Avaya Solution & Interoperability Test Lab

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

Abstract

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

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

NOTE: This Application Note is applicable with Avaya Aura® 6.2 which is currently in Controlled Introduction. Avaya Aura® 6.2 will be Generally Available in Summer 2012.

TABLE OF CONTENTS

1. Introduction

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

Avaya Aura® Session Manager is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. The Avaya SBC (Session Border Controller) for Enterprise (A-SBCE) is the point of connection between Avaya Aura® Session Manager and the Frontier Communications SIP Trunking service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

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

2. General Test Approach and Test Results

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

A simulated enterprise site using Communication Manager, Session Manager and Avaya Session Border Controller for Enterprise was connected to the public Internet using a broadband connection. The enterprise site was configured to connect to Frontier SIP Trunking service through the public IP network.

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various enterprise 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 enterprise 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. Both protocols were tested.
- Various call types including: local, long distance, outbound toll-free, operator, and local directory assistance (411).
- Codec G.711MU and G.729A.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation using DTMF for inbound and outbound calls.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call forwarding, transfer, conference and mobility (extension to cellular).
- T.38 Fax.

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls are supported but were not tested.
- International call (starting with 011) and operator-assisted call (0 + 10-digits) outbound from the enterprise are not supported on the test circuit used for the compliance test.

2.2. Test Results

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

- **Outbound Call** – Sometimes it took a long time (could be 10 seconds or more) for the destination PSTN phone to ring after "183 Session Progress with SDP" was received by the enterprise from the network. This long delay in destination ringing was caused by the Frontier SIP Trunking service hunting for the least-cost carrier to deliver the call.
- **Call Transfer to PSTN** – When an enterprise extension transferred a call with a PSTN phone (either inbound or outbound) off-net back to PSTN, Frontier responded to REFER from the enterprise with "403 Refer in bad call state" instead of “202 Accepted”. User experience was not negatively affected (i.e., the call was transferred successfully). This problem was reported to Frontier for further investigation.
- **T.38 Faxing** – Frontier supports outbound T.38 faxing only for local calls. Outbound long-distance T.38 faxing failed. Inbound T.38 faxing worked properly.
- **DTMF Payload** – If the internal general SIP trunk had **Initial Direct IP-IP Media** setting on (on Communication Manager signaling group form) and the service provider trunk did not, the DTMF value sent to the service provider was not the value set on the service provider SIP trunk group form on Communication Manager. Instead, it was 127

(default value when setting value is blank). This could lead to the asymmetric DTMF payload header issue where 2 different DTMF payload header values get used in each direction of the call which for some service providers can eventually lead to dropped calls or DTMF not working properly. In the compliance test, **Initial Direct IP-IP Media** for both the internal general SIP trunk and the service provider SIP trunk on Communication Manager was turned off.

- **Call Forward on No Answer** – When an inbound call was forwarded to an internal extension on no answer, and the internal extension hung up the call, the call would not terminate properly (A-SBCE responded to the BYE from Communication Manager with "481 - Call/Transaction Does Not Exist" and the BYE was not passed along to the service provider network). This problem was corrected in the compliance test by turning off **Initial Direct IP-IP Media** on the service provider SIP trunk (on Communication Manager signaling group form).
- **Call Display on Transfer to Internal Extension** – Attended transfer of outbound call from SIP phone to internal H.323 extension resulted in incorrect call display: the display of the H.323 station showed the transferring party and Communication Manager trunk access code instead of connected party name and/or number. The fix to this problem is included in Communication Manager 6.2 SP1 (tested/verified).
- **Call Display on Conference with internal Extension** – When a SIP phone conferenced a PSTN call (either inbound or outbound) with an internal H.323 extension, and the H.323 station dropped off the call, the call display on the SIP phone was incorrect: it showed the dropped party (H.323) as caller's name and PSTN number as the party's number. Only the PSTN should be part of the display. Communication Manager 6.2 SP1 fixed this problem (tested/verified).
- **Conferencing with PSTN from Soft Phone** – When using the Conference button directly on the one-X Communicator soft phone for conferencing a call with a PSTN party, there was only partial audio on the established conference. This problem was corrected in the compliance test by placing the original call on hold first and making an outbound call to PSTN before establishing the conference via the Conference button.
- **Media Anomaly Detection** – When an inbound call was forwarded off-net back out to PSTN, there was no audio occasionally on the answered call. This problem was corrected in the compliance test by turning off Media Anomaly Detection on A-SBCE (see **Section 7.7**). Media Anomaly Detection basically measures the jitter in the audio flow and is a bit overly sensitive in the tested software release (and also the past releases). Developers of A-SBCE are currently working on an improved implementation of this feature.

2.3. Support

For technical support on Frontier SIP Trunking, contact Frontier as follows:

- Use the Technical Support link for business customers at http://www.frontier.com, or
- Call the business customer support number at 877-462-8188 (for former Verizon customers) or 800-921-8102 (for other Frontier customers).

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the Frontier SIP Trunking (using a Frontier lab test circuit) through a public Internet WAN connection.

For security purposes, any actual public IP addresses used in the compliance test are masked in these Application Notes with the 3rd and 4th octet in the IP address replaced by **x** (e.g., 74.40.x.x and 135.10.x.x).

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

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

NOTE: This Application Notes document is applicable with Avaya Aura® 6.2 which is currently in Controlled Introduction. Avaya Aura® 6.2 will be Generally Available in summer 2012.

Located at the edge of the enterprise is the Avaya SBC for Enterprise. It has a public interface that connects to the external network and a private interface that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through this enterprise SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The transport protocol between the enterprise SBC and Frontier across the public IP network is UDP; the transport protocol between the enterprise SBC and Session Manager across the enterprise IP network is TCP.

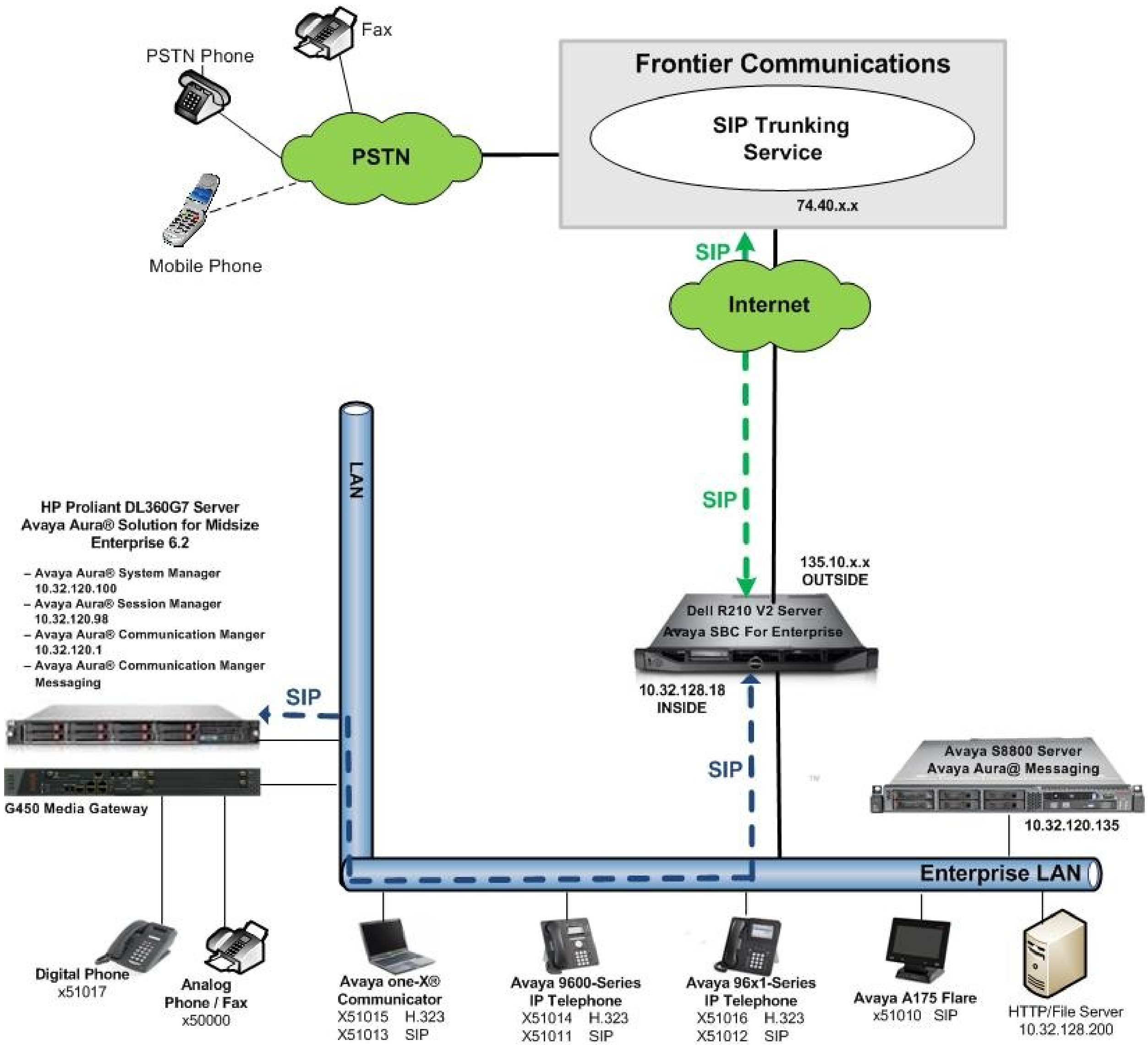


Figure 1: Avaya SIP Enterprise Solution Using Frontier Communications SIP Trunking

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

For inbound calls, the calls flow from the service provider to Avaya SBC for Enterprise then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case the Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound feature treatment such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to Avaya SBC for Enterprise. From the enterprise SBC, the call is sent to Frontier SIP Trunking through the public IP network.

The compliance test used Communication Manager Messaging for testing DTMF with voice messaging since the Avaya Aura® Solution for Midsize Enterprise 6.2 includes this voice messaging component. Other voice messaging application such as Avaya Aura® Messaging (as depicted in **Figure 1**) could have been used.

The compliance test used Communication Manager Messaging for testing voice mail access/navigation and MWI (Messaging Wait Indicator) on Avaya enterprise phones. Communication Manager Messaging was chosen since Avaya Aura® Solution for Midsize Enterprise 6.2 includes this voice messaging component. Other voice messaging application such as Avaya Aura® Messaging (as depicted in **Figure 1**) could have been used to satisfy this test purpose instead of Communication Manager Messaging.

The administration of Communication Manager Messaging and endpoints on Communication Manager are standard. Since the configuration tasks for Communication Manager Messaging and endpoints are not directly related to the inter-operation with Frontier SIP Trunking service, they are not included in these Application Notes.

4. Equipment and Software Validated

Avaya IP Telephony Solution Components	
Equipment/Software	**Release/Version**
Avaya Aura® Solution for Midsize Enterprise 6.2 running on HP Proliant DL360G7 Server • Avaya Aura® Communication Manager • Avaya Aura® Communication Manager Messaging • Avaya Aura® Session Manager • Avaya Aura® System Manager	 6.2 (R016x.02.0.823.0-19593) 6.2-22.0 (CMM-02.0.823.0-0002) 6.2.1.0.621010 6.2.0-SP1 (6.2.13.1.1871)
Avaya G450 Media Gateway	31.22.0
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.104S
Avaya 9620 IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 2.6.6
Avaya 9611 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.0 SP5
Avaya 9621 IP Telephone (SIP)	Avaya one-X® Deskphone Edition 6.0 SP3
Avaya A175 Flare™ Desktop Video Device (SIP telephone function)	SIP Version 1.1.0 (SIP_A175_1_1_0_012004)
Avaya one-X Communicator (H.323 & SIP)	6.1.3.09-SP3-Patch3-35953
Avaya 8410D Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Fax device	Ventafax Home Version 6.1.59.144
Avaya Session Border Controller for Enterprise running on Dell R210 V2 Server	4.0.5.Q09
Frontier SIP Trunking Components	
Equipment/Software	**Release/Version**
Acme Packet NET-NET SBC	6.2m8p4
Metaswitch CFS Soft Switch	7.3.0.00

The specific hardware and software listed in the table above were used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for Frontier SIP Trunking. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from Frontier. It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and Session Manager has been previously completed and is not discussed here.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the public IP addresses shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements 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 275 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 2
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 2
                       Maximum Administered SIP Trunks: 12000 275
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. System Features

Use the **change system-parameters feature** 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 values of ***anonymous*** for restricted and unavailable calls.

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

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

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

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

SCCAN PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses for Communication Manager ***(procr***) and Session Manager (***SM***). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM                  10.32.120.98
default             0.0.0.0
nwk-aes1            10.32.120.3
procr               10.32.120.1
procr6              ::
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 5 was used for this purpose. Frontier SIP Trunking supports G.729A and G.711MU. Thus, these codecs were included in this set. Enter ***G.729A*** and ***G.711MU*** in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

```
change ip-codec-set 5                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 5

    Audio        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 5                                           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
    Clear-channel   n                     0
```

5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 5 was chosen for the service provider trunk. Use the **change ip-network-region 5** command to configure region 5 with the following parameters:

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

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

On **Page 4**, define the IP codec set to be used for traffic between region 5 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 5 will be used for calls between region 5 (the service provider region) and region 1 (the rest of the enterprise).

```
change ip-network-region 5                                      Page   4 of  20

 Source Region: 5     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 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    5     y    NoLimit                                             n       t
 2
 3
 4
 5    5                                                                all
```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 5 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). This is necessary for Session Manager to distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to ***5261***.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer-Server** field will initially be set to ***Others*** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to ***SM*** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***SM*** This node name maps to the IP address of Session Manager as defined in **Section 5.3**

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completion.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to ***15***. This defines the number of seconds the Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before canceling the call.
- Set Initial **IP-IP Direct Media** to ***n***. See the **DTMF Payload** and **Call Forward on No Answer** bullet items in the test observation list in **Section 2.2** for explanation on this setting.
- Default values may be used for all other fields.

```
change signaling-group 5                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 5             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                  Far-end Node Name: SM
 Near-end Listen Port: 5261                 Far-end Listen Port: 5261
                                         Far-end Network Region: 5
                                   Far-end Secondary Node Name:
Far-end Domain: sip.avaya.com
                                              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): 15
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 5 was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***public-ntwrk***.
- Set **Member Assignment Method** to ***auto***.
- Set the **Signaling Group** to the signaling group created in **Section 5.6**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 5                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 5                    Group Type: sip          CDR Reports: y
  Group Name: AC SP Trunk                 COR: 1        TN: 1        TAC: *05
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 5
                                                     Number of Members: 10
```

On **Page 2**, set the **Redirect On OPTIM Failure** timer to the same amount of time as the **Alternate Route Timer** on the signaling group form in **Section 5.6**. Note that the **Redirect On OPTIM Failure** timer is defined in milliseconds. Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of ***600*** seconds was used.

```
add trunk-group 5                                               Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 15000

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

On **Page 3**, set the **Numbering Format** field to ***private***. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. The compliance test used 10 digit numbering format. Thus, **Numbering Format** was set to **private** and the **Numbering Format** field in the route pattern was set to ***unk-unk*** (see **Section 5.9**).

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

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


                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y


                                Modify Tandem Calling Number: no


 Show ANSWERED BY on Display? y

 DSN Term? n
```

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

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

```
add trunk-group 5                                                  Page   4 of  21
                              PROTOCOL VARIATIONS

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


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

5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs). It is used to authenticate the caller.

The screen below shows a subset of the DID numbers assigned for testing. These 4 numbers were mapped to the 4 enterprise extensions 51011, 51012, 51014 and 51016. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 4 extensions.

```
change private-numbering 0                                       Page   1 of   2
                              NUMBERING - PRIVATE FORMAT

Ext Ext              Trk         Private            Total
Len Code             Grp(s)      Prefix             Len
 0  attd                         0                  1      Total Administered: 21
 5  1                                               5         Maximum Entries: 540
 5  2                                               5
 5  3                                               5
 5  4                                               5
 5  5                                               5
 5  6                                               5
 5  7                                               5
 5  8                                               5
 5  51011            5           5853515307         10
 5  51012            5           5853515306         10
 5  51014            5           5853515308         10
 5  51016            5           5853515305         10
```

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 5 will send the calling party number as the **Private Prefix** plus the extension number.

```
change private-numbering 0                                       Page   1 of   2
                              NUMBERING - PRIVATE FORMAT

Ext Ext              Trk         Private            Total
Len Code             Grp(s)      Prefix             Len
 5  5                                                5     Total Administered: 10
 5  5                 5            90633             10       Maximum Entries: 540
```

5.9. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an "outside line". This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 9 of length 1 as a feature access code (**fac**).

```
change dialplan analysis                                        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  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *10
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *14
                      Announcement Access Code: *19
                       Answer Back Access Code:

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

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 5 which contains the SIP trunk to the service provider (as defined next).

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

          Dialed          Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
    0                    1    1     5        op           n
    0                    8    8     deny     op           n
    0                    11   11    4        op           n
    00                   2    2     deny     op           n
    01                   9    17    deny     iop          n
    011                  10   18    5        intl         n
    1732                 11   11    5        fnpa         n
    1800                 11   11    5        fnpa         n
    1877                 11   11    5        fnpa         n
    1908                 11   11    5        fnpa         n
    411                  3    3     5        svc1         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 5 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group ***5*** was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.
- **Pfx Mrk**: The prefix mark (**Pfx Mrk**) of ***1*** will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.

