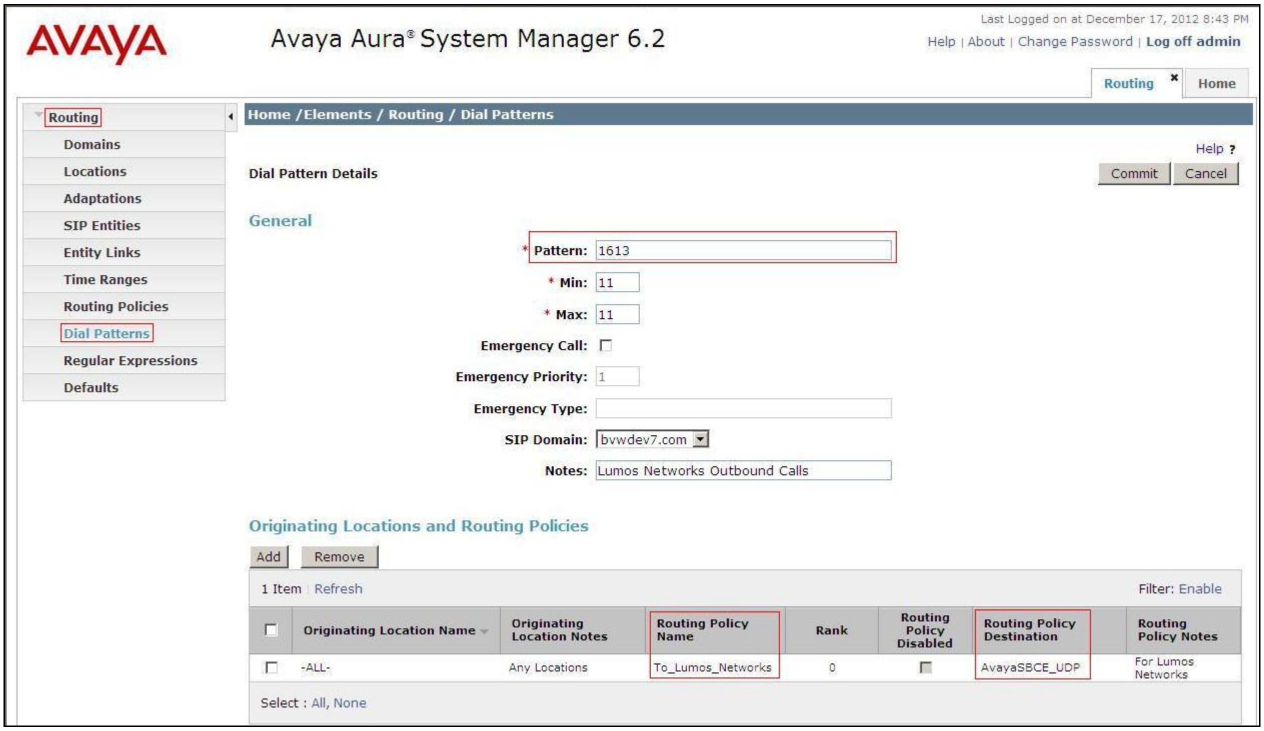
- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:**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

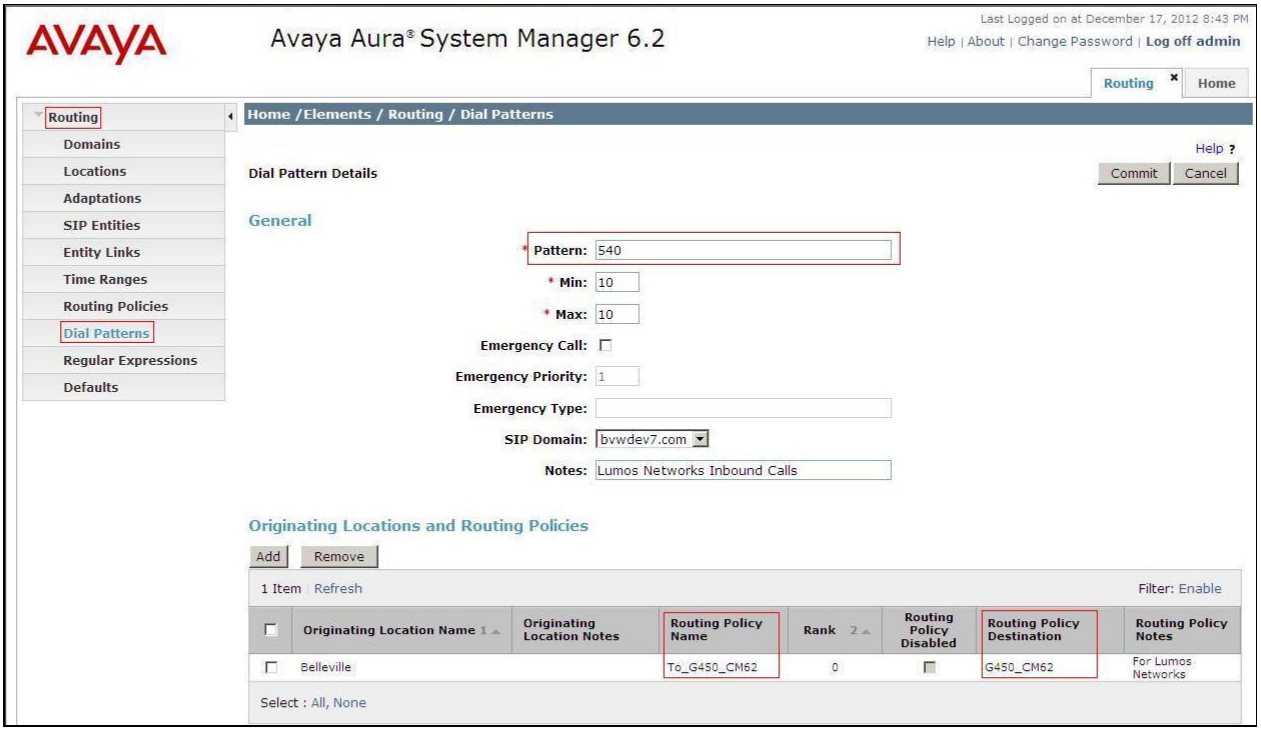
The first example shows that outbound 11-digit dialed numbers that begin with **1613** and have a destination SIP Domain of **bvwdev7.com** uses the **AvayaSBCE_UDP** Routing Policy as defined in **Section 6.7**.



