Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise 4.0.5 with Broadcore/Masergy SIP Trunk – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Broadcore/Masergy SIP Trunk and Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise 4.0.5.

Broadcore/Masergy 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 in the Avaya Solutions and Interoperability Test Lab, utilizing Broadcore/Masergy SIP Trunk Services.

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Broadcore/Masergy SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solutions consists of Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Aura® Session Manager 6.2, Avaya Session Border Controller for Enterprise (SBCE) 4.0.5 and various Avaya endpoints.

Broadcore/Masergy offers SIP trunk services with either Single Number Registration offered service or through Static IP Authentication. These Application Notes illustrate Single Number Registration offered service, and includes Avaya SBCE configuration differences for Static IP Authentication in **Appendix A**.

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

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Communication Manager, Session Manager and Avaya SBCE to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to Broadcore/Masergy SIP Trunk Service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

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. Phone types included 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. Phone types included 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 supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X Communicator also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Each supported protocol was tested.
- Various call types including: local, long distance and outbound toll-free
- Codecs G.711MU and G.729A
- DTMF transmission using RFC 2833
- T.38 Fax
- Caller ID presentation and Caller ID restriction
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, transfer, and conference
- Off-net call forwarding and mobility (extension to cellular)

Items not supported or not tested included the following:

- Inbound toll-free, international, operator, operator services (0 + 10 digits) and emergency calls (911) are supported but were not tested as part of the compliance test

2.2. Test Results

Interoperability testing of Broadcore/Masergy SIP Trunk Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Single Number Registration**: When using Broadcore/Masergy Single Number Registration offered service, the REQUEST-URI of an inbound call will include the main billing number of the SIP trunk, while the TO header will include the actual called number. Communication Manager routes calls based on the REQUEST-URI, so a SIP manipulation is necessary to replace the User portion of the REQUEST-URI with information residing in the TO header. Similarly outbound calls require the FROM header to include the main billing number and the P-Asserted-Identity (PAI) header to have the actual DID number. The Avaya SBCE is used to perform the required SIP manipulation. See **Section 7.5**.
- **Fax:** When an outbound fax call is first setup with G.729 codec, Broadcore/Masergy will send a re-INVITE to G.711 first before sending an INVITE to T.38. If G.729 is the only codec listed by Communication Manager, the fax will fail with a 488 Not Acceptable Here. To prevent this failure, it is necessary to always include G.711 as an available codec choice if fax will be used.
- **SendOnly SIP Parameter:** With the Network Call Redirection feature enabled, Communication Manager will use the SIP parameter “Sendonly” to signal any hold call conditions. Broadcore/Masergy will responds with an inactive media when it receives “Sendonly” instead of responding with “Recvonly”. As a result, the originating side hears music provided by Broadcore/Masergy instead of locally sourced music on hold. The Avaya SBCE is used to remove the “Sendonly” parameter to allow local hold music to be received properly. See **Section 7.5**.
- **EC500 Confirm Answer:** EC500 has safeguards built in for cellular voicemail detection to prevent the call from being answered by the mobile phone’s voicemail. An optional supplement to this is to activate the “Confirmed Answer” feature. This feature ensures

the call is answered and it will not deliver the call until a DTMF digit is received. It was observed during testing that the EC500 Confirmed Answer feature in Communication Manager did not function properly when the Initial IP-IP Direct Media feature was enabled in Communication Manager signaling group. Disabling the IP-IP Direct Media, as shown in **Section 5.7**, will allow normal operation of the Confirmed Answer feature. This issue is under investigation by the Communication Manager product team.

Broadcore/Masergy SIP Trunk Service 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 the Broadcore/Masergy SIP Trunk Service, contact Broadcore/Masergy using the Customer Care links at www.broadcore.com.

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya Customer Premises Equipment (CPE) location connected via a T1 Internet connection to the Broadcore/Masergy SIP Trunks service. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, Avaya SBCE provides NAT functionality and SIP header manipulation. Avaya SBCE receives traffic from Broadcore/Masergy SIP Trunk on port 5060 and sends traffic to the Broadcore/Masergy SIP Trunk using destination port 5060, using the UDP protocol. For security reasons, any actual public IP addresses used in the configuration have been either replaced with private IP addresses or have been blocked out. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.

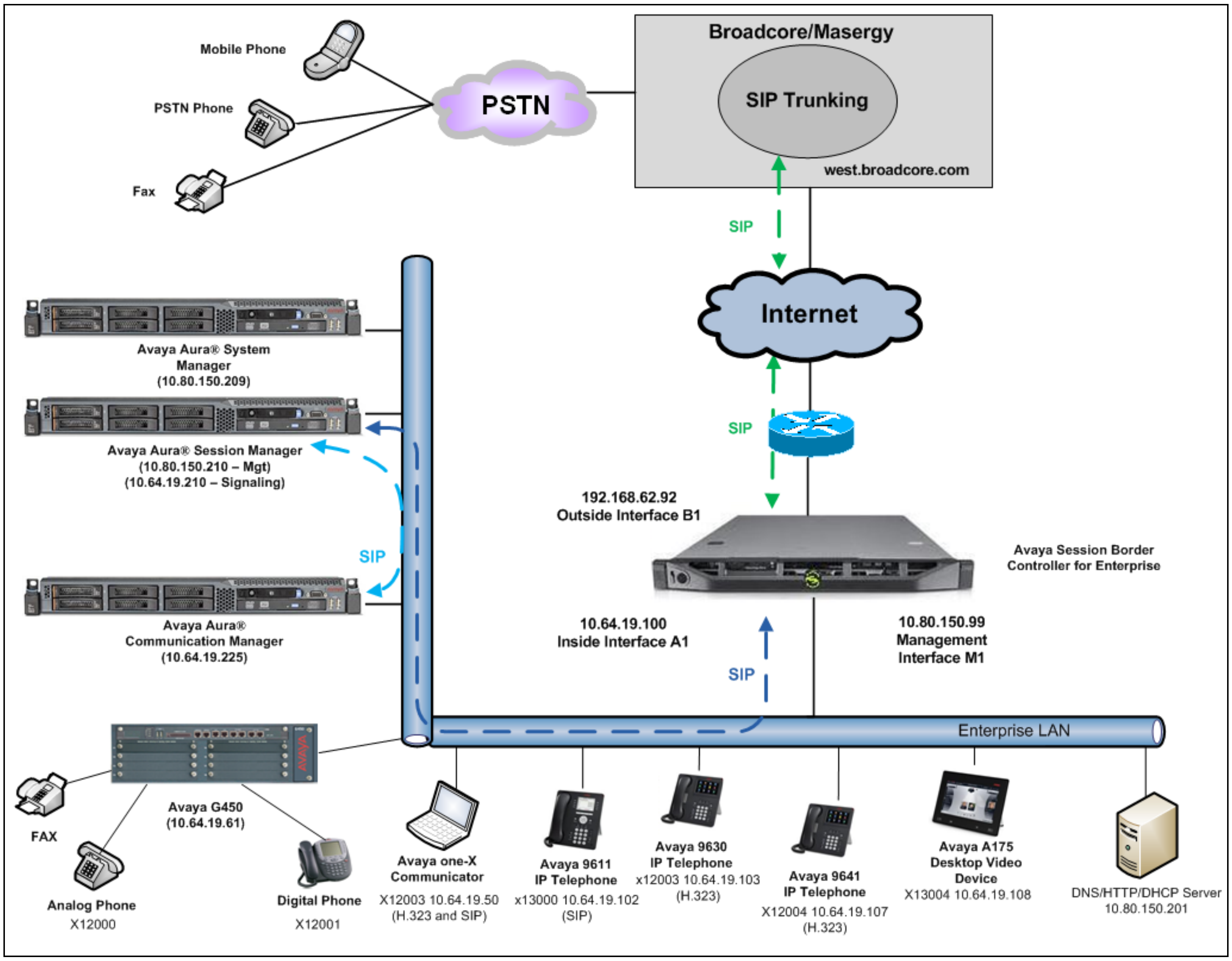


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manger	R016x.02.0.823.0 -20199
Avaya Aura® System Manager	6.2.0 – SP3
Avaya Aura® Session Manager	6.2.3.0.623006
Avaya Session Border Controller for Enterprise	4.0.5Q19
Avaya G450	31.24.0
Avaya A175 Desktop Video Device	Avaya Flare® Experience 1.1.1
Avaya 9641 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.2209
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.104S
Avaya 9611 IP Telephone (SIP)	Avaya one-X® Deskphone Edition 6.2.0.72
Avaya 9608 IP Telephone (SIP)	Avaya one-X® Deskphone Edition 6.2.0.72
Avaya one-X® Communicator	6.1.5.07-SP5-37495
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Broadsoft/Masergy SIP Trunking Solution Components	
Component	Release
Broadsoft	R17 SP4

Table 1: Equipment and Software Tested

The specific configuration above was used for the compatibility testing.

Note: 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 Broadcore/Masergy SIP Trunk Service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from Broadcore/Masergy. It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and Session Manager has been previously completed and is not discussed here.

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.

Note: IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN numbers are not revealed.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that **12000** licenses are available and **285** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

```
display system-parameters customer-options                        Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 36000 3
                   Maximum Video Capable IP Softphones: 18000 1
                       Maximum Administered SIP Trunks: 12000 285
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                            Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 250   2
           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
```

5.2. System Features

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

```
change system-parameters features                               Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
```

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **Anonymous** for both types of calls.

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

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

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

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

ENBLOC DIALING 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 **display node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and for Session Manager (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.7**.

```
display node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name               IP Address
CMM                 10.64.19.205
SM                  10.64.19.210
default             0.0.0.0
procr               10.64.19.205
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 2 was used for this purpose. The Broadcore/Masergy SIP Trunk Service supports G.729A, G.729AB and G.711MU. During compliance testing each of the supported codecs were tested independently by changing the order of preference to list the codec being tested as the first choice. The true order of preference is defined by the end customer. In the example below, **G.729A** and **G.711MU** were entered in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

                          IP Codec Set

    Codec Set: 2

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

On **Page 2**, set the **Fax Mode** to **T.38-standard**.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

                Mode                Redundancy
    FAX         t.38-standard        0
    Modem       off                  0
    TDD/TTY     US                   3
```

5.5. IP Interface for procr

The **add ip-interface procr** or **change ip-interface procr** command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the PE for SIP Trunk Signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones and H.248 gateways in the sample configuration.

```
change ip-interface procr                                      Page   1 of   2
                                 IP INTERFACES


                  Type: PROCR
                                                     Target socket load: 1700

      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: 10.80.150.225


           Subnet Mask: /24
```

5.6. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 2 was chosen for the service provider trunk. IP network region 1 is the default IP network region and encompasses the rest of the enterprise. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Location** field to match the enterprise location for this SIP trunk.
- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avayalab.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. To enable shuffling, 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**.
- Set the **UDP Port Min** and **UDP Port Max** fields to a range suitable for RTP traffic.
- Default values can be used for all other fields.

```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avayalab.com
    Name: SIP Trunks
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                         RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

```
change ip-network-region 2                                      Page   4 of  20

 Source Region: 2     Inter Network Region Connection Management     I        M
                                                                     G  A     t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G     c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L     e
 1    2     y    NoLimit                                             n        t
 2    2
 3
 4
```

5.7. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for Session Manager.

- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). The use of different ports allows Communication Manager to distinguish different types of calls arriving from the same 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. The Peer Server field will automatically change to **SM** once Communication Manager has detected a Session Manager peer.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.6**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Initial IP-IP Direct Media?** to **n**. See **Section 2.2** for details.
- Default values may be used for all other fields.

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

 Group Number: 2              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n                                           SIP Enabled LSP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM
 Near-end Listen Port: 5081                Far-end Listen Port: 5081
                                        Far-end Network Region: 2

Far-end Domain: avayalab.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
```

5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.7**. For the compliance test, trunk group 2 was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 2                                               Page   1 of  21
                                 TRUNK GROUP

Group Number: 2                  Group Type: sip           CDR Reports: y
  Group Name: SIP SP 2                  COR: 1        TN: 1        TAC: *02
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 2
                                                    Number of Members: 10
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

```
add trunk-group 2                                                 Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y
```

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end.

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

```
add trunk-group 2                                                Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                    Maintenance Tests? y



                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y



                                Modify Tandem Calling Number: no



 Show ANSWERED BY on Display? n
```

On **Page 4**, set the **Network Call Redirection** field to **y**. This allows inbound calls transferred back to the PSTN to use the SIP REFER method, see **Reference** [**13**]. Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is necessary to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Support Request History** field to **n**. Set the **Telephone Event Payload Type** to **101**, the value preferred by Broadcore/Masergy. Default values may be used for all other fields.

```
add trunk-group 2                                                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. Inbound Routing

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 using an Adaptation as shown in **Section 6.4**, and digit manipulation via Communication Manager incoming call handling table may not be necessary. If the DID number sent by Broadcore/Masergy 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. Both Session Manager digit conversion and Communication Manager incoming call handling treatment methods were created and tested successfully.

Use the **change inc-call-handling-trmt trunk-group** command to create an entry for any DID numbers unchanged by Session Manager. As an example, the following screen illustrates a conversion of DID number **2135552009** to extension **10000**.

```
change inc-call-handling-trmt trunk-group 2                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 2135552009       10  10000
```

5.10. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since public numbering was selected to define the format of this number (**Section 5.8**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

In the bolded row shown in the example below, a specific Communication Manager extension (x12004) is mapped to a DID number that is known to Broadcore/Masergy for this SIP Trunk connection (2135552009), when the call uses trunk group 2.

```
change public-unknown-numbering 5 ext-digits 12000 trunk-group 5Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext            Trk       CPN            CPN
Len Code           Grp(s)    Prefix         Len
                                                  Total Administered: 16
 5  12001          2         4245556554     10       Maximum Entries: 9999
 5  12004          2         2135552009     10
 5  12005          2         2135554088     10    Note: If an entry applies to
 5  13000          2         3235557674     10    a SIP connection to Avaya
 5  13001          2         2135559117     10    Aura(R) Session Manager,
 5  13002          2         2135559117     10    the resulting number must
 5  13004          2         4245553665     10    be a complete E.164 number.
```

5.11. 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
   0           1   attd
   1           5   ext
   2           5   ext
   3           5   ext
   4           5   ext
   5           5   ext
   6           5   ext
   7           5   ext
   8           5   ext
   9           1   fac
   *           3   dac
   #           3   dac
```

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

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

      Auto Alternate Routing (AAR) Access Code: *00
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *33    Deactivation: #33
Call Forwarding Activation Busy/DA: *30    All: *31    Deactivation: #30
   Call Forwarding Enhanced Status:        Act:        Deactivation:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9.

- **Dialed String:** enter the leading digits (e.g., **13**) necessary to uniquely select the desired route pattern.
- **Total Min:** enter the minimum number of digits (e.g., **11**) expected for this PSTN number.
- **Total Max:** enter the maximum number of digits (e.g., **11**) expected for this PSTN number.
- **Route Pattern:** enter the route pattern number (e.g., **1**) to be used. The route pattern (to be defined next) will specify the trunk group(s) to be used for calls matching the dialed number.
- **Call Type: fnpa** the call type for North American 1+10 digit calls. For local 7 or 10 digit calls enter **hnpa**. For 411 and 911 calls use **svcl** and **emer** respectively. The call type tells Communication Manager what kind of call is made to help decide how to handle the dialed string and whether or not to include a preceding 1. For more information and a complete list of Communication Manager call types, see **Reference** [**3**] and [**4**].

The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 1 which contains the SIP trunk to the service provider (as defined next).

```
change ars analysis 1                                          Page   1 of   2
                              ARS DIGIT ANALYSIS TABLE
                                    Location: all           Percent Full: 0

          Dialed            Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    12                    11   11    1        fnpa         n
    13                    11   11    1        fnpa         n
    14                    11   11    1        fnpa         n
    15                    11   11    1        fnpa         n
    16                    11   11    1        fnpa         n
    17                    11   11    1        fnpa         n
    18                    11   11    1        fnpa         n
    19                    11   11    1        fnpa         n
    2                     10   10    1        hnpa         n
    3                     10   10    1        hnpa         n
    4                     10   10    1        hnpa         n
    411                   3    3     1        svcl         n
    5                     10   10    1        hnpa         n
    555                   7    7     deny     hnpa         n
    6                     10   10    1        hnpa         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 1 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **2** was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk**: **1** The prefix mark (**Pfx Mrk**) of 1 will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: Broadcore SIP TRK
                             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: 2    0       1                                                     n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

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

Use the **change ars digit-conversion** command to manipulate the routing of dialed digits that match the DIDs to prevent these calls from going out the PSTN and using unnecessary SIP trunk resources. The example below shows the DID numbers assigned by Broadcore/Masergy being converted to 5 digit extensions.

```
change ars digit-conversion 1                                      Page   1 of   2
                       ARS DIGIT CONVERSION TABLE
                                 Location: all                Percent Full: 0

  Matching Pattern      Min    Max    Del    Replacement String   Net  Conv ANI Req

  2135552009            10     10     10     12004                ext   y       n
  2135554088            10     10     10     12005                ext   y       n
  2135559117            10     10     10     13001                ext   y       n
  3235557674            10     10     10     13000                ext   y       n
  4245553665            10     10     10     13004                ext   y       n
  4245556554            10     10     10     12001                ext   y       n
```

5.12. Saving Communication Manager Configuration Changes

The command **save translation all** can be used to save the configuration.