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

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

6. Configure Avaya Aura® Session Manager

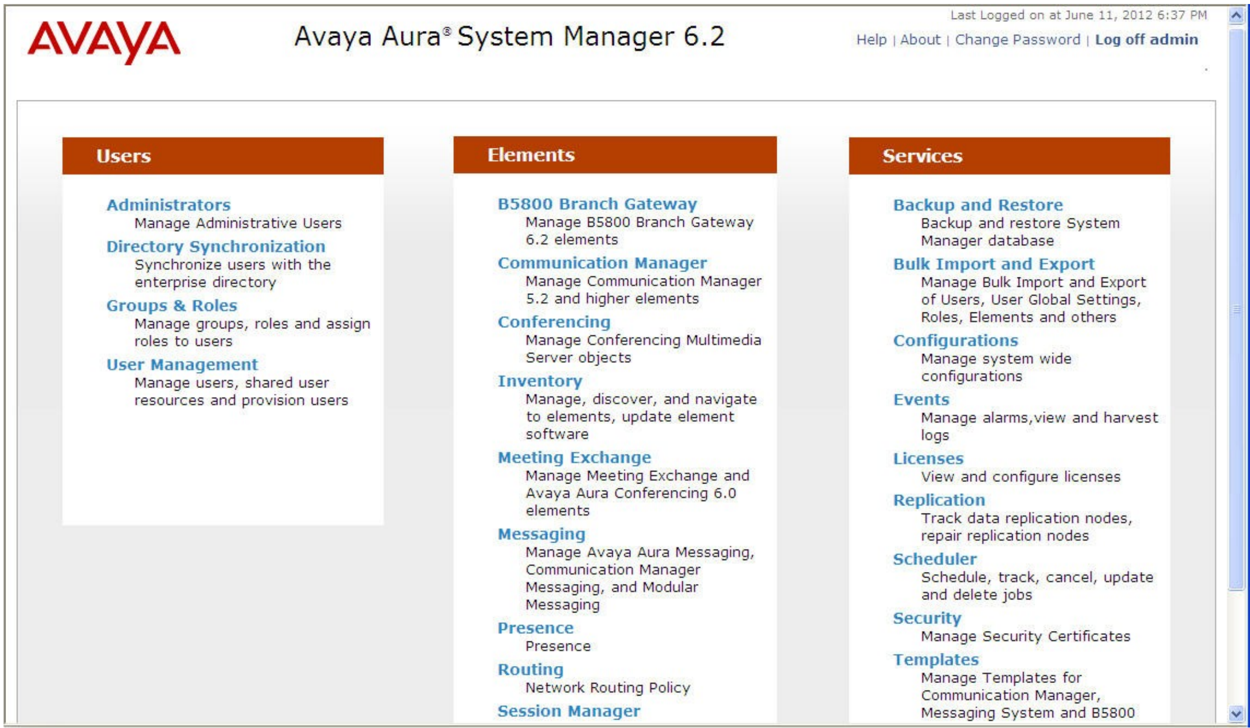
This section provides the procedures for configuring Session Manager. The procedures include the following items:

- Specify SIP domain
- Add logical/physical Location that can be occupied by SIP Entities at the enterprise site
- Add Adaptation module to perform dial plan manipulation
- Add SIP Entities corresponding to Communication Manager, Avaya SBC for Enterprise and Session Manager
- Add Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Add Routing Policies, which define route destinations and control call routing between the SIP Entities
- Add Dial Patterns, which specify dialed digits and govern to which SIP Entity a call is routed
- Add/View Session Manager, corresponding to the Session Manager to be managed by System Manager.

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

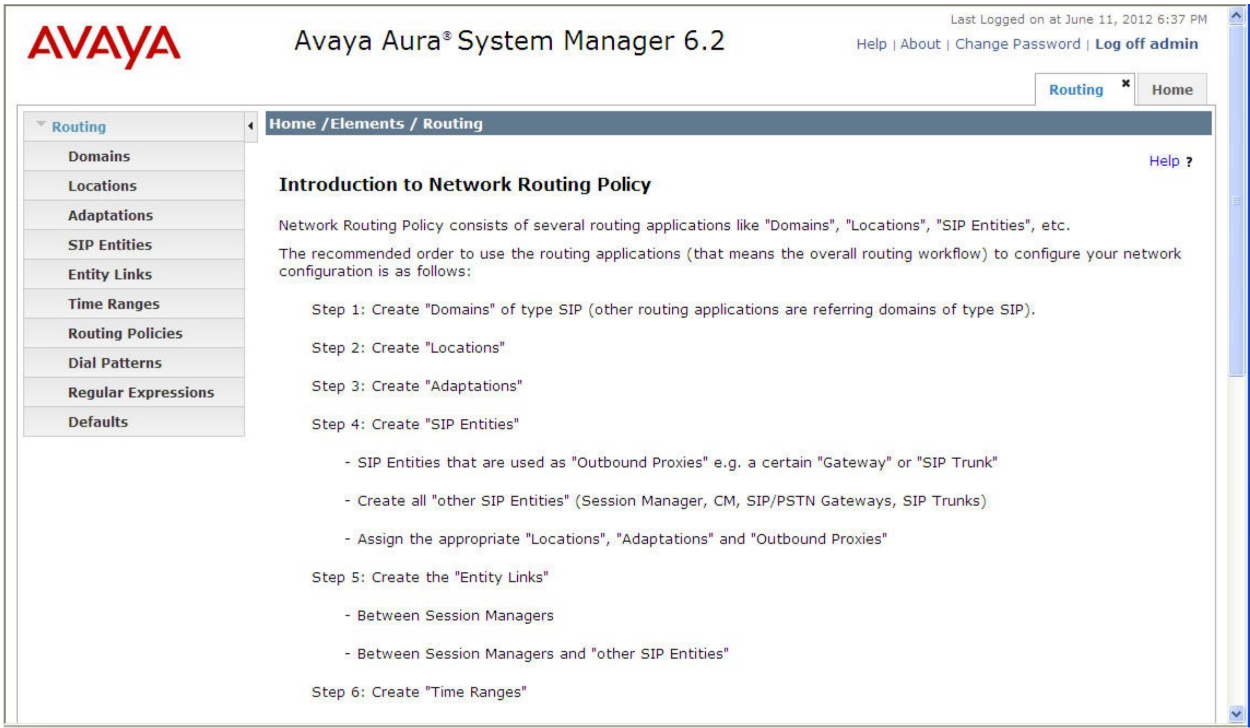
6.1. System Manager Login and Navigation

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



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

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

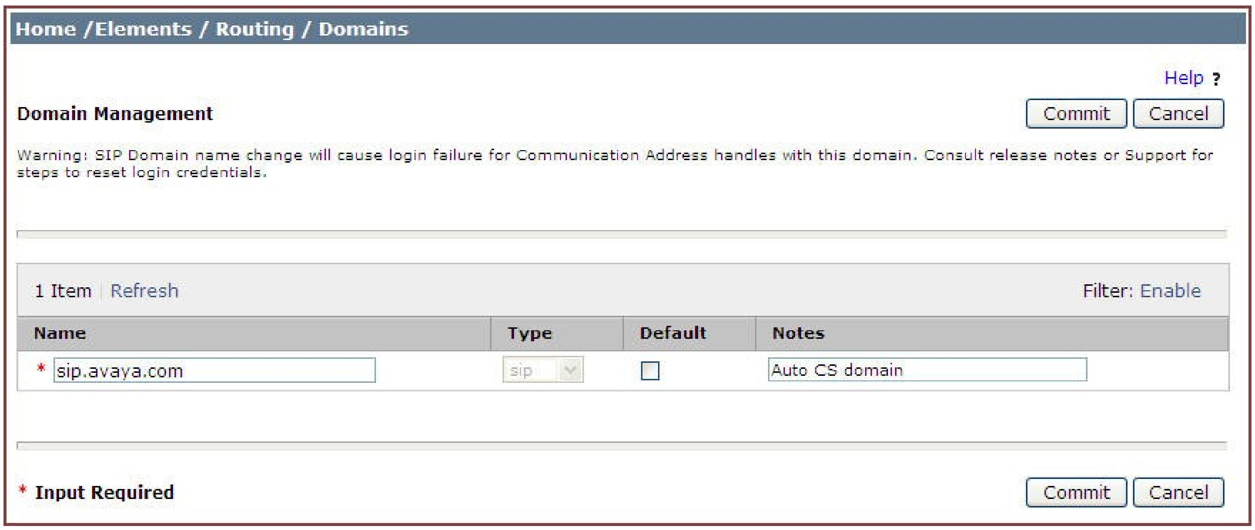


6.2. Specify SIP Domain

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

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

Click **Commit**. The screen below shows the entry for the enterprise domain.



6.3. Add Location

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

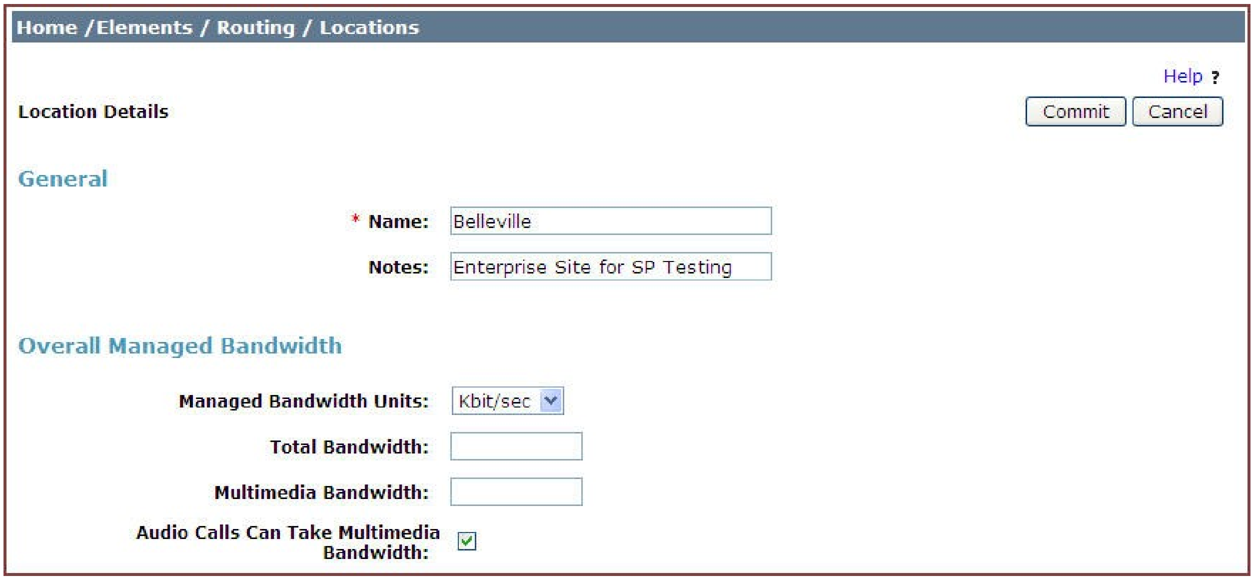
In the **General** section, enter the following values:

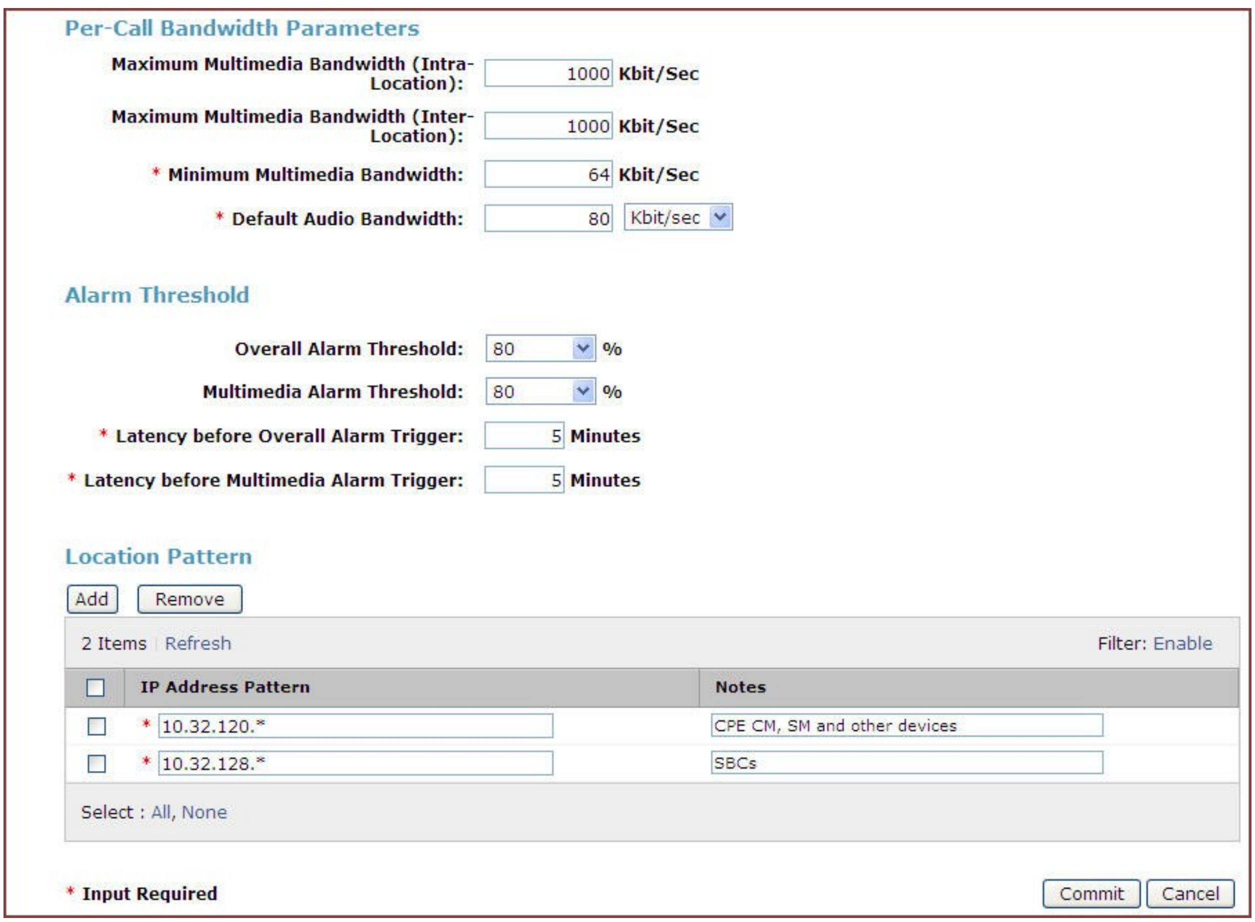
- **Name:** Enter a descriptive name for the Location.
- **Notes:** Add a brief description (optional).

In the **Location Pattern** section (see 2nd screen below), click **Add** and enter the following values:

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

Displayed below are the top and bottom halves of the screen for addition of the ***Belleville*** Location, which includes all equipment on the enterprise network. Click **Commit** to save.





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

6.4. Add Adaptation Module

Session Manager can be configured with Adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic Adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other Adaptation modules are built on this generic, and can modify other headers to permit interoperability with third party SIP products.

For interoperability with Frontier SIP Trunking, one Adaptation is needed. This Adaptation is applied to the Communication Manager SIP Entity and maps inbound DID numbers from Frontier to local Communication Manager extensions.

To create an Adaptation, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

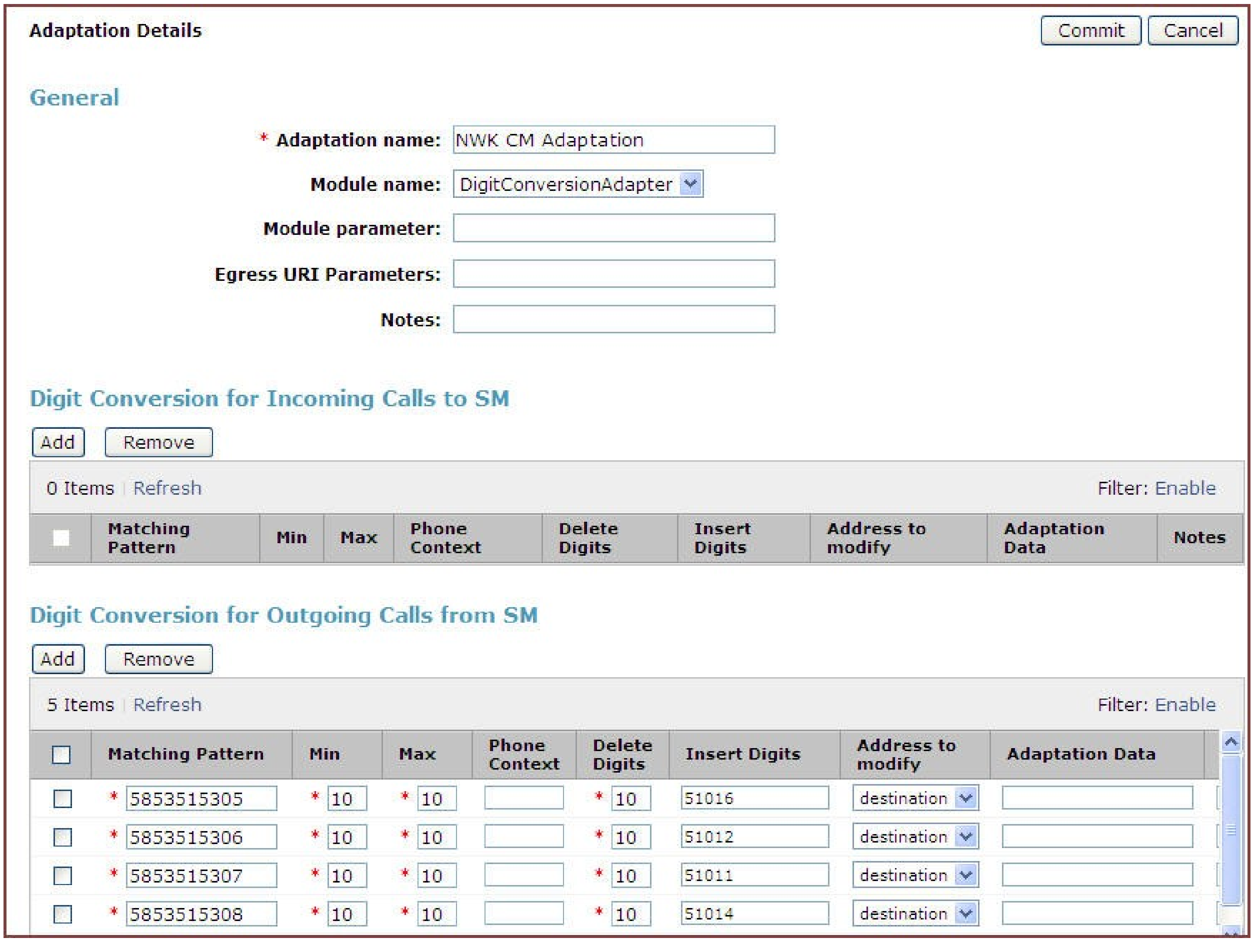
In the **General** section, enter the following values. Use default values for all remaining fields:

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter ***DigitConversionAdapter***

To map inbound DID numbers from Frontier to Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DID to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields:

- **Matching Pattern:** Enter a digit string used to match the inbound DID number.
- **Min:** Enter a minimum dialed number length used in the match criteria.
- **Max:** Enter a maximum dialed number length used in the match criteria.
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number.
- **Insert Digits:** Enter the number of digits to insert at the beginning of the received number.
- **Address to modify:** Select ***destination***.

Click **Commit** to save.



Adaptation Details

Commit | Cancel

General

* Adaptation name: NWK CM Adaptation

Module name: DigitConversionAdapter

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add | Remove

0 Items | Refresh — Filter: Enable

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

Digit Conversion for Outgoing Calls from SM

Add | Remove

5 Items | Refresh — Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
	* 5853515305	* 10	* 10		* 10	51016	destination	
	* 5853515306	* 10	* 10		* 10	51012	destination	
	* 5853515307	* 10	* 10		* 10	51011	destination	
	* 5853515308	* 10	* 10		* 10	51014	destination	

In the example shown above, if a user on the PSTN dials 585-351-5306, Session Manager will convert the number to 51012 before sending out the SIP INVITE to Communication Manager. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the DID number to its corresponding extension. For an outbound call, the Communication Manager private-numbering form was configured with an entry to convert 51012 to 5853515306 before sending the call on the trunk group to Session Manager (as shown in **Section 5.8**).