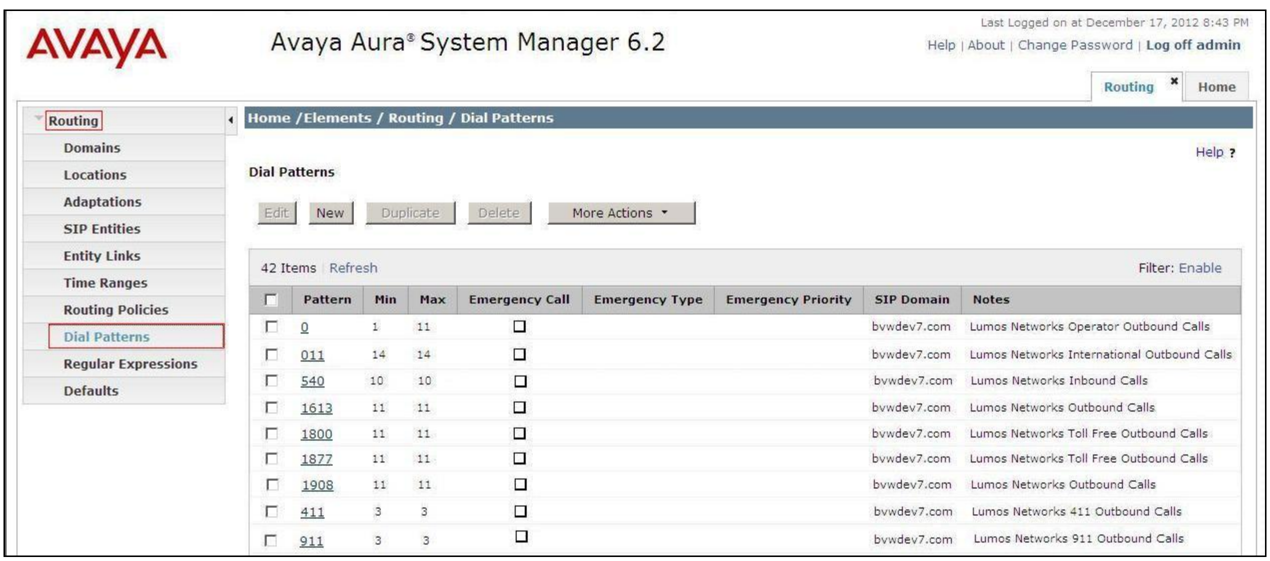
Note that the above Dial Pattern did not restrict outbound calls to specific US area codes. In real deployments, appropriate restriction can be exercised (e.g., use Dial Pattern 1908, etc. with 11 digits) per customer business policies.

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.



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



7. Configure Avaya Session Border Controller for Enterprise

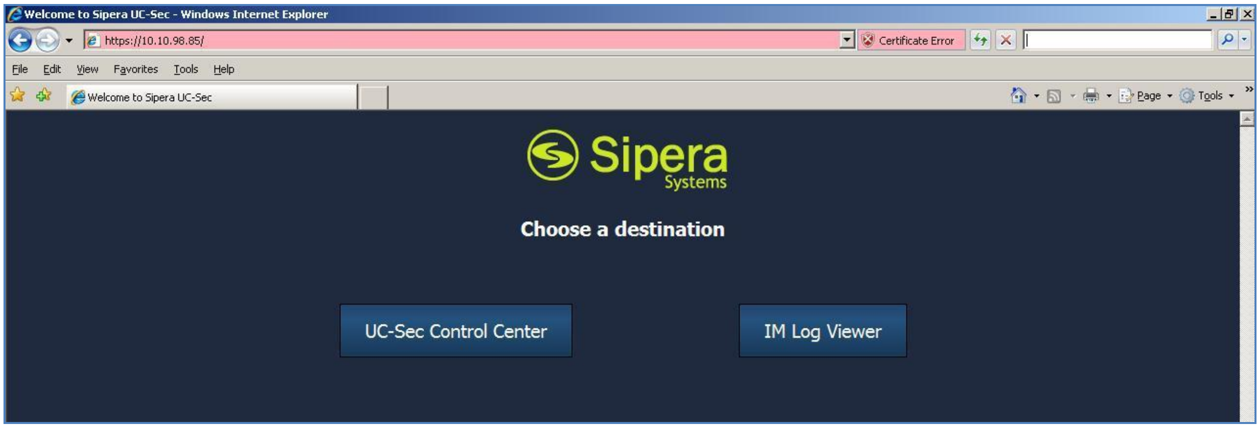
This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and Lumos Networks system.

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.

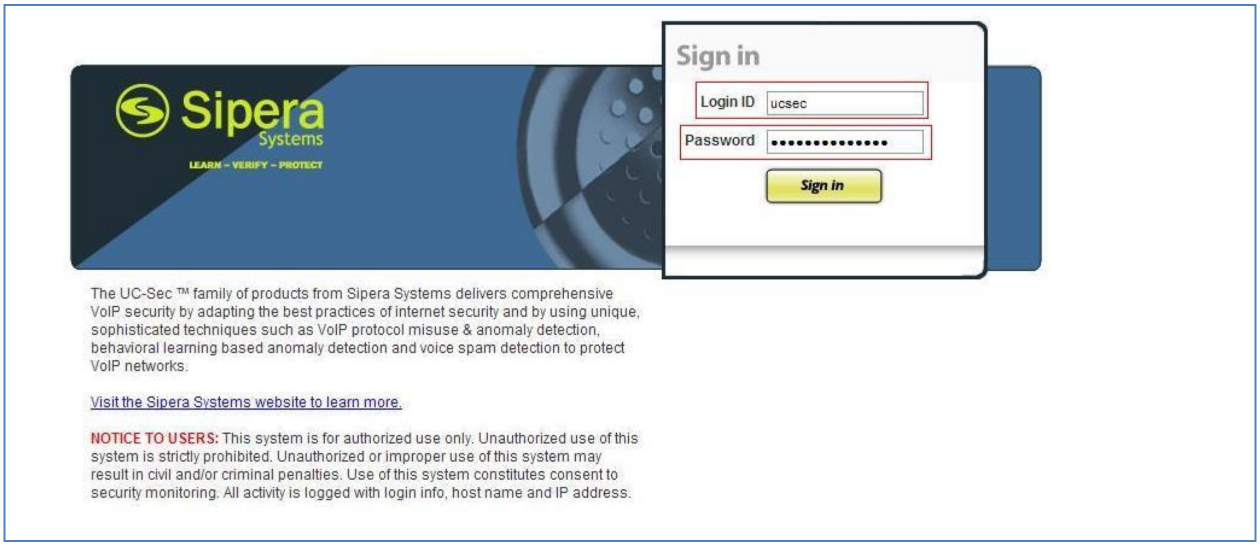
Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see **Section 11** of these Application Notes.

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**.