```
save translation all

                               SAVE TRANSLATION

           Command Completion Status                                Error Code

           Success                                                  0
```

6. Configure Avaya Aura® Session Manager

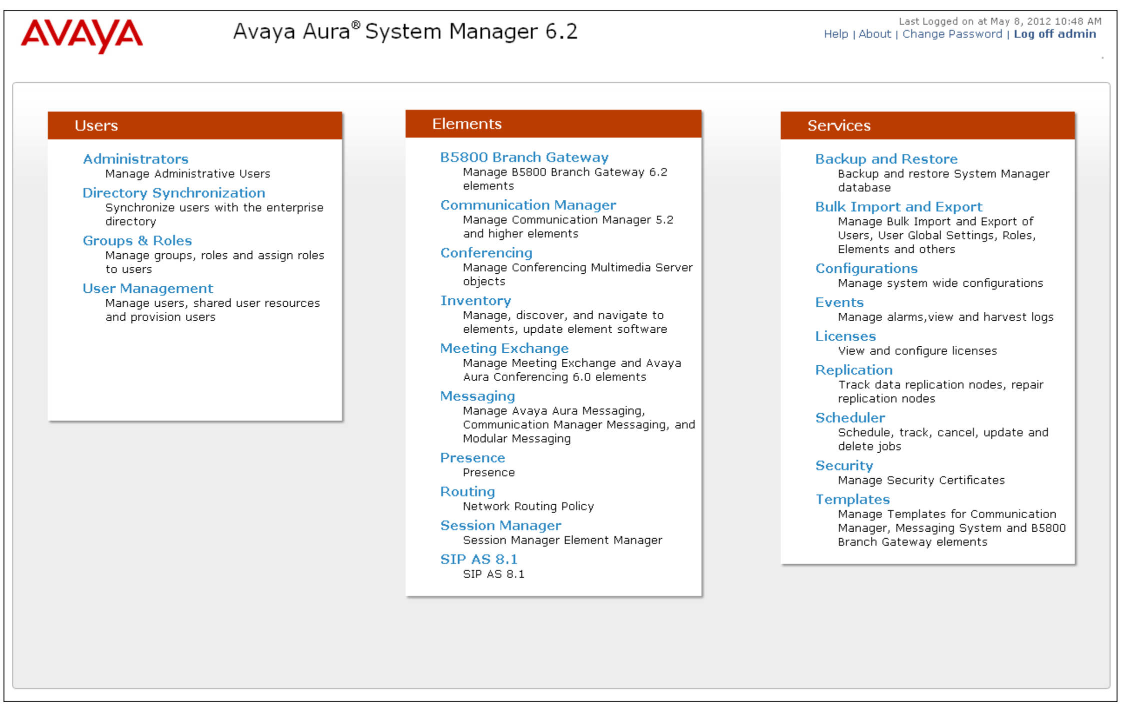
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, Avaya 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 control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager Instance, corresponding to the Session Manager server to be administered in System Manager

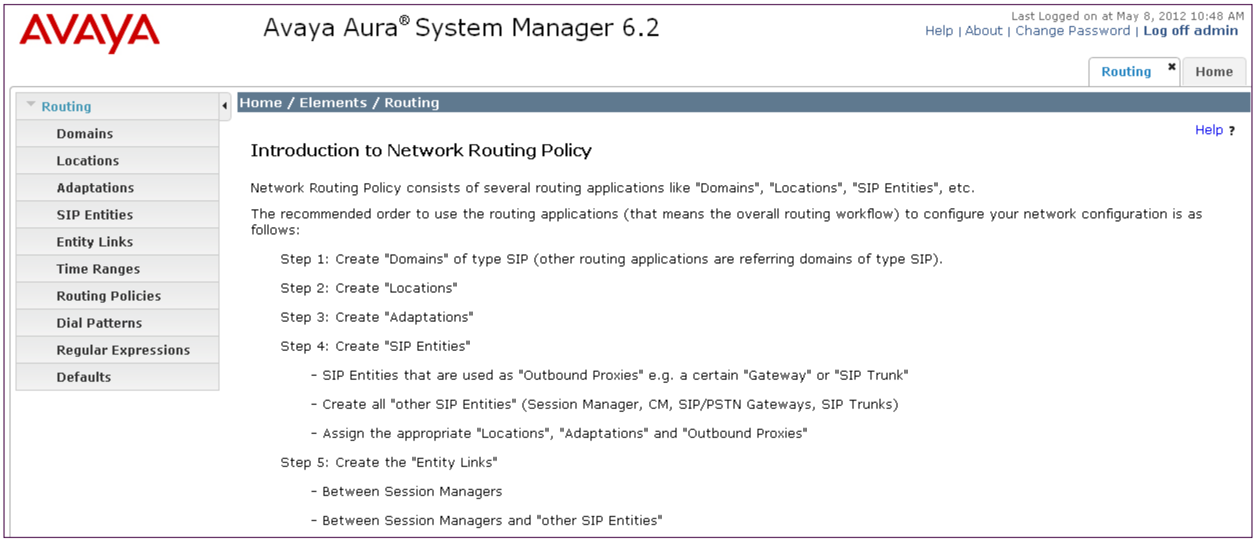
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. Avaya Aura® System Manager Login and Navigation

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



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

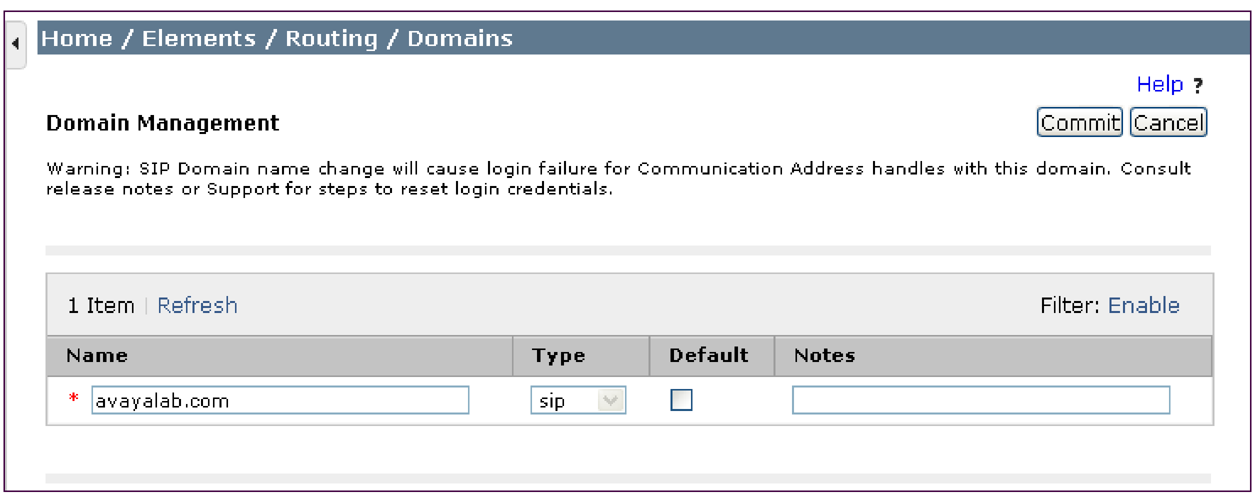


6.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avayalab.com**). Navigate to **Routing → Domains** and click the **New** button in the right pane (not shown). In the new right pane that appears, 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**. The screen below shows the entry for the **avayalab.com** domain.



6.3. Add Location

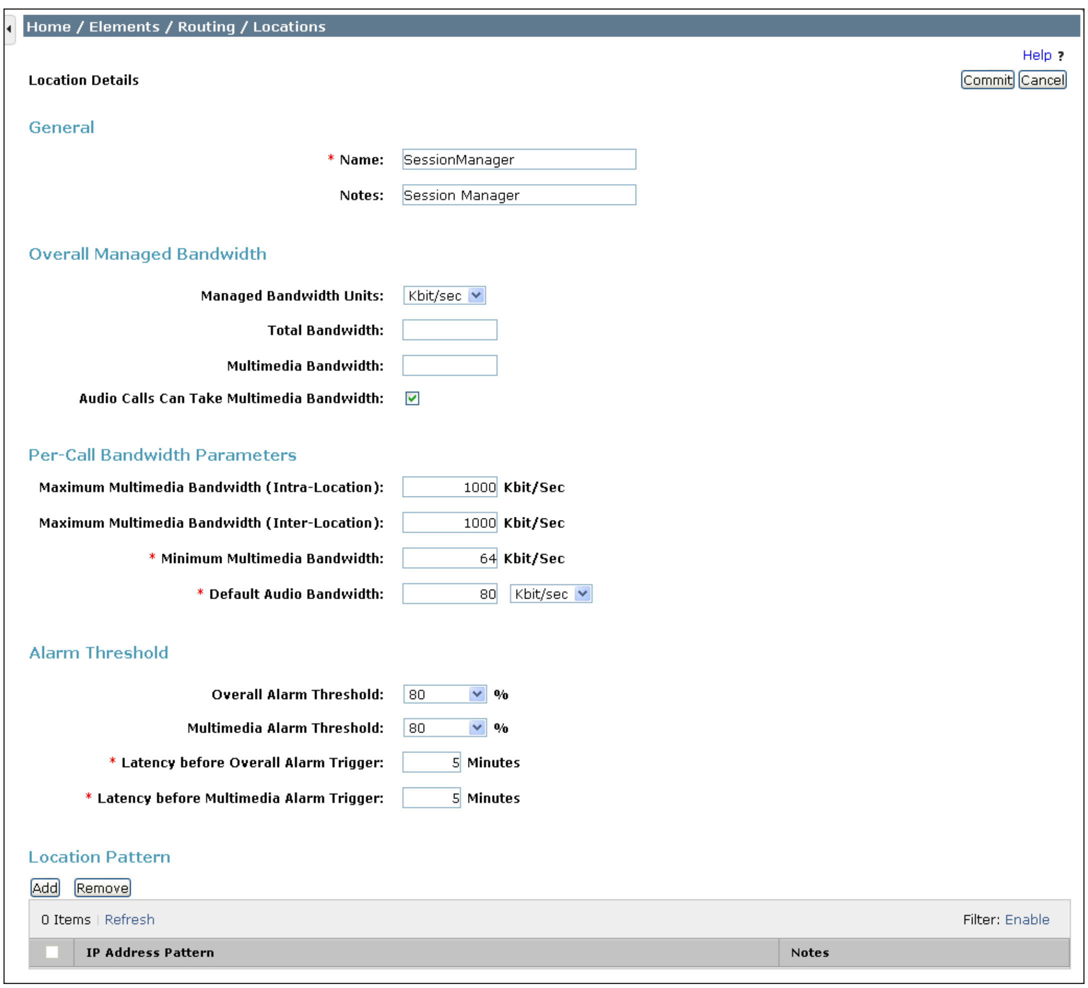
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

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

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

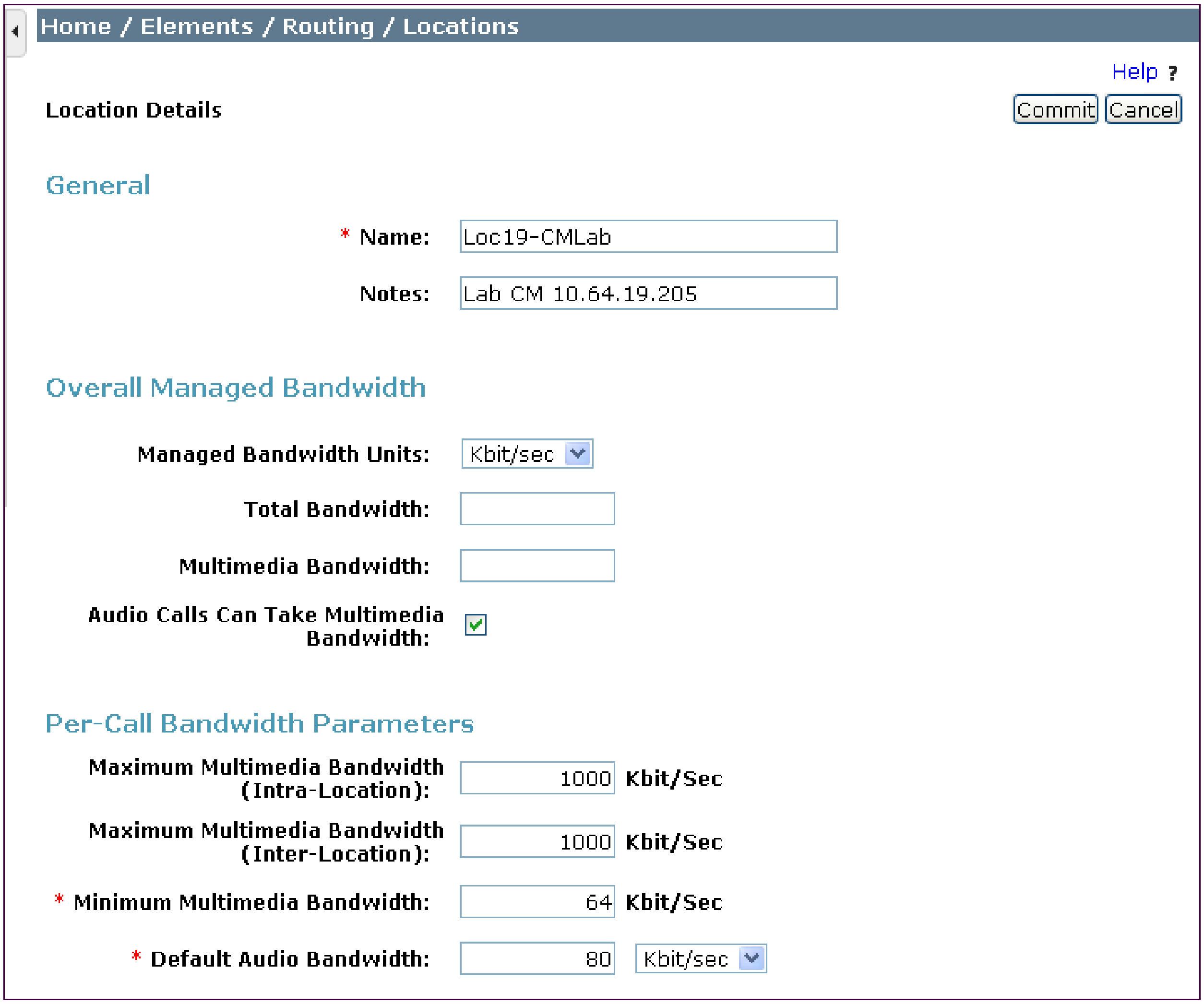
The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In this sample configuration Locations are added to SIP Entities (**Section 6.5**), so it was not necessary to add a pattern.

The following screen shows the addition of **SessionManager**, this location will be used for Session Manager. Click **Commit** to save.

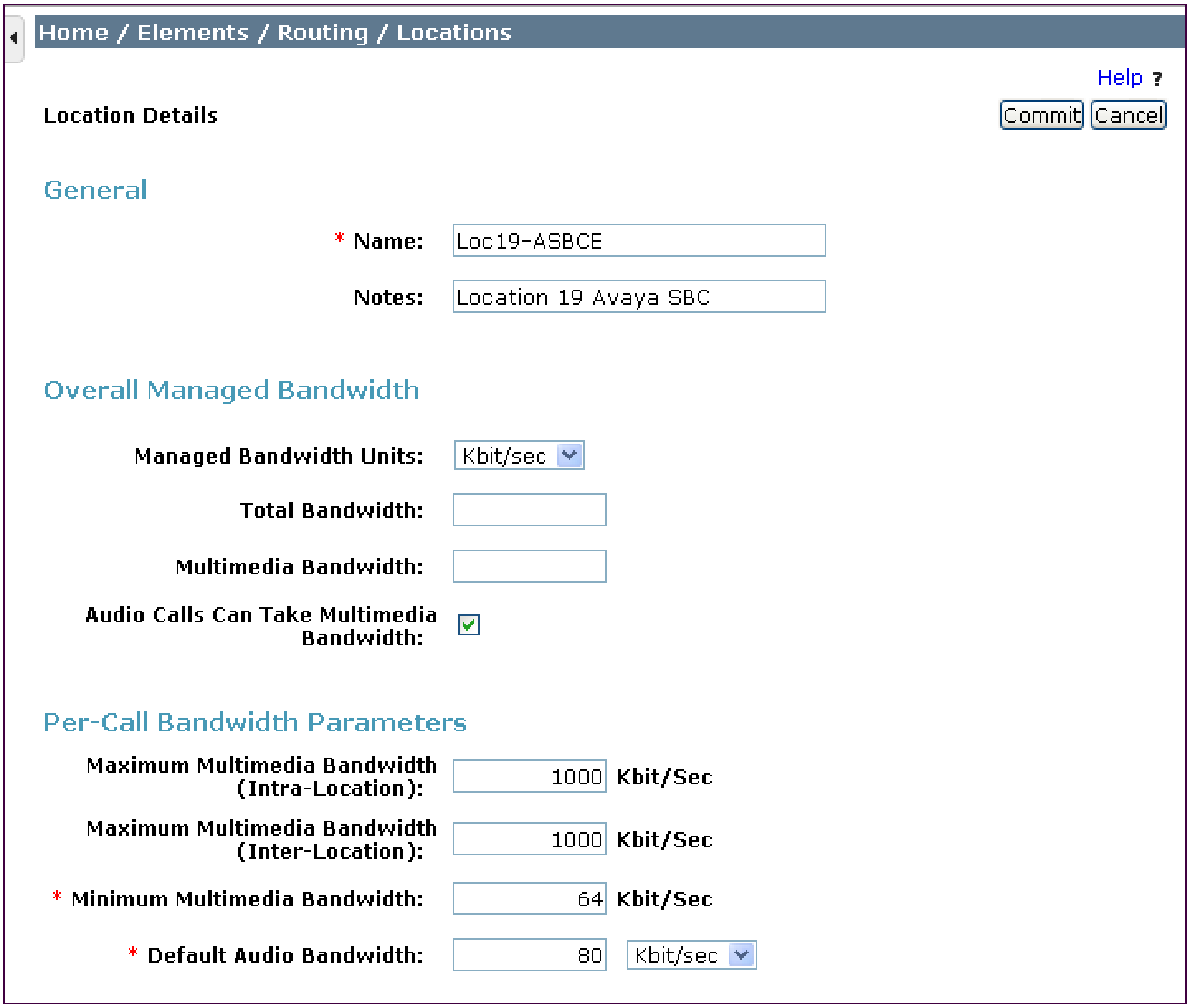


Note: Call bandwidth management parameters should be set per customer requirement.

Repeat the preceding procedure to create a separate Location for Communication Manager and Avaya SBCE. Displayed below is the screen for **Loc19-CMLab** used for Communication Manager.



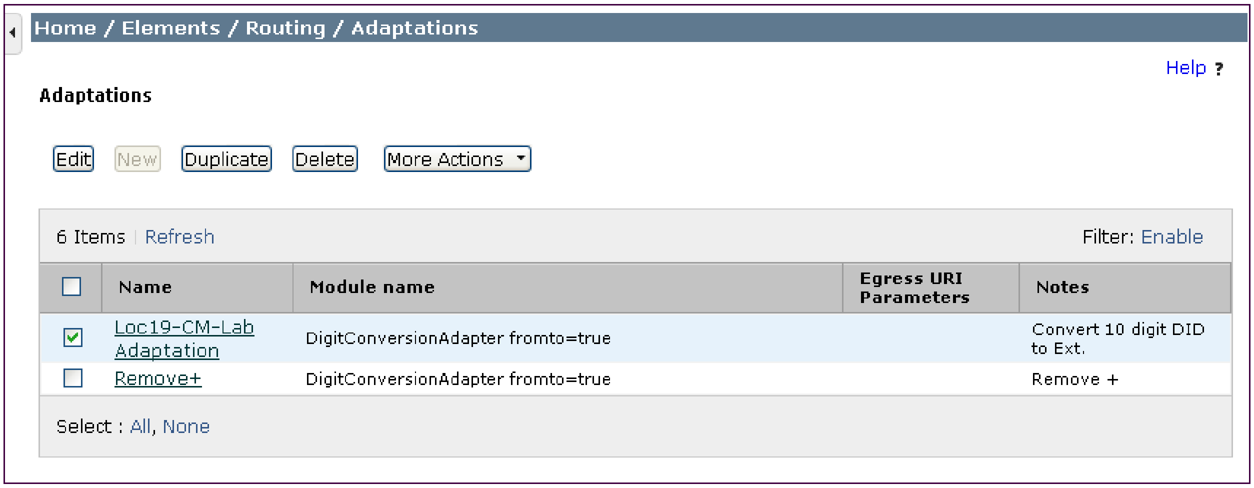
Below is the screen for **Loc19-ASBCE** used for Avaya SBCE.



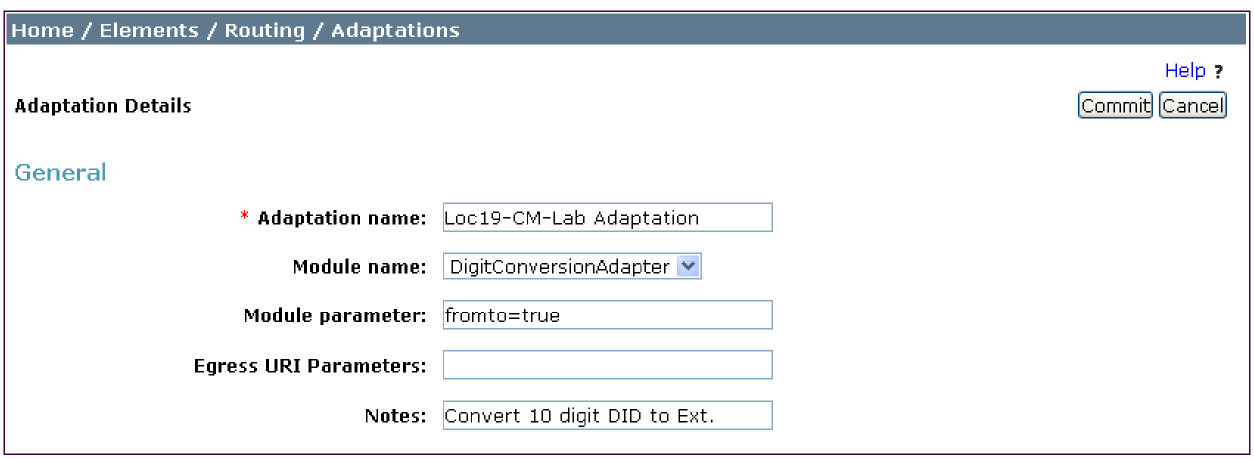
6.4. Adaptations

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed.

The following screen shows the adaptations that were available in the sample configuration.



The adapter named **Loc19-CM-Lab Adaptation** will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls involving Broadcore/Masergy SIP Trunking. This adaptation uses the **DigitConversionAdapter** to convert digits between Communication Manager and Broadcore/Masergy. The **Module parameter fromto=true** will include the FROM and TO headers in the digit conversion.



Scrolling down, the following screen shows a portion of the **Loc19-CM-Lab Adaptation** adapter that can be used to convert digits between the Communication Manager extension numbers (user extensions, VDNs) and the DID numbers assigned by Broadcore/Masergy.

An example portion of the settings for **Digit Conversion for Outgoing Calls from SM** (i.e., inbound to Communication Manager) is shown below. Both Session Manager digit conversion and Communication Manager incoming call handling treatment methods were created and tested successfully.

Digit Conversion for Outgoing Calls from SM

Add Remove

7 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
	* 4245556553	* 10	* 10		* 10	12000	both		
	* 4245556554	* 10	* 10		* 10	12001	both		
	* 2135552009	* 10	* 10		* 10	12004	both		
	* 2135554088	* 10	* 10		* 10	12005	both		
	* 3235557674	* 10	* 10		* 10	13000	both		
	* 2135559117	* 10	* 10		* 10	10000	both		
	* 4245553665	* 10	* 10		* 10	13004	both		

Select : All, None

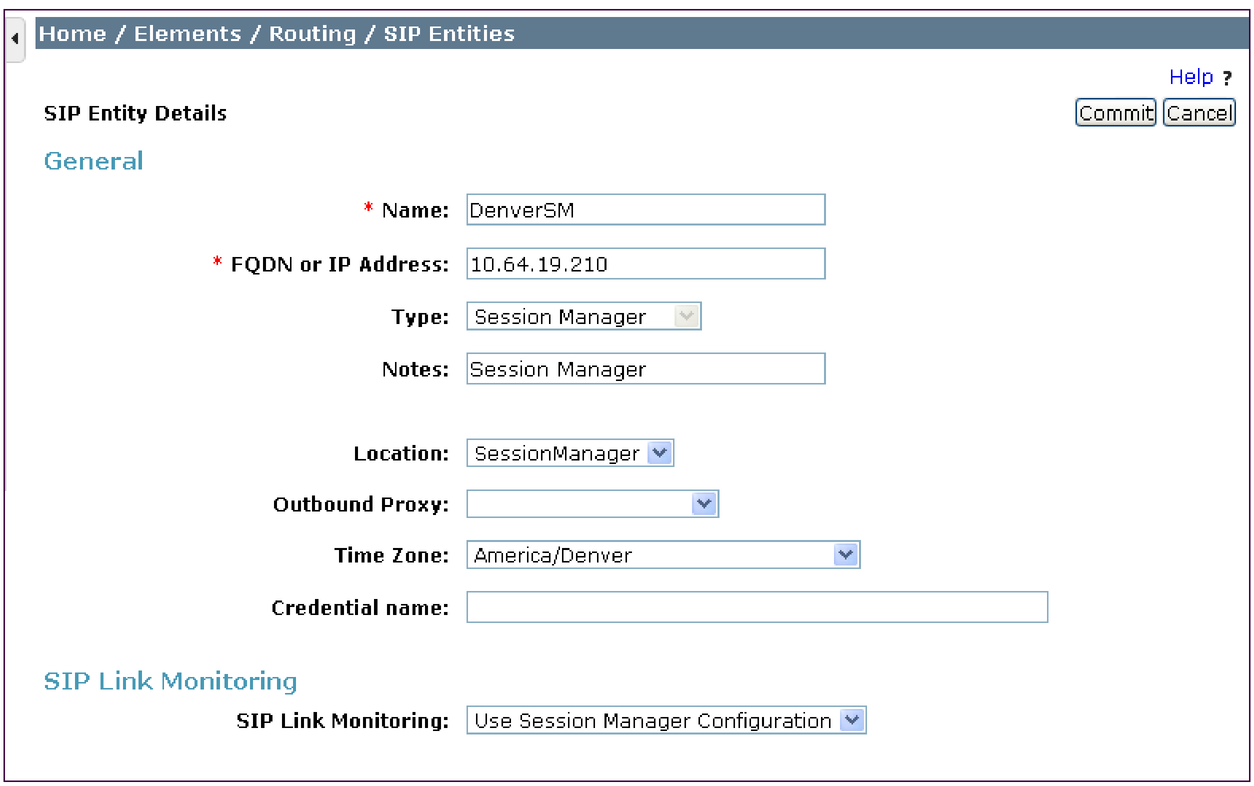
* Input Required Commit Cancel

6.5. Add SIP Entities

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

- **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** — Enter **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**. If applicable, select the **Adaptation Name** that will be applied to this entity
- **Location** — Select one of the locations defined previously
- **Time Zone** — Select the time zone for the location above

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



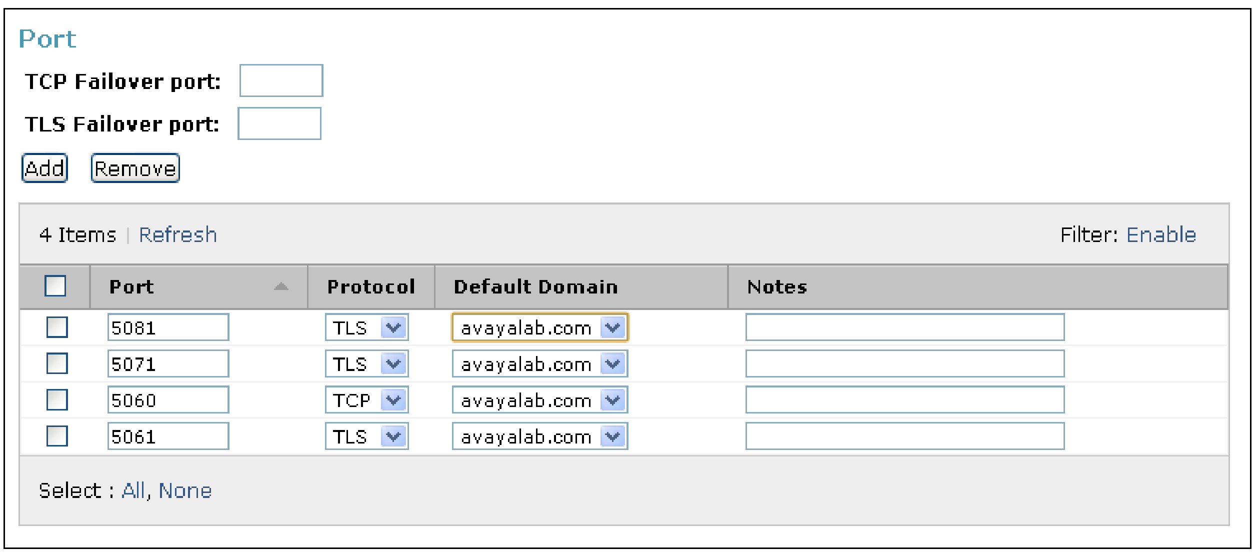
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.6**.

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

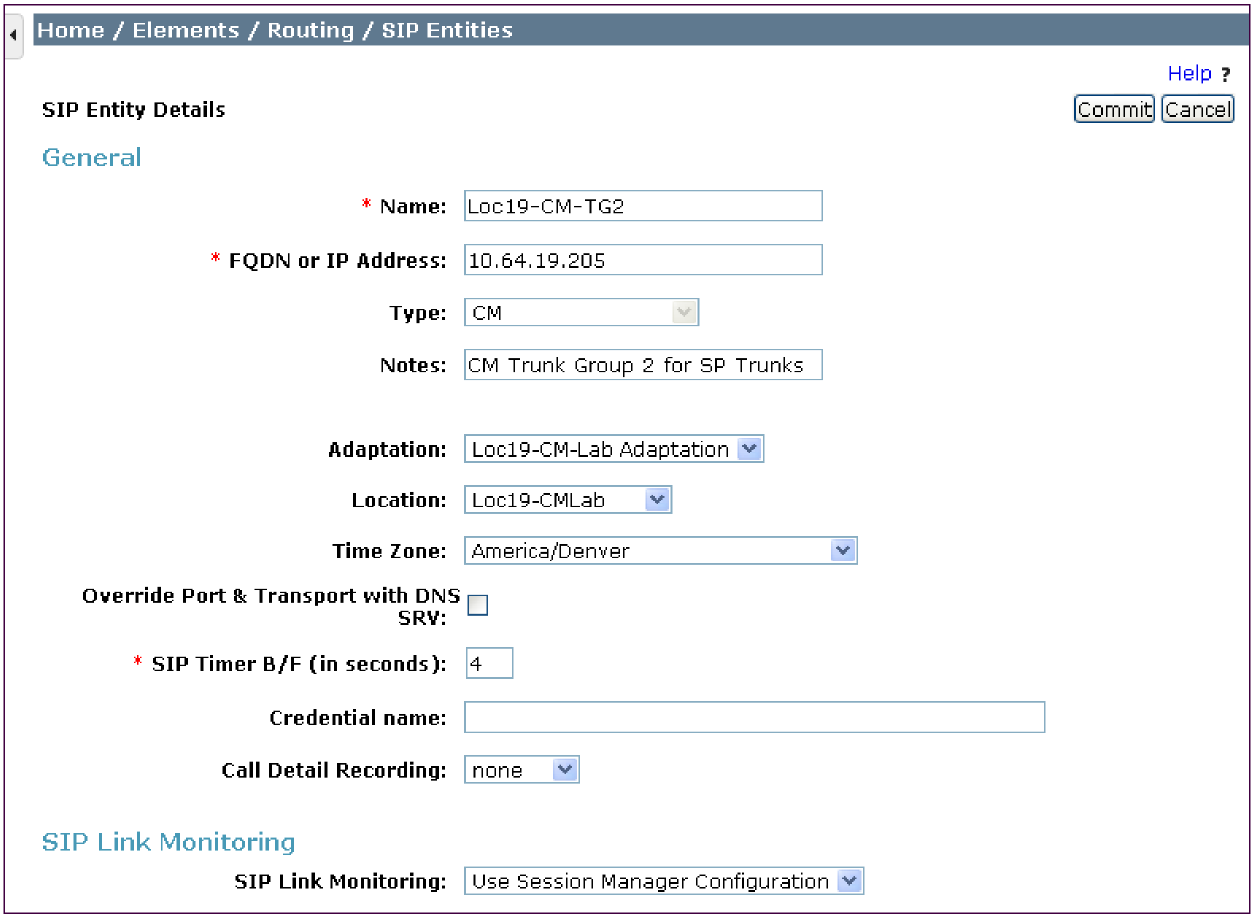
- **Port** Port number on which Session Manager can list for SIP Requests
- **Protocol** Transport protocol to be used to send SIP Requests
- **Default Domain** The domain used for the enterprise

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

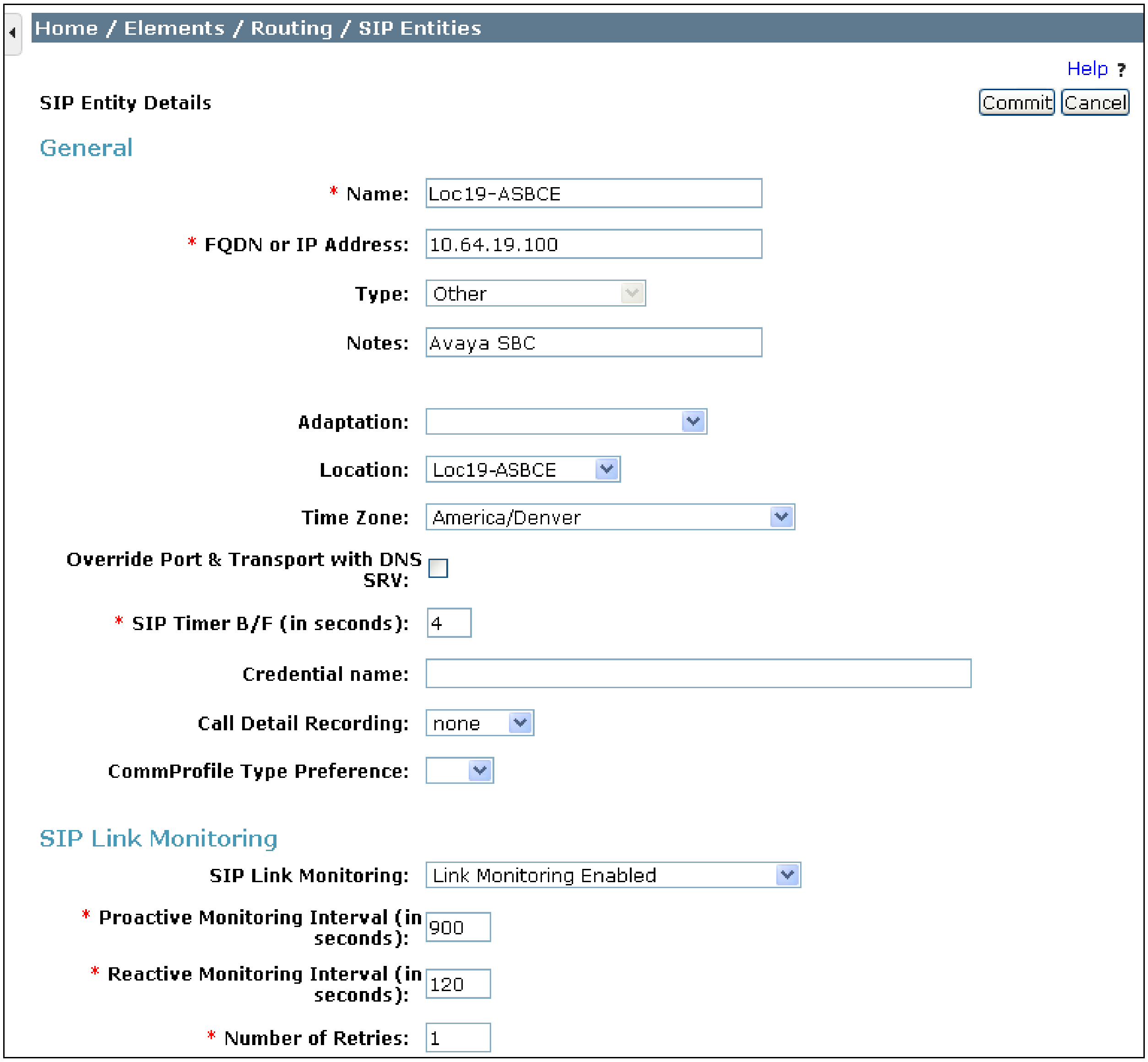
For the compliance test, four **Port** entries were added.



The following screen shows the addition of Communication Manager. The **FQDN or IP Address** field is set to the IP address defined in **Section 5.3** of the procr interface on Communication Manager. The **Adaptation** field is set to the Adaptation created in **Section 6.4** and the Location is set to the one defined for Communication Manager in **Section 6.3**.



The following screen shows the addition of Avaya SBCE SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The Location is set to the one defined for Avaya SBCE in **Section 6.3**. **Link Monitoring Enabled** was selected for **SIP Link Monitoring** using the specific time settings for **Proactive Monitoring Interval (in seconds)** and **Reactive Monitoring Interval (in seconds)** for the compliance test. These time settings should be adjusted or left at their default values per customer needs and requirements.



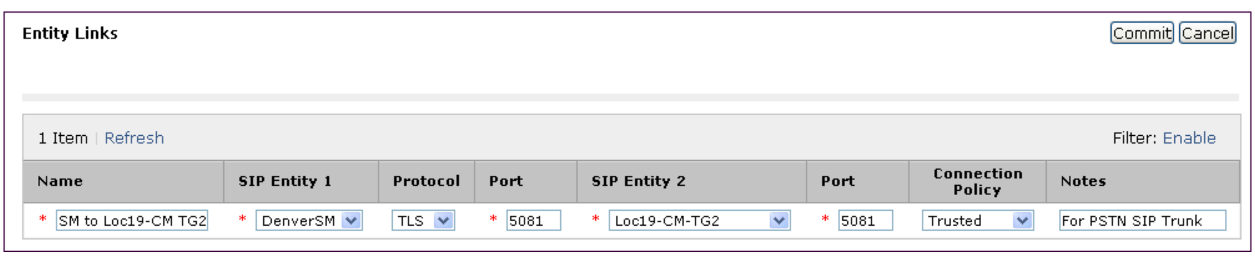
6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described as an Entity Link. Two Entity Links were created; one to Communication Manager for use only by service provider traffic and one to Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