During the compliance test, the digit conversions (or number mappings) in Session Manager Adaptation as well as in private-numbering table on Communication Manager were varied to route inbound calls to various destinations (including access number to Communication Manager Messaging and Communication Manager Vector Directory Numbers) for different test cases.

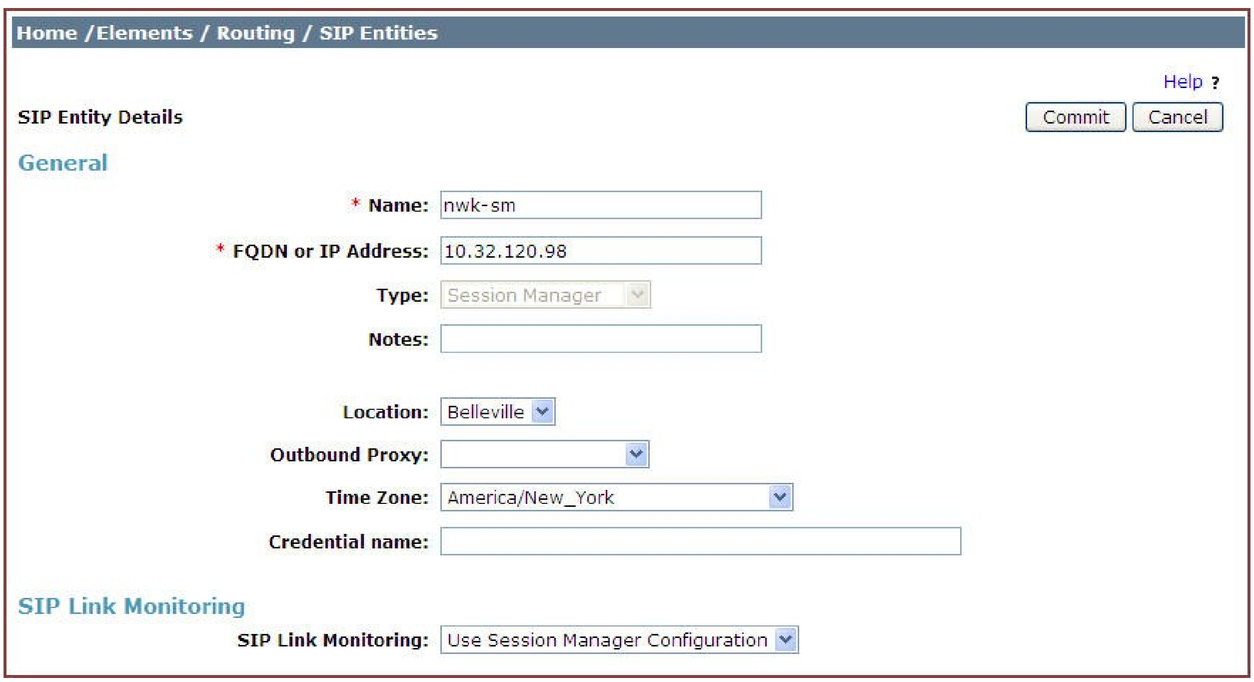
6.5. Add SIP Entities

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

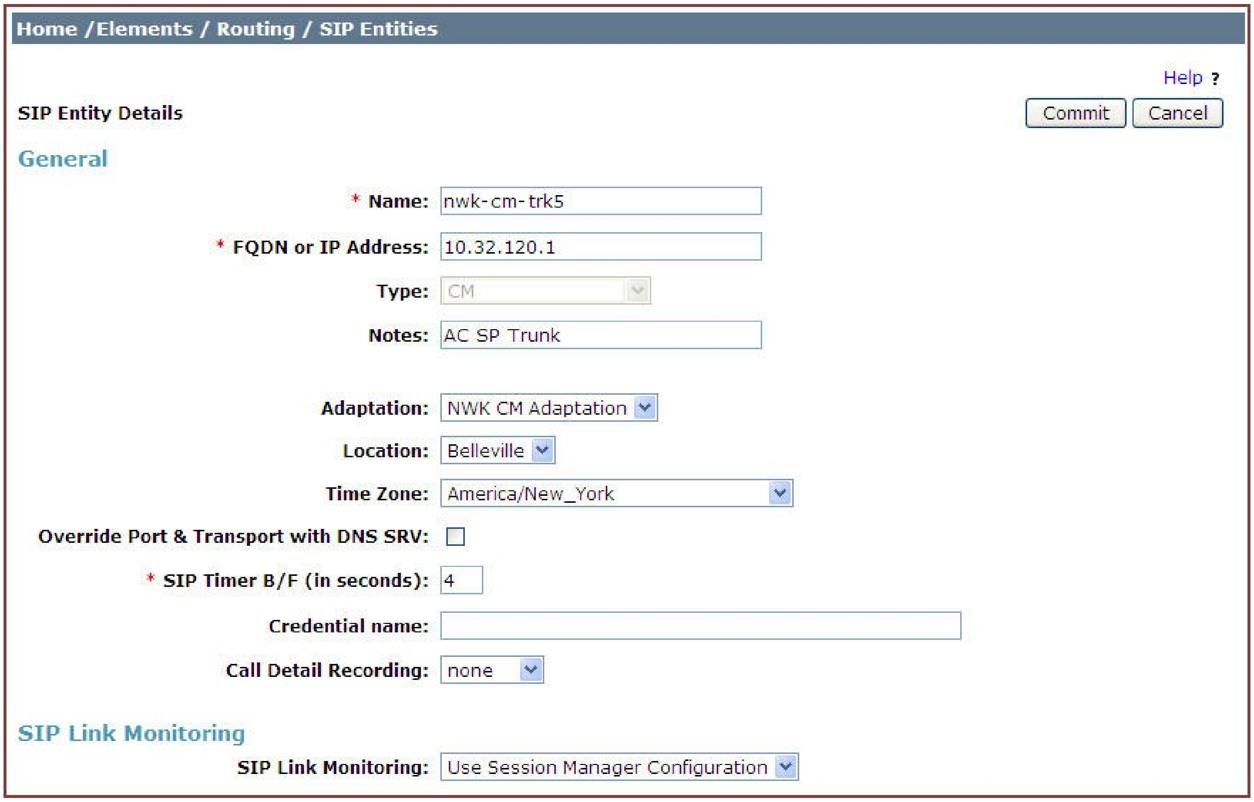
In the **General** section, enter the following values. Use default values for all remaining fields:

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

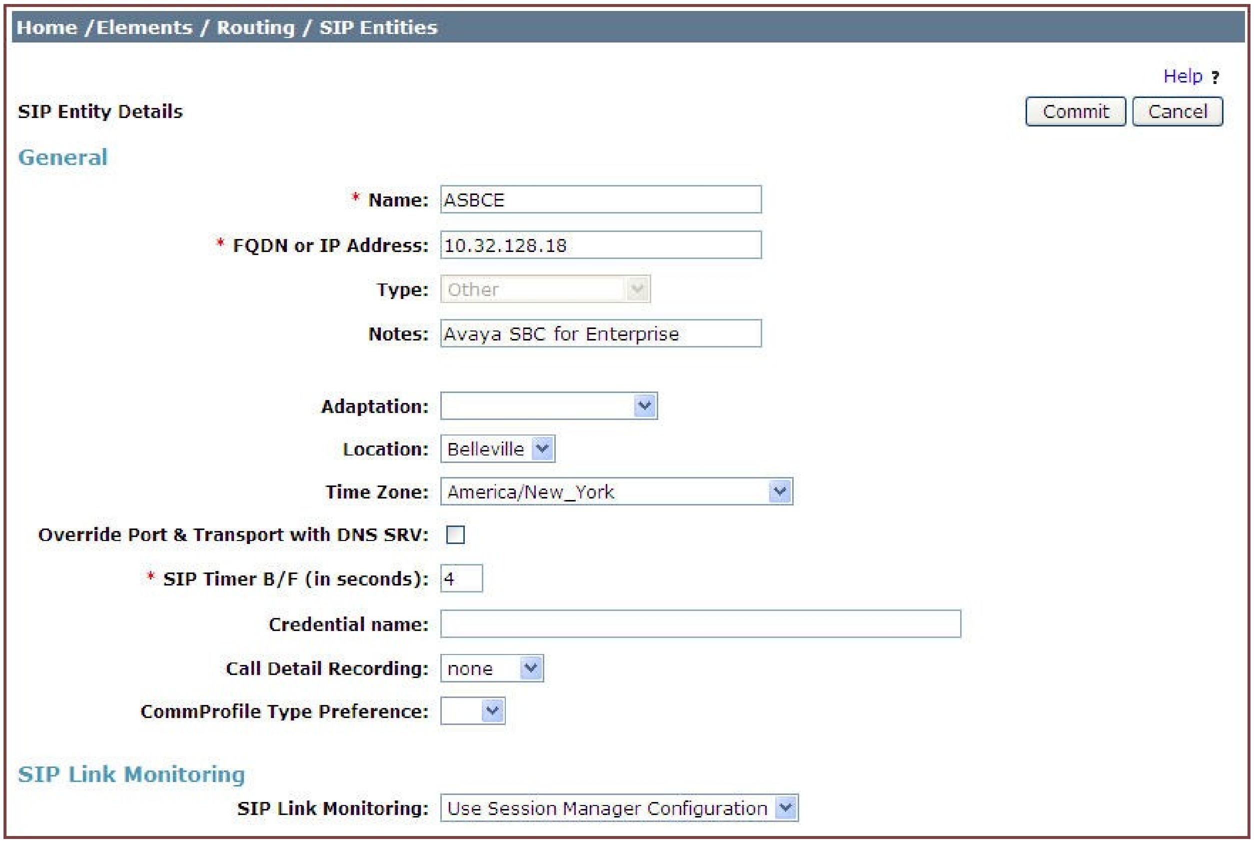
The following screen shows the addition of the Session Manager SIP Entity. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.



The following screen shows the addition of the Communication Manager SIP Entity. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created at Session Manager installation for use with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of Communication Manager. For the **Adaptation** field, select the Adaptation module previously defined for digit manipulation in **Section 6.4**.



The following screen shows the addition of the SIP Entity for Avaya SBC for Enterprise. The **FQDN or IP Address** field is set to the IP address of the SBC's inside network interface (see **Figure 1**).



6.6. Add Entity Links

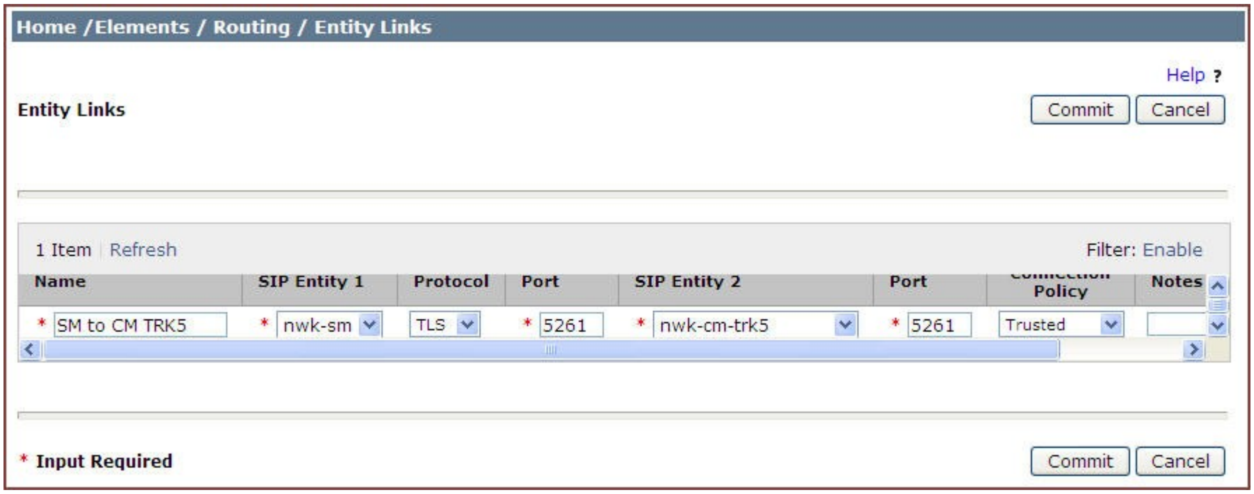
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to Communication Manager for use only by service provider traffic and the other to Avaya SBC for Enterprise. To add an Entity Link, navigate to **Routing → Entity Links** in the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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager SIP Entity.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied.*

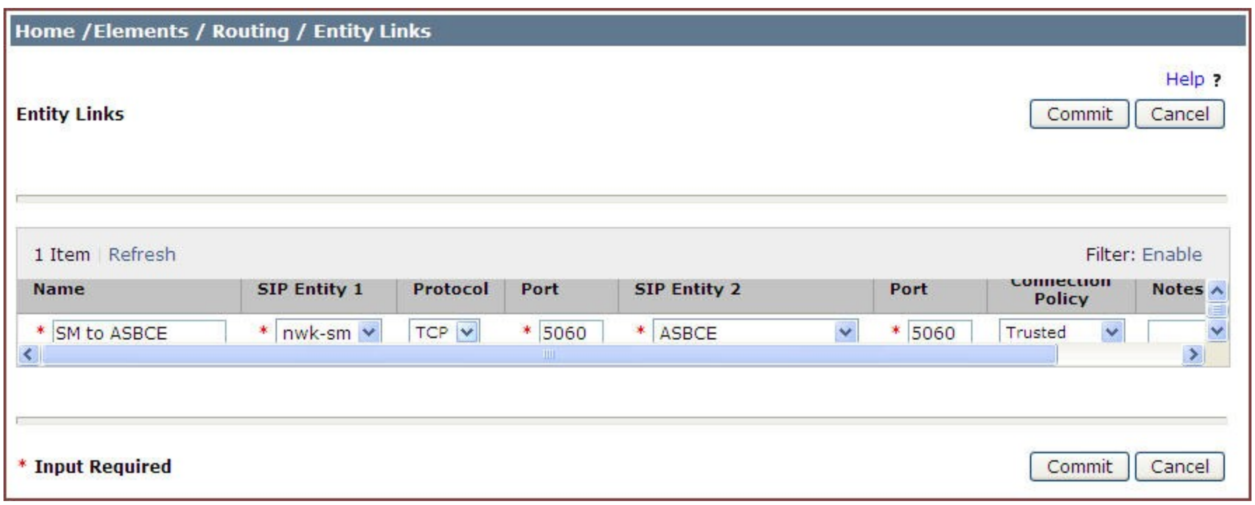
Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and Avaya SBC for Enterprise. It should be noted that in a customer environment the Entity Link to Communication Manager would normally use TLS. TCP can be used to aid in troubleshooting since the signaling traffic would not be encrypted. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.

Entity Link to Communication Manager:



Entity Link to Avaya SBC for Enterprise:



Note that a separate Entity Link existed between Communication Manager and Session Manager using port 5061 and TLS (not shown) for carrying SIP traffic between Session Manager and Communication Manager that is not necessarily related to calls to and from the service provider, such as traffic related to SIP Telephones registered to Session Manager, or traffic related to Communication Manager Messaging, which has SIP integration to Session Manager.

6.7. Add Routing Policies

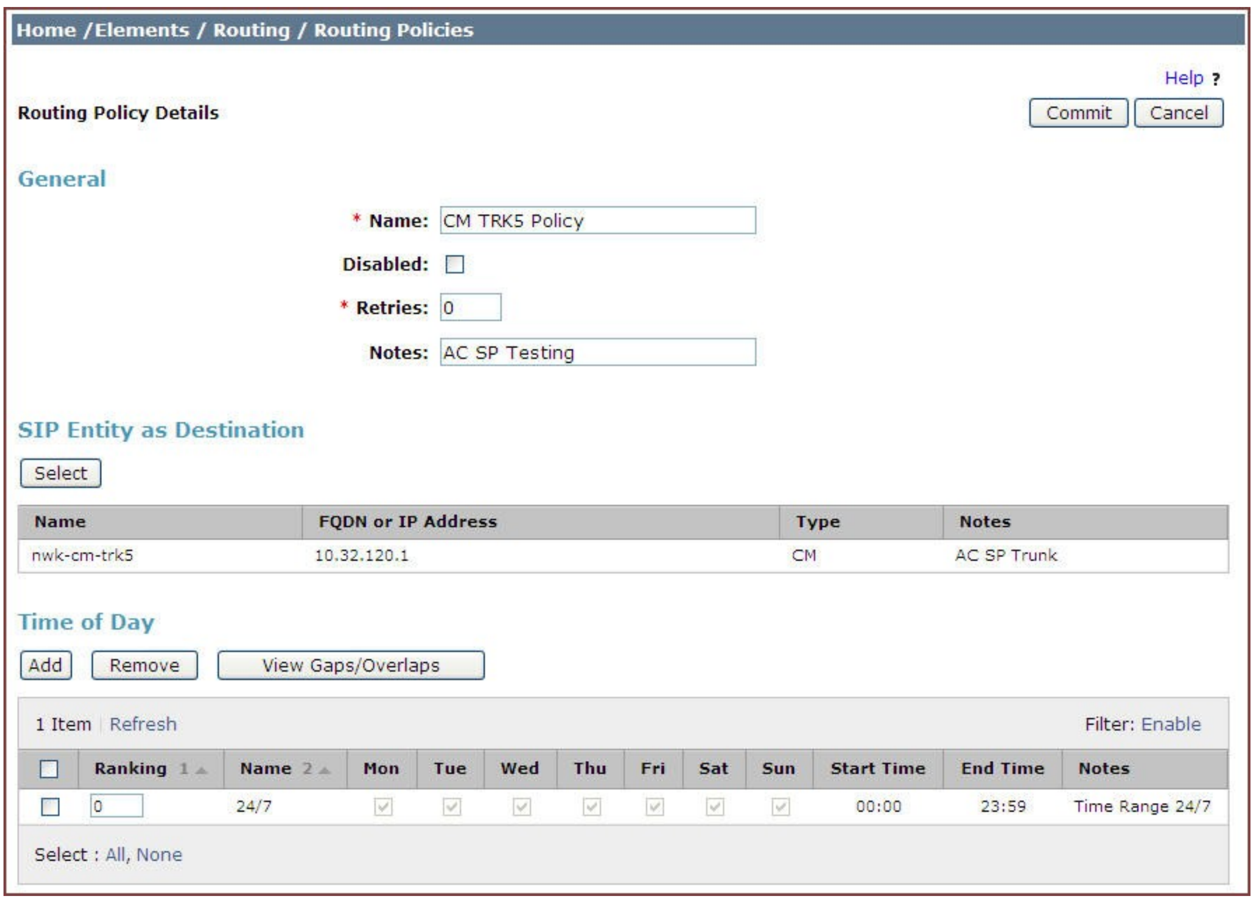
Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two Routing Policies must be added: one for Communication Manager and the other for Avaya SBC for Enterprise. To add a routing policy, navigate to **Routing → Routing Policies**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