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

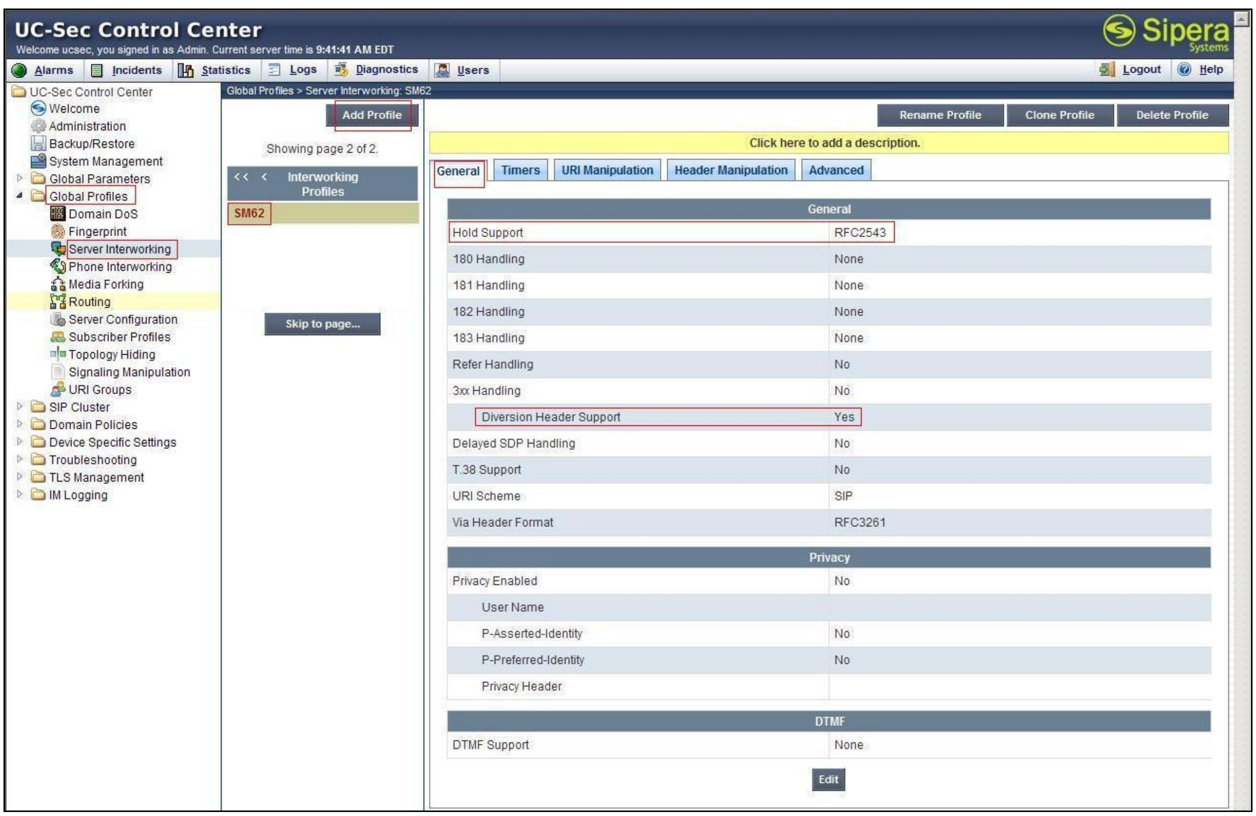
Server Interworking allows administrator to configure and manage various SIP call server-specific capabilities such as call hold, 180 Handling, etc.

From the menu on the left-hand side, select **Global Profiles → Server Interworking → 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.



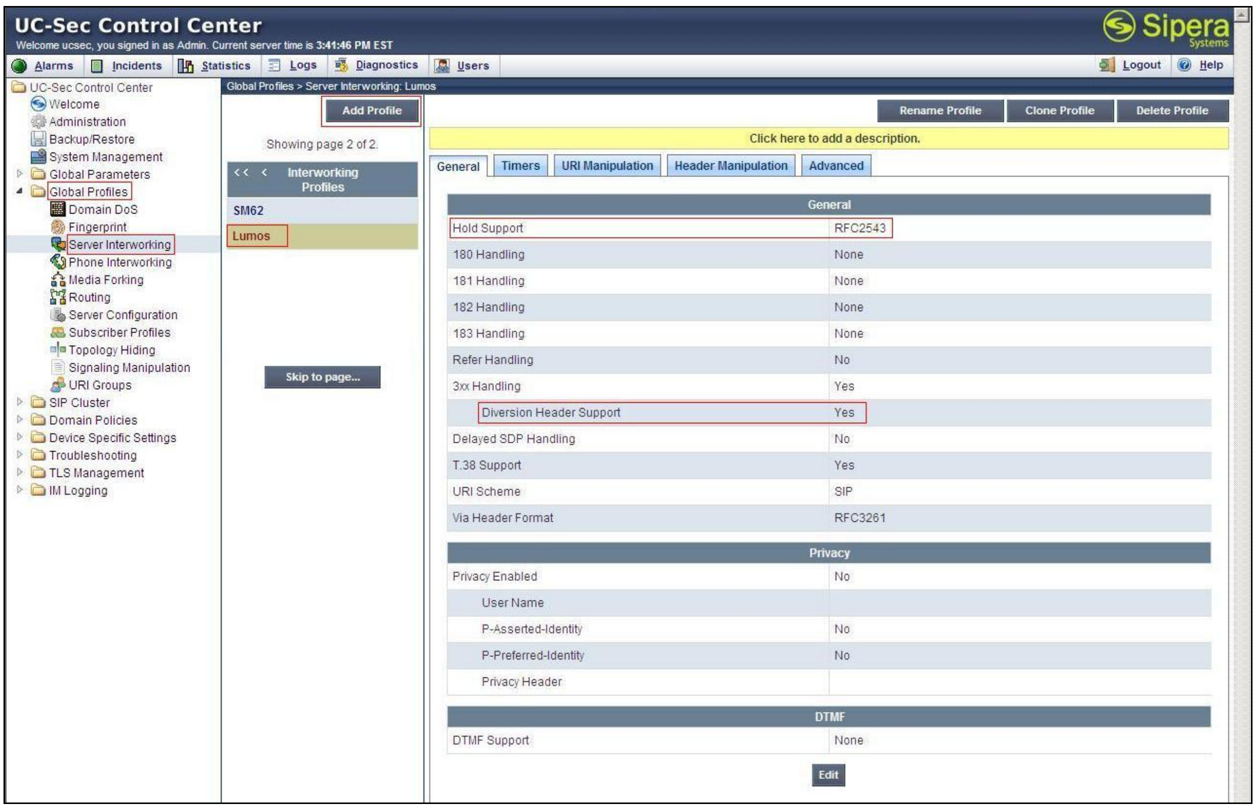
7.2.2. Configure Server Interworking – Lumos Networks site

From the menu on the left-hand side, select **Global Profiles → Server Internetworking → 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.



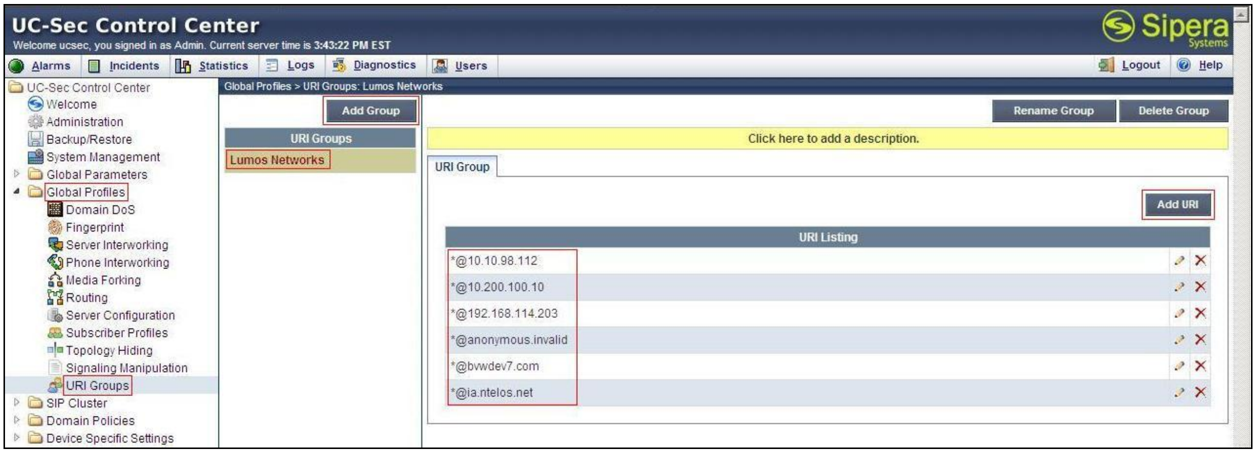
7.2.3. Configure URI Groups

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 → URI Groups**

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

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



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 → Routing → 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).