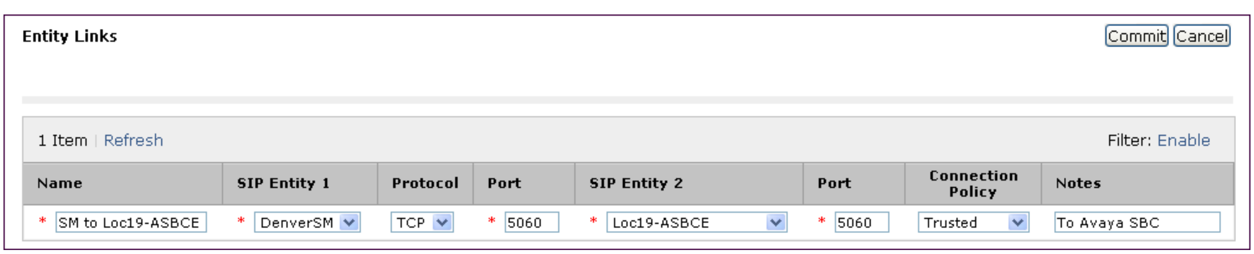
- **Name** — Enter a descriptive name
- **SIP Entity 1** — Select the SIP Entity for Session Manager
- **Protocol** — Select the transport protocol used for this link
- **Port** — Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**
- **SIP Entity 2** — Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.5**.
- **Port** — Port number on which the other system receives SIP requests from the Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**
- **Trusted** — Check this box. **Note**: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied.

Click **Commit** to save. The following screens illustrate the Entity Links to Communication Manager and Avaya SBCE.

Entity Link to Communication Manager:



Entity Link to Avaya SBCE:



6.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added; one for Communication Manager and one for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The screen below is displayed. Fill in the following:

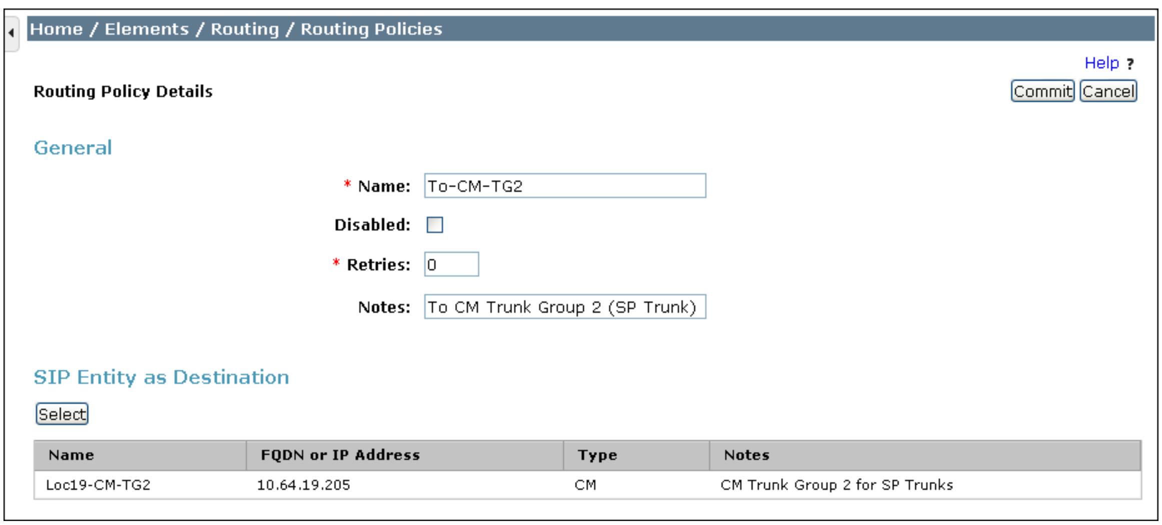
In the **General** section, enter the following values. Use default values for all remaining fields:

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

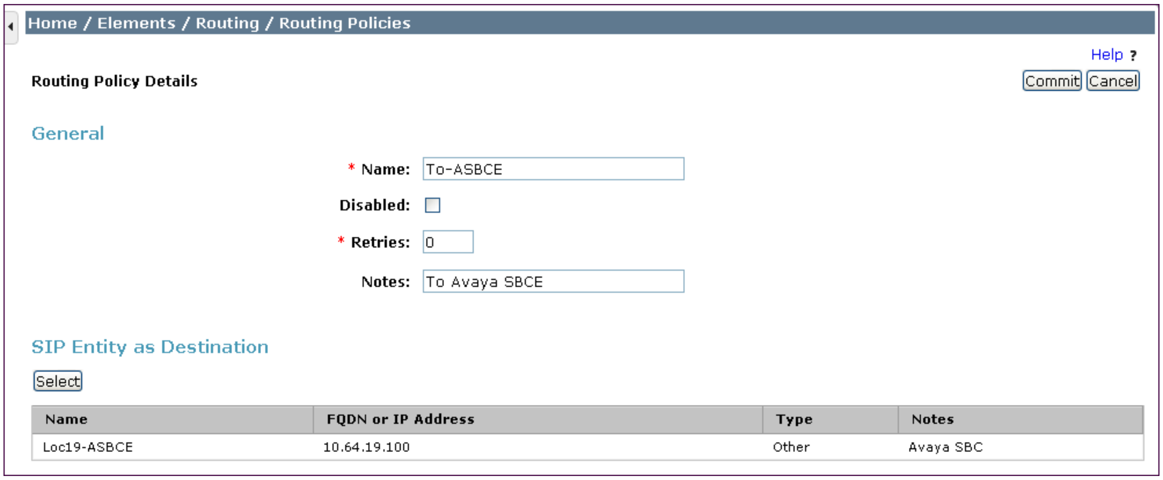
In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select** (not shown)**.** The selected SIP Entity displays on the **Routing Policy Details** page as shown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

The following screens show the Routing Policies for Communication Manager and Avaya SBCE.

Routing Policy for Communication Manger:



Routing Policy for Avaya SBCE:



6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were created to route calls from Communication Manager to Broadcore/Masergy and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

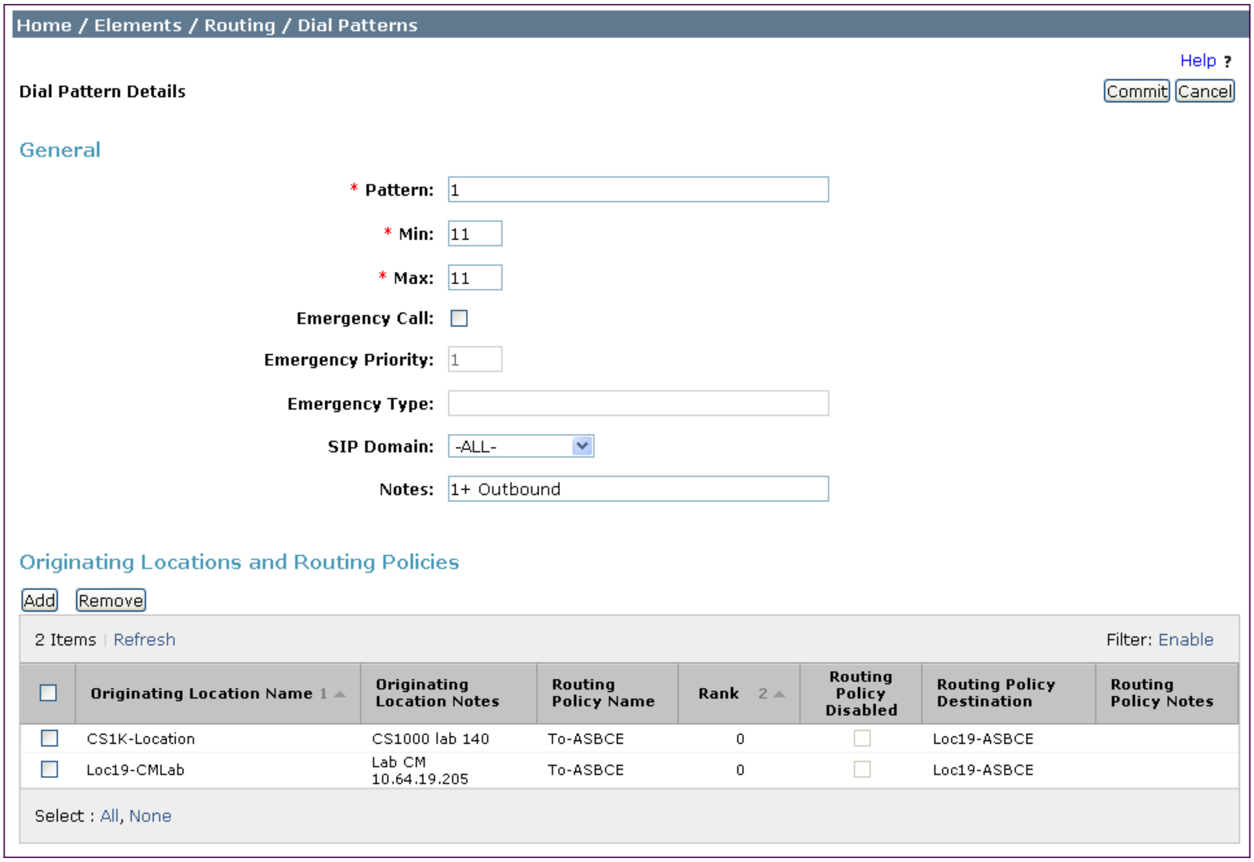
In the **General** section, enter the following values. Use default values for all remaining fields:

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

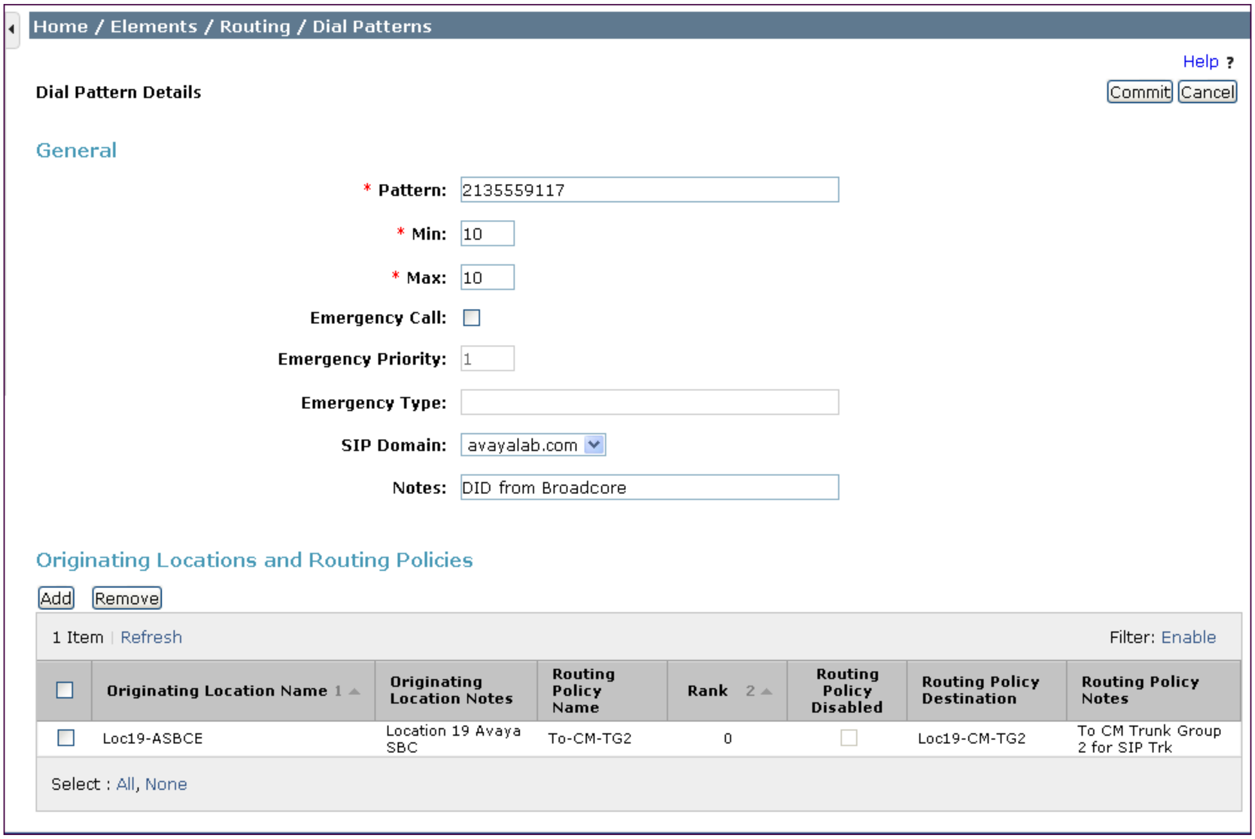
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used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

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

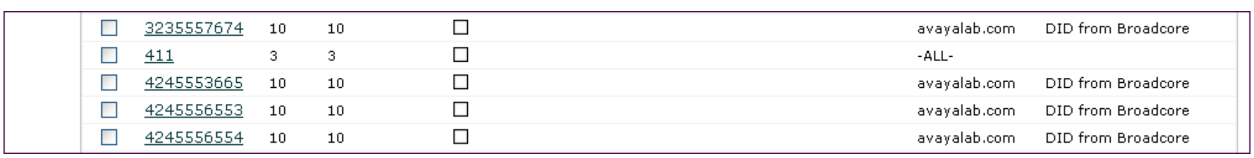
Two examples of the dial patterns used for the compliance test are shown below. The first example shows that that in the shared test environment, 11 digit dialed numbers that begin with **1** originating from **Loc19-CMLab** uses route policy **To-ASBCE**.



The second example shows that a **10** digit number **2135559117** and originating from **Loc19-ASBCE** uses route policy **To-CM-TG2**. This is a DID number assigned to the enterprise from Broadcore/Masergy.



The following show a subset of DID entries added to Session Manager.



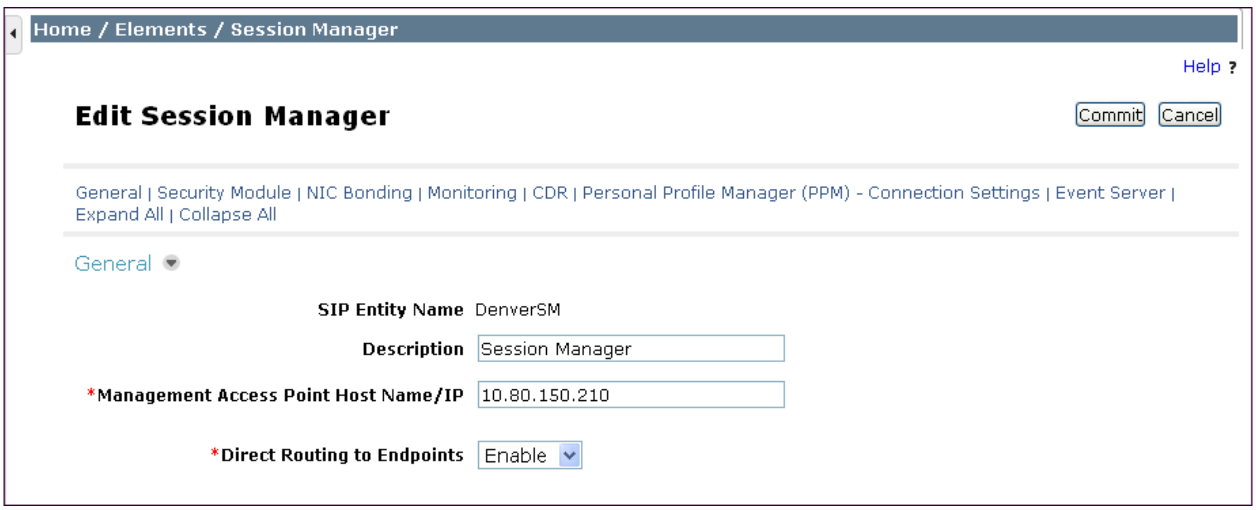
6.9. Add/Verify Avaya Aura® Session Manager Instance

The creation of a Session Manager Instance provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager instance already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the screen below:

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

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

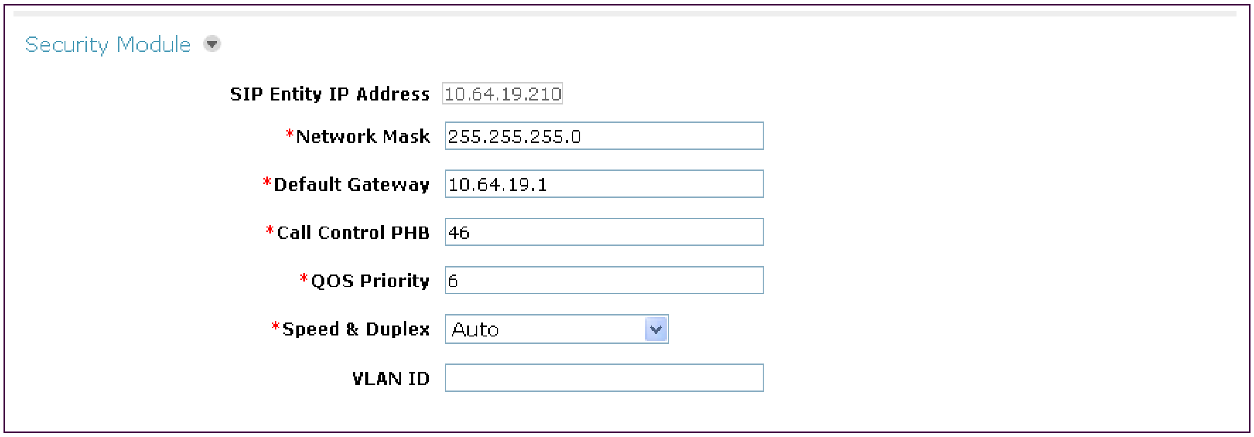
The screen below shows the Session Manager values used for the compliance test.



In the **Security Module** section, enter or verify the following values:

- **SIP Entity IP Address**: Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager.

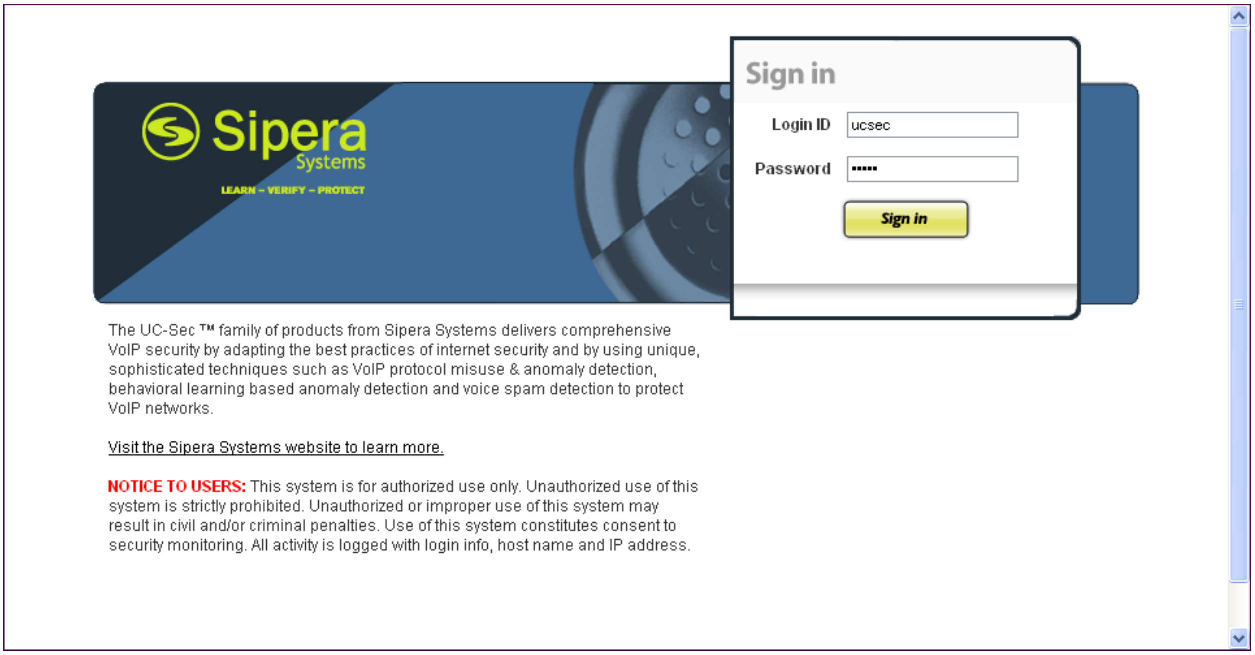
Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the remaining Session Manager values used for the compliance test.



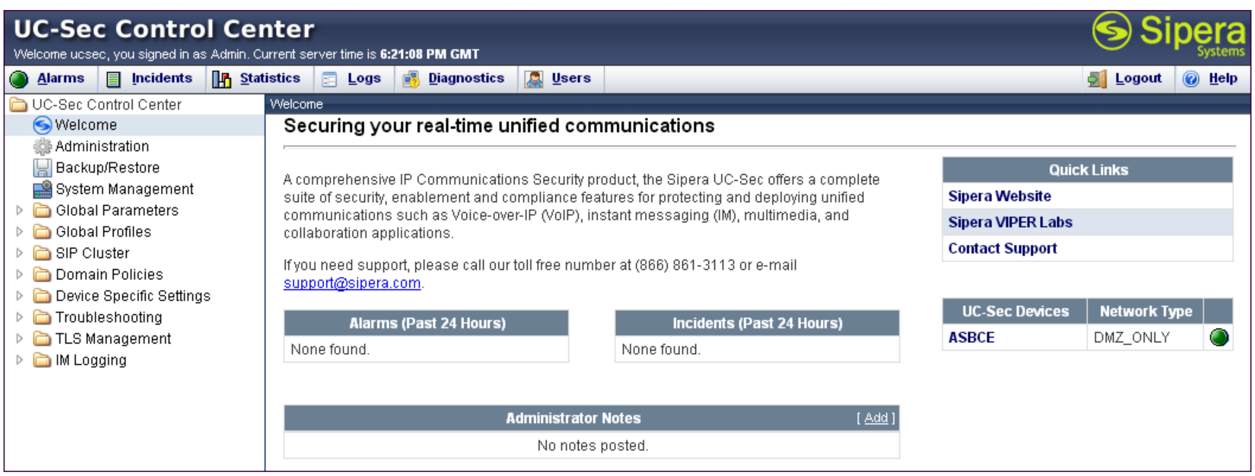
7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed.

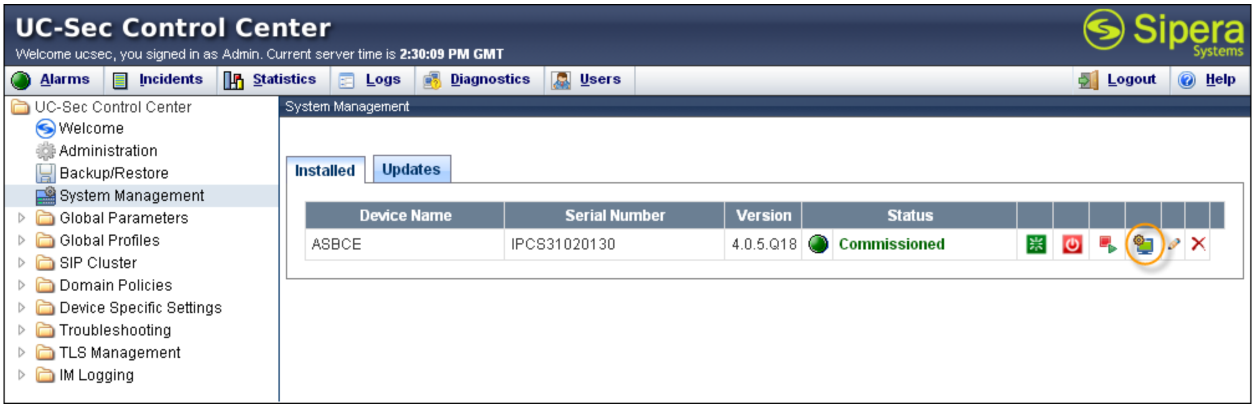
Log in with the appropriate credentials. Click **Sign In**.



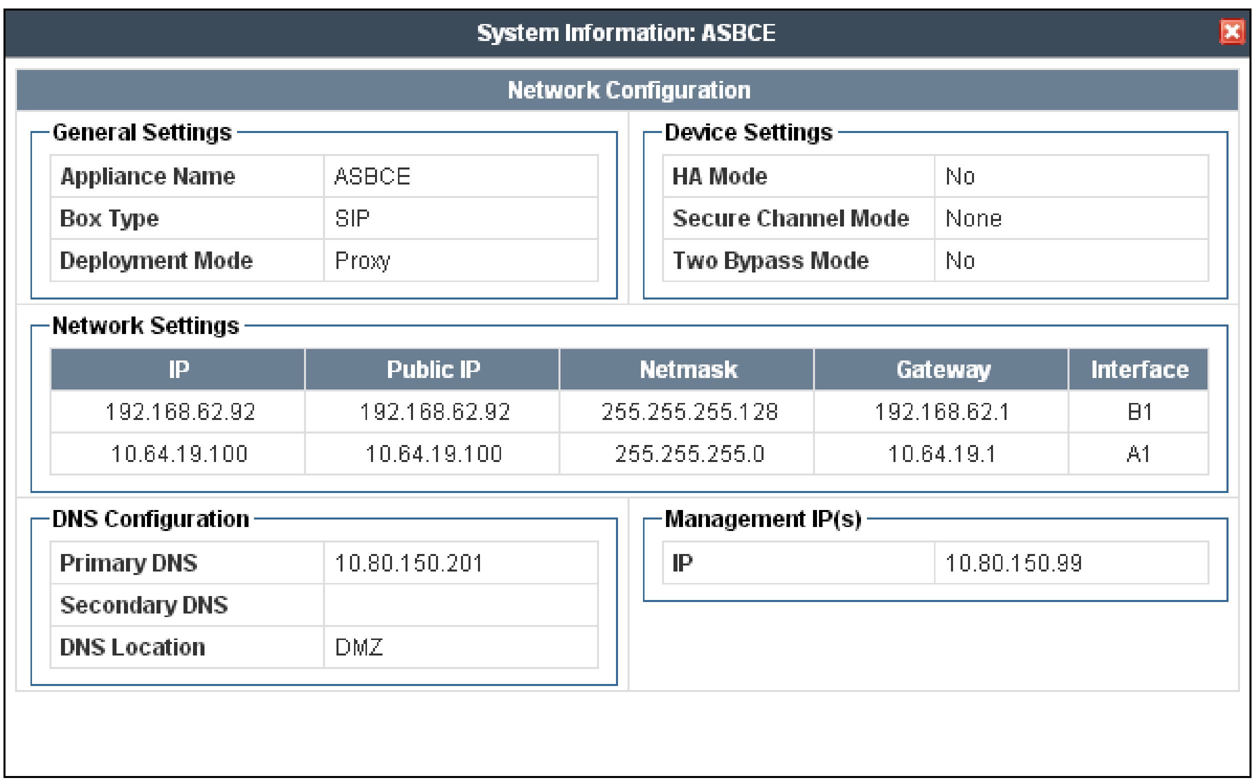
The main page of the UC-Sec Control Center will appear.



To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **ASBCE** is shown. To view the configuration of this device, click the monitor icon as highlighted below.

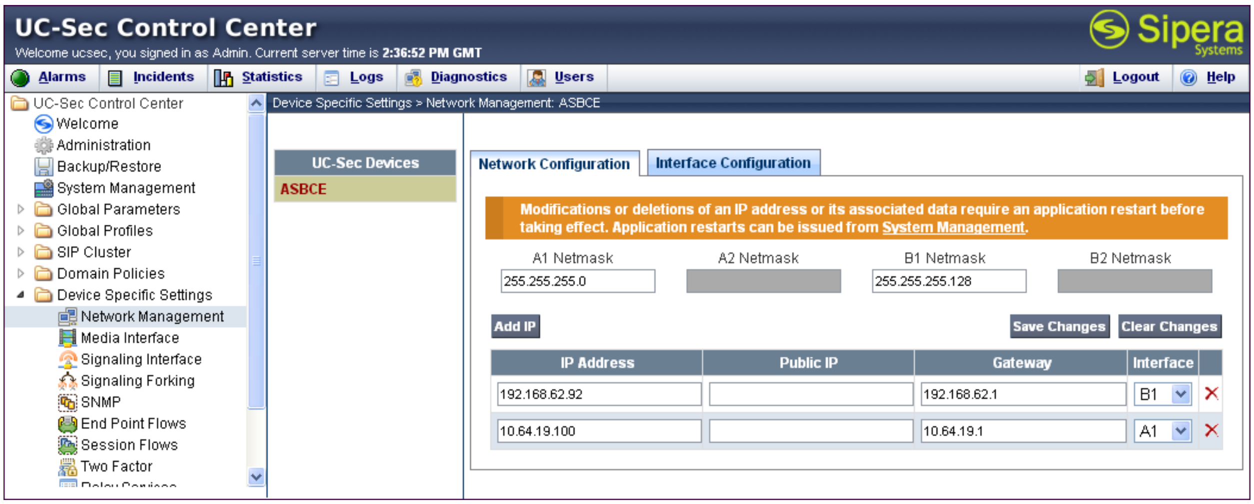


The **System Information** screen shows the **Network Settings, DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other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

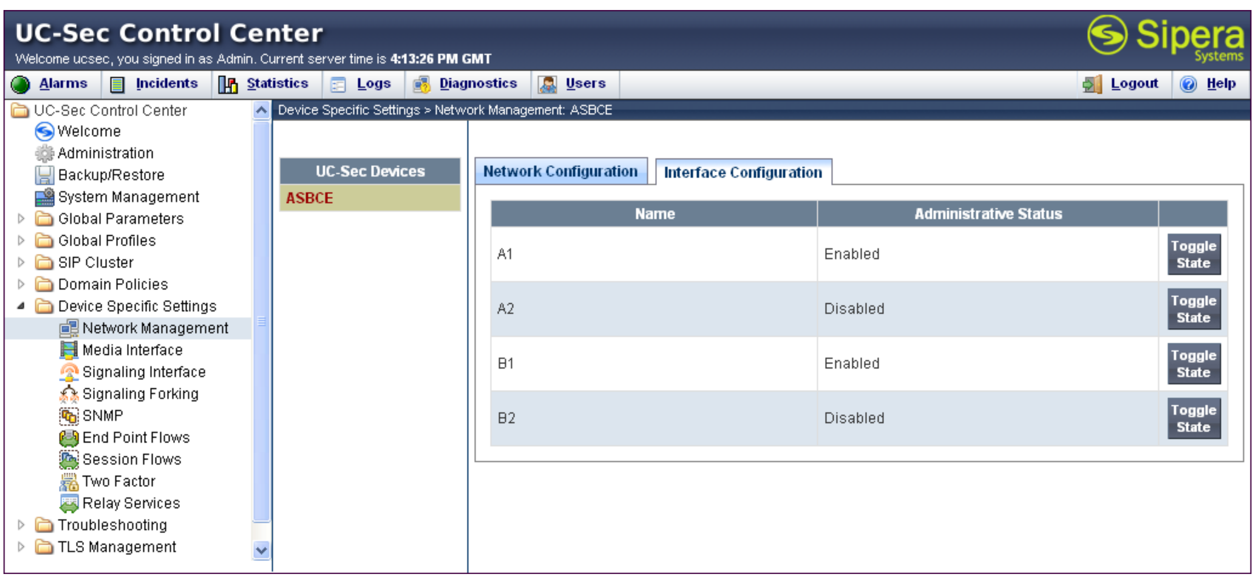


7.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the external interface is assigned to **B1**.



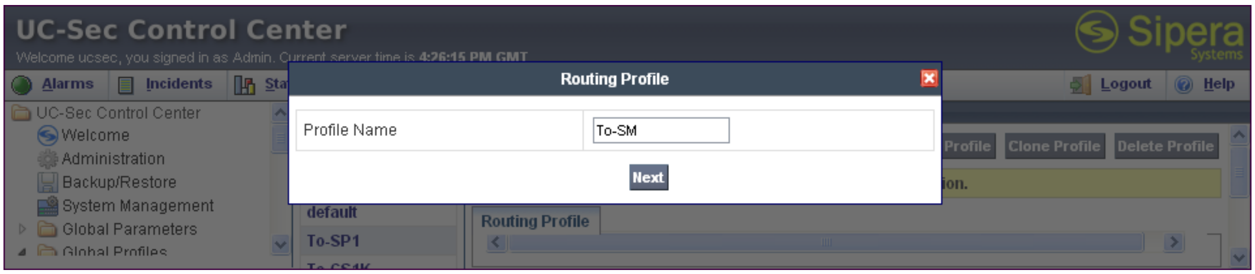
The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click its **Toggle State** button.



7.2. Routing Profile

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.

Create a Routing Profile for Session Manager and Broadcore/Masergy SIP Trunk Service. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.

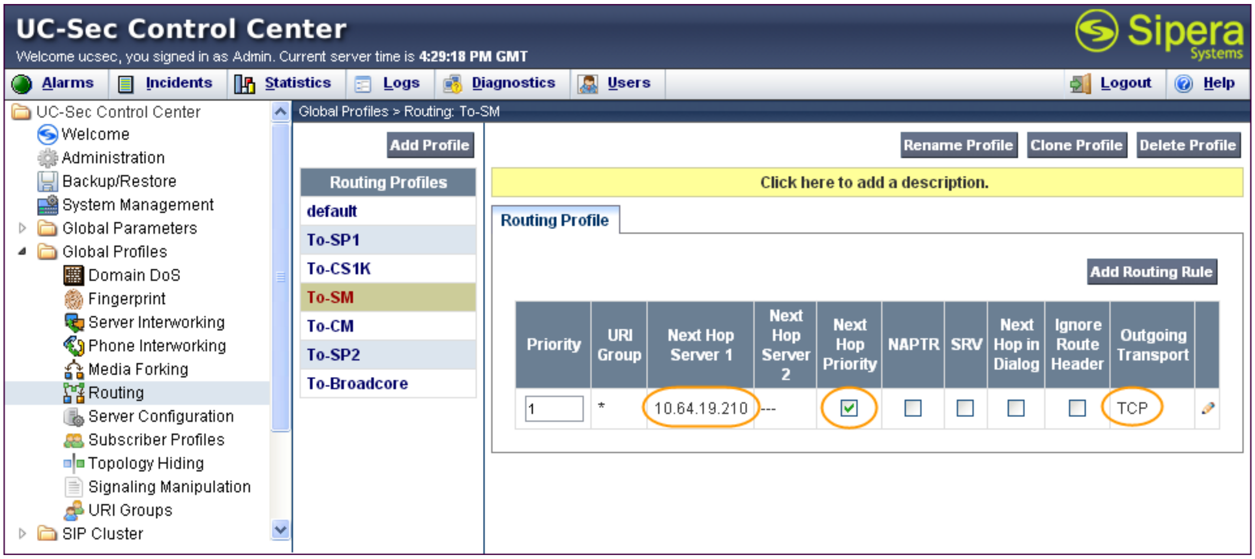


In the new window that appears (not shown), enter the following values. Use default values for all remaining fields:

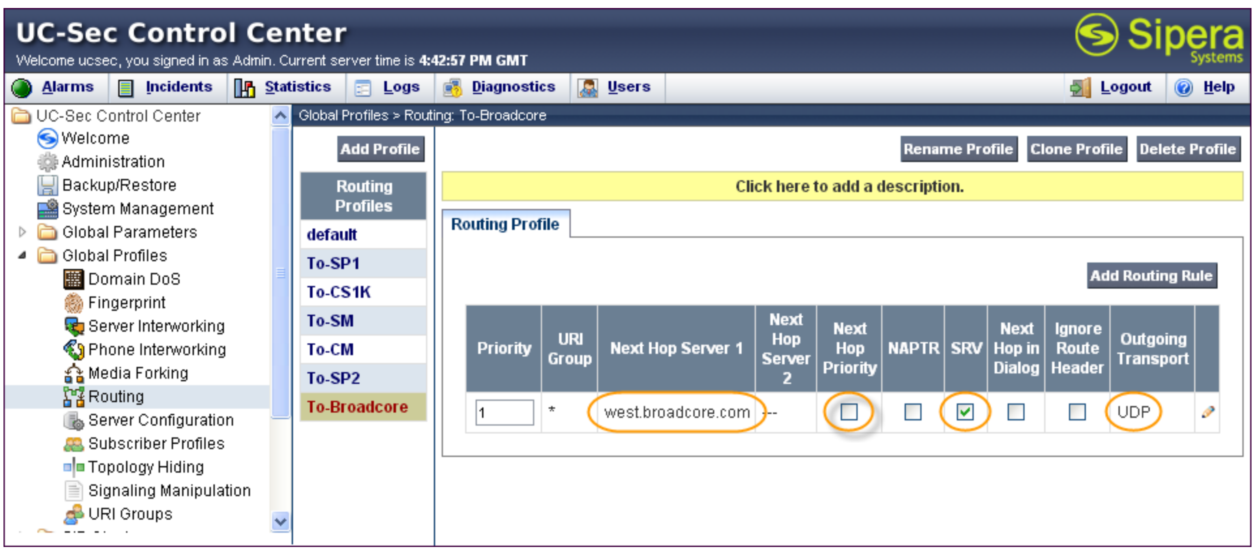
- **URI Group:** Select “*****” from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
- **Routing Priority Based on Next Hop Server**: Checked.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets.

Click **Finish**.

In the shared test environment the following screen shows Routing Profile **To-SM** created for Session Manager. The **Next Hop Server 1** IP address must match the IP address of Session Manager Entity created in **Section 6.5**. The **Outgoing Transport** is set to **TCP** and matched the **Protocol** set in the Session Manager Entity Link for Avaya SBCE in **Section 6.6**.



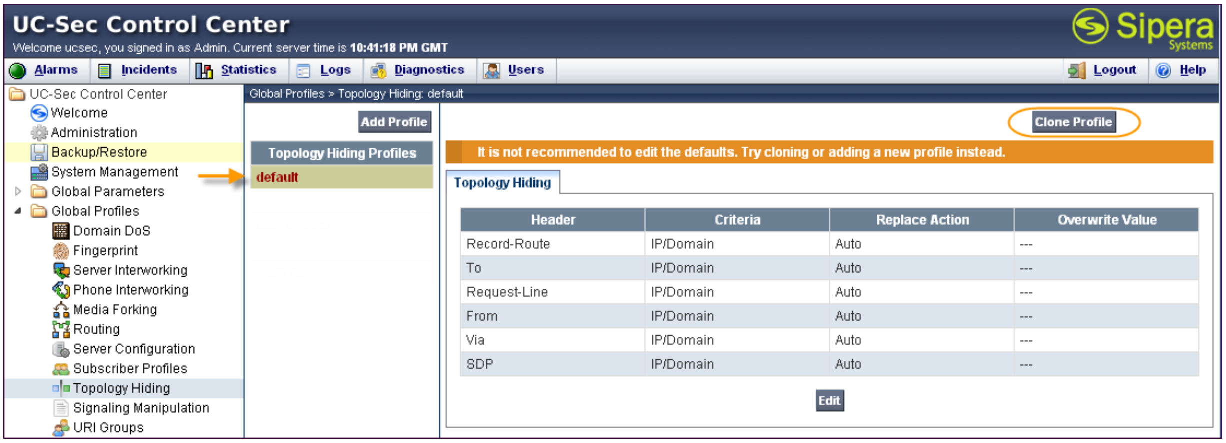