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

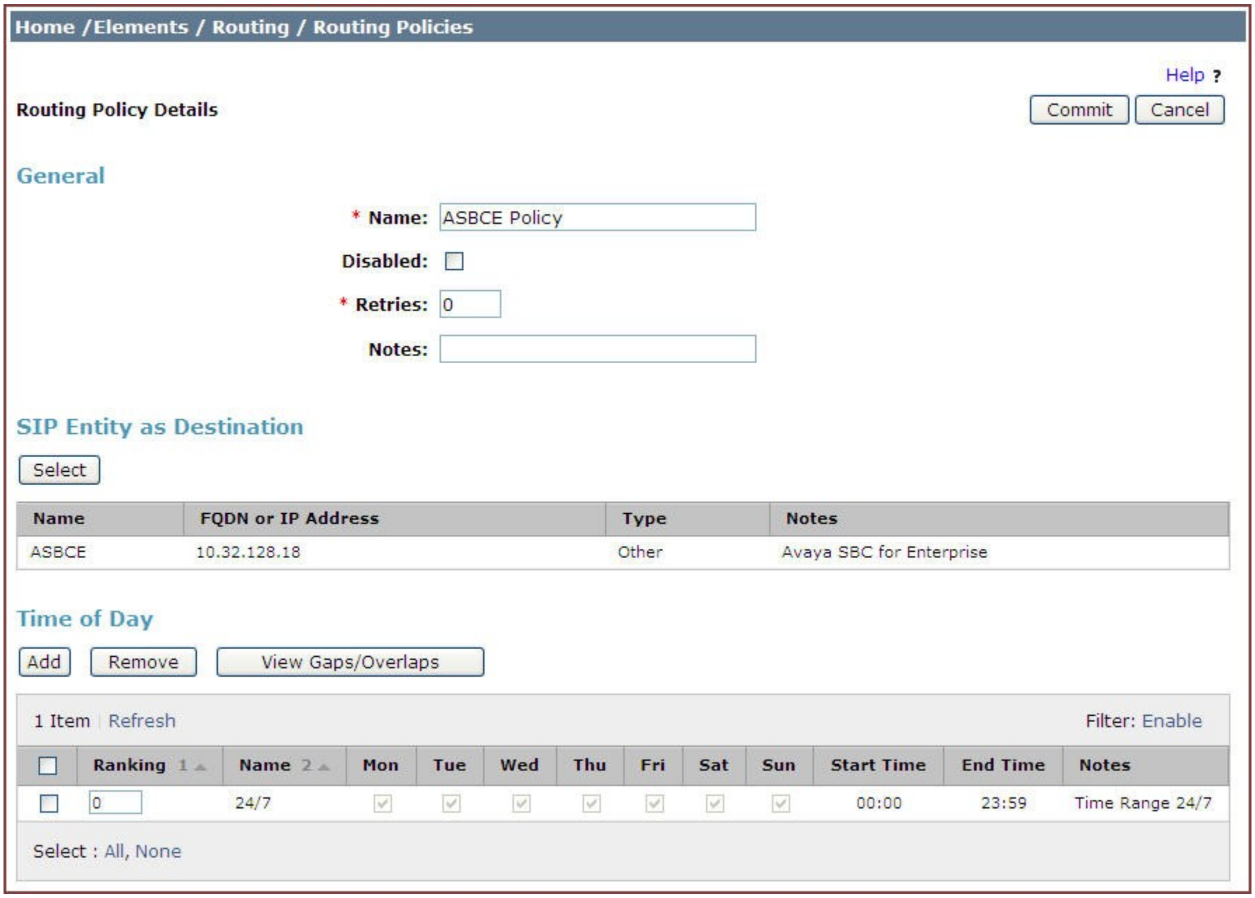
- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

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

Routing Policy for Communication Manager:



Routing Policy for Avaya SBC for Enterprise:



6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were needed to route calls from Communication Manager to Frontier and vice versa. Dial Patterns specifies which Routing Policy (that defines the route destination) will be selected for a particular call based on the dialed digits, destination SIP Domain and originating Location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

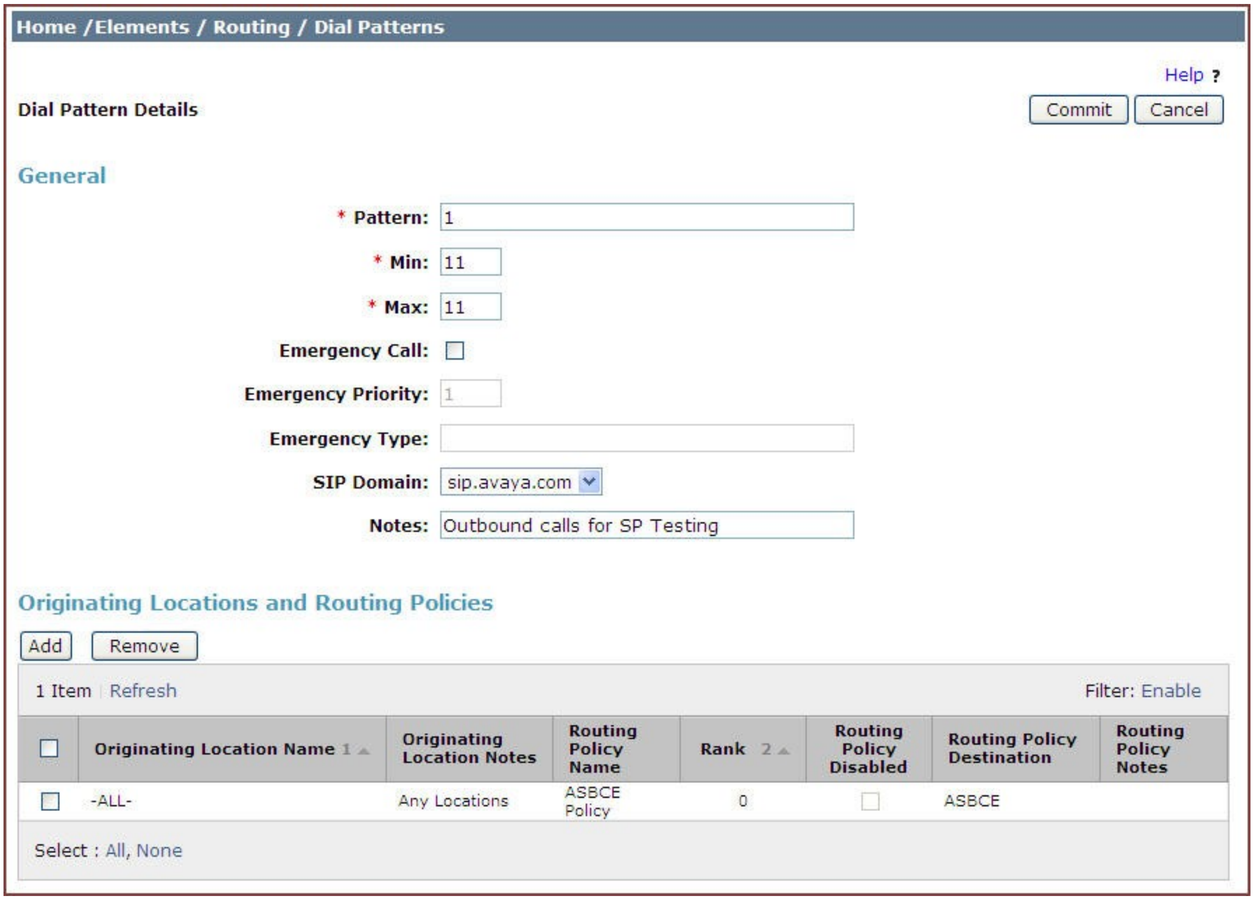
- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination SIP Domain used in the match criteria.
- **Notes:**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

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

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

Two examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other Dial Patterns (e.g., 411 directory assistance call, etc.) were similarly defined.

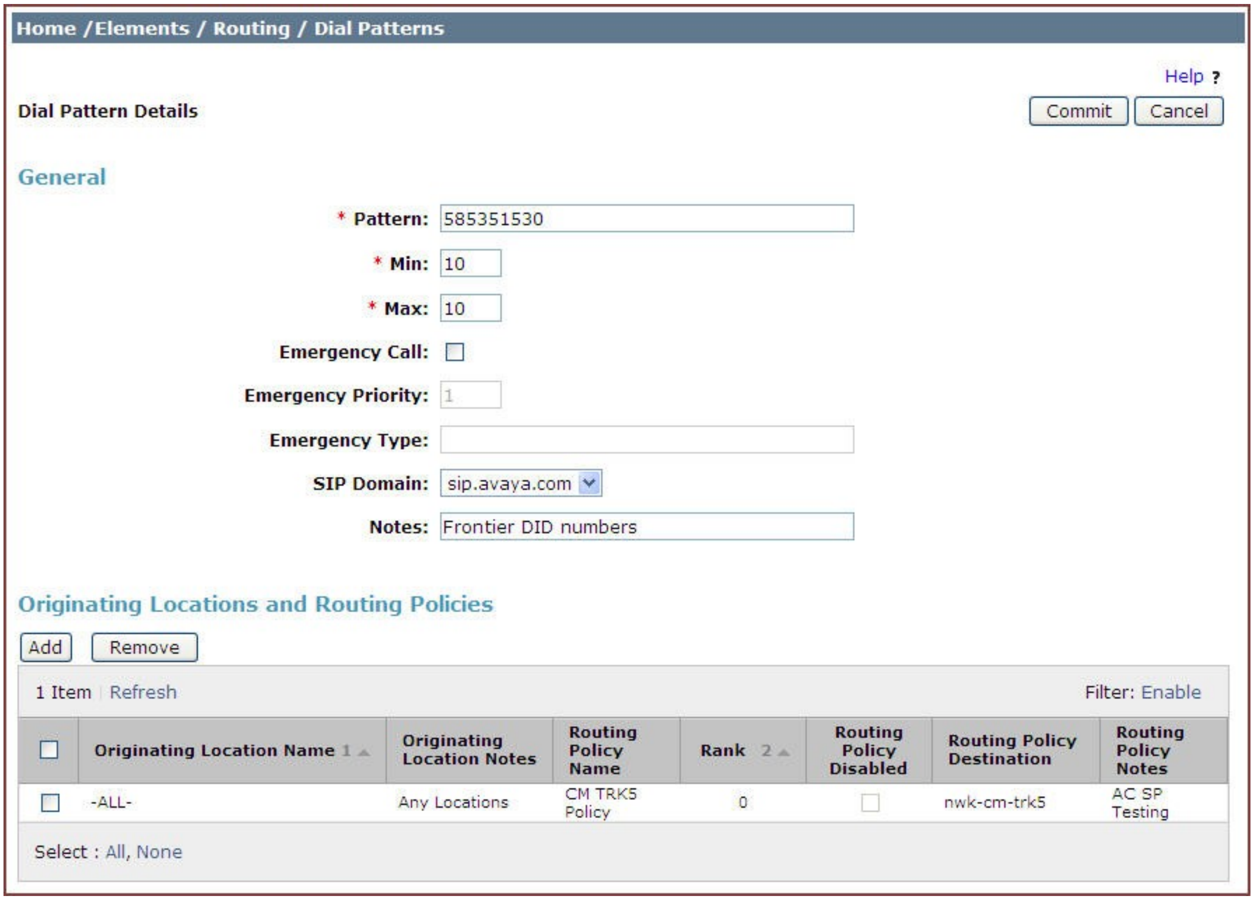
The first example shows that 11-digit dialed numbers that begin with ***1*** and have a destination SIP Domain of ***sip.avaya.com*** uses the ***ASBCE Policy*** Routing Policy as defined in **Section 6.7**.



Note that the compliance test did not restrict outbound calls to specific US area codes. In real deployments, appropriate restriction can be exercised (e.g., use Dial Pattern 1908, 1732, etc. with 11 digits) per customer business policies.

Also note that ***-ALL-*** was selected for Originating Location. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed outbound back to the PSTN. For straight-forward outbound calls, like 411 local directory call, the enterprise Location ***Belleville*** could have been selected.

The second example shows that inbound 10-digit numbers that start with ***585351530*** uses Routing Policy ***CM TRK5 Policy*** as defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by Frontier.



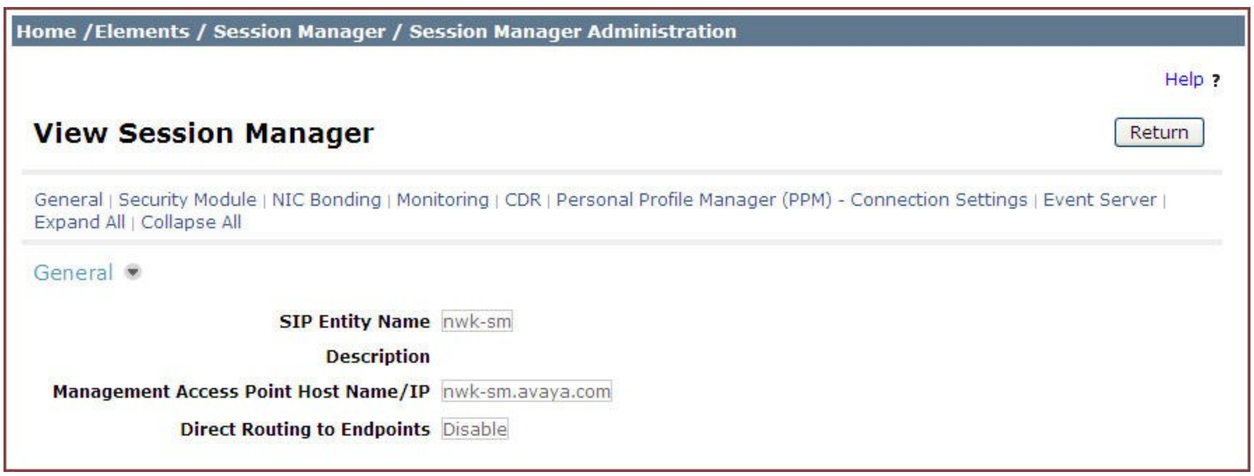
6.9. Add/View Session Manager

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

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

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

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

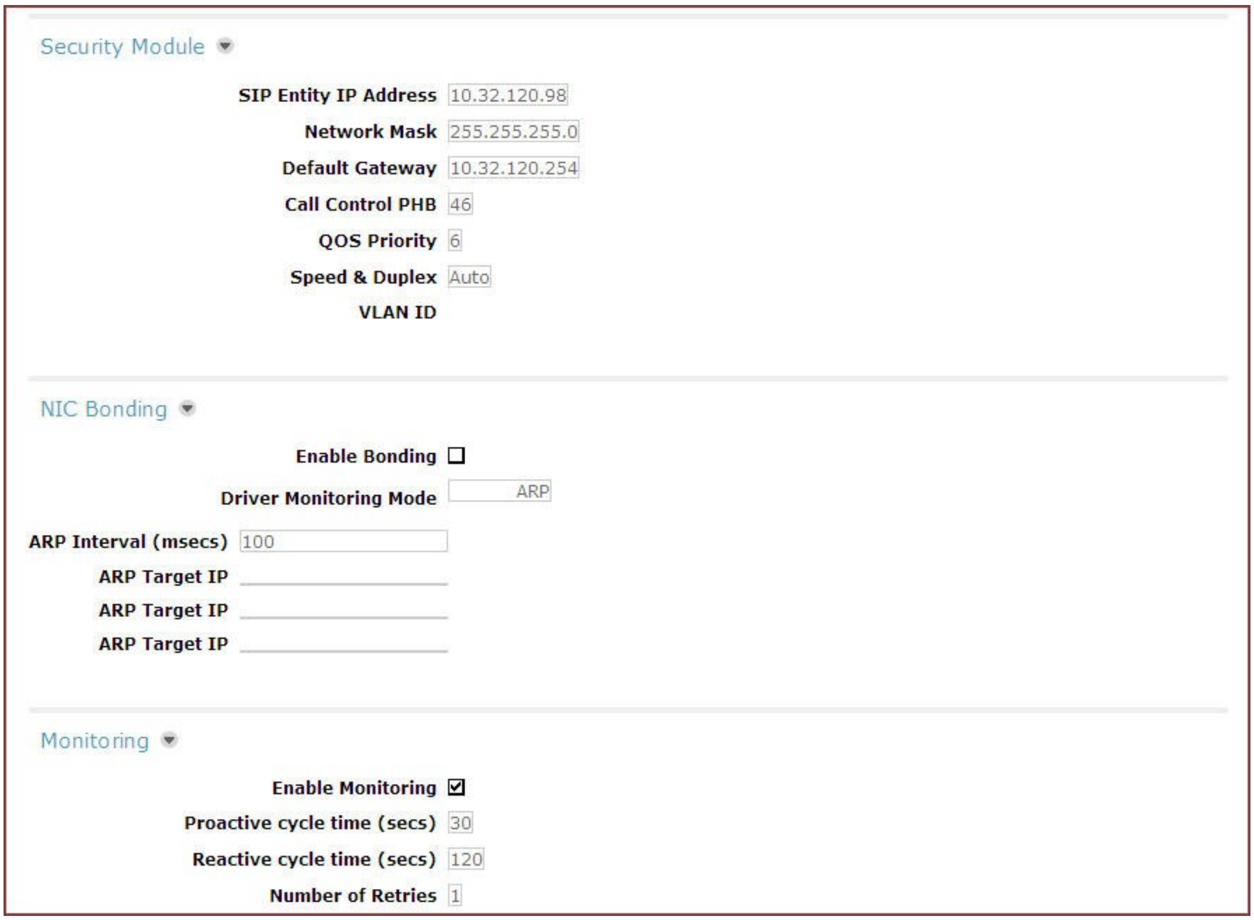


In the **Security Module** section, enter the following values:

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

In the **Monitoring** section, enter a desired value for **Proactive cycle time (secs)** which determines the interval at which Session Manager sends out OPTIONS message to the connected SIP Entities for checking reachability.