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 → Routing →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).

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 → Server Configuration →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**

On the **Advanced** tab:

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

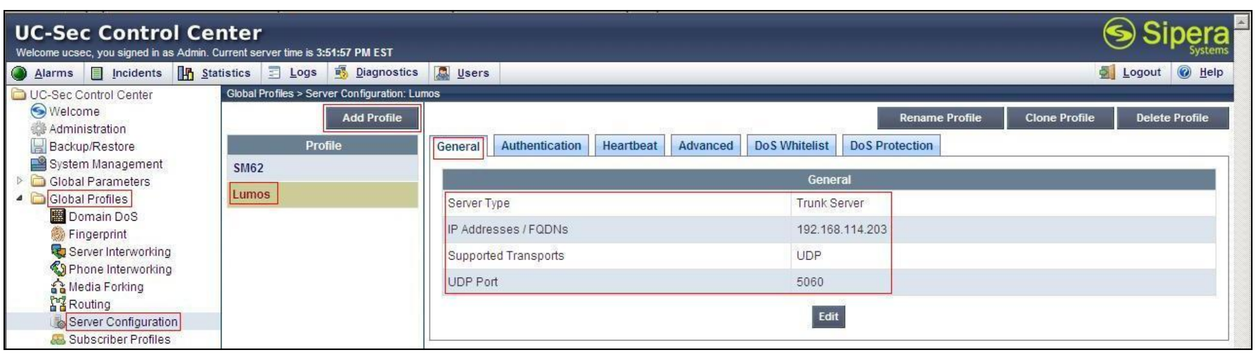
7.2.7. Configure Server – Lumos Networks ACME Packet SBC

From the menu on the left-hand side, select **Global Profiles → Server Configuration → 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**

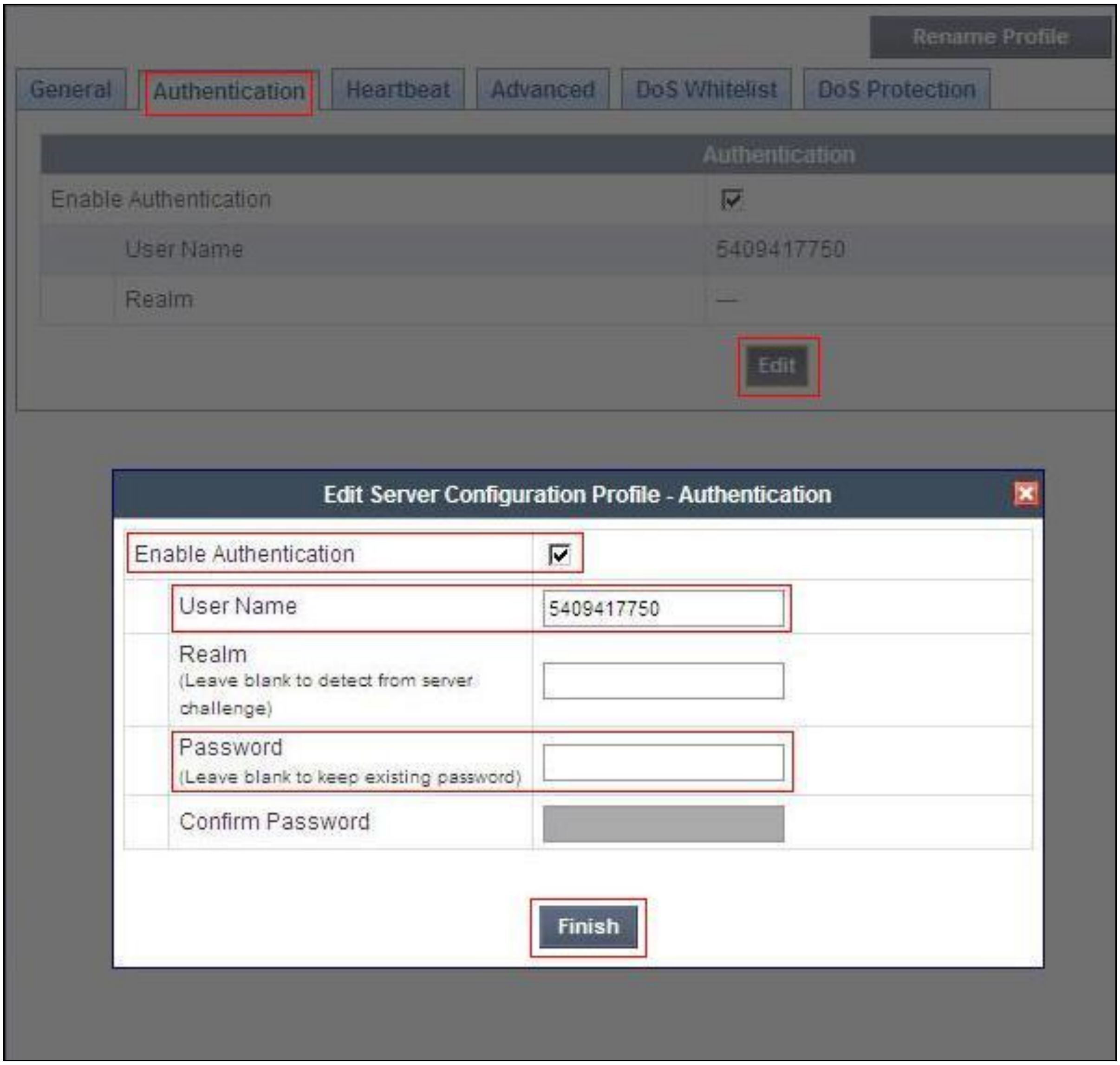


On the **Advanced** tab:

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

On the **Authentication** tab:

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



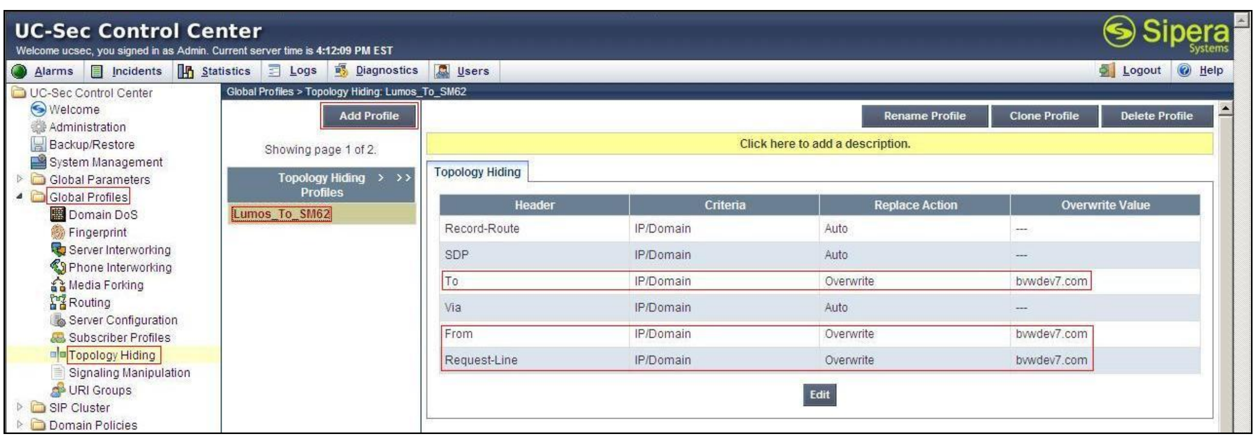
- On the **Heartbeat** tab, click **Edit** button.
  - Check **Enable Heartbeat**.
  - Select **Method**: **REGISTER**
  - Add the value of **Frequency**: **60** seconds
  - Add **From URI**: **5409417750@ia.ntelos.net**
  - Add **To URI**: **5409417750@ia.ntelos.net**
  - Check **TCP Probe**
  - Add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

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**

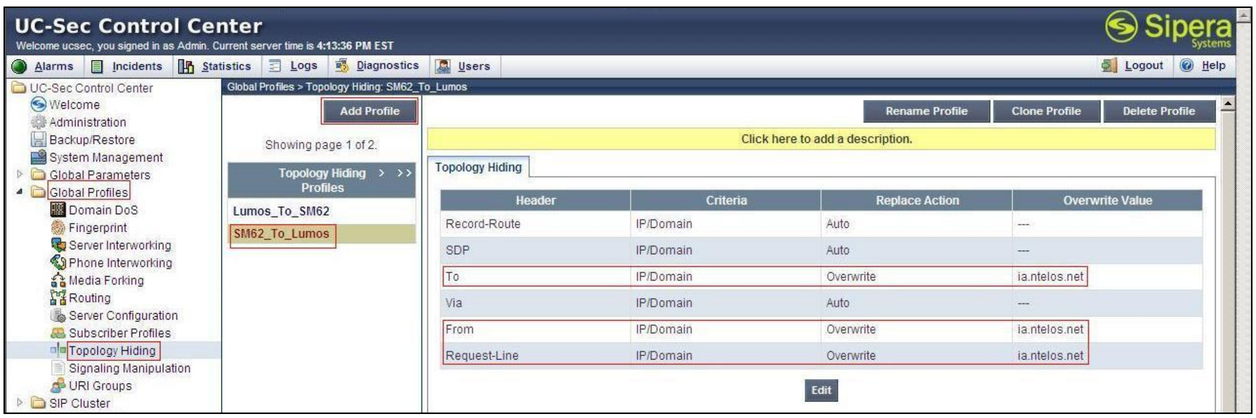
- For the Header **To,**
  - In the **Criteria** column select: **IP/Domain**
  - In the **Replace Action** column select**: Overwrite**
  - In the **Overwrite Value** column enter**: bvwdev7.com**
- For the Header **From,**
  - In the **Criteria** column, select: **IP/Domain**
  - In the **Replace Action**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



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

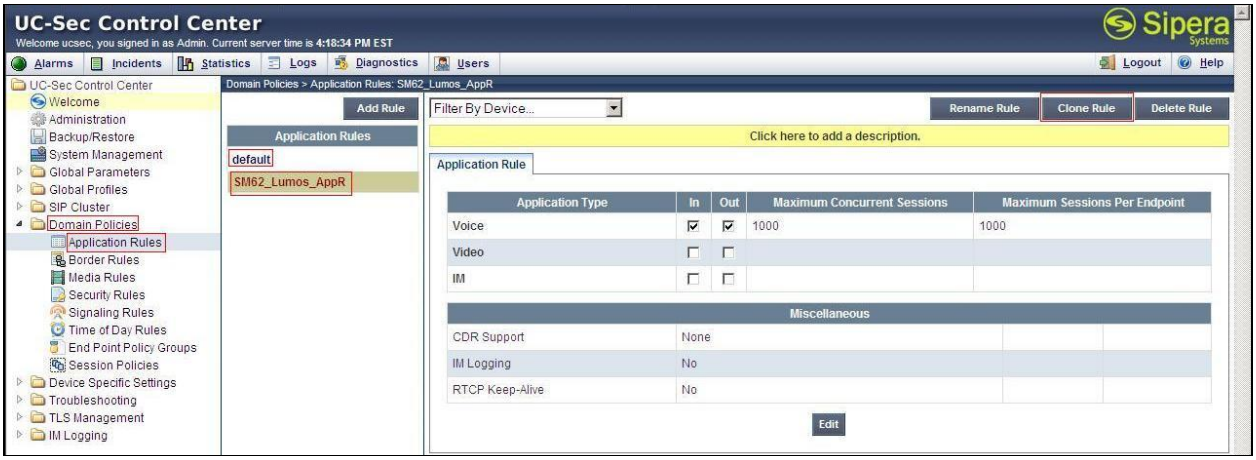
The Domain Policies feature allows administrator to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies 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.

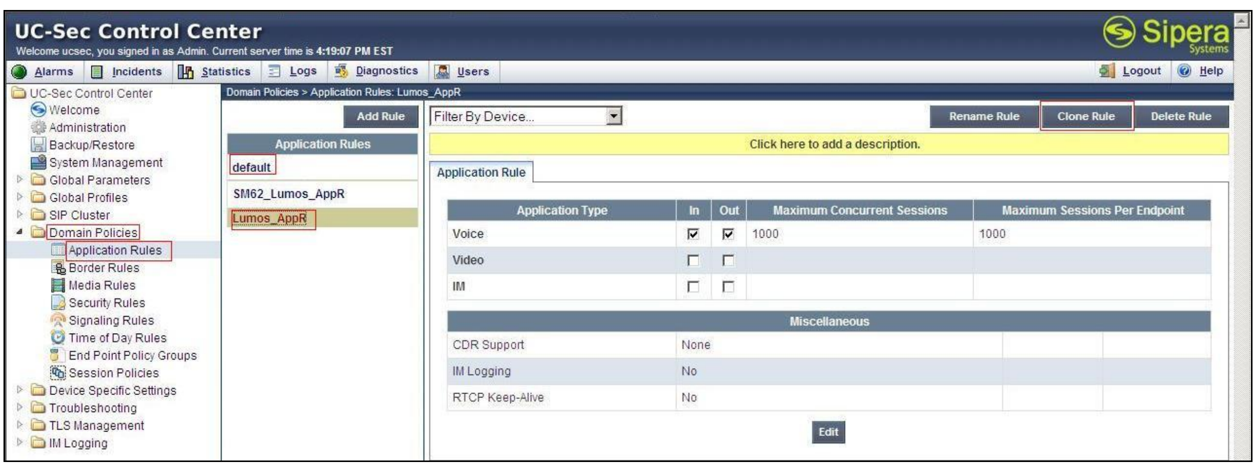
From the menu on the left-hand side, select **Domain Policies → Application Rules**