The following screen shows Routing Profile **To-Broadcore** created for Broadcore/Masergy. In the **Next Hop Server 1** field enter the Fully Qualified Domain Name that Broadcore/Masergy uses to listen for SIP traffic. In the sample configuration **west.broadcore.com** was used. Uncheck **Next Hop Priority** and select **SRV**. Enter **UDP** for the **Outgoing Transport field**.



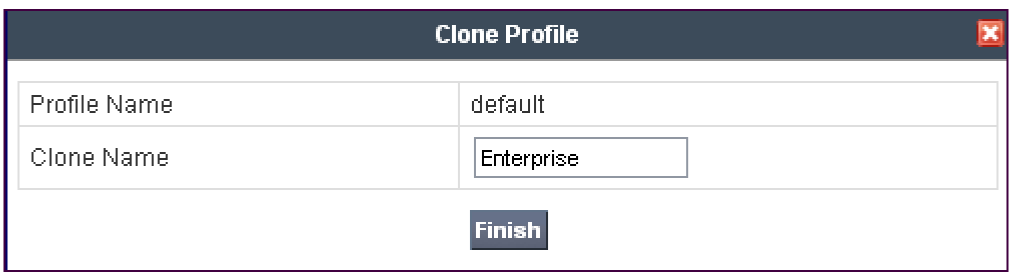
7.3. Topology Hiding Profile

The Topology Hiding profile manages 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.

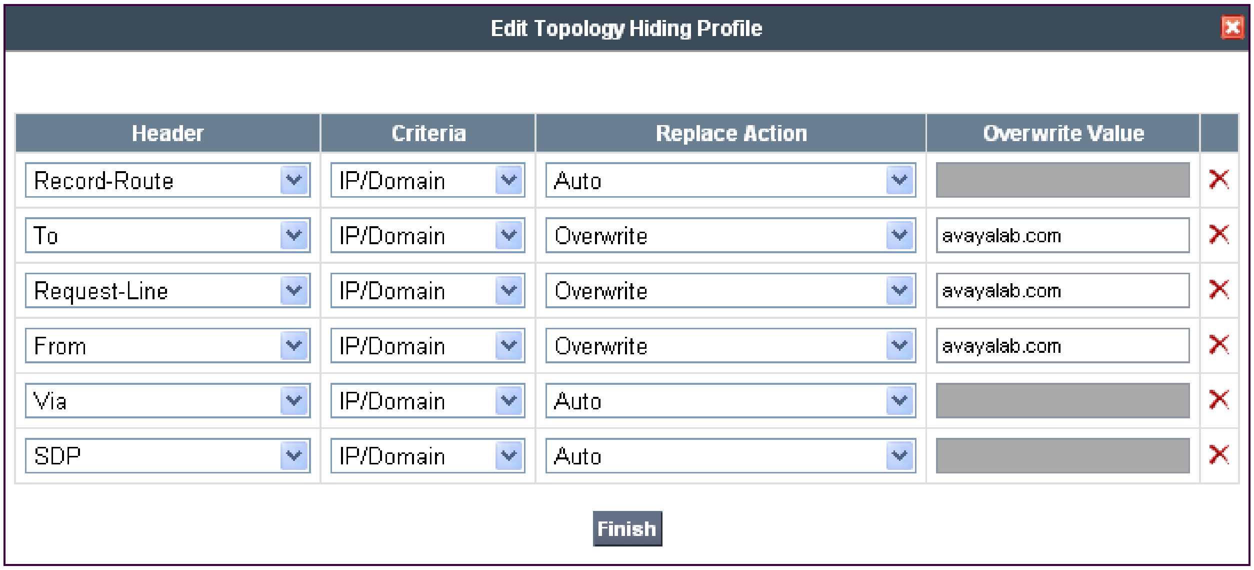
Create a Topology Hiding Profile for the enterprise and Broadcore/Masergy SIP Trunk Service. In the sample configuration, the **Enterprise** and **Broadcore Topology** profiles were cloned from the default profile. To clone a default profile, navigate to **UC-Sec Control Center → Global Profiles → Topology Hiding**. Select the **default** profile and click on **Clone Profile** as shown below.



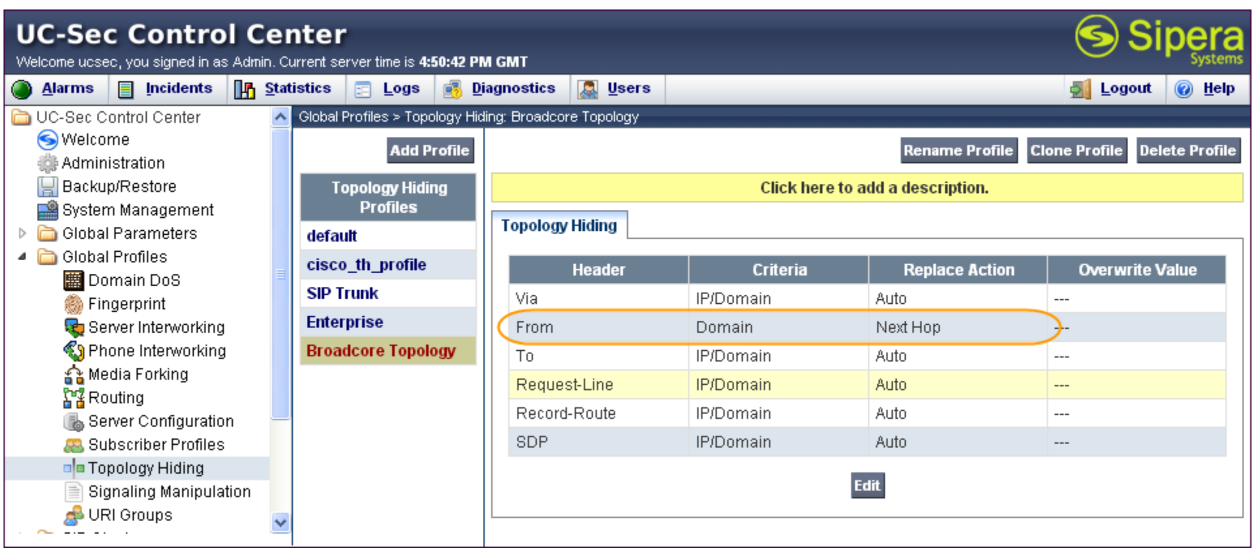
Enter a descriptive name for the new profile and click **Finish**.



Edit the **Enterprise** profile to overwrite the headers shown below to the enterprise domain. The **Overwrite Value** should match the Domain set in Session Manager (**Section 6.2**). Click **Finish** to save the changes.



Use the same procedure to clone the default profile for Broadcore/Masergy. Edit the profile to change the **FROM** header's **Criteria** to **Domain** and **Replace Action** to **Next Hop** as shown below.



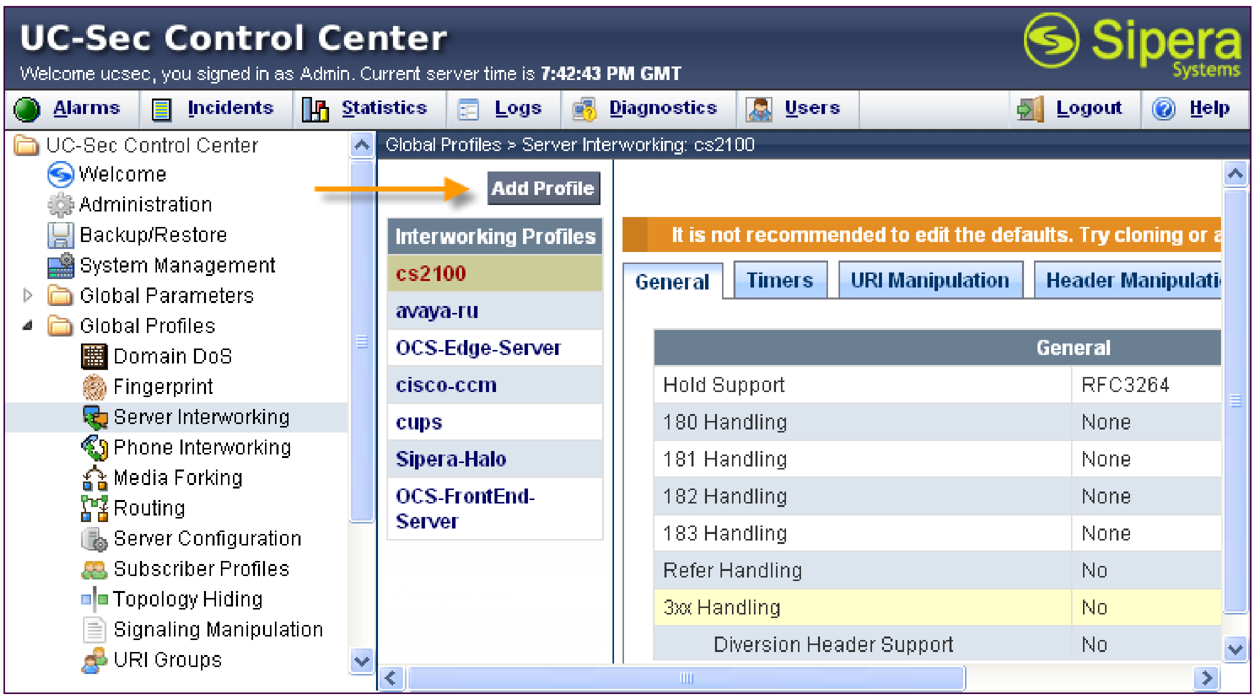
7.4. Server Interworking Profile

The Server Internetworking profile configures and manages various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters (for HA deployments), DoS security statistics, and trusted domains. Interworking Profile features are configured based on different Trunk Servers. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

In the sample configuration, separate Server Interworking Profiles were created for Enterprise and Broadcore/Masergy.

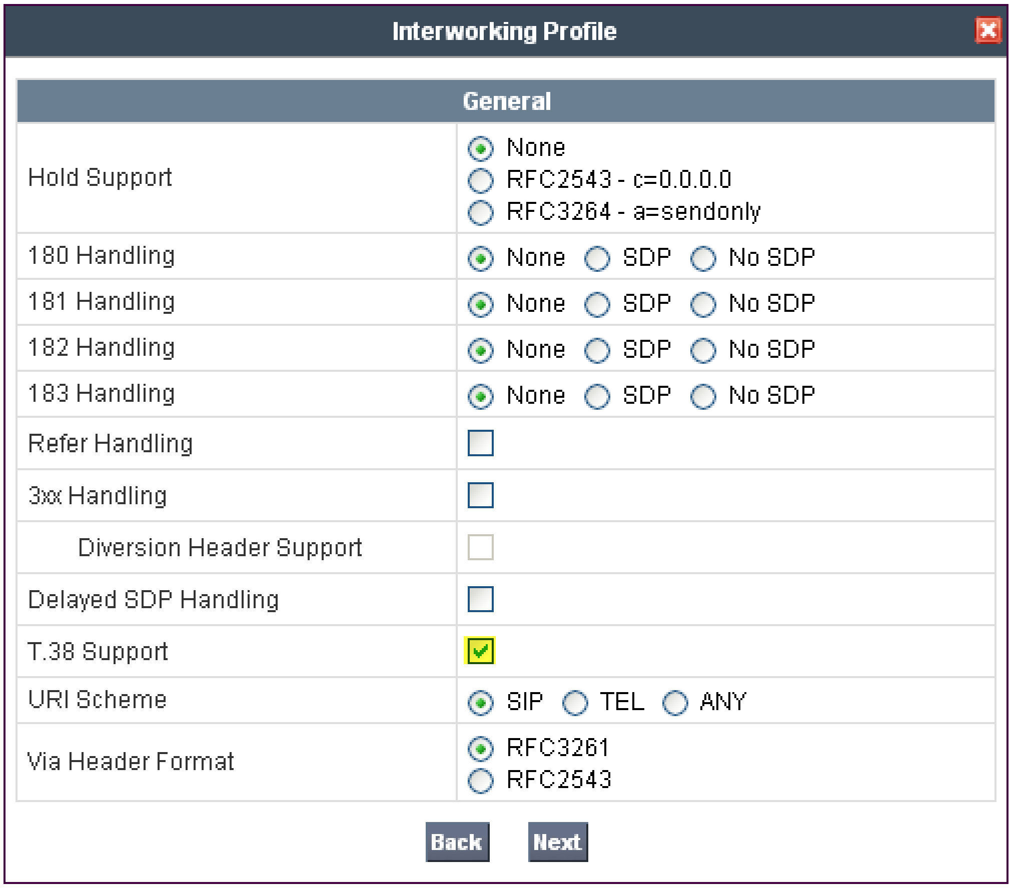
7.4.1. Server Interworking Profile – Enterprise

To create a new Server Interworking Profile for the enterprise, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking** and click on **Add Profile** as shown below.

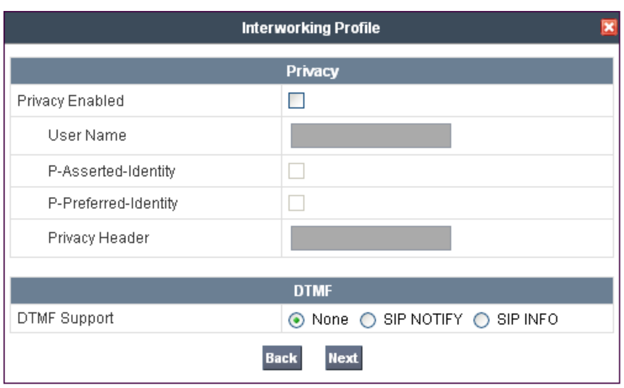


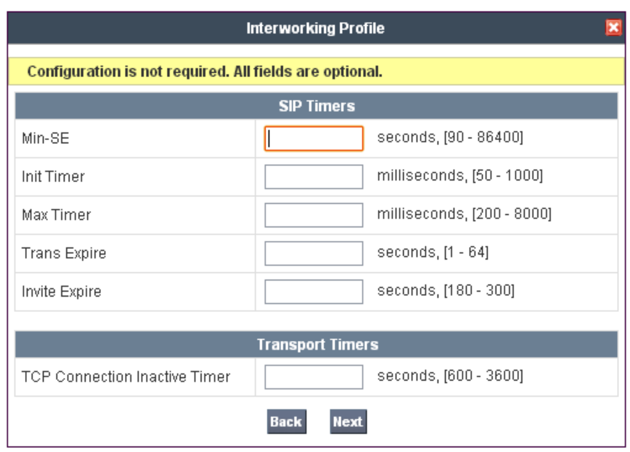
Enter a descriptive name for the new profile and click **Next** to continue.

In the new window that appears, check the **T.38 Support** field. Use default values for all remaining fields. Click **Next** to continue.



Default values can be used for the next two windows that appear. Click **Next** to continue.

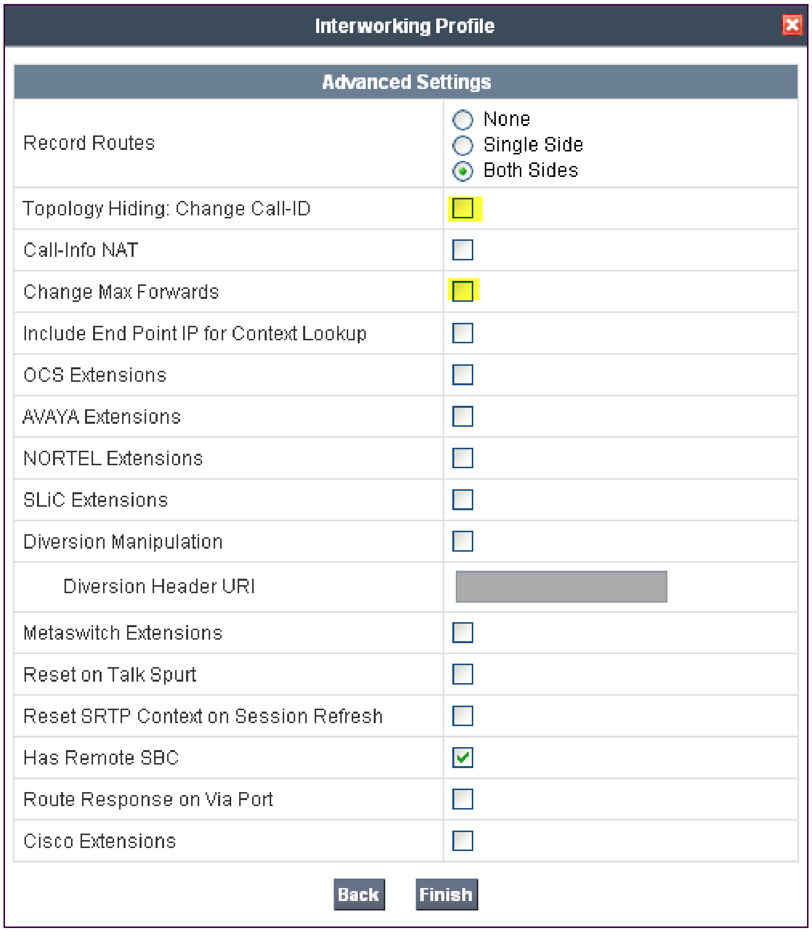




On the **Advanced Settings** window uncheck the following default settings:

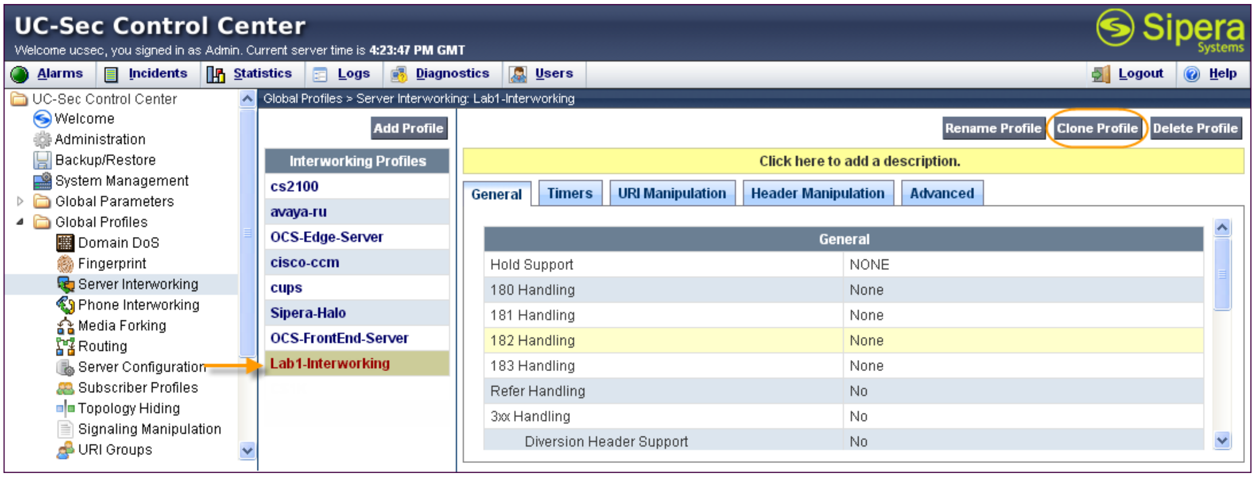
- **Topology Hiding: Change Call-ID**
- **Change Max Forwards**

Click **Finish** to save changes.

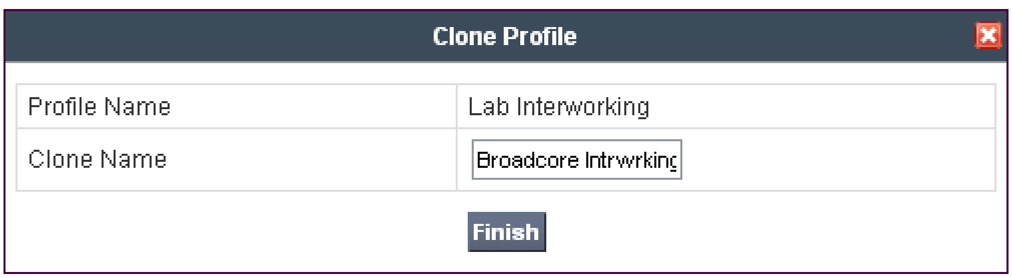


7.4.2. Server Interworking Profile – Broadcore/Masergy

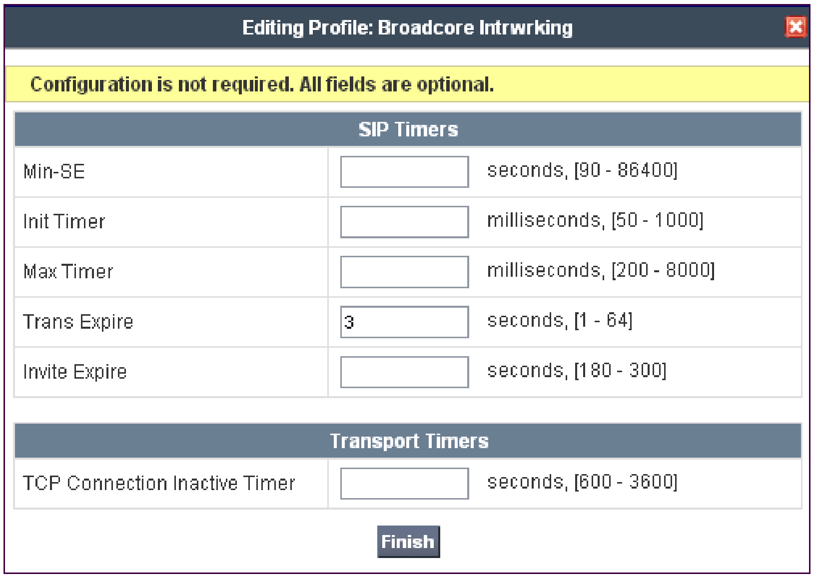
The Broadcore/Masergy profile will be created by cloning the Enterprise profile created in the previous section. To clone a Server Interworking Profile for Broadcore/Masergy, navigate to **UC-Sec Control Center →Global Profiles → Server Interworking** and click on the previously created profile for the enterprise, then click on **Clone Profile** as shown below.



Enter a descriptive name for the new profile and click **Finish** to save the profile.



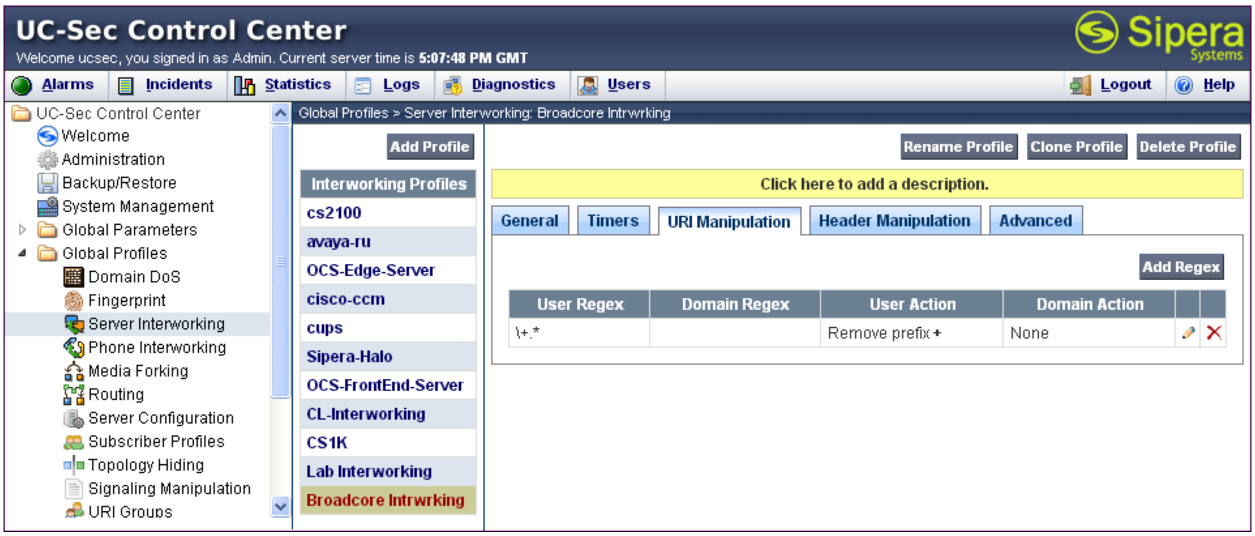
Select the **Timers** tab and click the **Edit** button (not shown). The Edit Profile screen is presented. Enter a value in the **Trans Expire** field to set the allotted time the Avaya SBCE will try the first primary server before trying the secondary server. Click **Finish** to save the changes.



Beginning with Communication Manager 6.0 public numbers are automatically preceded with a + sign (E.164 numbering format). Broadcore/Masergy does not support the E.164 numbering format, therefore the + sign must be removed. Create a URI Manipulation to remove the + sign Communication Manager places in the FROM, CONTACT, and P-Asserted Identity headers.

Within the **Broadcore Intrwrking** Profile, select the **URI Manipulation** tab and click the **Add Regex** button. The Add Regex screen is presented (not shown). In the **User Regex** field, enter a regular expression to match. In the sample configuration "**\+.***" was entered. In this expression the backslash is used to escape the special meaning of "**+**" in a regular expression. The expression "**.***" will match anything after the plus sign. In the **User Action** field, select **Remove prefix [Value]** from the drop-down box. In the **User Values** field enter "**+**". Click **Finish** to save the configuration.

The following screen shows the completed URI Manipulation for Broadcore/Masergy.



7.5. Signaling Manipulation

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

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE. Using this language, a script can be written and tied to a given flow through the Avaya SBCE GUI. The Avaya SBCE appliance then interprets this script at the given entry point or "hook point".

These application notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing. The sample script was used to change the FROM user to the pilot number for outbound calls in order to be authenticated on the Broadcore/Masergy network. It also removes the "epv" parameter Session Manager places in the CONTACT header that contains Endpoint-View information, including the internal domain. For inbound calls the script was used to change the SIP trunk pilot number presented in the Request URI to the number in the TO header so calls can be routed properly through Communication Manger.

To create a new Signaling Manipulation, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script**. A new blank SigMa Editor window will pop up.

In this compliance testing, the script named **Broadcore Script** was created as shown below:

```
within session "ALL"
{
 act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
//Insert Pilot number in the FROM header
  %fromuser = %HEADERS["From"][1].URI.USER;
  %HEADERS["From"][1].URI.USER = "4245556553";

//OPTIONAL- Remove epv parameter from CONTACT header to hide domain
  remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);

//Remove "sendonly" attribute for Music on Hold
  if(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]="") then
   {
    remove(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]);
   }
  }
}
within session "ALL"
{
 act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {

//Replace Pilot number in "REQUEST-LINE" with "TO" number
  %HEADERS["Request_Line"][1].URI.USER = %HEADERS["To"][1].URI.USER;
  }
}

// Return FROM header to original form
within session "ALL"
{
 act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
  %HEADERS["From"][1].URI.USER = %fromuser;
  }
}
```

In the Signaling Manipulation script named **BroadcoreSingleRegScript** above, the statement **act on request where %DIRECTION="OUTBOUND" and%ENTRY_POINT="POST_ROUTING"** specifies the portion of the script that will take effect on request SIP messages for an outbound call and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

-SigMa rules to populate the Pilot DID in the From header. All calls must have the Pilot DID in the From header in order to be authenticated on the Broadcore/Masergy network. The original FROM user is saved as variable "%fromuser" so it can be converted back later on in the script. Then it is changed to the pilot number.

```
//Insert Pilot number in the FROM header
  %fromuser = %HEADERS["From"][1].URI.USER;
  %HEADERS["From"][1].URI.USER = "4245556553";
```

-SigMa rules to delete unnecessary header parameter. This is an optional statement that is used to prevent the internal domain from being propagated to Broadcore/Masergy to hide the enterprise topology.

```
//OPTIONAL- Remove epv parameter from CONTACT header to hide domain
  remove(%HEADERS["Contact"][1].URI.PARAMS["epv"])
```

-SigMa rules to delete the Sendonly attribute. This will remove the media attribute sent by Communication Manager when a call is placed on hold. The Broadcore/Masergy SIP Trunk Service will play its own music source when the "sendonly" media attribute is received. The "sendrecv" media attribute is assumed as the default for the session when no other attribute is sent. So rather than replacing "sendonly" with "sendrecv", the "sendonly" media attribute was simply removed. This allows internal music/message on hold to be played while the call is on hold.

```
//Remove "sendonly" attribute for Music on Hold
  if(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]="") then
   {
    remove(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]);
   }
  }
}
```

In the Signaling Manipulation script named **BroadcoreSingleRegScript** further above, the statement **act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"** specifies the portion of the script that will take effect on request SIP messages (i.e., initial INVITE) for an inbound call and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement.

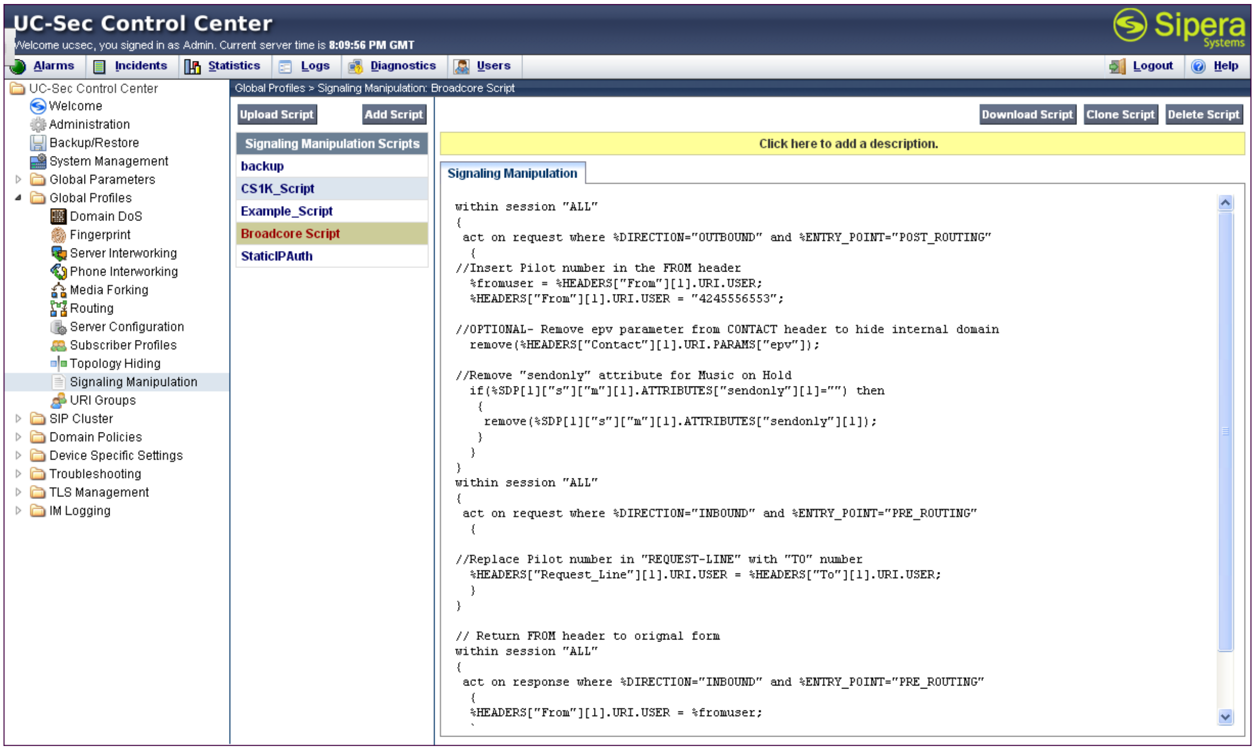
-SigMa rules to manipulate the calling number in Request URI header. For incoming calls the Request URI will always be the Pilot DID as defined by Broadcore/Masergy. The Pilot DID needs to be removed and the actual called number should be populated in its place. The called number is populated in the To header. The statement below will copy the To URI User into the Request URI header so the call can be properly processed by the Avaya network.

```
within session "ALL"
{
 act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {

//Replace Pilot number in "REQUEST-LINE" with "TO" number
  %HEADERS["Request_Line"][1].URI.USER = %HEADERS["To"][1].URI.USER;
  }
}
```

-SigMa rules to return From header to original form. The From header changed in outbound request messages need to be changed back for inbound responses. This is done by saving the original From User to variable "%fromuser" created previously in the script and applying the variable to the From header for inbound responses (i.e., 180 Ringing and 200 OK).