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



7. Configure Avaya Session Border Controller for Enterprise

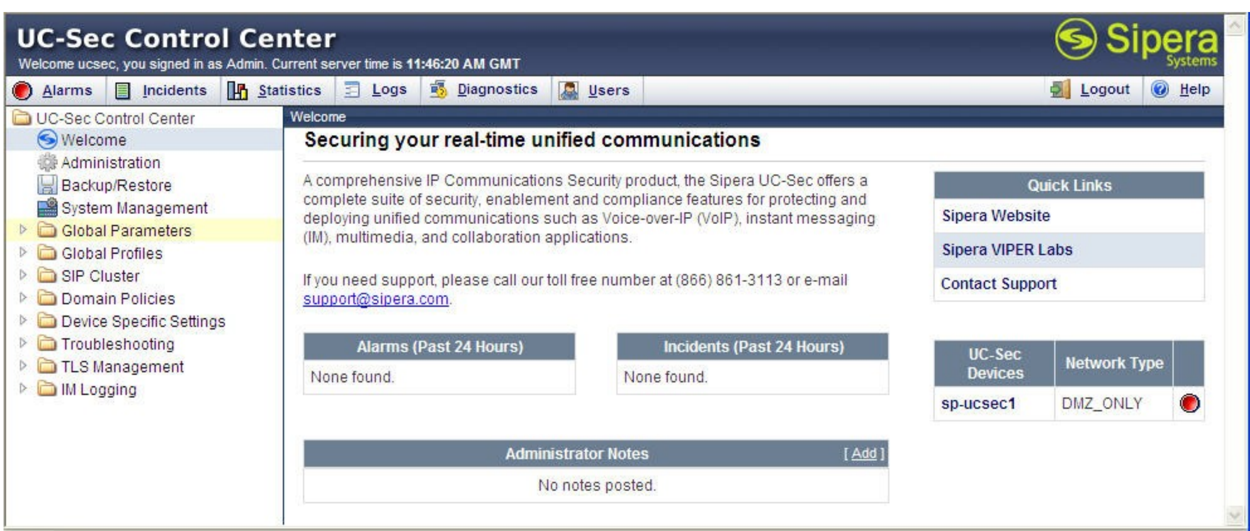
In the sample configuration, an Avaya SBC for Enterprise is used as the edge device between the Avaya CPE and Frontier SIP Trunking service.

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

7.1. Access Management Interface

Use a WEB browser to access the web management interface of A-SBCE by entering URL https://<ip-addr>, where <ip-addr> is the management LAN IP address assigned during installation. Select **UC-Sec Control Center** on the displayed web page, and log in using proper login credentials (not shown).

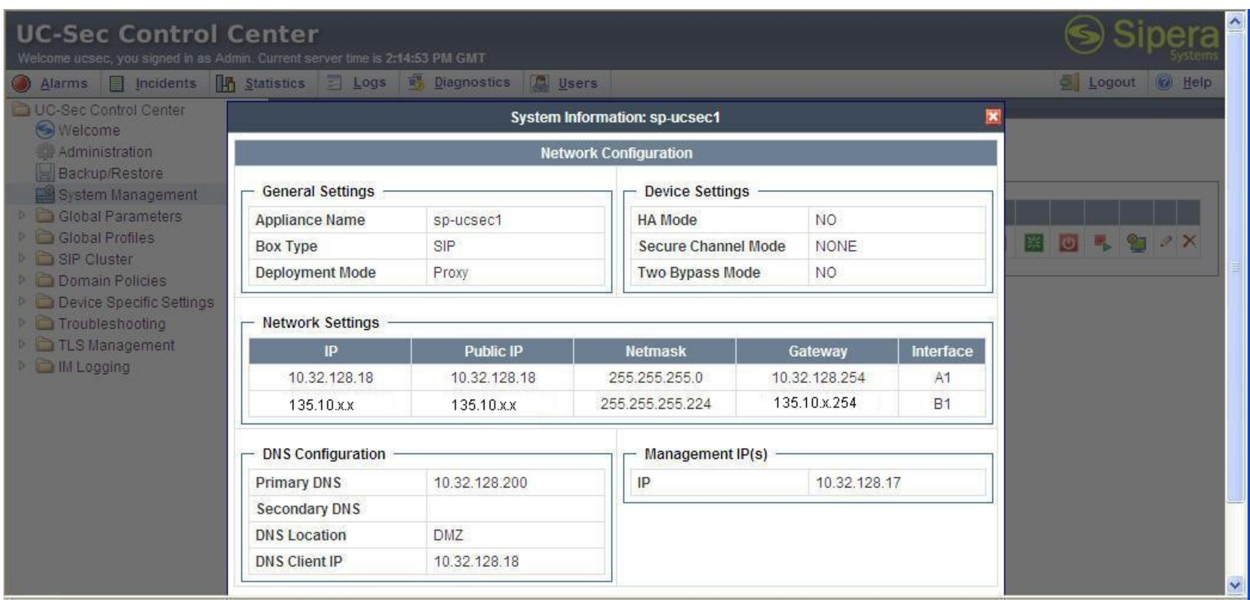
Once logged in, a Welcome screen will be presented. The following image illustrates the menu items available on the left-side of the UC-Sec Control Center screen.



7.2. System Status

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 ***sp-ucsec1*** is shown. Device **Status** "Commissioned" should be displayed as shown below.

To view the network information of this device assigned during installation, click the **View Config** icon button (the third icon from the right). A **Network Configuration** window is displayed as shown below. Note that the A1 and B1 interface IP addresses correspond to the inside and outside interface IP's for the A-SBCE as shown in **Figure 1**.



7.3. Global Profiles – Server Interworking

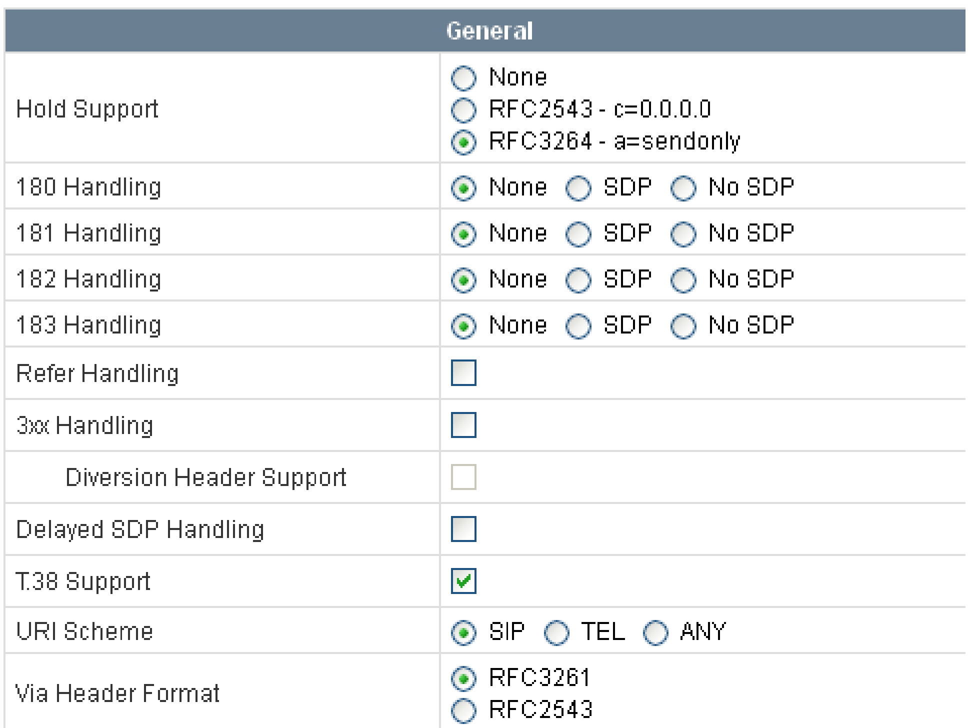
Server interworking is defined for each server connected to A-SBCE. For the compliance test, the Frontier network-edge SBC serves as the Trunk Server and the Session Manager serves as the Call Server.

Navigate to **Global Profiles → Server Interworking** to configure Server Interworking profiles.

7.3.1. Server Interworking: Avaya-SM

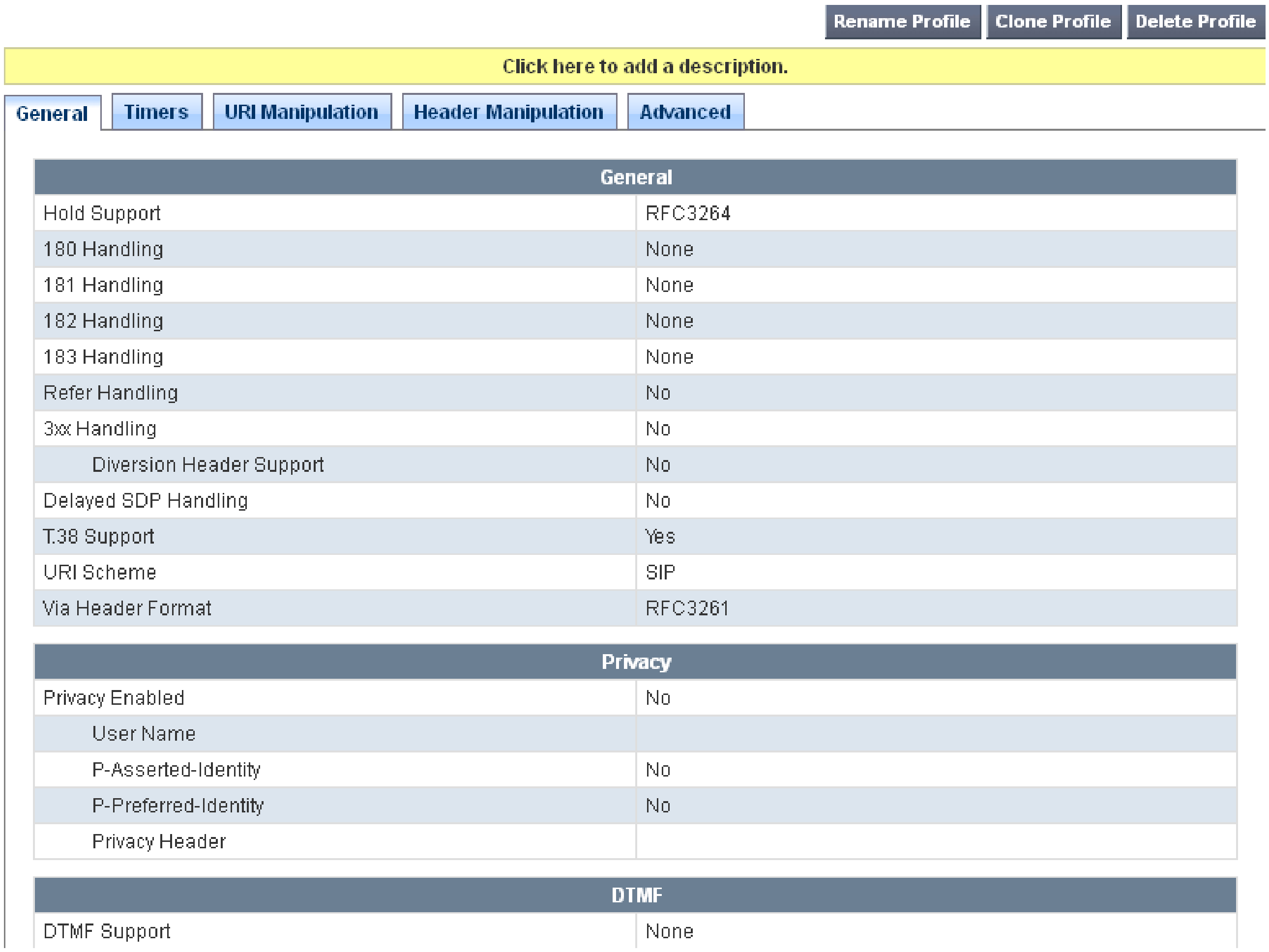
Click the **Add Profile** button (not shown) to add a new profile or select an existing Server Interworking profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as ***Avaya-SM*** shown below. Click **Next**.

The following screens illustrate the **General** parameters used in the sample configuration for the Interworking Profile named "Avaya-SM". Most parameters retain default values. In the sample configuration, **T.38 Support** was checked and **Hold Support** was set for ***RFC3264***.



General	
Hold Support	○ None ○ RFC2543 - c=0.0.0.0 ◉ RFC3264 - a=sendonly
180 Handling	◉ None ○ SDP ○ No SDP
181 Handling	◉ None ○ SDP ○ No SDP
182 Handling	◉ None ○ SDP ○ No SDP
183 Handling	◉ None ○ SDP ○ No SDP
Refer Handling	☐
3xx Handling	☐
Diversion Header Support	☐
Delayed SDP Handling	☐
T.38 Support	☑
URI Scheme	◉ SIP ○ TEL ○ ANY
Via Header Format	◉ RFC3261 ○ RFC2543

Click **Next** (not shown) to advance to configure **Privacy** and **DTMF** general parameters, which can retain default values. The following screen shows the complete **General** tab used in the sample configuration for Server Interworking profile named "Avaya-SM"



The parameters in all other tabs may retain default settings.

7.3.2. Server Interworking: SP-Frontier

A second Server Interworking profile named "SP-Frontier" was similarly created. The following screens illustrate the **General** parameters used in the sample configuration for the "SP- Frontier" Server Interworking profile. Most parameters retain default values. In the sample configuration, **T.38 Support** was set to ***Yes*** and **Hold Support** was set for ***RFC3264***.

General | Timers | URI Manipulation | Header Manipulation | Advanced

General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	
DTMF	
DTMF Support	None

Edit

The parameters in all other tabs may retain default settings.

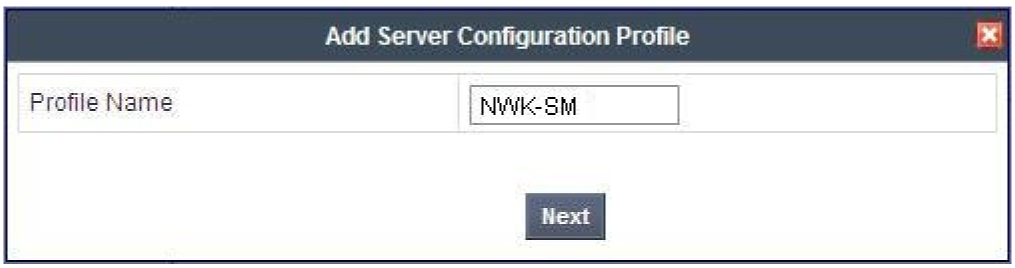
7.4. Global Profiles – Server Configuration

In the compliance test, the Frontier network-edge SBC is connected as the Trunk Server and the enterprise Session Manager is connected as the Call Server.

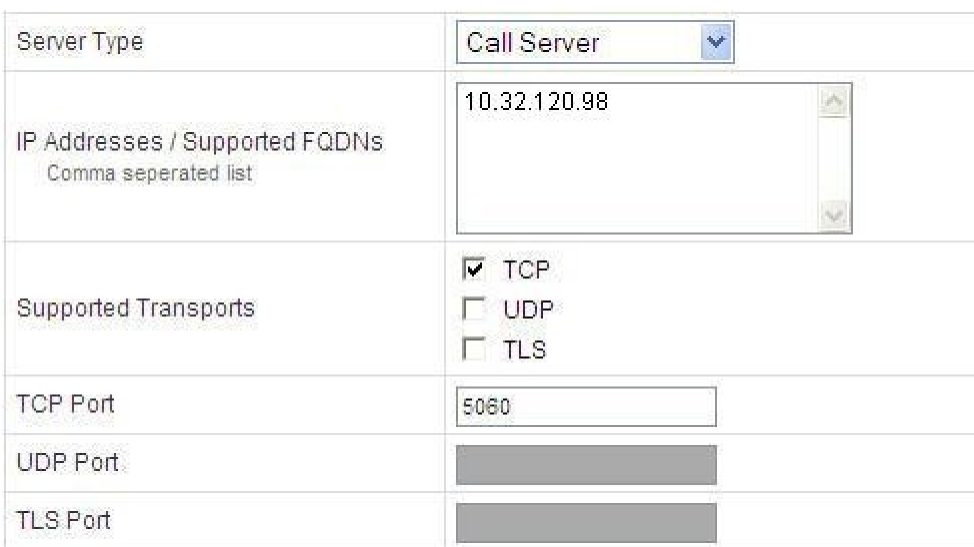
Navigate to **Global Profiles → Server Configuration** to configure the 2 servers.

7.4.1. Server Configuration for Session Manager

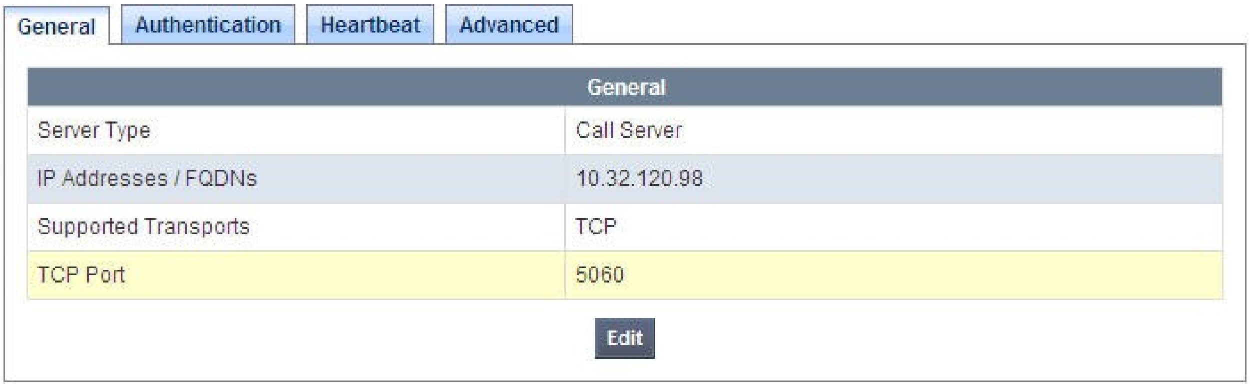
Click the **Add Profile** button (not shown) to add a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as ***NWK-SM*** shown below. Click **Next**.



The following screens illustrate the Server Configuration with Profile name "NWK-SM". 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 should be entered. In the **Supported Transports** area, ***TCP*** is selected, and the **TCP Port** is set to ***5060***. This configuration corresponds with the Session Manager configuration for the Entity Link connecting to the A-SBCE (see **Section 6.6**). If adding a new profile, click **Next**. If editing an existing profile, click **Finish** (buttons not shown).