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



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

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

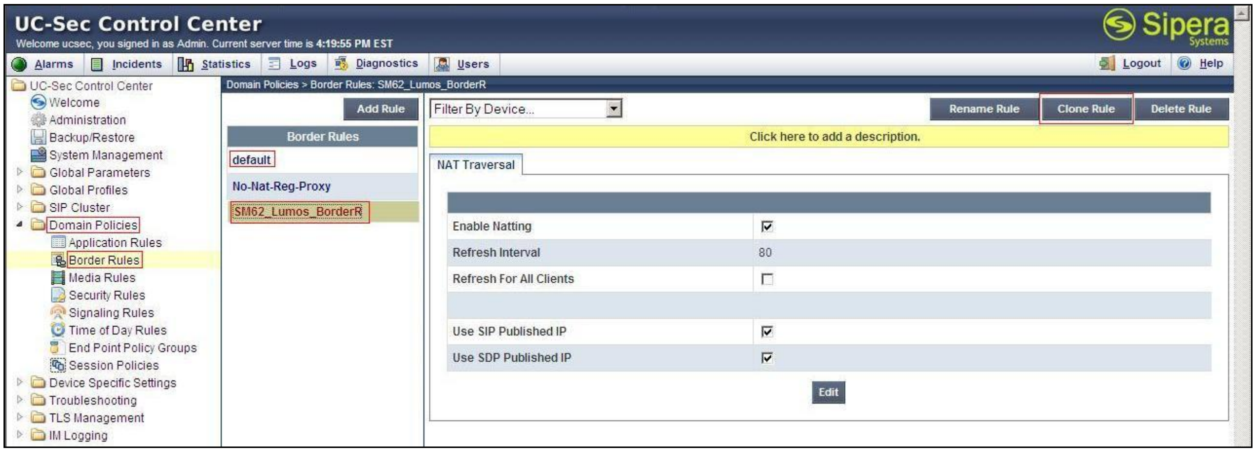


7.3.2. Create Border Rules

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.

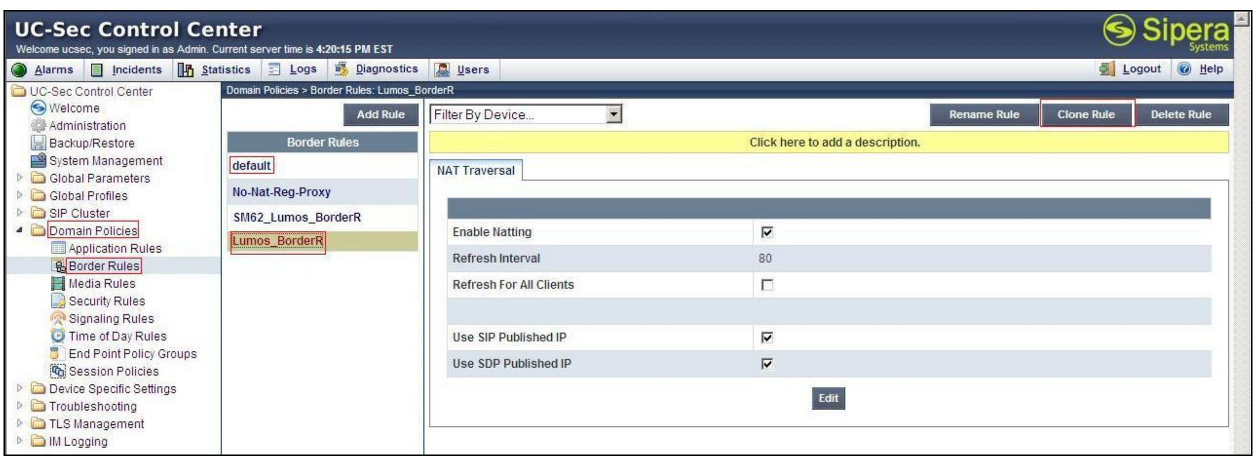
From the menu on the left-hand side, select **Domain Policies →Border Rules**

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



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

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



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 → Media Rules**

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

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

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

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)

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

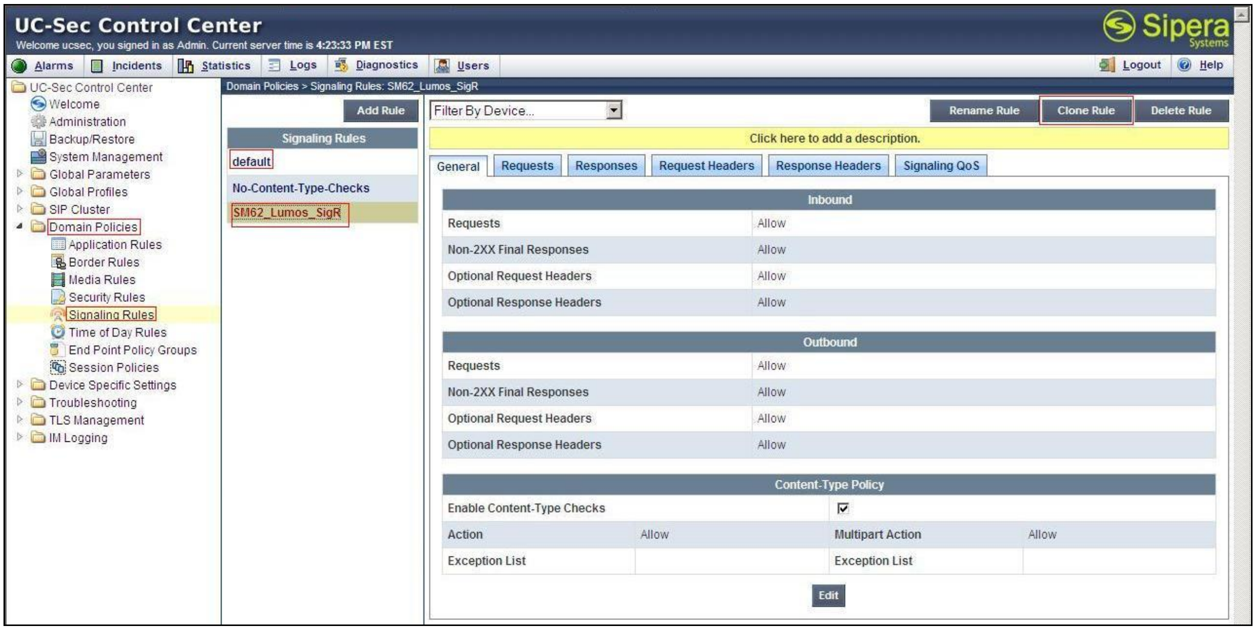
- Select the **default-med** Rule
- Select **Clone Rule** button
    - Enter **Clone Name: Lumos_SecR**
    - Click **Finish** (not shown)**.**

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.