```
// Return FROM header to original form
within session "ALL"
{
 act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
  %HEADERS["From"][1].URI.USER = %fromuser;
  }
}
```

The following screen shows the finished Signaling Manipulation Script **Broadcore Script** used during compliance testing. This script will later be applied to the Broadcore/Masergy Server Configuration in **Section 7.6.2**.



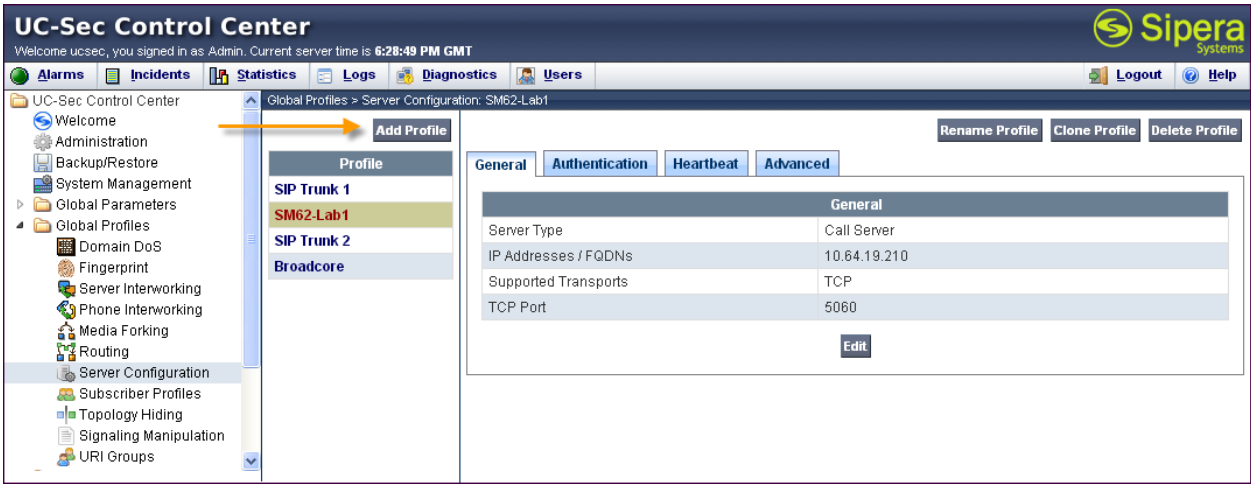
7.6. Server Configuration

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

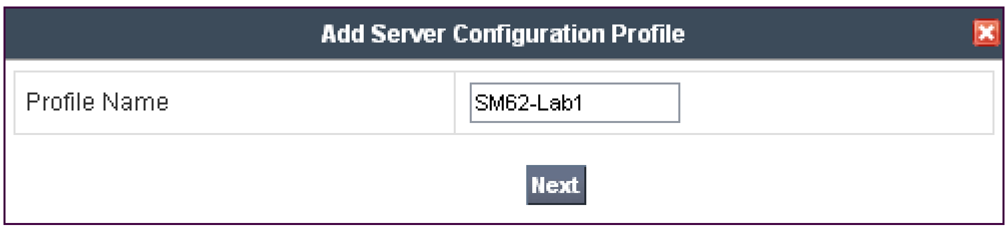
In the sample configuration, separate Server Configurations were created for Session Manager and Broadcore/Masergy.

7.6.1. Server Configuration – Session Manager

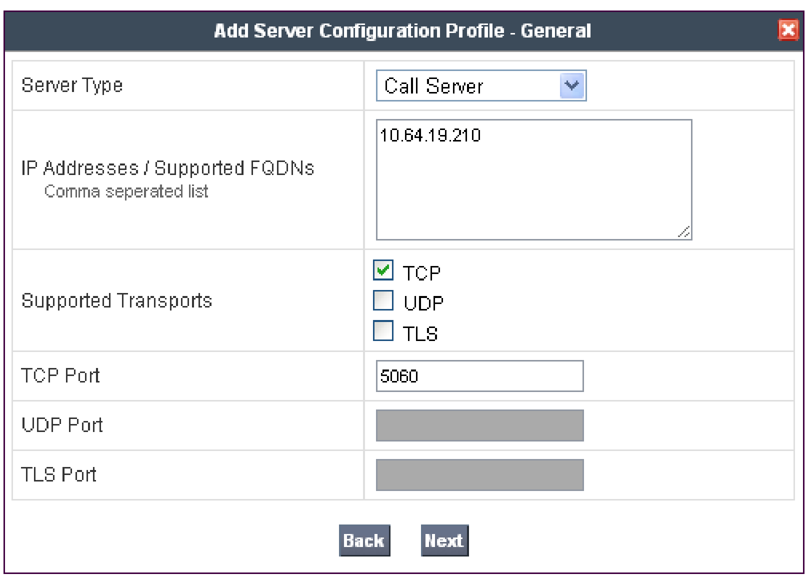
To add a Server Configuration Profile for Session Manager, navigate to **UC-Sec Control Center → Global Profiles → Server Configuration** and click on **Add Profile**.



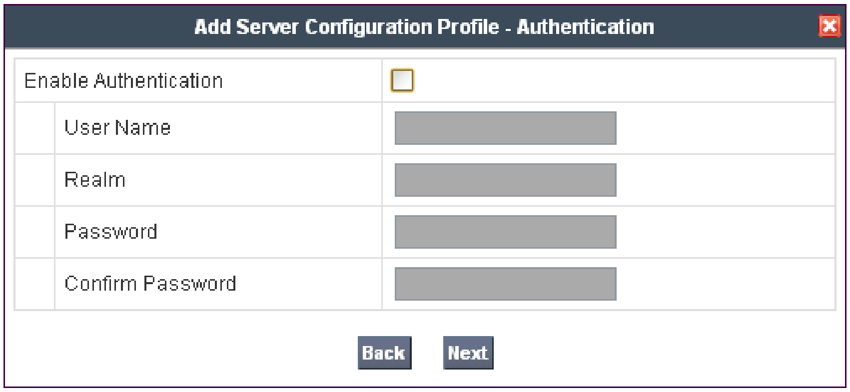
Enter a descriptive name for the new profile and click **Next**.



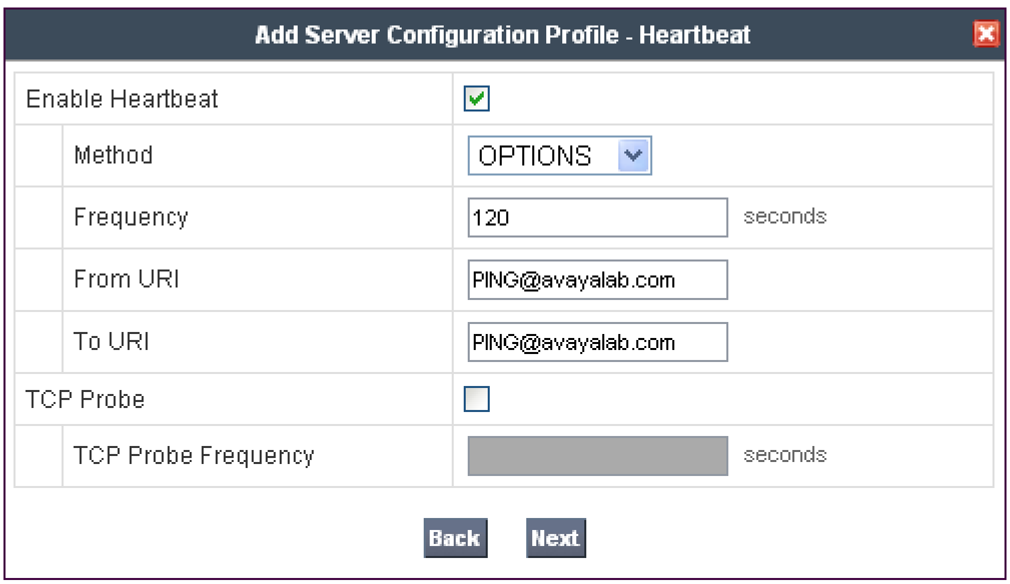
The following screens illustrate the Server Configuration for the Profile name **SM62-Lab1**. On the **General** tab, select **Call Server** from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the IP Address of the Session Manager SIP signaling interface in the sample configuration is entered. This IP Address is 10.64.19.210. In the **Supported Transports** area, **TCP** is selected, and the **TCP Port** is set to **5060**. This configuration corresponds with the Session Manager entity link configuration for the entity link to the Avaya SBCE created in **Section 6.6**. If adding a new profile, click **Next**. If editing an existing profile, click **Finish** (not shown).



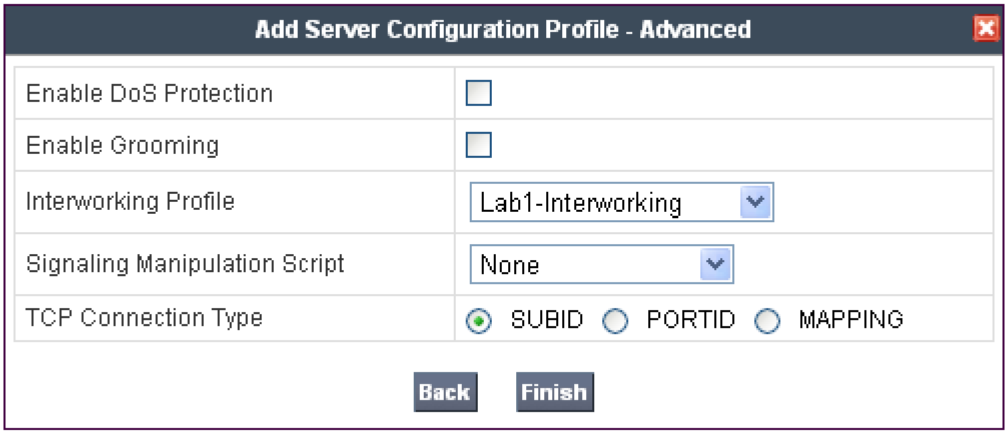
Verify **Enable Authentication** is unchecked as Session Manager does not require authentication. Click **Next** to continue.



In the new window that appears, check the **Enable Heartbeat** box. Select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBC will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the SBC. Click **Next** to continue.

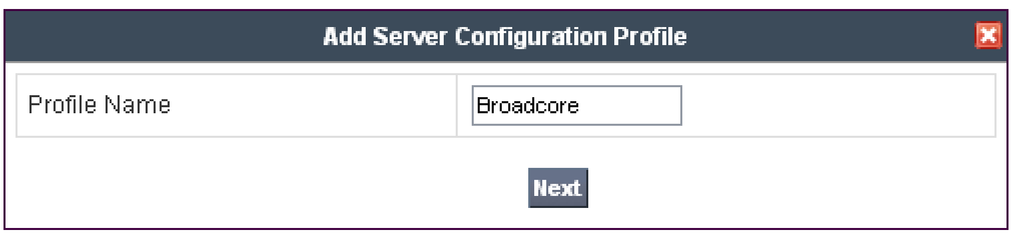


In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 7.4.1**. Use default values for all remaining fields. Click **Finish** to save the configuration.

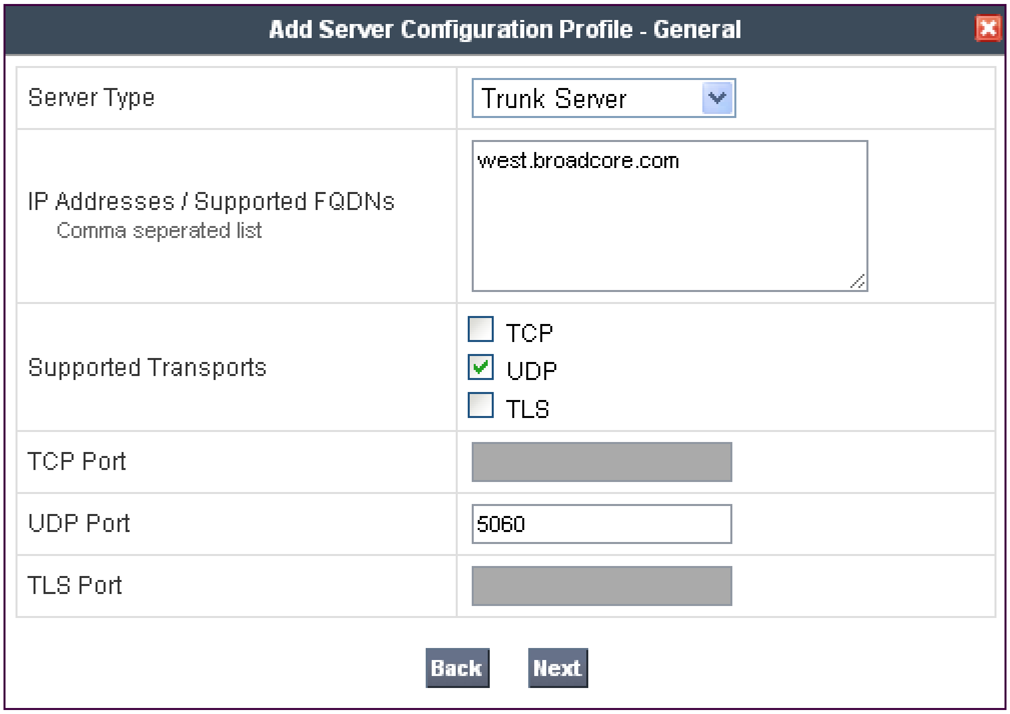


7.6.2. Server Configuration - Broadcore/Masergy

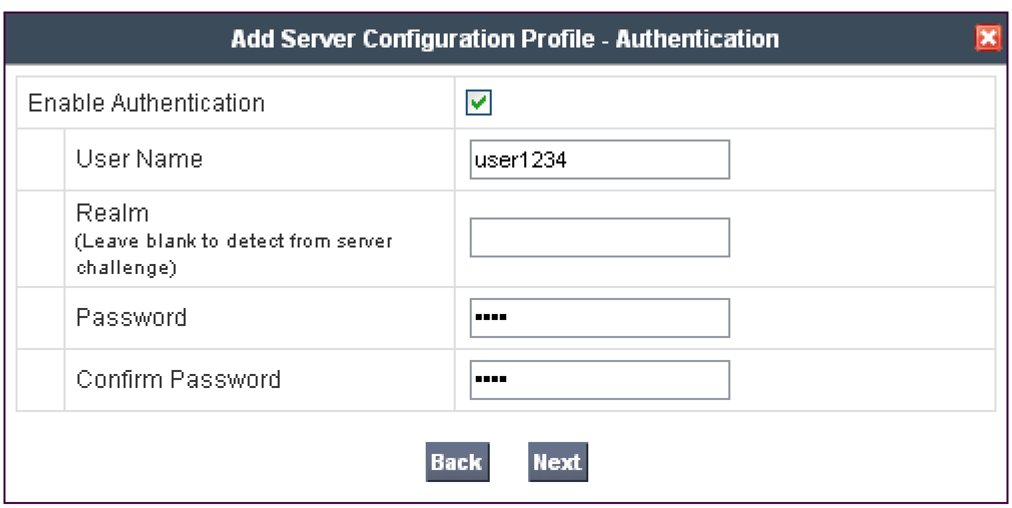
To add a Server Configuration Profile for Broadcore/Masergy, navigate to **UC-Sec Control Center → Global Profiles → Server Configuration** and click on **Add Profile** (not shown). Enter a descriptive name for the new profile and click **Next**.



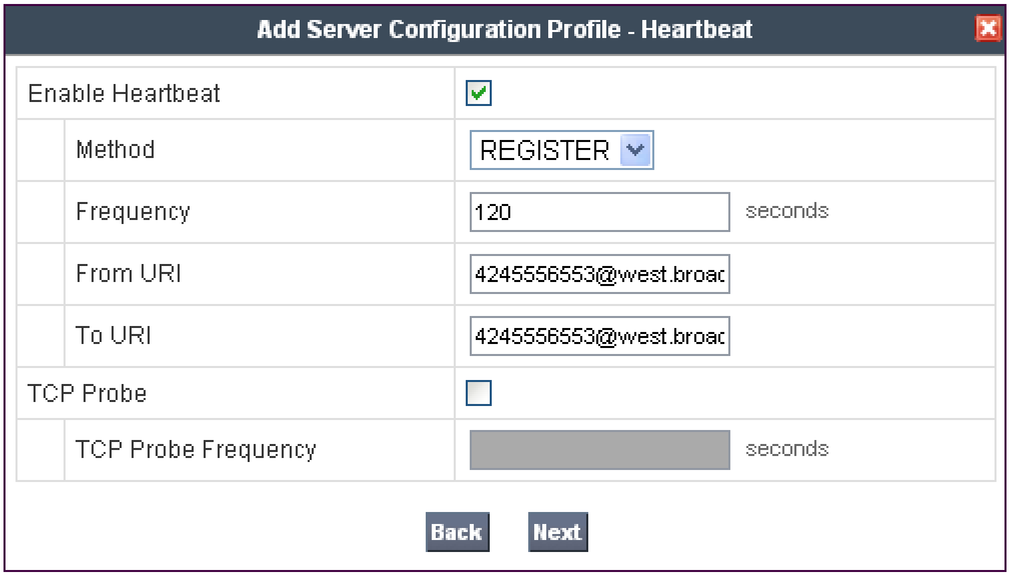
The following screens illustrate the Server Configuration for the Profile name **Broadcore**. In the **General** parameters, select **Trunk Server** from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the Broadcore/Masergy provided Fully Qualified Domain Name is entered. This is **west.broadcore.com**. In the **Supported Transports** area, UDP is selected, and the **UDP Port** is set to **5060**. If adding a new profile, click Next. If editing an existing profile, click Finish (not shown).



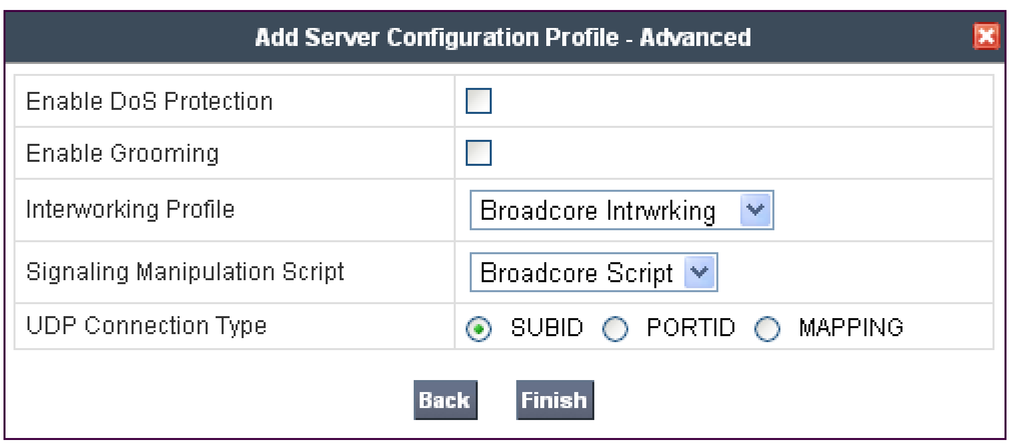
Select **Enable Authentication**. Enter the user name provided by Broadcore/Masergy in the **User Name** field. Leave the **Realm** blank to have it detected from the server challenge. Enter the password provided by Broadcore/Masergy in the **Password** field. Click **Next** to continue.



In the new window that appears, check the **Enable Heartbeat** box. Select **REGISTER** from the **Method** drop-down menu. Select the desired frequency that the SBC will source REGISTERs. The **From URI** and **To URI** are filled in with <number >@west.broadcore.com, where <number> is the pilot number provided by Broadcore/Masergy. Click **Next** to continue.



In the new window that appears, select the **Interworking Profile** created for Broadcore/Masergy in **Section 7.4.2**. Select the **Signaling Manipulation Script** created in **Section 7.5**. Use default values for all remaining fields. Click **Finish** to save the configuration.

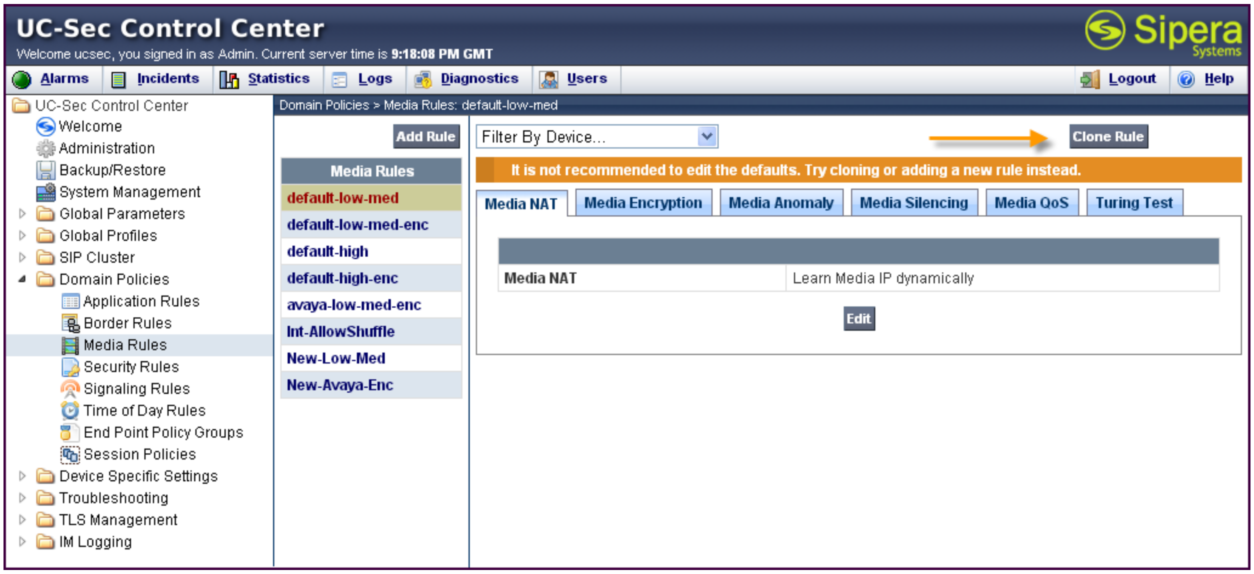


7.7. Media Rule

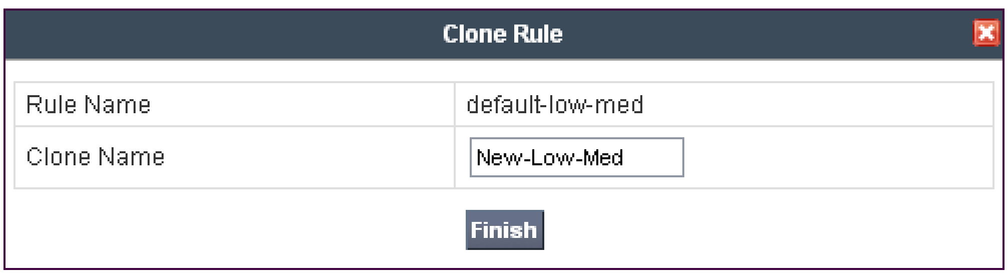
Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be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

Create a custom Media Rule to set the Quality of Service. The sample configuration shows a custom Media Rule **New-Low-Med** created for Broadcore/Masergy SIP Trunk Service and the enterprise.

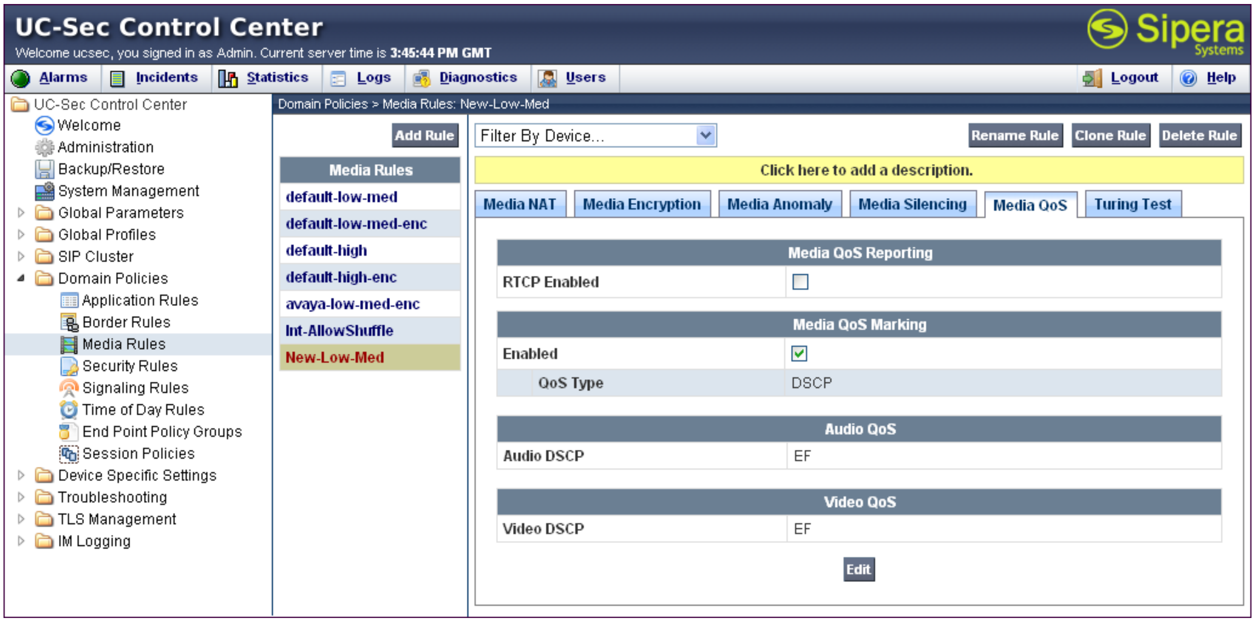
To create a custom Media Rule, navigate to **UC-Sec Control Center → Domain Policies → Media Rules**. With **default-low-med** selected, click **Clone Rule** as shown below.



Enter a descriptive name for the new rule and click **Finish**.



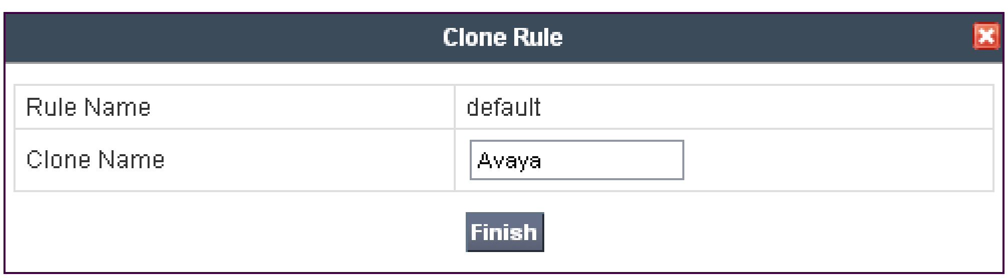
On the **Media QoS** tab select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Service policies for the media. The following screen shows the QoS values used for compliance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



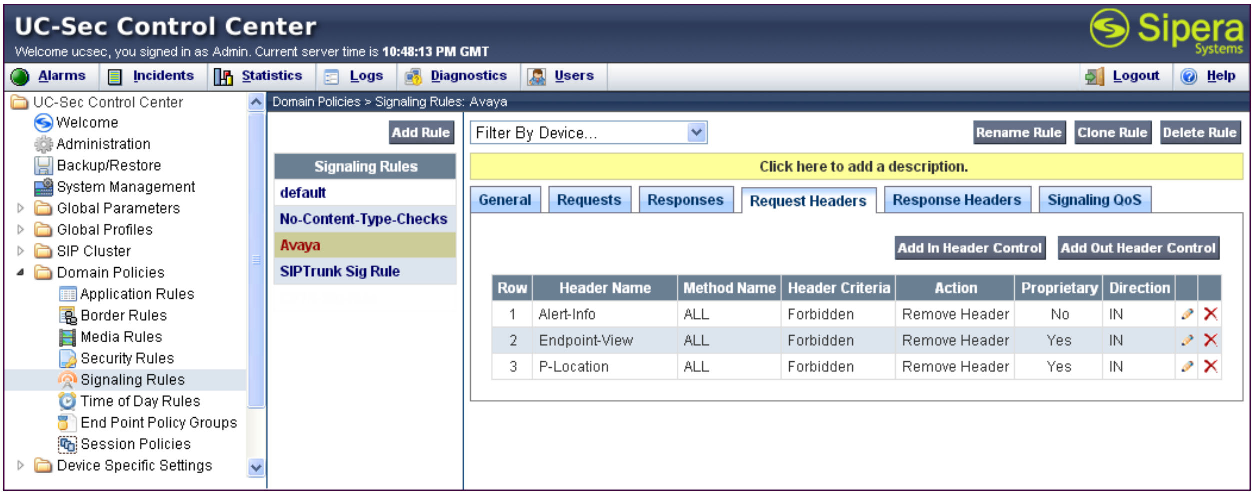
7.8. Signaling Rule

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

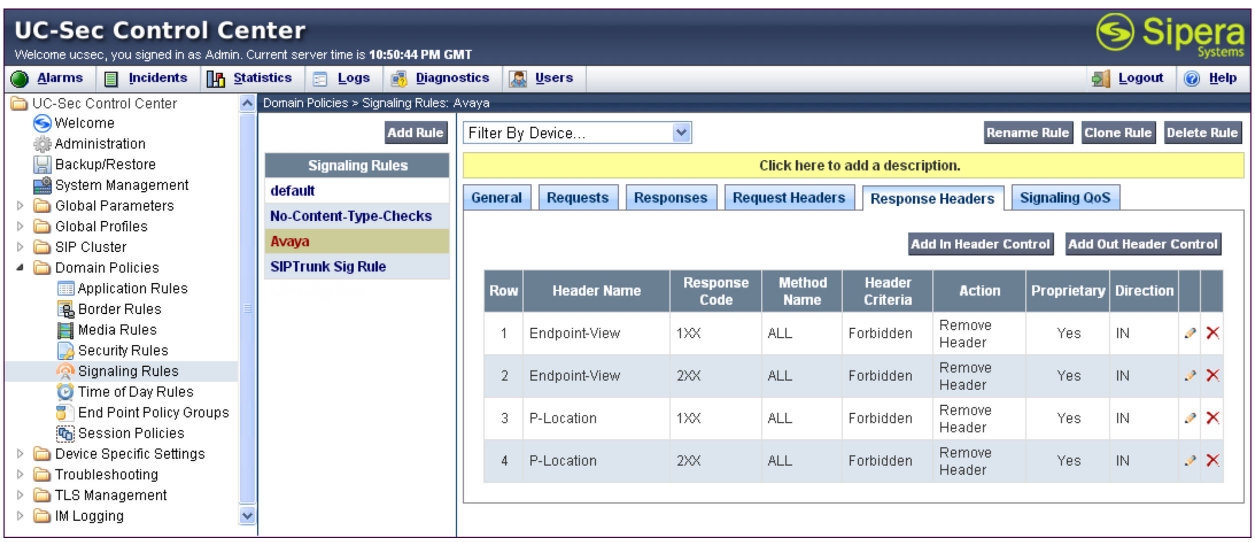
Clone and modify the default signaling rule to remove unnecessary SIP headers and add the proper quality of service to the SIP message. To clone a signaling rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** (not shown). Enter a descriptive name for the new rule and click **Finish**.



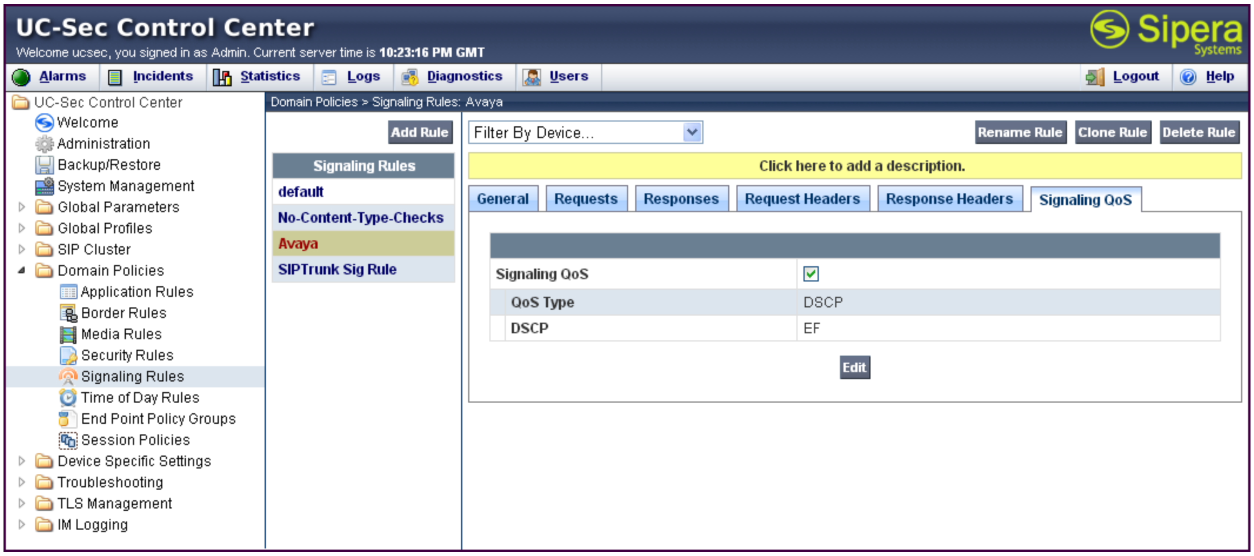
In the sample configuration, signaling rule **Avaya** was created for Session Manager to prevent certain headers in the SIP messages sent from Session Manager from being propagated to Broadcore/Masergy. Select this rule in the center pane, then select the **Request Headers** tab to view the manipulations performed on the request messages such as the initial INVITE or UPDATE message. The following screen shows the **Alert-Info**, **Endpoint-View**, and **P-Location** headers removed during the compliance test.



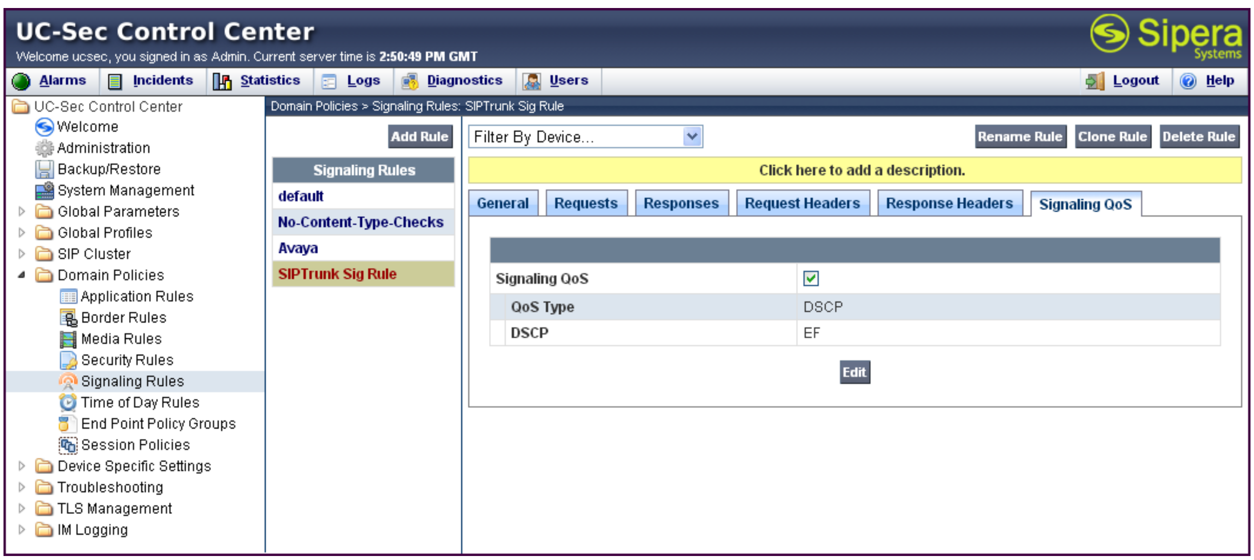
Similarly, manipulations can be performed on the SIP response messages. These can be viewed by selecting the **Response Headers** tab as shown below.



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



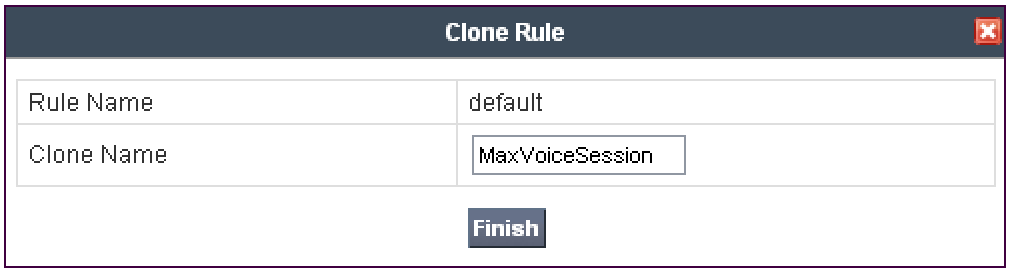
A separate signaling rule **SIPTrunk Sig Rule** was created for Broadcore/Masergy SIP Trunk Service by cloning the **default** signaling rule and changing the **Signaling QoS** parameters as shown below.



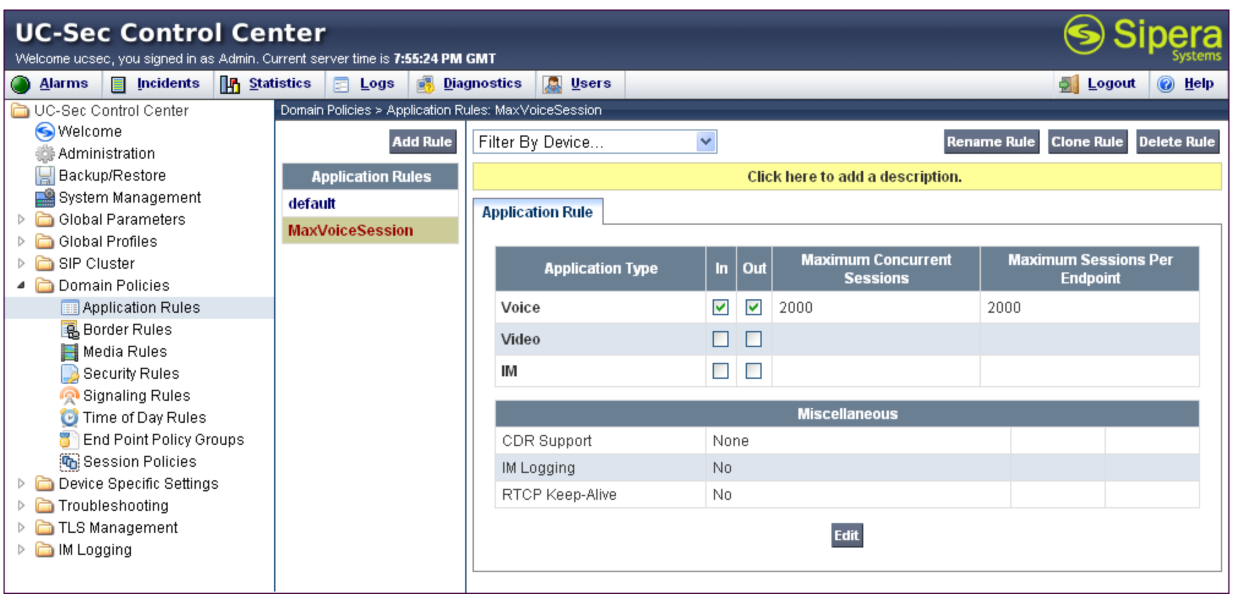
7.9. Application Rule

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

Create an Application Rule to increase the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**. To clone an application rule, navigate to **UC-Sec Control Center → Domain Policies → Application Rules**. With the **default** rule chosen, click on **Clone Rule** (not shown). Enter a descriptive name for the new rule and click **Finish**.



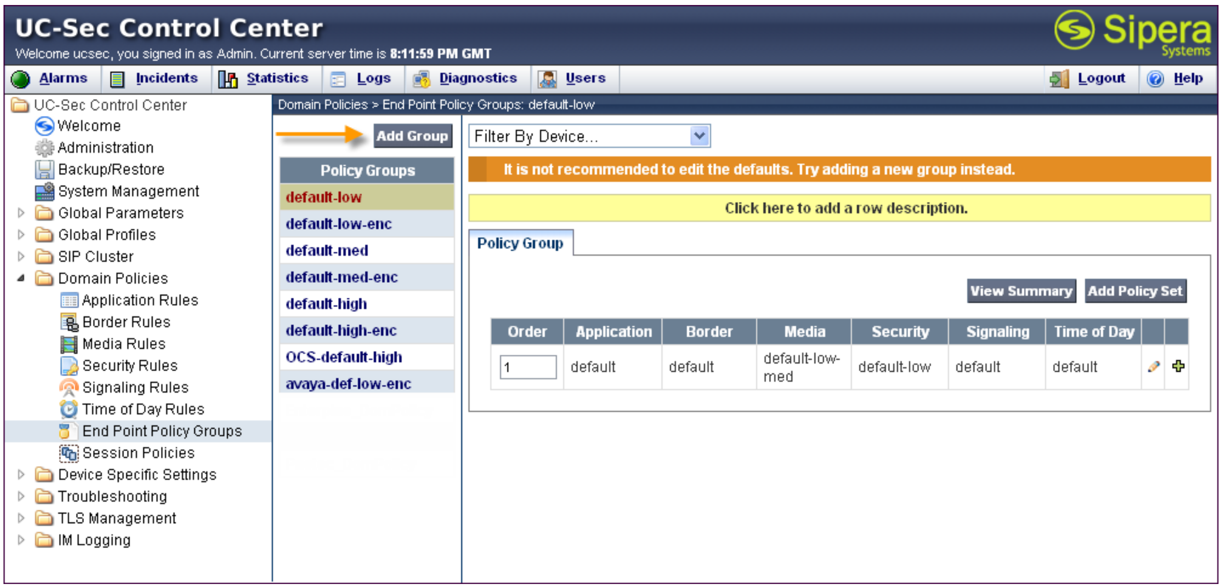
Modify the rule by clicking the **Edit** button. The following screen shows the modified Application Rule **MaxVoiceSession** created in the sample configuration. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** to **2000**.



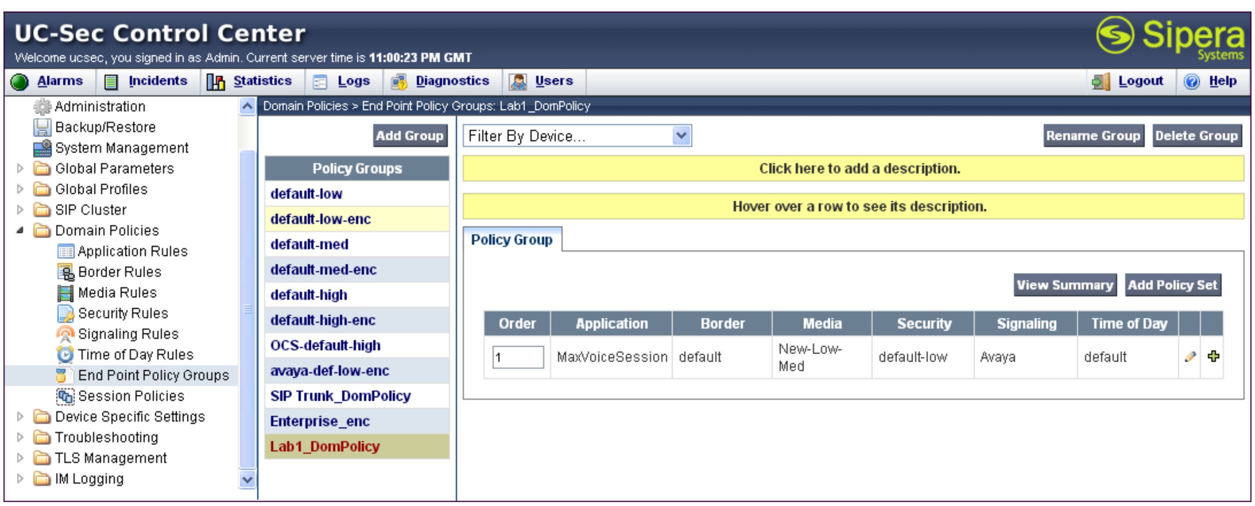
7.10. Endpoint Policy Group

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 7.13**. Create a separate Endpoint Policy Group for the enterprise and the Broadcore/Masergy SIP Trunk Service.

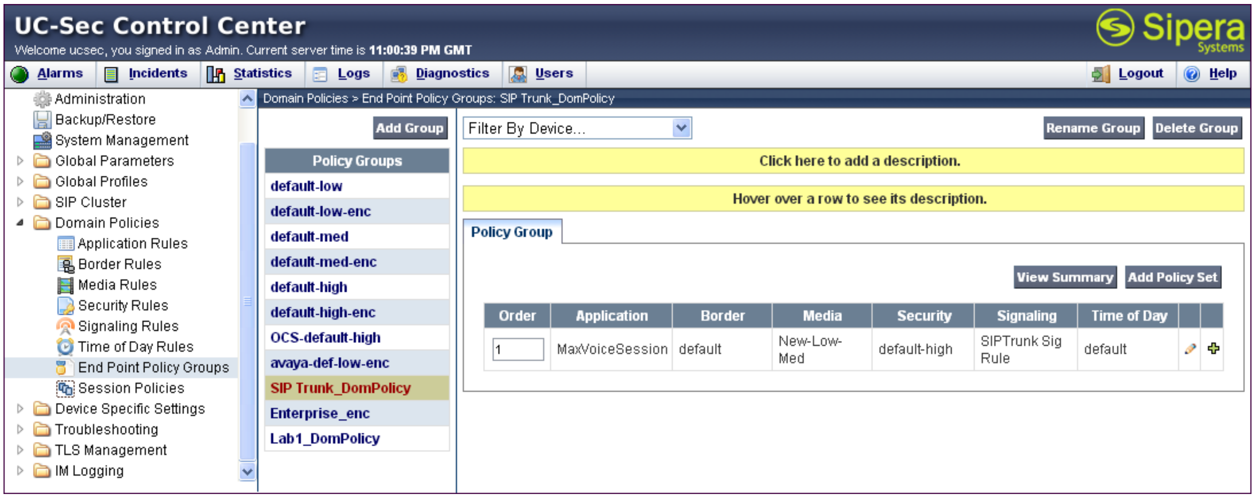
To create a new policy group, navigate to **UC-Sec Control Center → Domain Policies → Endpoint Policy Groups** and click on **Add Group** as shown below.



The following screen shows **Lab1_DomPolicy** created for the enterprise. Set the **Application**, **Media**, and **Signaling** rules to the ones previously created for the enterprise. Set the **Border**, **Security** and **Time of Day** rules to either the **default** or **default-low** policies.



The following screen shows **SIP Trunk_DomPolicy** created for Broadcore/Masergy. Set the **Application**, **Media**, and **Signaling** rules to the one previously created for Broadcore/Masergy. Set the **Border**, **Security**, and **Time of Day** rules to either the **default** or **default-high** policies.



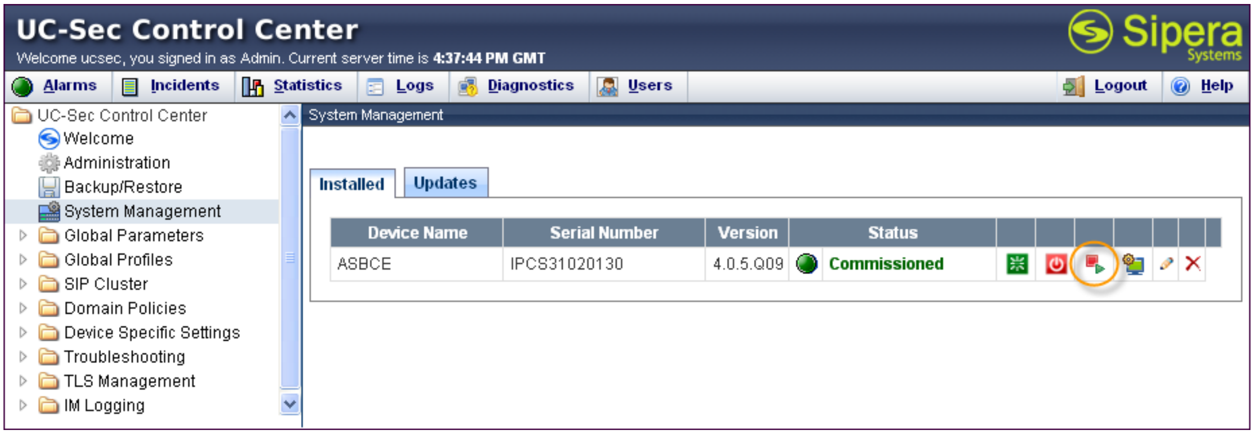
7.11. Media Interface

The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will send SIP media on the defined ports. Create a SIP Media Interface for both the inside and outside IP interfaces.

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

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

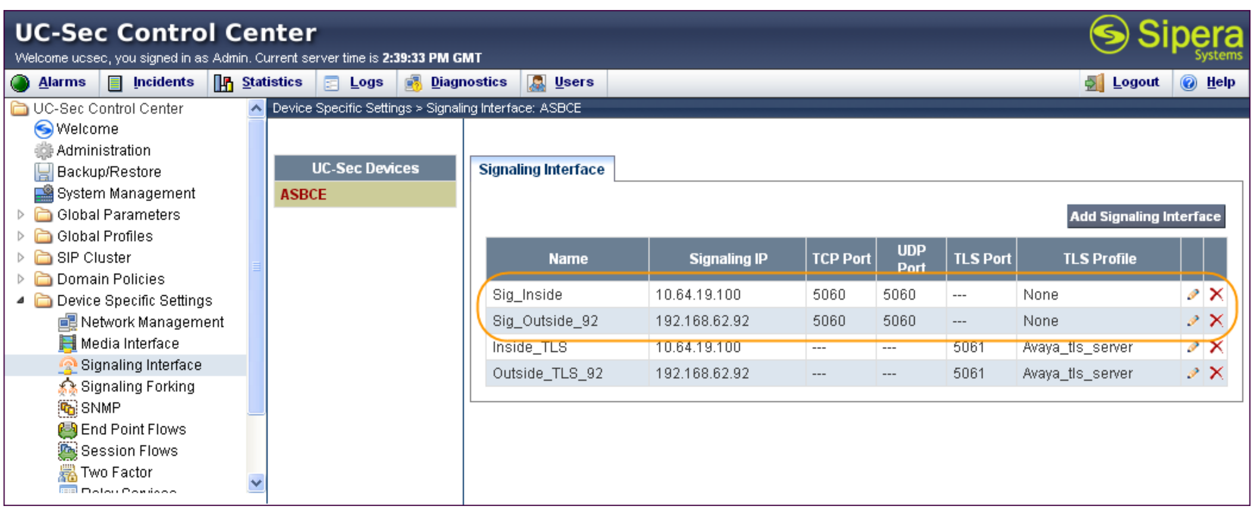
After the media interfaces are created, an application restart is necessary before the changes will take effect. Navigate to **UC-Sec Control Center → System Management** and click the forth icon from the right to restart the applications as highlighted below.



7.12. Signaling Interface

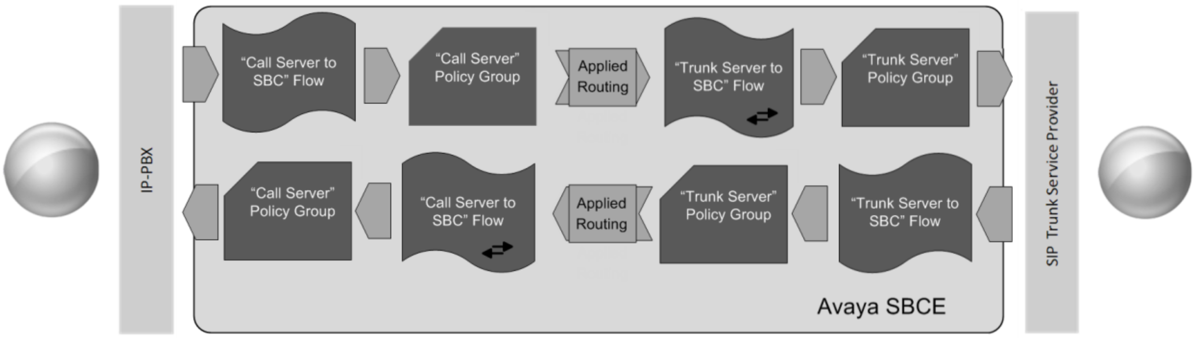
The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces. To create a new Signaling Interface, navigate to **UC-Sec Control Center → Device Specific Settings → Signaling Interface** and click **Add Signaling Interface.**

In the shared test environment the following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.

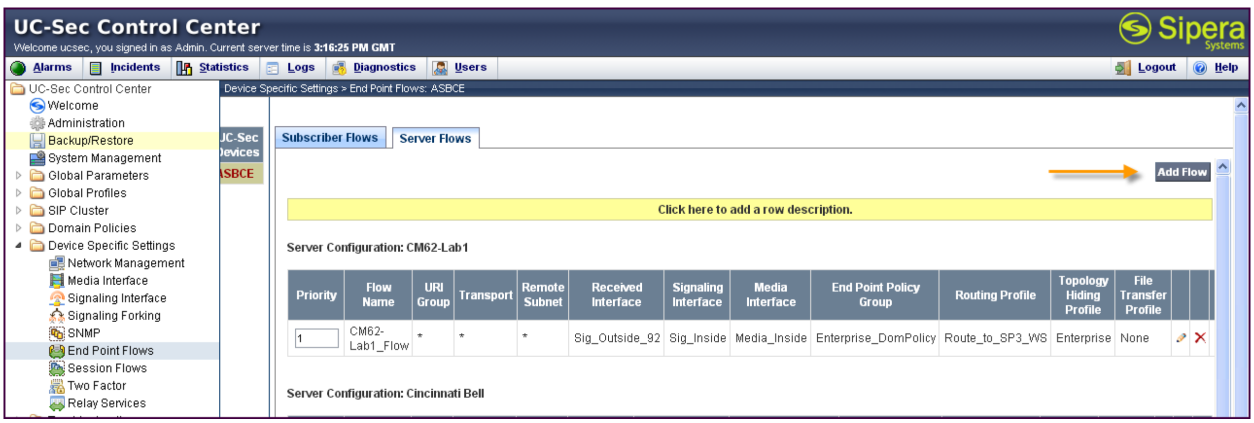


7.13. End Point Flows - Server Flow

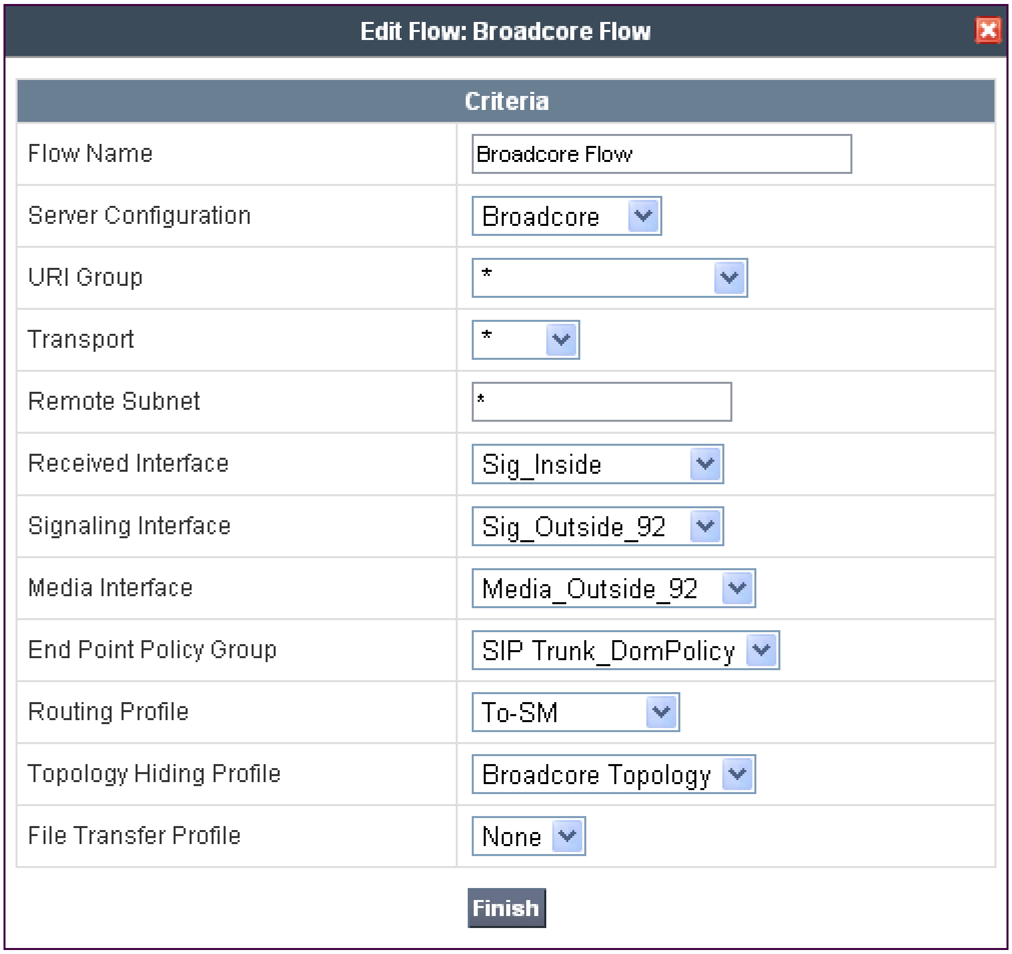
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing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



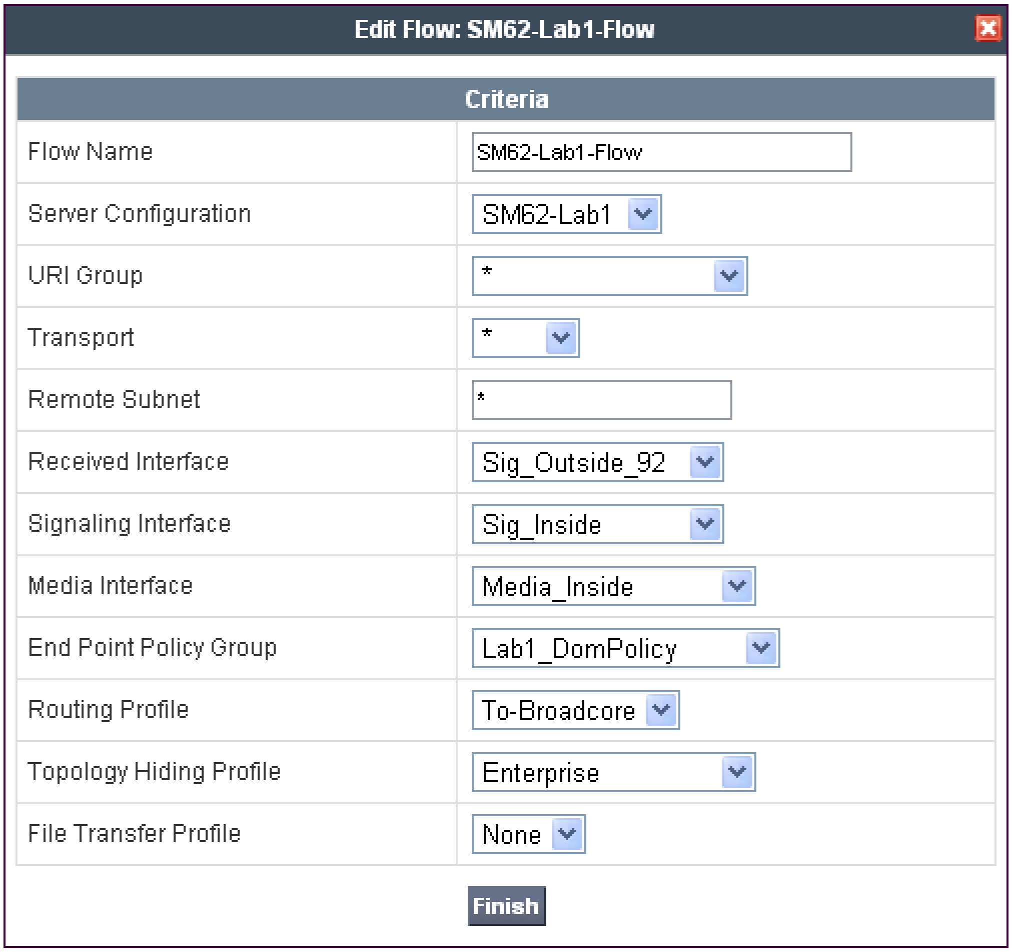
Create a Server Flow for Session Manager and Broadcore/Masergy SIP Trunk Service. To create a Server Flow, navigate to **UC-Sec Control Center → Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** as shown in below.



The following screen show the flow named **Broadcore Flow** created in the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections. Click **Finish**.



Once again, select the **Server Flows** tab and click **Add Flow**. The following screen shows the flow named **SM62-Lab1-Flow** created in the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections. Click **Finish**.



8. Broadcore/Masergy SIP Trunk Configuration

To use Broadcore/Masergy SIP Trunk Service, a customer must request the service from Broadcore/Masergy using their sales processes. This process can be initiated by contacting Broadcore/Masergy via the corporate web site at www.broadcore.com and requesting information via the online sales links or telephone numbers.

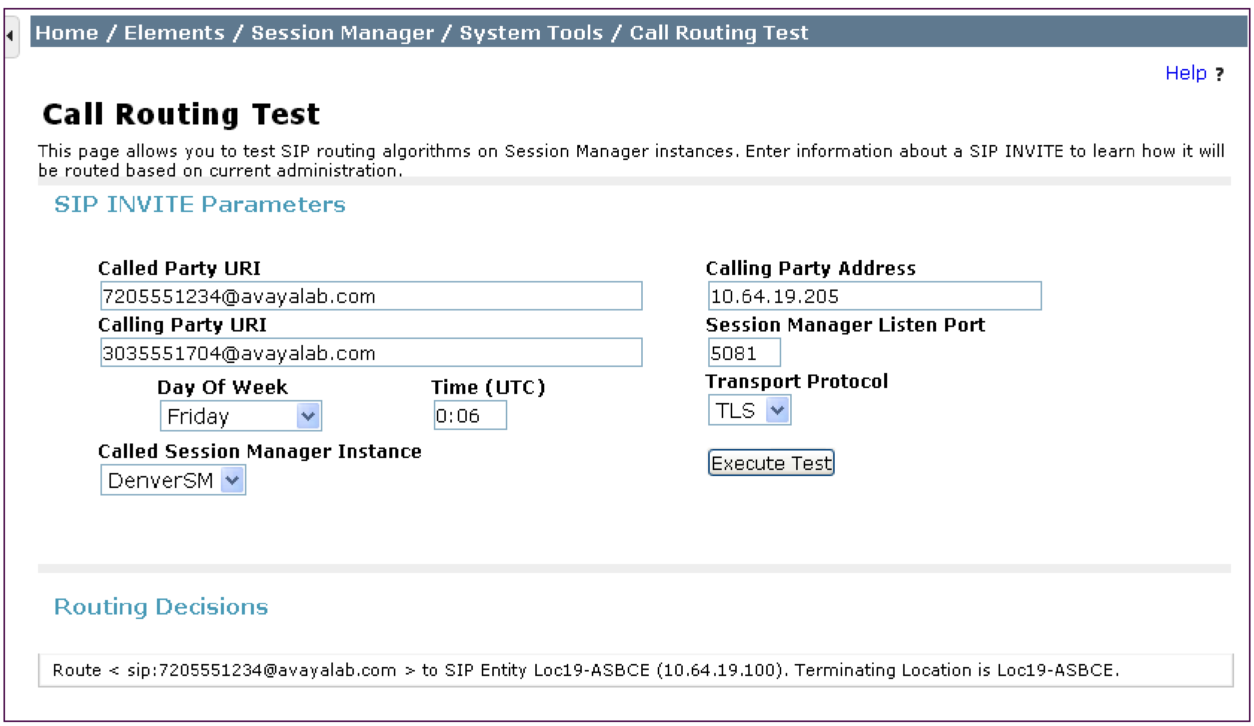
9. Verification and Troubleshooting

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

9.1. Verification

The following steps may be used to verify the configuration:

1. Verify the call routing administration on Session Manager by logging in to System Manager and executing the Call Routing Test. Expand **Elements → Session Manager → System Tools → Call Routing Test**. Populate the field for the call parameters of interest. For example, the following screen shows an example call routing test for an outbound call to PSTN via Broadcore/Masergy. Under **Routing Decisions**, observe the call will rout via the Avaya SBCE SIP Entity to Broadcore/Masergy. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



2. 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.
3. 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.
4. Verify that the user on the PSTN can end an active call by hanging up.
5. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Use the SAT interface on Communication Manager to verify status of SIP trunks. Specifically use the **status trunk n** command to verify the active call has ended, where **n** is the trunk group number used for Broadcore/Masergy SIP Trunk Service defined in **Section 5.8**.

Below is an example of an active call.