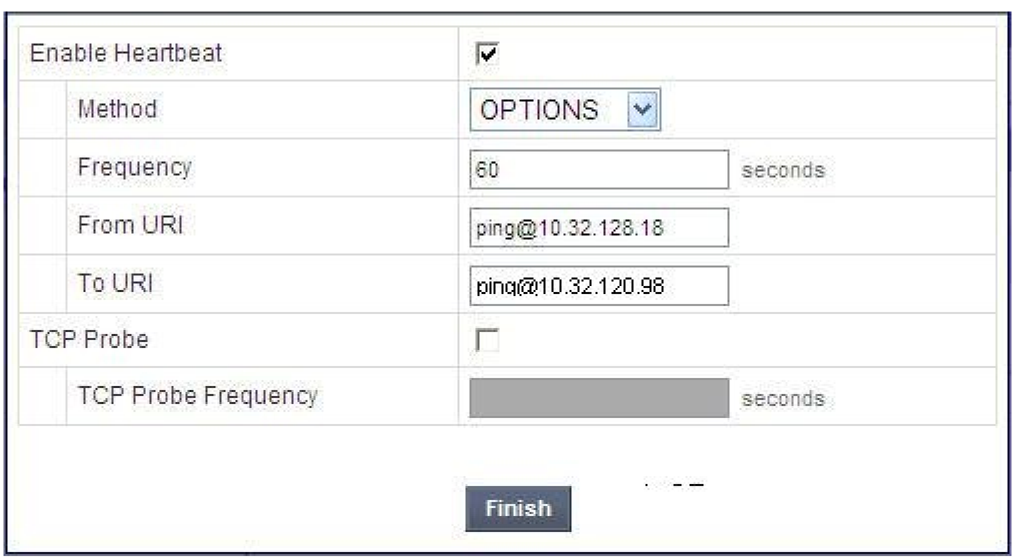
Once configuration is completed, the **General** tab for the configured “NWK-SM” Call Server will appear as shown below.



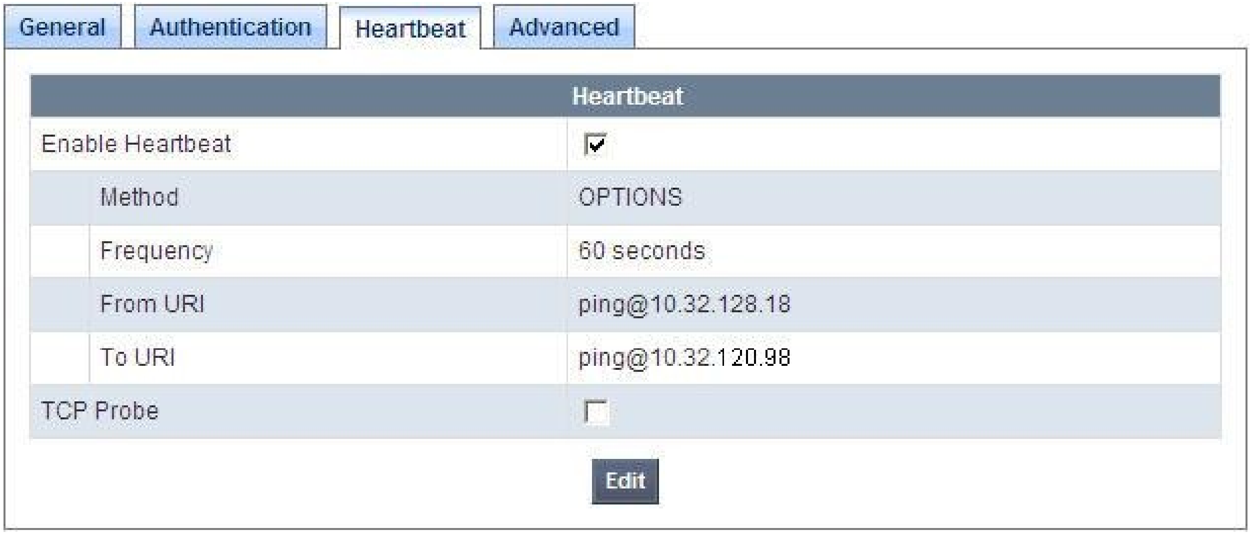
If adding the profile, click **Next** to accept default parameters for the **Authentication** tab, and advance to the **Heartbeat** area. If editing an existing profile, select the **Heartbeat** tab and click **Edit**.

The SBC can be configured to source “heartbeats” in the form of SIP OPTIONS. In the sample configuration, with one connected Session Manager, this configuration is optional.

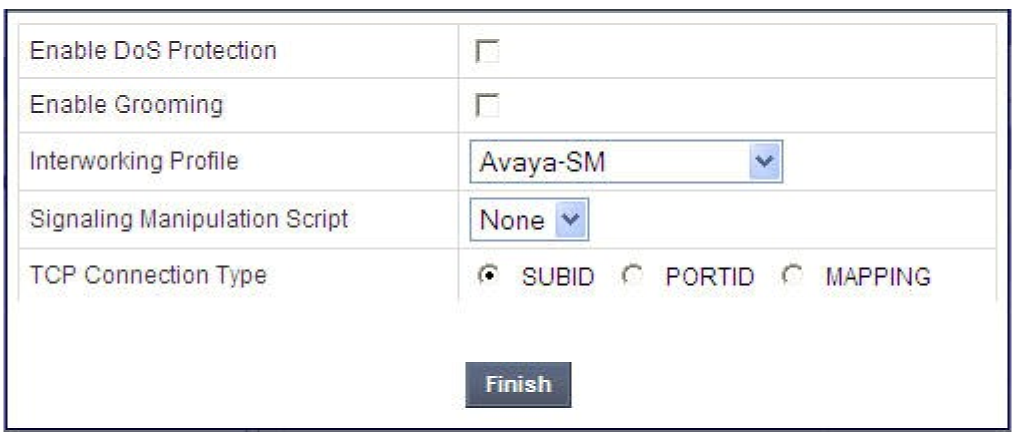
If SBC-sourced OPTIONS messages are desired, check the **Enable Heartbeat** box. Select ***OPTIONS*** from the **Method** drop-down menu. Enter the desired **Frequency** that the SBC will source OPTIONS to this server. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the SBC toward Session Manager. If adding a new profile, click **Next**. If editing an existing profile, click **Finish**.



If SBC sourced OPTIONS is configured, the **Heartbeat** tab for the "NWK-SM" server profile will appear as shown below.



If adding a profile, click **Next** to continue to the **Advanced** settings. If editing an existing profile, select the **Advanced** tab and click **Edit**. In the resultant screen, select the **Interworking Profile** ***Avaya-SM*** created in **Section 7.3.1**. Click **Finish**.



Once configuration is completed, the **Advanced** tab for the call server “NWK-SM” will appear as shown below.

General | Authentication | Heartbeat | Advanced

Advanced	
Enable DoS Protection	☐
Enable Grooming	☐
Interworking Profile	Avaya-SM
Signaling Manipulation Script	None
TCP Connection Type	SUBID

Edit

7.4.2. Server Configuration for Frontier SIP Trunking

A second Server Configuration profile named “SP-Frontier” was similarly created for the Trunk Server.

The following screen illustrates the General tab of the configured “SP- Frontier” server profile. Note the ***Trunk Server*** setting for **Server Type**. The **IP Addresses / Supported FQDNs** is set to the Frontier-provided SIP Trunking service network IP Address. The **Supported Transports** and **UDP Port** are set corresponding with specifications from Frontier.

General | Authentication | Heartbeat | Advanced

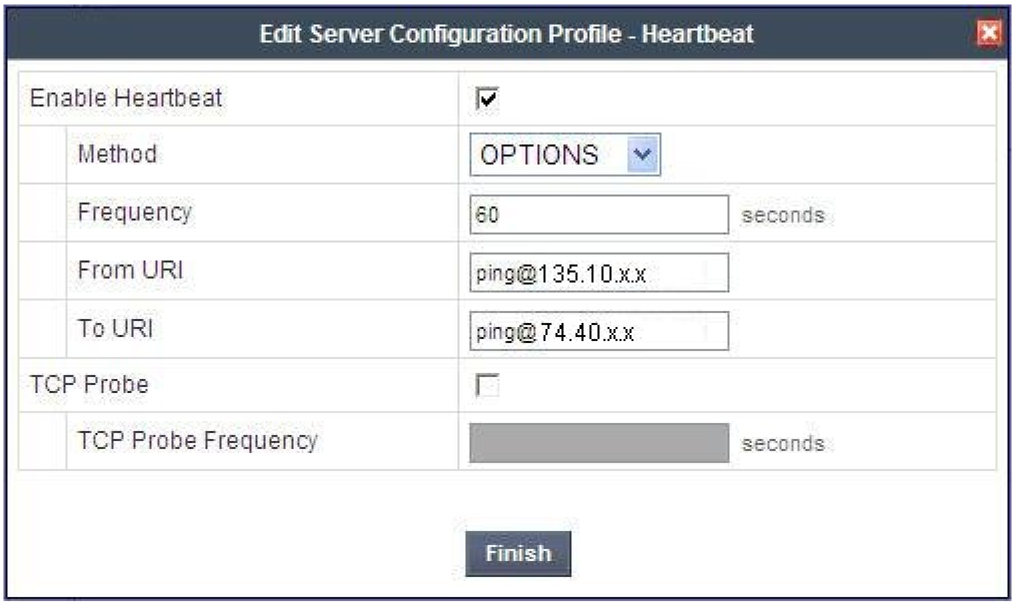
General	
Server Type	Trunk Server
IP Addresses / FQDNs	74.40.x.x
Supported Transports	UDP
UDP Port	5060

Edit

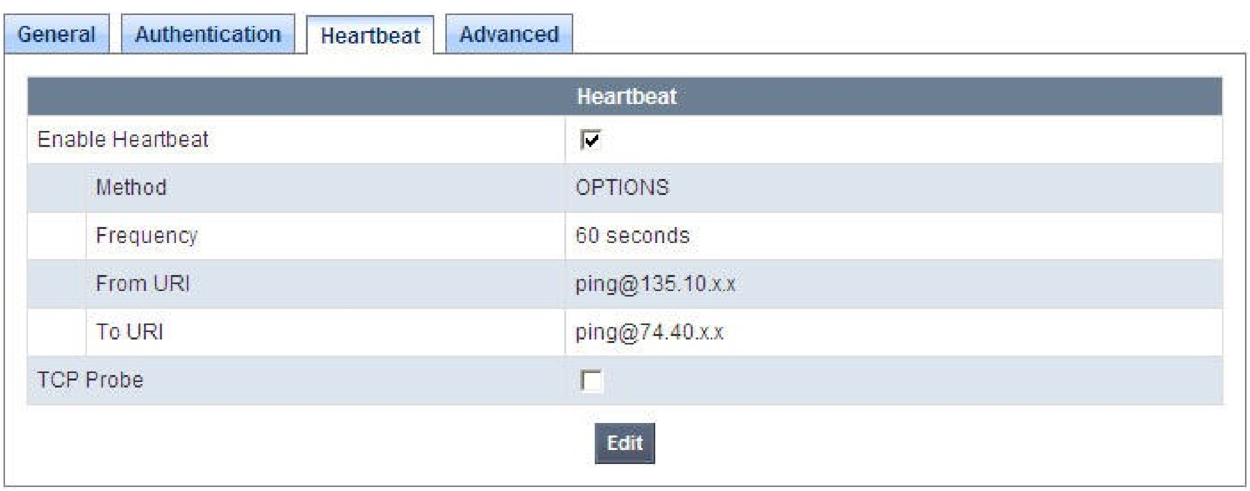
If adding the profile, click **Next** to accept default parameters for the **Authentication** tab, and advance to the **Heartbeat** area. If editing an existing profile, select the **Heartbeat** tab and click **Edit**.

The SBC can be configured to source “heartbeats” in the form of SIP OPTIONS towards Frontier. This configuration is optional. Independent of whether the SBC is configured to source OPTIONS towards Frontier, Frontier will receive OPTIONS from the enterprise site as a result of the SIP Entity Monitoring configured for Session Manager. When Session Manager sends OPTIONS to the inside private IP Address of the SBC, the SBC will pass OPTIONS to Frontier. When Frontier responds, the SBC will pass the response to Session Manager.

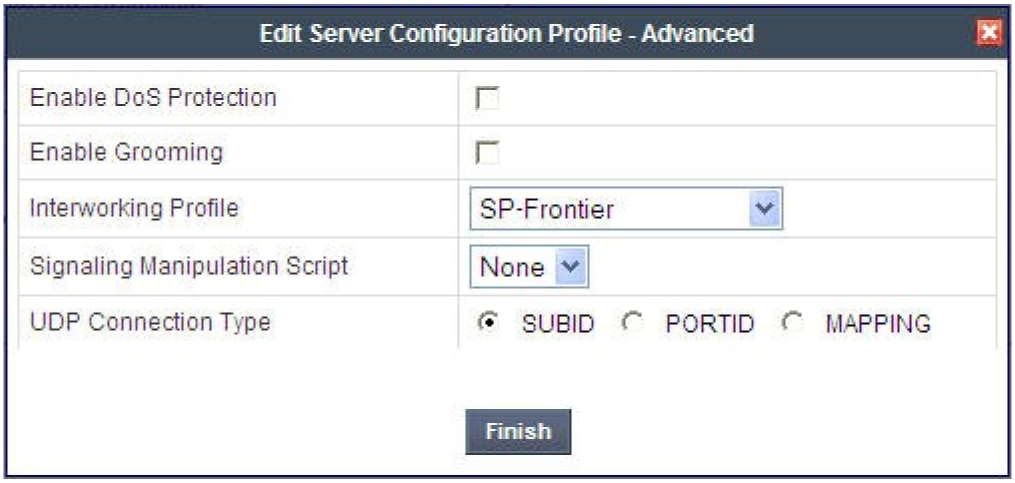
If SBC-sourced OPTIONS is desired, select ***OPTIONS*** from the **Method** drop-down menu. Enter the desired OPTIONS **Frequency**. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the SBC. If adding a new profile, click **Next**. If editing an existing profile, click **Finish**.



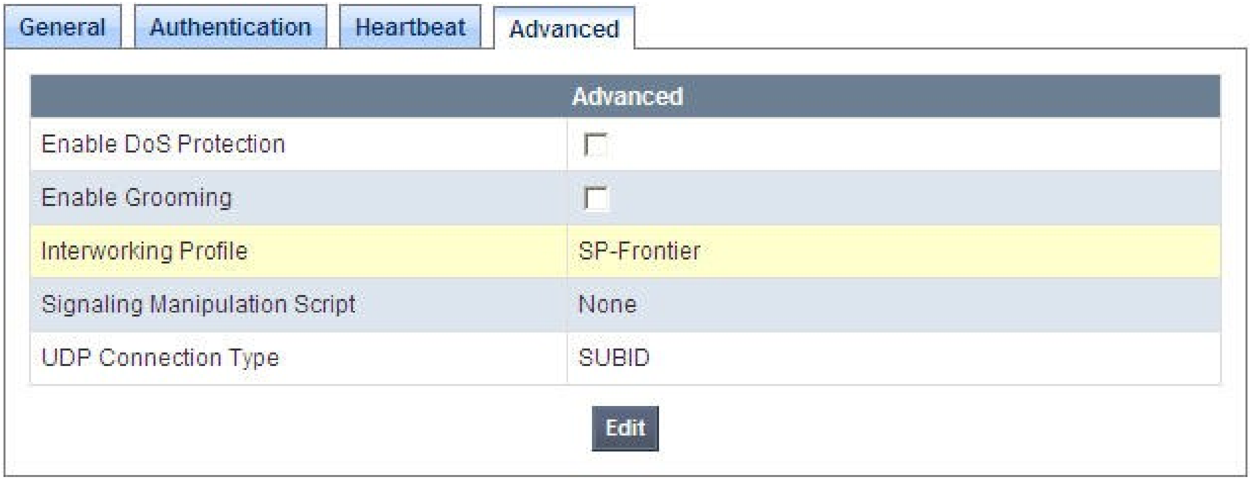
If the optional SBC sourced OPTIONS is configured, the **Heartbeat** tab for the "SP-Frontier" server profile will appear as shown below.



If adding a profile, click **Next** to continue to the **Advanced** settings. If editing an existing profile, select the **Advanced** tab and click **Edit**. In the resultant screen, select the **Interworking Profile** ***SP-Frontier*** created in **Section 7.3.2**. Click **Finish**.



Once configuration is completed, the **Advanced** tab for the “SP-Frontier” server profile will appear as shown below.



7.5. Global Profiles – Routing

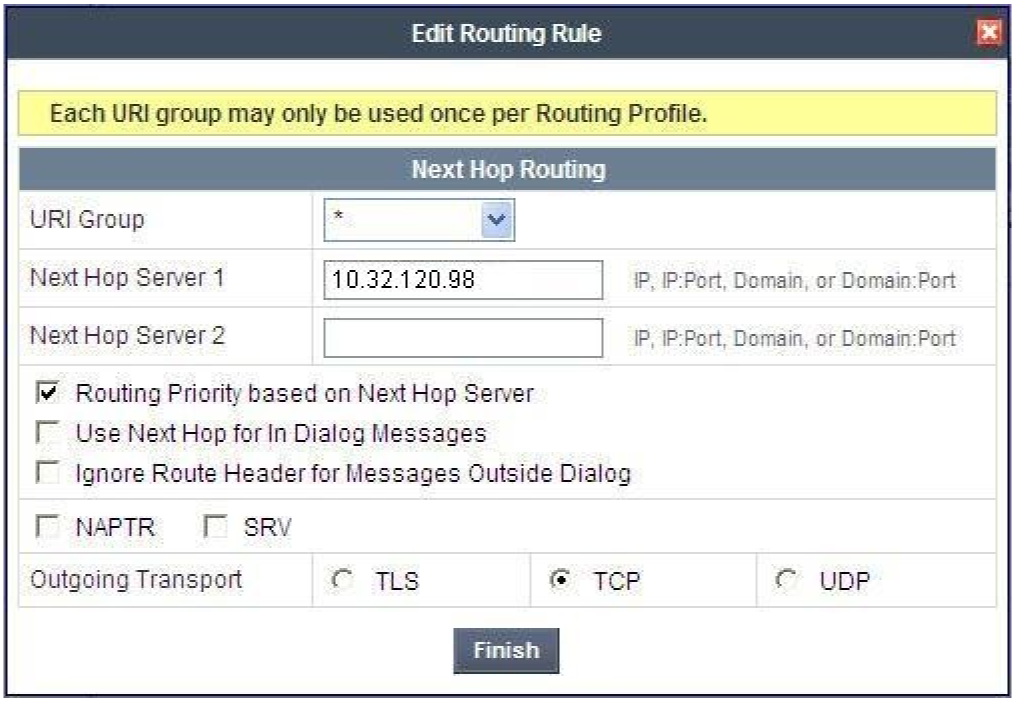
Routing information is required for routing to Session Manager on the internal side and Frontier network on the external side. The IP addresses and ports defined here will be used as the destination addresses for signaling. If no port is specified, default 5060 is used.

Navigate to **Global Profiles → Routing** to configure Routing profiles.