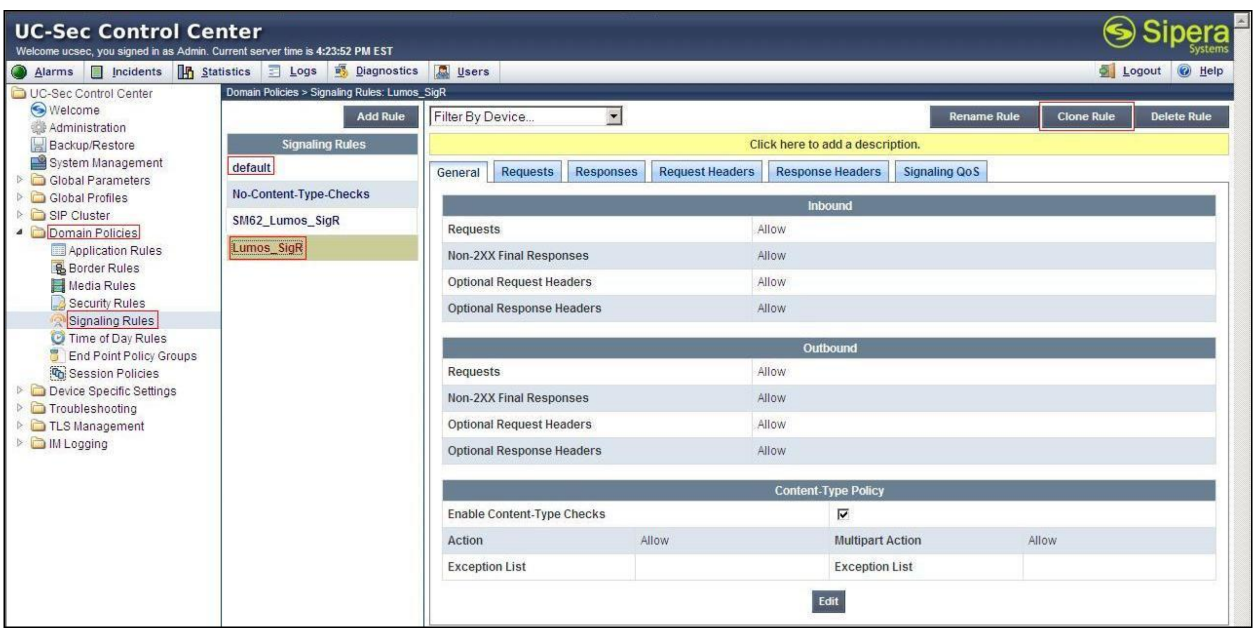
From the menu on the left-hand side, select **Domain Policies → Signaling Rules**

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



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).

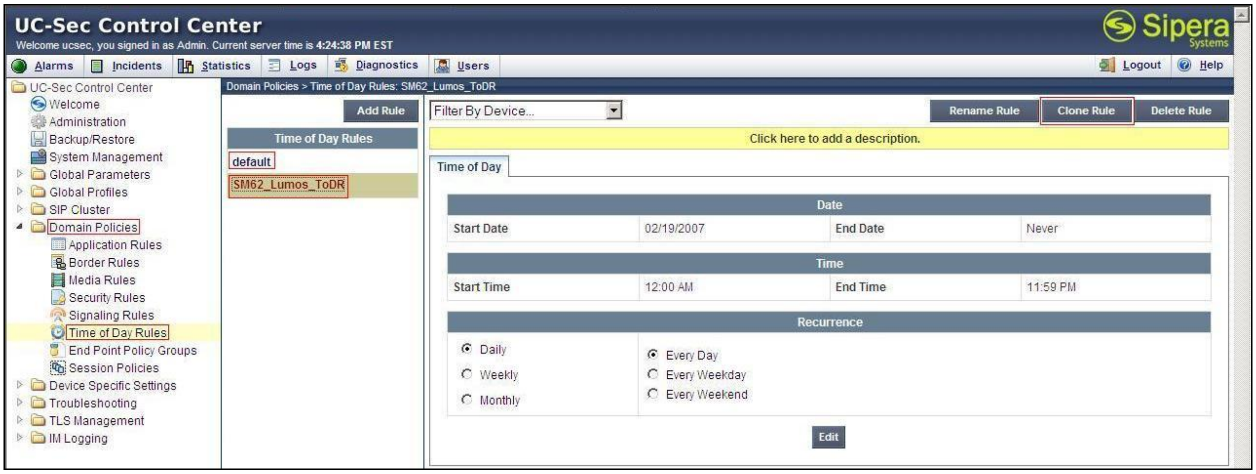


7.3.6. Create Time of Day Rules

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 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.

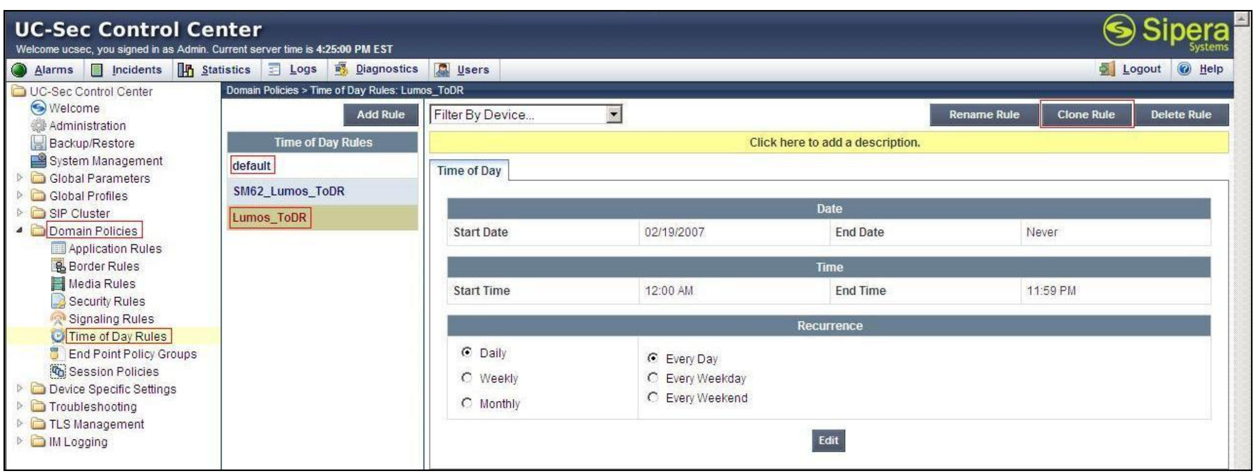
From the menu on the left-hand side, select **Domain Policies → Time of Day Rules**

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



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: Lumos_ToDR**
  - Click **Finish** (not shown).