```
status trunk 2

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/active  no   S00000
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
```

Verify the port returns to **in-service/idle** after the call has ended.

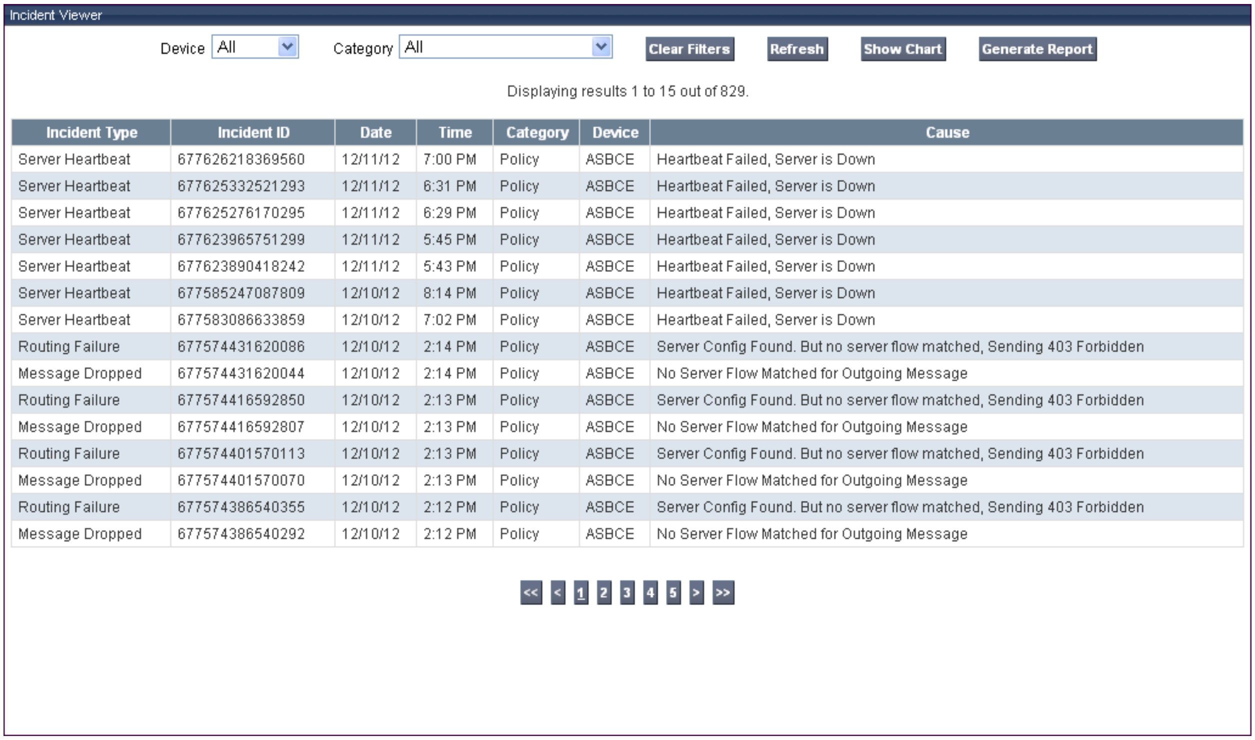
```
status trunk 2