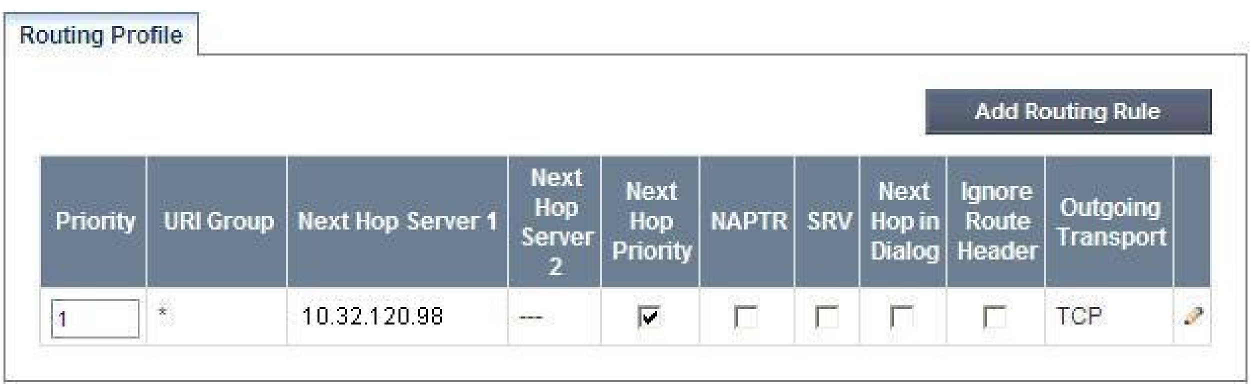
7.5.1. Routing Configuration for Session Manager

Click the **Add Profile** button (not shown) to add a new profile, or select an existing routing profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as ***To_SM*** shown below. Click **Next**.

In the **Next Hop Routing** configuration, enter the IP Address of the Session Manager SIP signaling interface with port number (optional if port number is 5060) as **Next Hop Server 1**, as shown below. Check **Routing Priority based on Next Hop Server**. Choose ***TCP*** for **Outgoing Transport**.

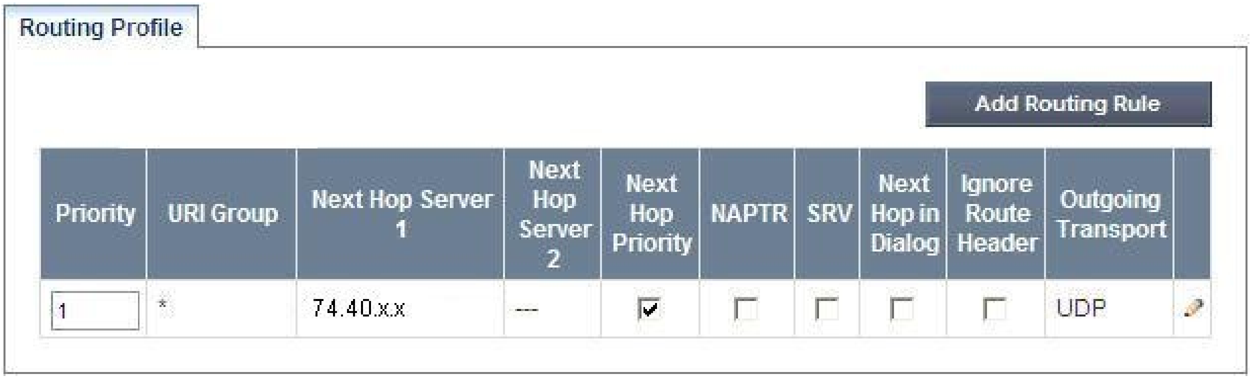


Once configuration is completed, the **Routing Profile** for "To_SM" will appear as follows.



7.5.2. Routing Configuration for Frontier SIP Trunking

A Routing Profile named “To_Trunks” for routing calls to the Trunk Server was similarly configured as shown below. Note the IP address of the Frontier network for **Next Hop Server 1** and ***UDP*** for **Outgoing Transport**.



Routing Profile

Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport	
1	*	74.40.x.x	---	☑	☐	☐	☐	☐	UDP	

7.6. Global Profiles – Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the un-trusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in selected SIP headers to meet expectations by Session Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

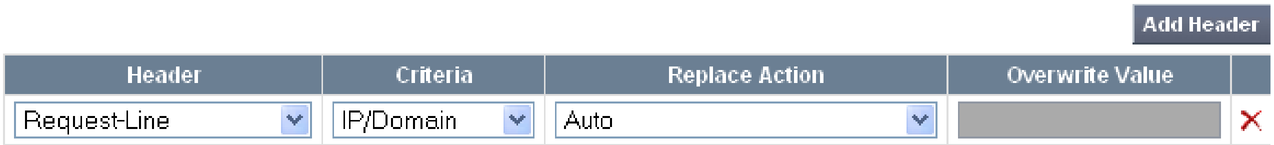
For the compliance test, only the minimum configuration required to achieve interoperability was performed.

Navigate to **Global Profiles → Topology Hiding** to configure Topology Hiding profiles.

7.6.1. Topology Hiding for Session Manager

Click the **Add Profile** button (not shown) to add a new profile, or select an existing topology hiding profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as ***NWK-SM*** shown below. Click **Next**.

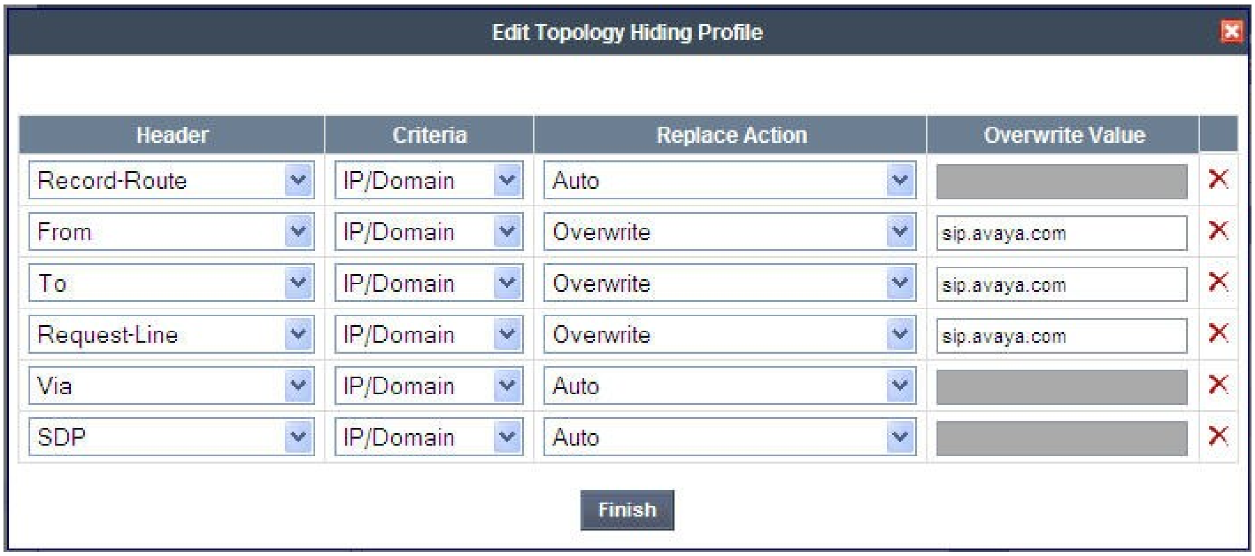
In the resultant screen, click the **Add Header** button to reveal additional headers.



Add Header

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	

To ensure that the domain received by Session Manager from the SBC is the expected enterprise domain, select "Overwrite" as the **Replace Action** for the To, From, and Request-Line headers. Enter the enterprise domain in the **Overwrite Value** column as shown below. In the example below, the domain received by Session Manager is changed by the SBC to ***sip.avaya.com***. Click **Finish**.

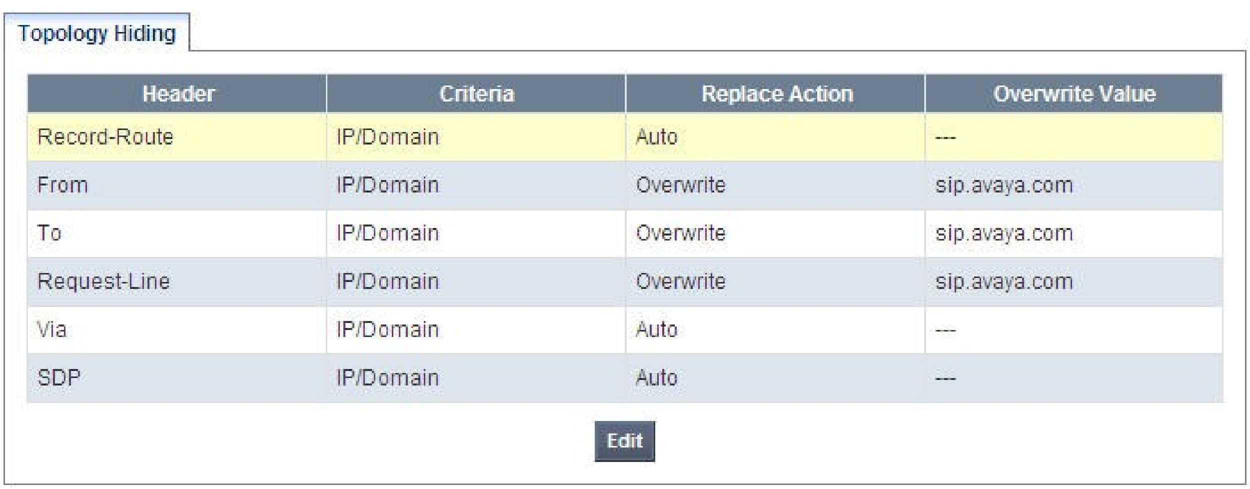


Edit Topology Hiding Profile

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

Finish

After configuration is completed, the Topology Hiding profile "NWK-SM" will appear as follows.



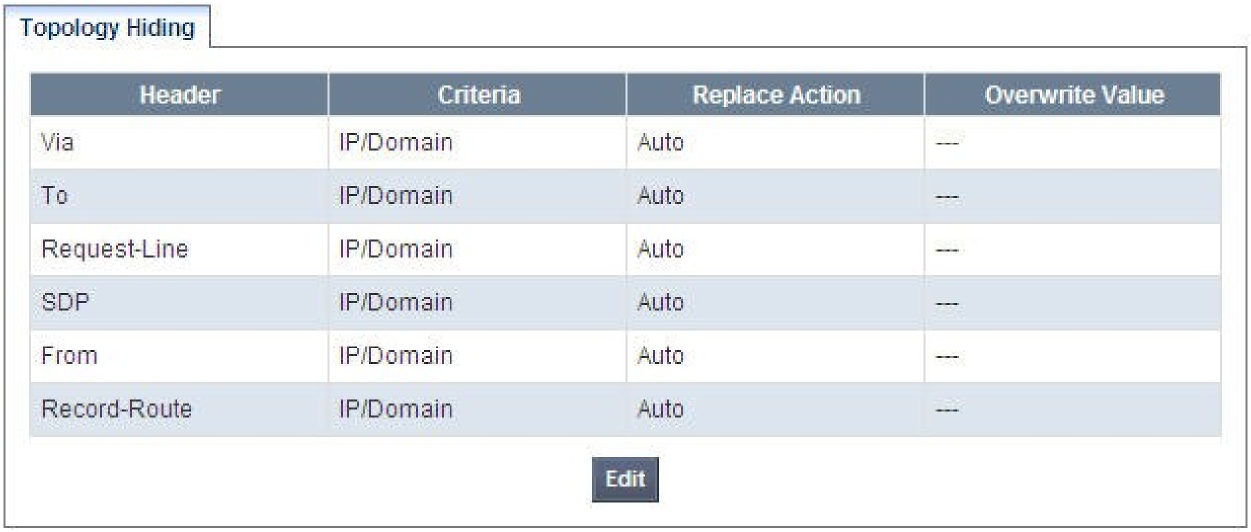
Topology Hiding

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

Edit

7.6.2. Topology Hiding for Frontier SIP Trunking

A Topology Hiding profile named "SP-Frontier" for Frontier was similarly configured as shown below. The default ***Auto*** behaviors are sufficient.



Topology Hiding

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

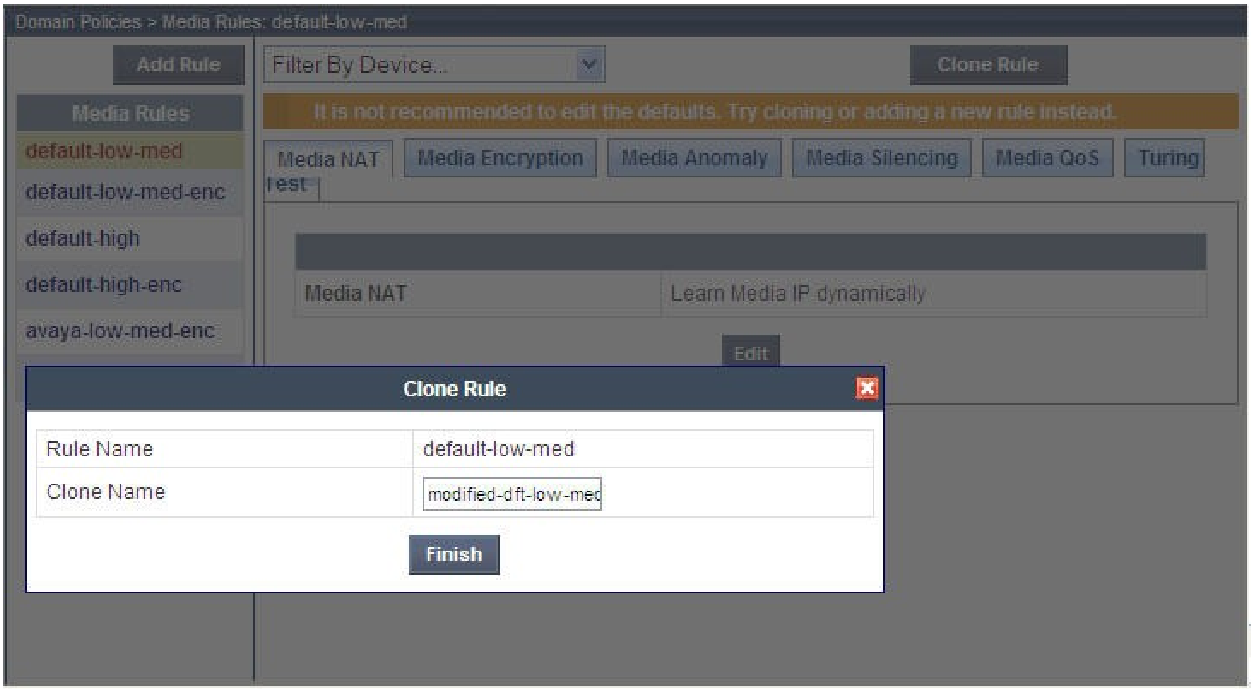
Edit

7.7. Domain Policies – Media Rules

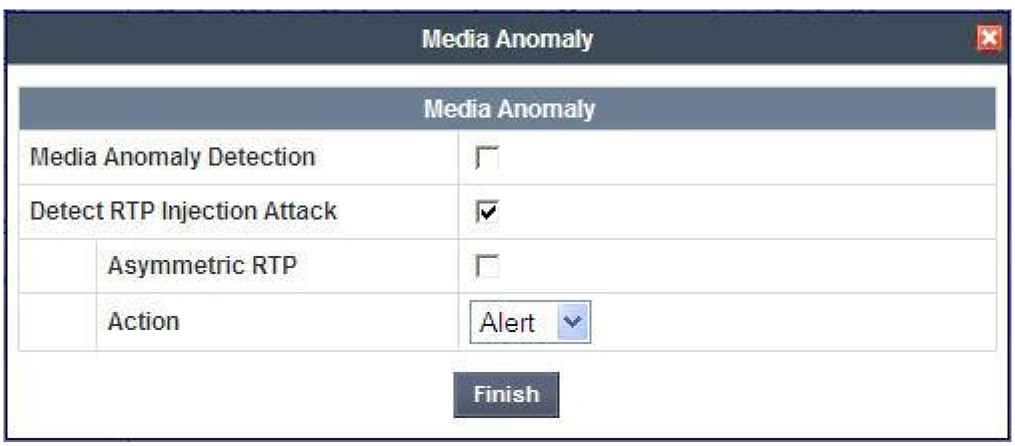
Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

Navigate to **Domain Policies → Media** to configure Media Rules.

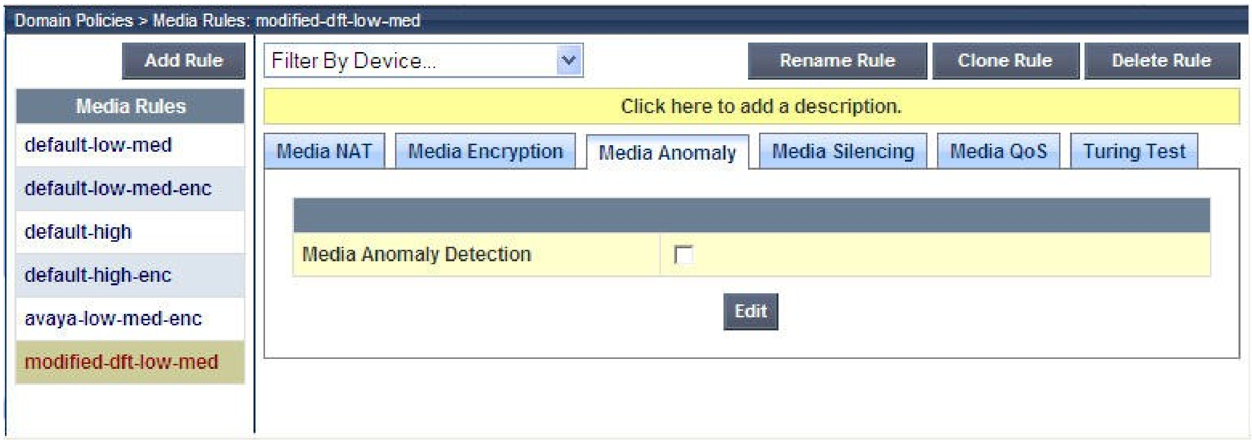
In the sample configuration, a single media rule was used. This media rule was cloned from the default rule "default-low-med" by selecting the default rule "default-low-med" then clicking the **Clone Rule** button in the upper right corner as shown below.



Enter a descriptive **Clone Name**, and then click **Finish**. The cloned media rule will be displayed in the **Media Rules** list on the left. Select this cloned rule from the list, then select **Media Anomaly** tab and click **Edit** (not shown). In the displayed Media Anomaly edit window, uncheck **Media Anomaly Detection** as shown below.



Click **Finish**. The rule named "modified-dft-low-med" is shown below with the Media Anomaly tab selected. This rule is sufficient for the compliance test. See the **Media Anomaly Detection** item of the observation list in **Section 2.2** on reason for turning off this feature.



7.8. Signaling Rules and Signaling Manipulation

Signaling Rules define the actions to be taken (*Allow*, *Block*, *Block with Response*, etc.) on signaling request and response messages. They also allow the control of the Quality of Service of the signaling packets.

The P-Location, P-Charging-Vector and Endpoint-View headers are sent in various SIP messages from Session Manager to the service provider network. These headers should not be exposed external to the enterprise. For simplicity, these headers were simply removed (blocked) from both request and response messages originated from Session Manager.