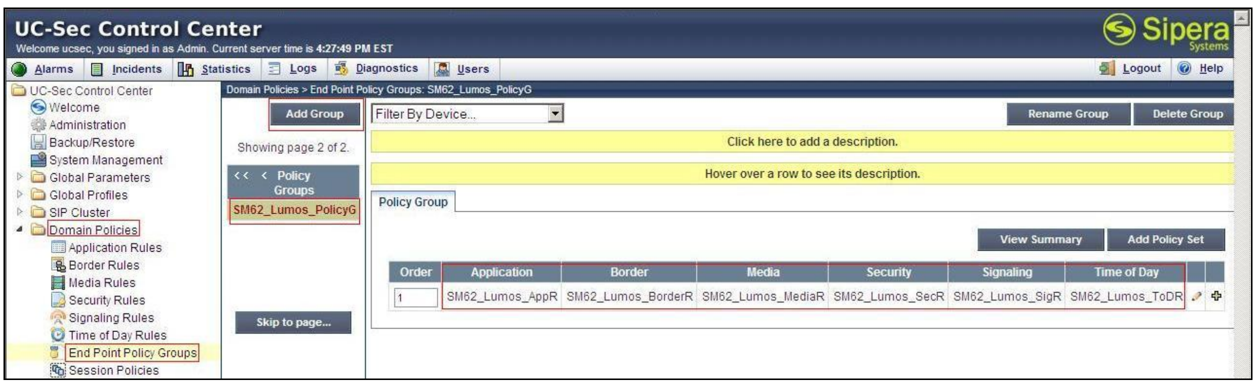


7.3.7. Create Endpoint Policy Groups

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 → 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)**.**



From the menu on the left-hand side, select **Domain Policies → 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).

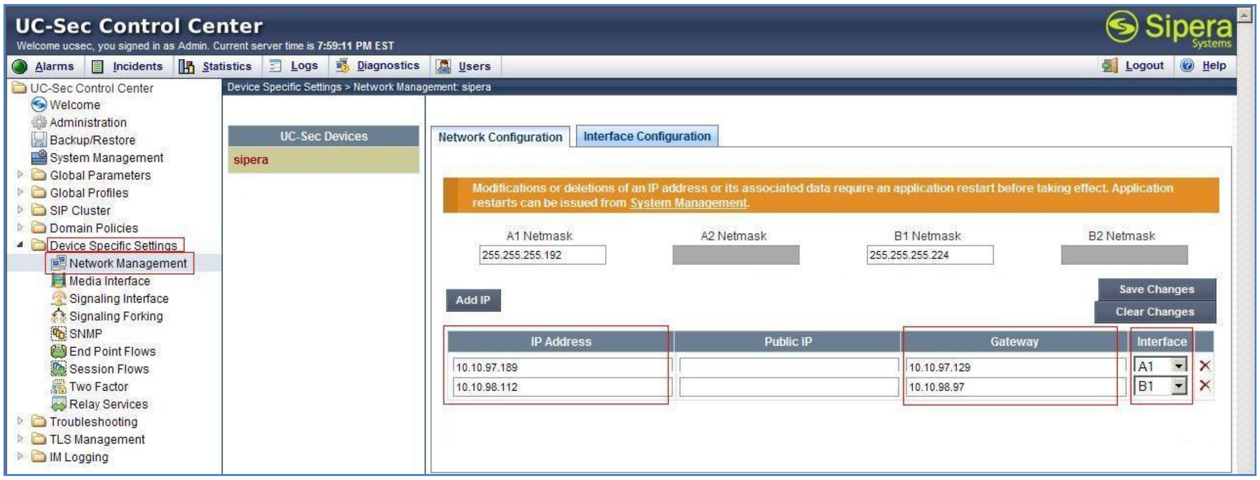
7.4. Device Specific Settings

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

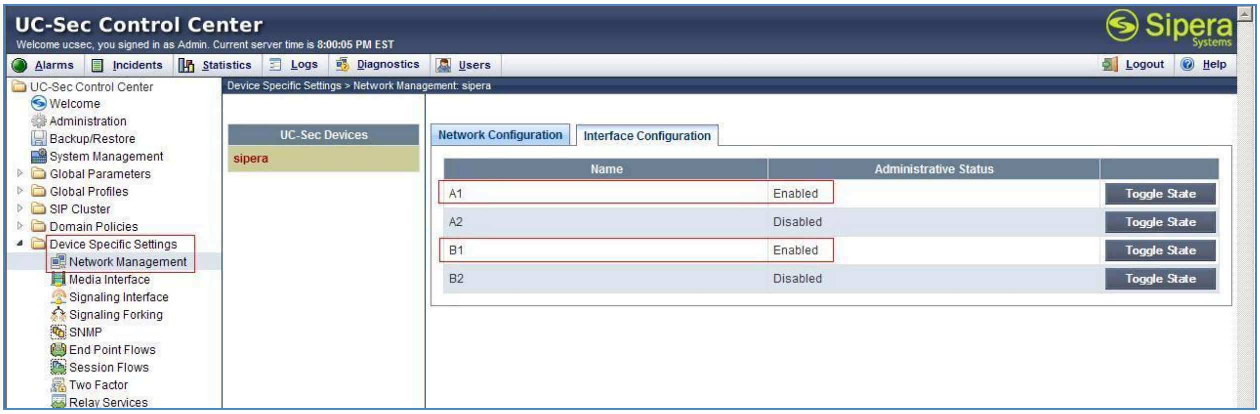
From the menu on the left-hand side, select **Device Specific Settings → Network Management**.

- 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**



- Select the **Interface Configuration** Tab.

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



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 → 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).

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**

- 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).

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

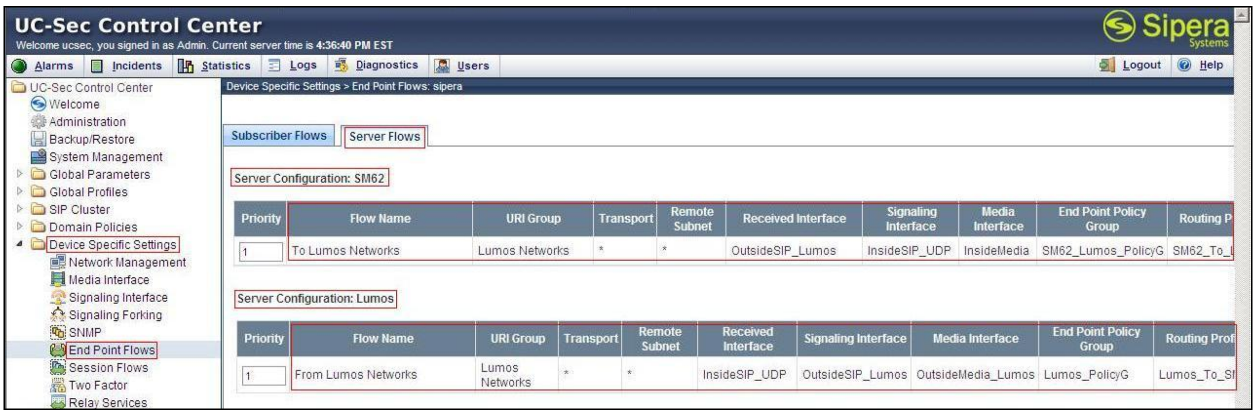
From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**

- 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).



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.

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:
http://support.avaya.com/

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*, http://www.ietf.org/
[16] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/

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