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
```

9.2. Troubleshooting

1. Communication Manager:
    - **list trace station** <extension number> - Traces calls to and from a specific station.
    - **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
    - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
    - **status trunk** <trunk access code number> - Displays trunk group information.

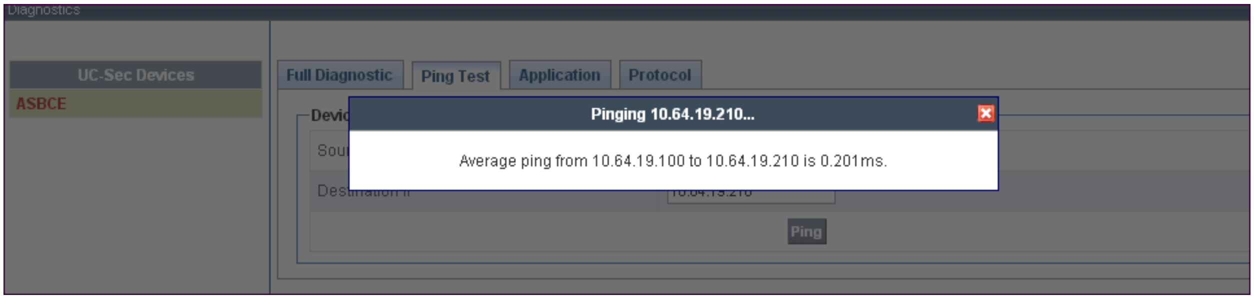
2. Session Manager: **traceSM -x –uni** – Session Manager command line tool for traffic analysis. Login to the Session Manager management interface to run this command.

3. Avaya SBCE:
   - **Incidences –** Displays alerts captured by the UC-Sec appliance.

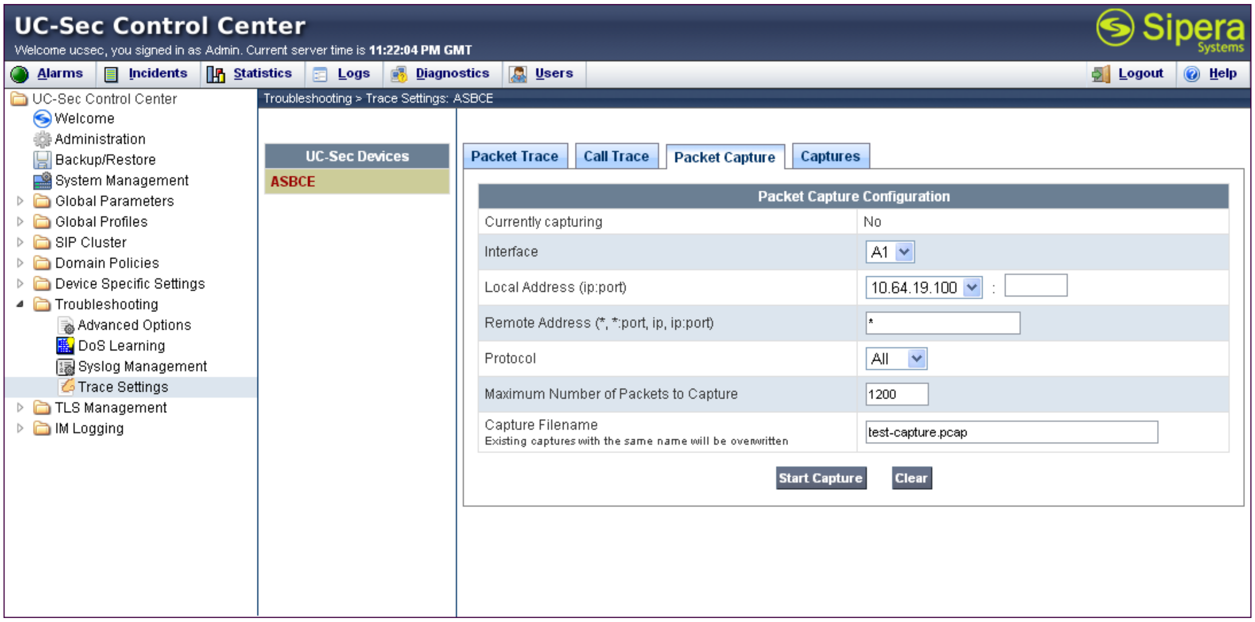


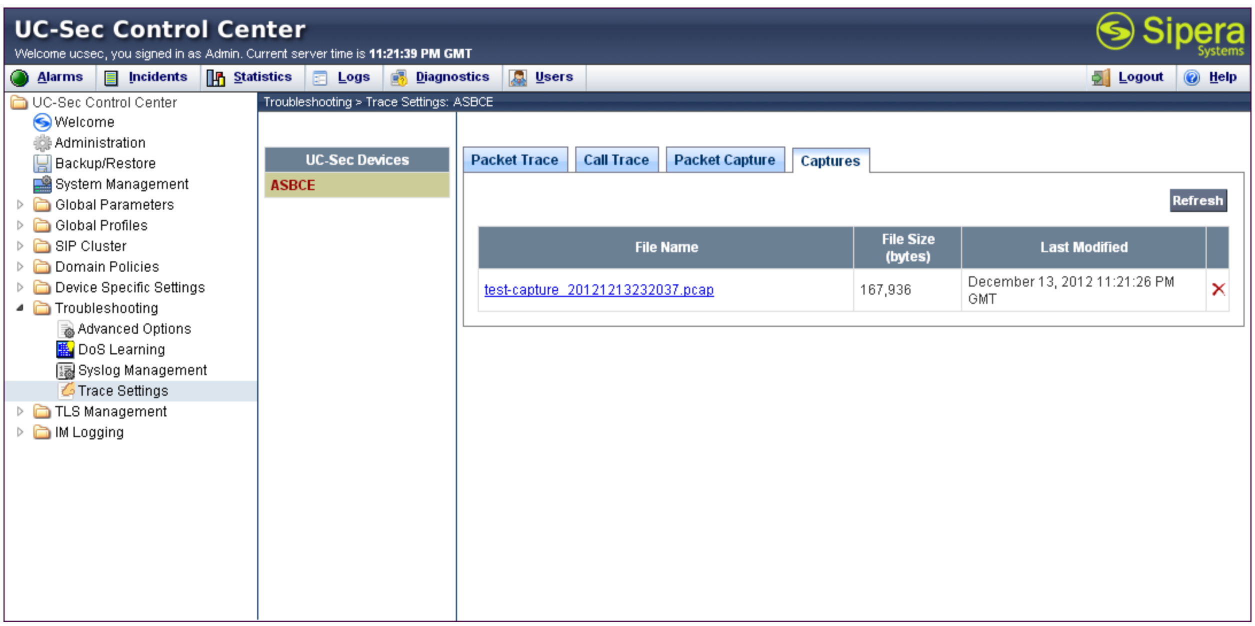
Incident Type	Incident ID	Date	Time	Category	Device	Cause
Server Heartbeat	677626218369560	12/11/12	7:00 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677625332521293	12/11/12	6:31 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677625276170295	12/11/12	6:29 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677623965751299	12/11/12	5:45 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677623890418242	12/11/12	5:43 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677585247087809	12/10/12	8:14 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677583086633859	12/10/12	7:02 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Routing Failure	677574431620086	12/10/12	2:14 PM	Policy	ASBCE	Server Config Found. But no server flow matched, Sending 403 Forbidden
Message Dropped	677574431620044	12/10/12	2:14 PM	Policy	ASBCE	No Server Flow Matched for Outgoing Message
Routing Failure	677574416592850	12/10/12	2:13 PM	Policy	ASBCE	Server Config Found. But no server flow matched, Sending 403 Forbidden
Message Dropped	677574416592807	12/10/12	2:13 PM	Policy	ASBCE	No Server Flow Matched for Outgoing Message
Routing Failure	677574401570113	12/10/12	2:13 PM	Policy	ASBCE	Server Config Found. But no server flow matched, Sending 403 Forbidden
Message Dropped	677574401570070	12/10/12	2:13 PM	Policy	ASBCE	No Server Flow Matched for Outgoing Message
Routing Failure	677574386540355	12/10/12	2:12 PM	Policy	ASBCE	Server Config Found. But no server flow matched, Sending 403 Forbidden
Message Dropped	677574386540292	12/10/12	2:12 PM	Policy	ASBCE	No Server Flow Matched for Outgoing Message

   - **Diagnostics –** Allows for PING tests and displays application and protocol use.

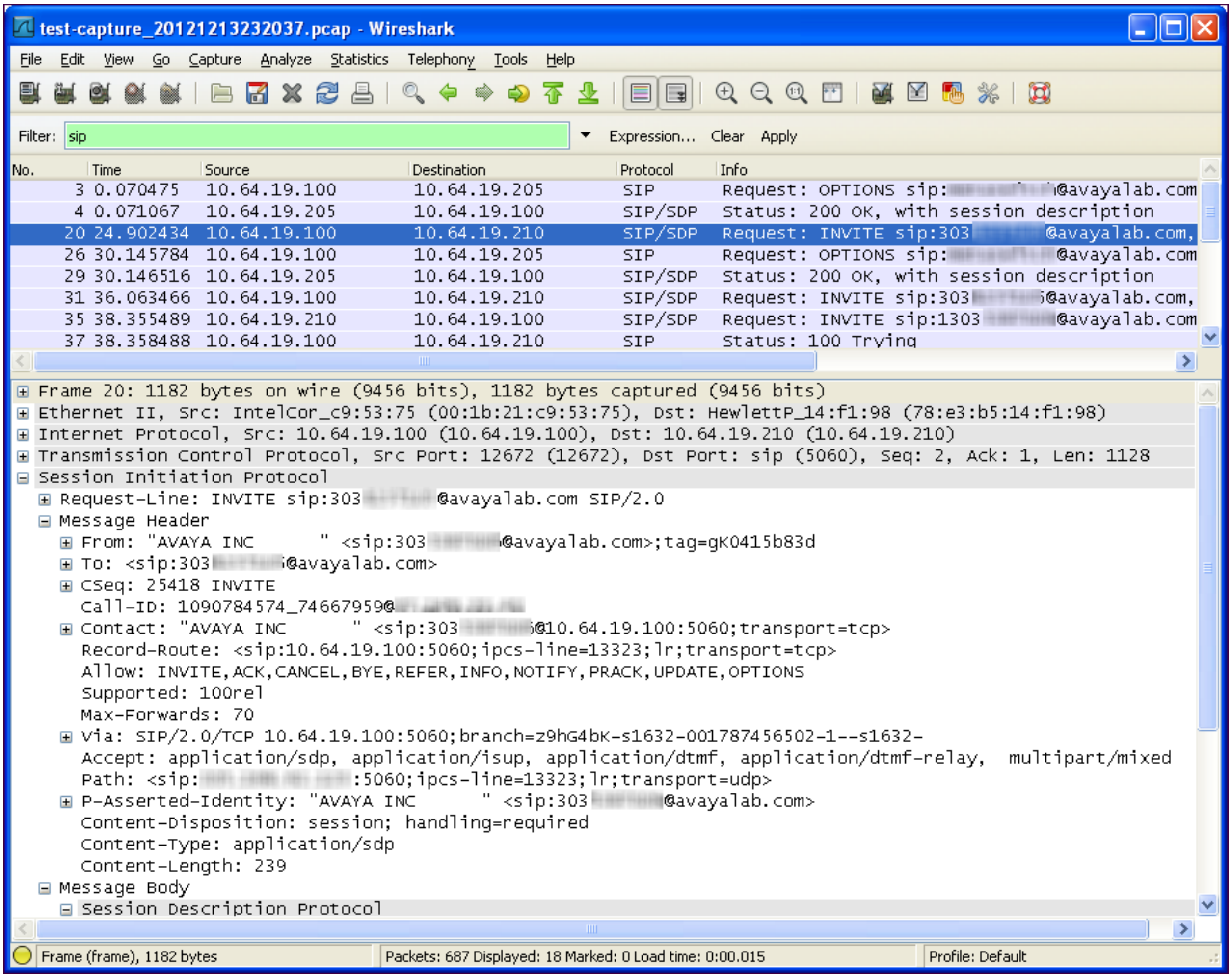


- **Troubleshooting → Trace Settings** – Configure and display call traces and packet captures for the UC-Sec appliance.





The packet capture file can be downloaded and viewed using a Network Protocol Analyzer like WireShark:



10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, and Avaya Session Border Controller for Enterprise to the Broadcore/Masergy SIP Trunk Service. The Broadcore/Masergy SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The Broadcore/Masergy SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. Additional References

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

[1] *Installing and Configuring Avaya Aura® System Platform, Release 6.2.0*, March 2012.
[2] *Administering Avaya Aura® System Platform, Release 6.2.0*, February 2012.
[3] *Implementing Avaya Aura® Communication Manager Solution Release 6.2*, February 2012 Document Number 03-603559
[4] *Administering Avaya Aura ® Communication Manager*, Release 6.2, February 2012, Document Number 03-300509
[5] *Avaya Aura® Communication Manager Feature Description and Implementation*, June 2010, Document Number 555-245-205.
[6] *Implementing Avaya Aura ® System Manager*, Release 6.2, March 2012
[7] *Installing Service Packs for Avaya Aura® Session Manager*, February 2012, Document Number 03-603863
[8] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473.
[9] *Avaya one-X Deskphone H.323 Administrator Guide*, May 2011, Document Number 16-300698.
[10] *Avaya one-X Deskphone SIP Administrator Guide Release 6.1*, December 2010, Document Number 16-603838
[11] *Administering Avaya one-X Communicator*, July 2011
[12] *Administering Avaya Session Border Controller*, Document Number 08-604063, Sept. 2012
[13] *RFC 3261 SIP: Session Initiation Protocol, http://www.ietf.org/*
[14] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method, http://www.ietf.org/*
[15] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/*
[16] *RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, http://www.ietf.org/*

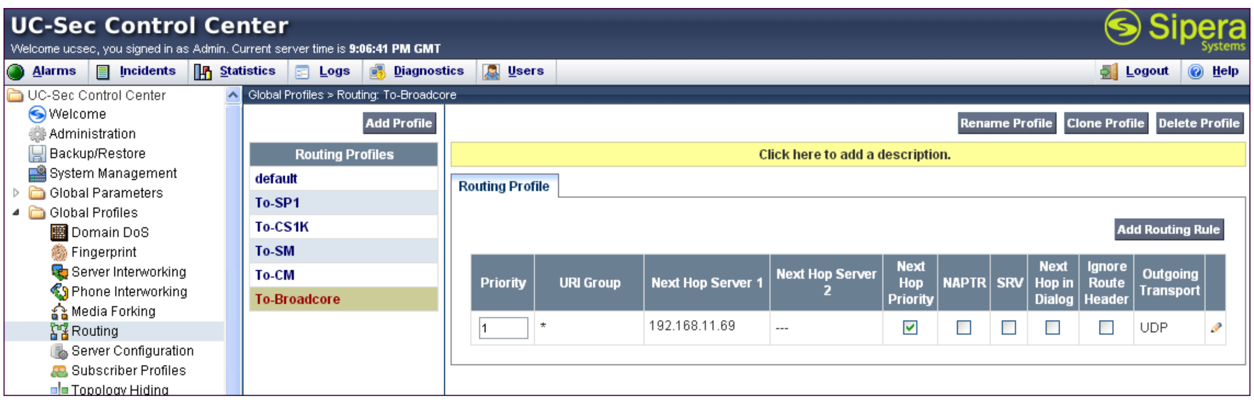
Appendix A: Static IP Authentication

Static IP Authentication is a Broadcore/Masergy offered service that is an alternative to Single Number Registration. This feature allows Customers to register a SIP trunk by using the IP address of the Avaya SBCE outside interface rather than sending REGISTER messages using a username and password. The Avaya SBCE will also route calls based on a static IP address rather than using DNS SRV to discover the IP address.

The procedures outlined in these Application Notes are used to support static IP authentication with the exception of the changes outlined in this section for the Avaya SBCE.

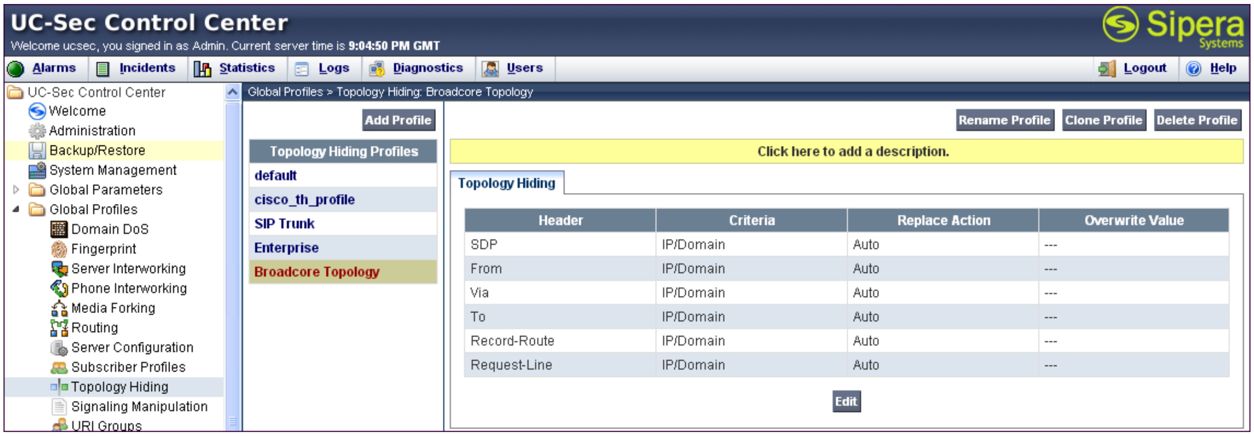
Login to Avaya SBCE as shown in **Section 7** above, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue (not shown).

The following screen shows the Routing Profile **To-Broadcore** created for Static IP Authentication. In the **Next Hop Server 1** field enter the IP Address that Broadcore/Masergy uses to listen for SIP traffic. In the sample configuration **192.168.11.69** was used. Select **Next Hop Priority** and enter **UDP** for the **Outgoing Transport field**.



Navigate to **UC-Sec Control Center → Global Profiles → Topology Hiding**. Select the **default** profile and click on **Clone Profile** (not shown).

The following screen shows the Topology Hiding Profile **Broadcore Topology** created for Static IP Authentication.

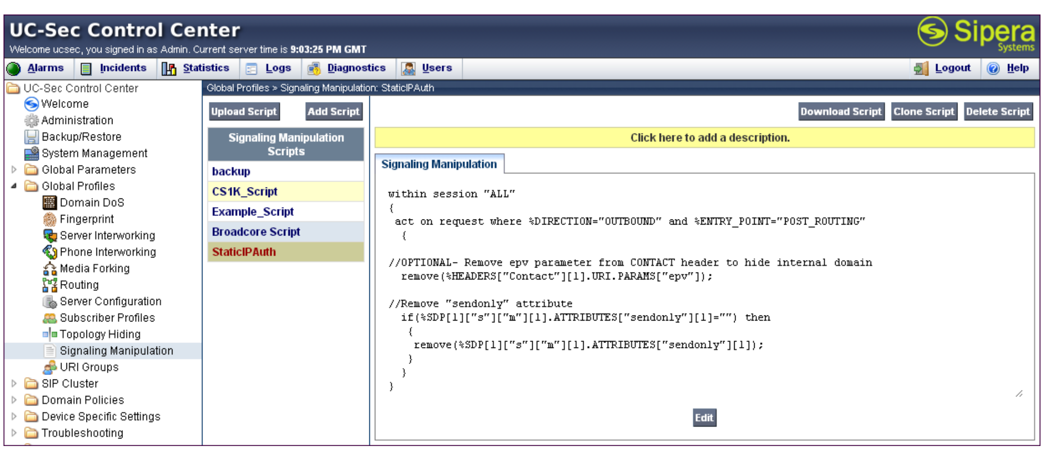


Navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script**. A new blank SigMa Editor window will pop up.

In this compliance testing, the script named **StaticIPAuth** was created as shown below. See **Section 7.5** for more information regarding signaling manipulation.

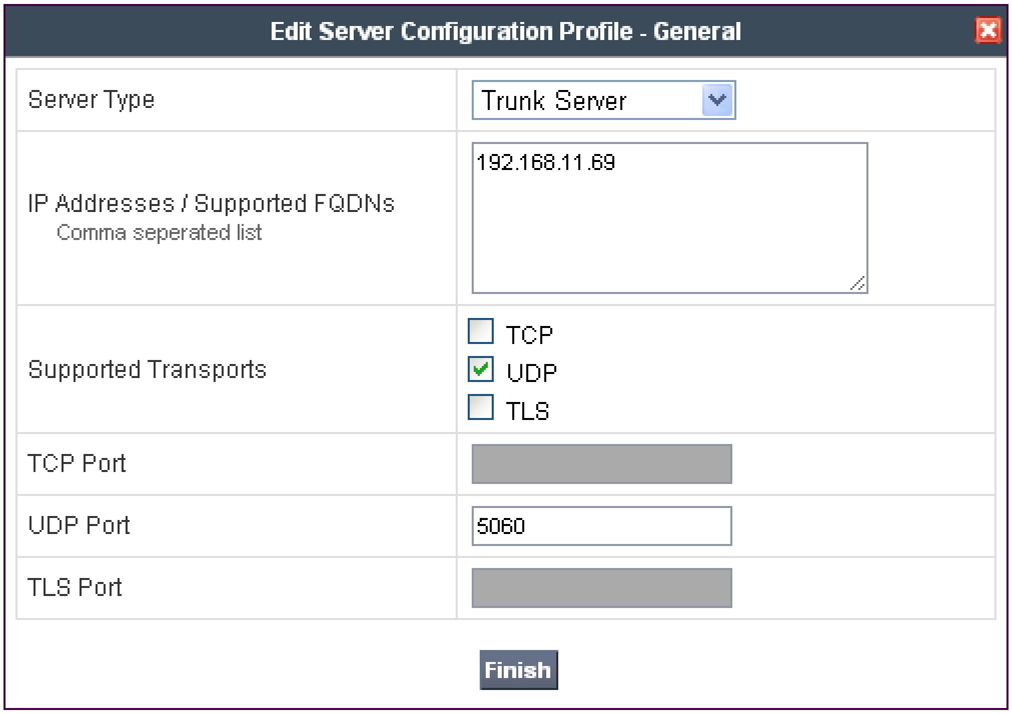
```
within session "ALL"
{
 act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
//OPTIONAL- Remove epv parameter from CONTACT header to hide internal domain
  remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);

//Remove "sendonly" attribute
  if(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]="") then
   {
    remove(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]);
   }
  }
}
```

The following screen shows the finished Signaling Manipulation **StaticIPAuth** used in the sample configuration.

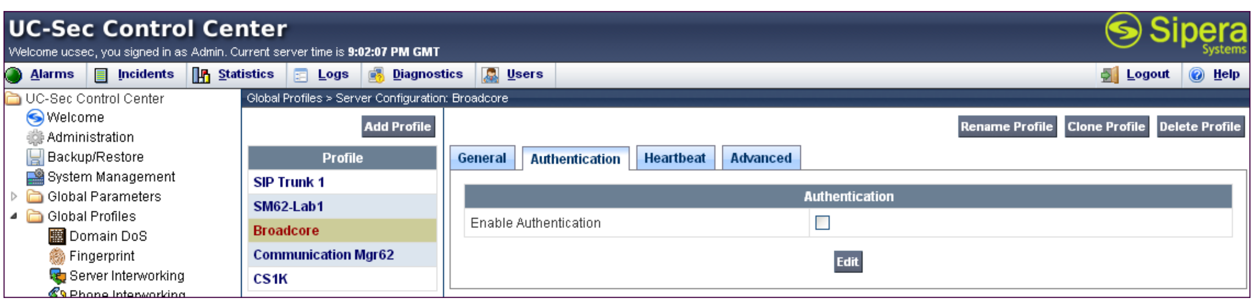


Navigate to **UC-Sec Control Center → Global Profiles → Server Configuration** and click on **Add Profile** (not shown).

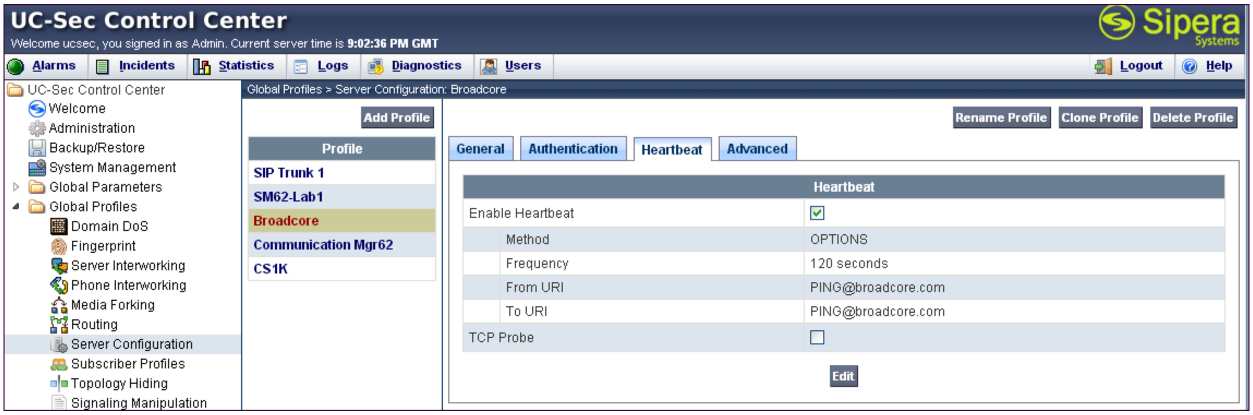
The following screens illustrate the Server Configuration for the Profile name **Broadcore** used for Static IP Authentication. In the **General** parameters, select **Trunk Server** from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the Broadcore/Masergy provided IP address is entered. In the sample configuration **192.168.11.69** was used. In the **Supported Transports** area, UDP is selected, and the **UDP Port** is set to **5060**.



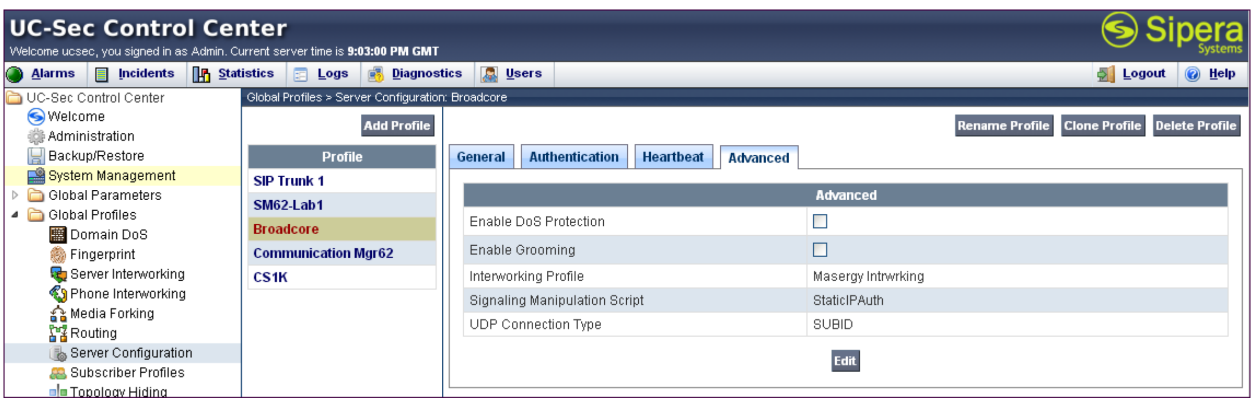
On the Authentication tab, verify **Enable Authentication** is unchecked as Broadcore/Masergy does not require authentication for this type of configuration.



On the Advanced tab, check the **Enable Heartbeat** box. Select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBC will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the SBC.



On the Advanced tab, select the **Interworking Profile** created for Broadcore/Masergy in **Section 7.4.2**. Select the **Signaling Manipulation Script** created in this section. Use default values for all remaining fields.



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.