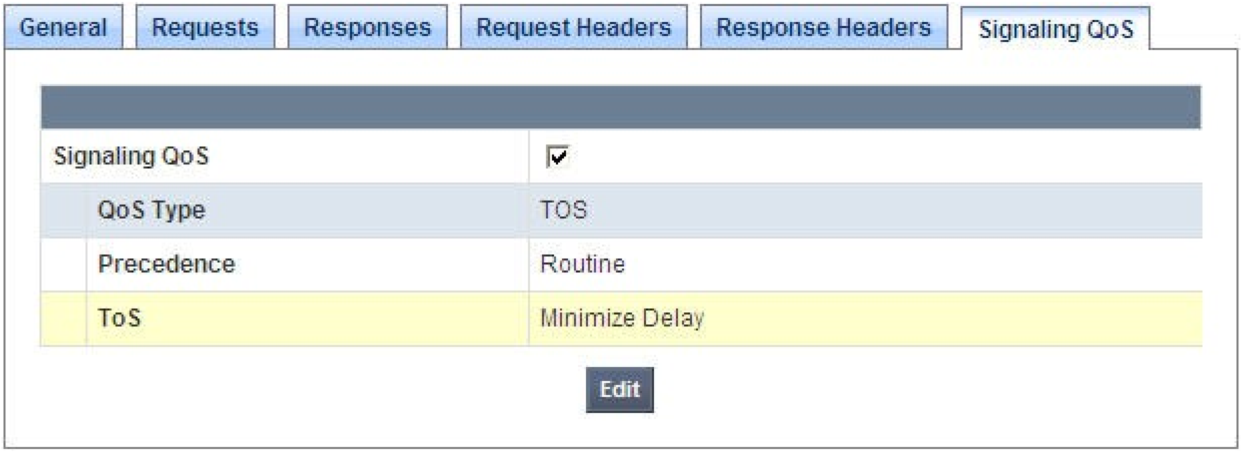
7.8.1. Remove Headers through Signaling Rules Configuration

Navigate to **Domain Policies → Signaling Rules** to configure Signaling Rules.

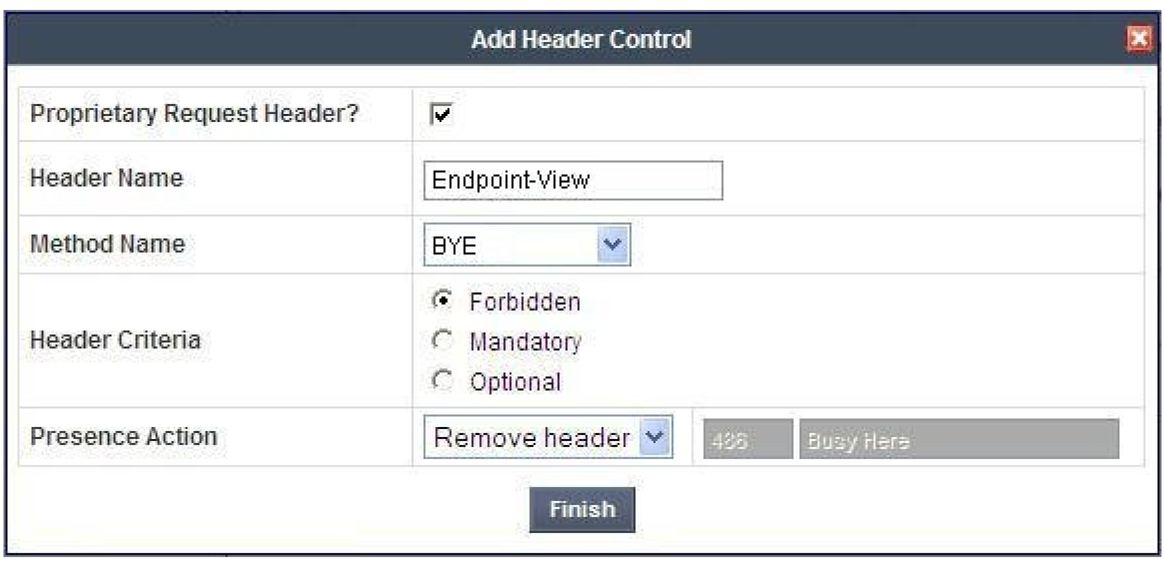
Click the **Add Rule** button (not shown) to add a new signaling rule. In the **Rule Name** field, enter an appropriate name, such as ***SessMgr_SigRules***.

In the subsequent screen (not shown), click **Next** to accept defaults. In the Signaling QoS screen, click **Finish** (not shown).

After this configuration, the new “SM_SigRules” rule will appear as follows.



Select the **Request Headers** tab, and select the **Add In Header Control** button (not shown). In the displayed Add Header Contol window, check the **Proprietary Request Header?** checkbox. In the **Header Name** field, type ***Endpoint-View***. Select ***BYE*** as the **Method Name**. For **Header Criteria**, select ***Forbidden***. Retain the ***Remove header*** selection for **Presence Action selection**. The intent is to remove the Endpoint-View header which is inserted by Session Manager, but not needed by Frontier SIP Trunking service.



Similarly, configure additional header control rules to

- Remove the Endpoint-View header in the inbound PRACK
- Remove the P-Charging-Vector header in the inbound UPDATE

Once complete, the **Request Headers** tab appears as follows.

General | Requests | Responses | Request Headers | Response Headers | Signaling QoS

Add In Header Control | Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Endpoint-View	BYE	Forbidden	Remove Header	Yes	IN		
2	Endpoint-View	PRACK	Forbidden	Remove Header	Yes	IN		
3	P-Charging-Vector	UPDATE	Forbidden	Remove Header	Yes	IN		

Select the **Response Headers** tab and repeat the above configuration steps to

- Remove the Endpoint-View header in the 200 OK response to INVITE
- Remove the P-Charging-Vector header in the 200 OK response to INVITE and UPDATE
- Remove the P-Location header in the 181, 183 and 200 responses to INVITE

Once configuration is completed, the **Response Headers** tab for the "SessMgr_SigRules" signaling rule will appear as follows.

General | Requests | Responses | Request Headers | Response Headers | Signaling QoS

Add In Header Control | Add Out Header Control

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Endpoint-View	200	INVITE	Forbidden	Remove Header	Yes	IN		
2	P-Charging-Vector	200	INVITE	Forbidden	Remove Header	Yes	IN		
3	P-Charging-Vector	200	UPDATE	Forbidden	Remove Header	Yes	IN		
4	P-Location	181	INVITE	Forbidden	Remove Header	Yes	IN		
5	P-Location	183	INVITE	Forbidden	Remove Header	Yes	IN		
6	P-Location	200	INVITE	Forbidden	Remove Header	Yes	IN		

Since the Frontier SIP Trunking test circuit was configured for shared use, the Route header in the CANCEL, INVITE and OPTIONS messages from Frontier needed to be removed during the compliance test in a Signaling Rule named “Frontier_SigRules”, as shown below, to achieve interoperability.

General | Requests | Responses | Request Headers | Response Headers | Signaling QoS

Add In Header Control | Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	Route	CANCEL	Forbidden	Remove Header	No	IN
2	Route	INVITE	Forbidden	Remove Header	No	IN
3	Route	OPTIONS	Forbidden	Remove Header	No	IN

7.8.2. Remove Headers through Signaling Manipulation

In addition to the Signaling Rules configuration which handles a standard set of SIP messages and headers, the **Signaling Manipulation** feature allows the ability to add, change and delete any of the headers in any SIP messages. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called Sigma.

To create a Signaling Manipulation script, navigate to **Global Profiles → Signaling Manipulation**. Click on **Add Script** (not shown), then type in a script title and enter the script statements/commands. Save the script by clicking on **Save** (not shown).

For the compliance test, a script named “RmHdrsInINVITE-ACK” was created. The script is shown as below.

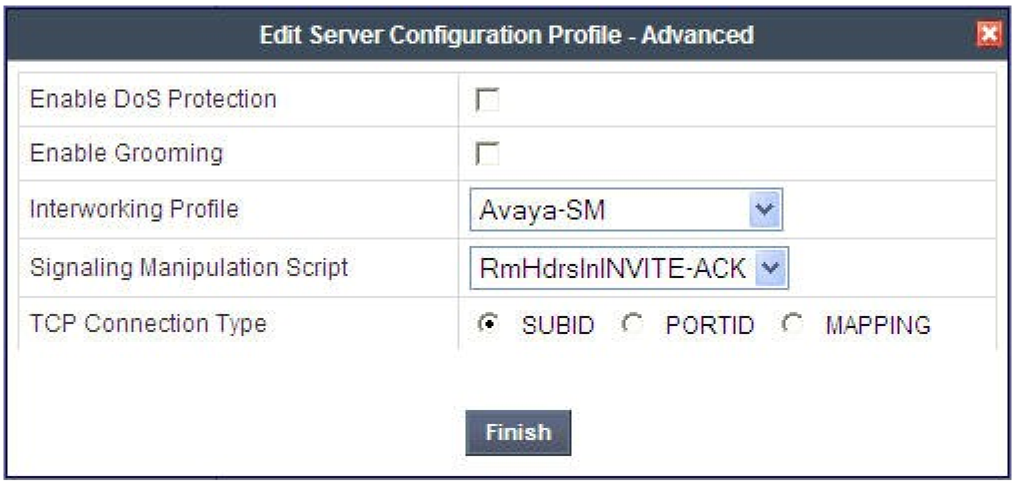
Signaling Manipulation

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

// Remove unwanted Headers

remove(%HEADERS["Endpoint-View"][1]);
remove(%HEADERS["P-Charging-Vector"][1]);
remove(%HEADERS["P-Location"][1]);

 }
}
```

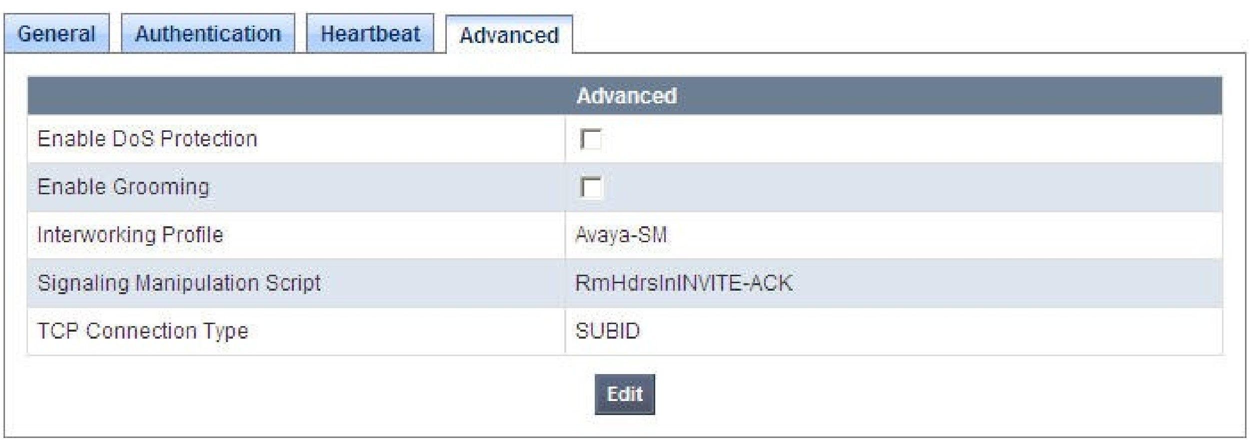
Edit

This script removes the proprietary Endpoint-View, P-Charging-Vector and P-Location headers from the INVITE and ACK (to INVITE) messages from Session Manager. Note that Signaling Rules configuration in Domain Policies allows removal of these proprietary headers from INVITE, but not from ACK, hence the need for the above script.

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



The screen below shows the **Advanced** tab of the NWK-SM server after the signaling manipulation script was added.



7.9. Domain Policies – End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the SBC.

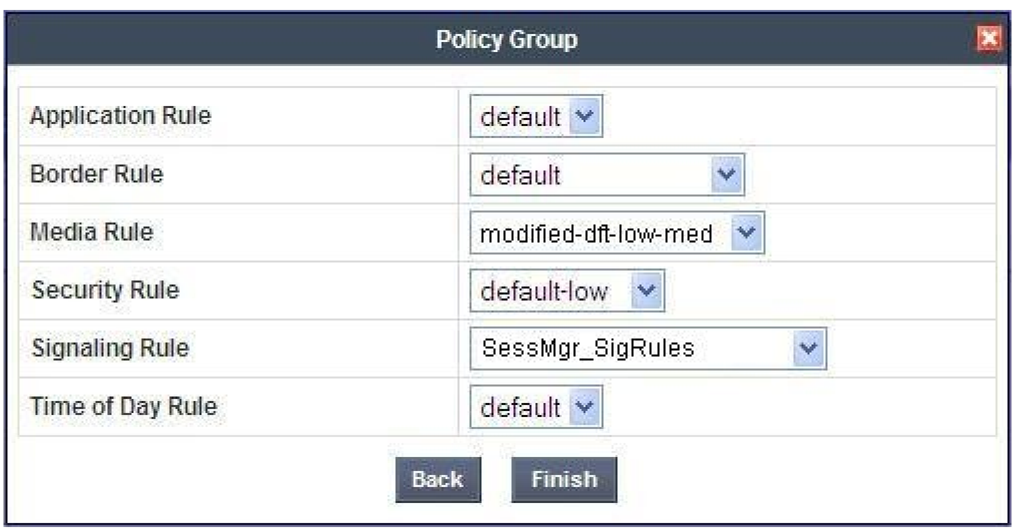
Navigate to **Domain Policies → End Point Policy Groups** to configure End Point Policy Groups.

Select the **Add Group** button (not shown). Enter a name in the **Group Name** field, such as ***SM*** as shown below. Click **Next**.

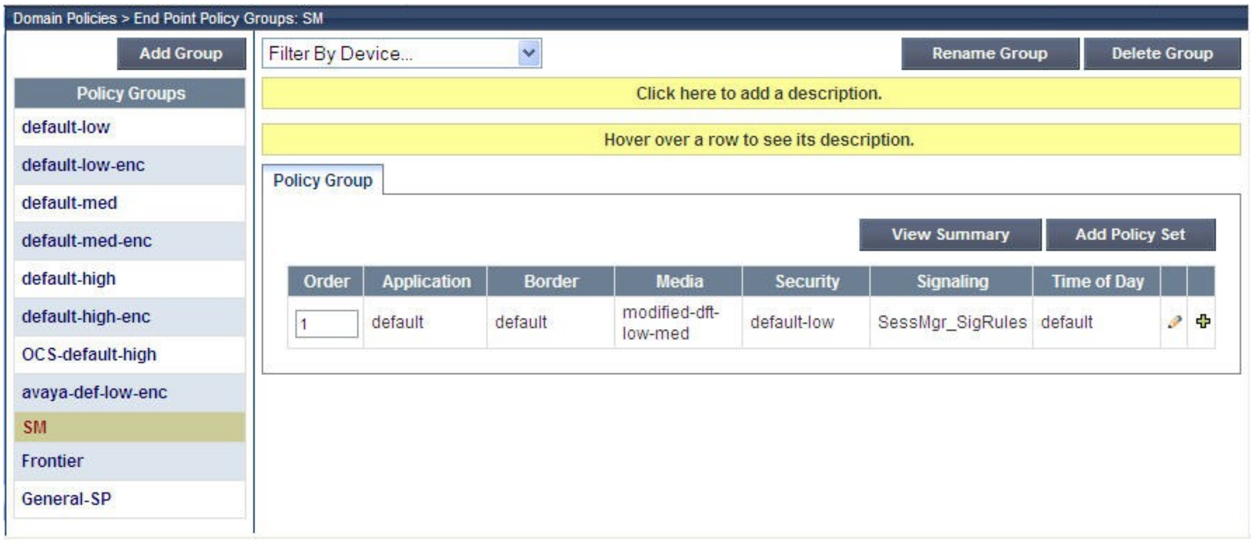
In the sample configuration, defaults were selected for all fields, with the exception of

- **Media Rule**, which was set to the ***modified-dft-low-med*** media rule as defined in **Section 7.7**
- **Signaling Rule**, which was set to the ***SessMgr_SigRules*** signaling rule as defined in **Section 7.8**

Click **Finish**.

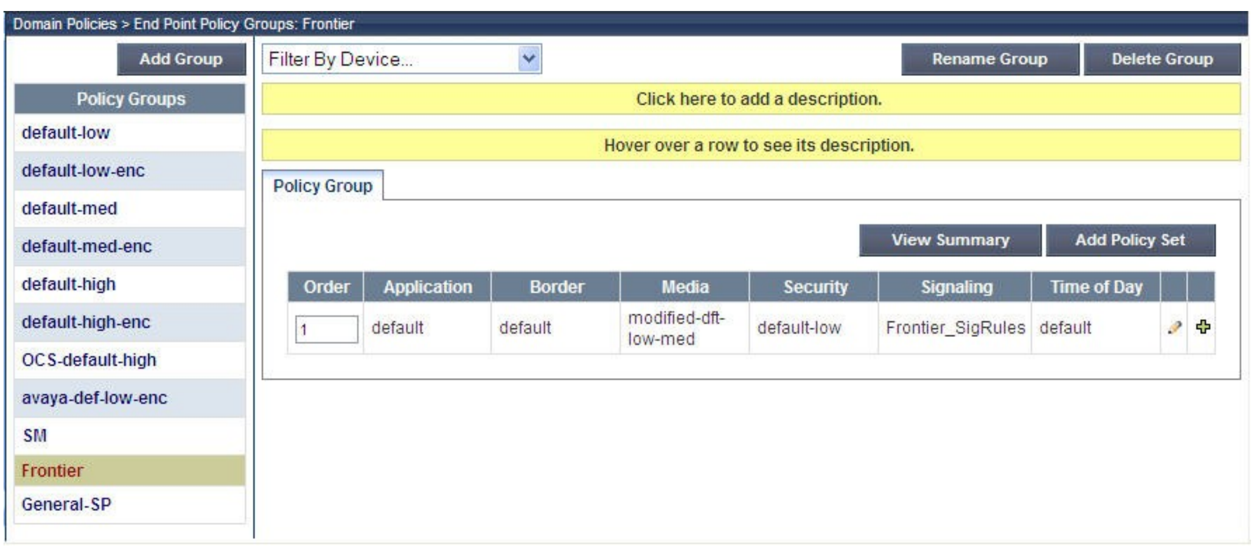


Once configuration is completed, the “SM” End Point Policy Group will appear as follows.



Repeat the above configuration steps to create a 2nd End Point Policy Group named “Frontier” for the network side as shown below.

Note that this End Point Policy Group uses the same Media Rule (“modified-dft-low-med”) for disabling Media Anomaly Detection and the “Frontier_SigRules” signaling rule as defined in **Section 7.8**.

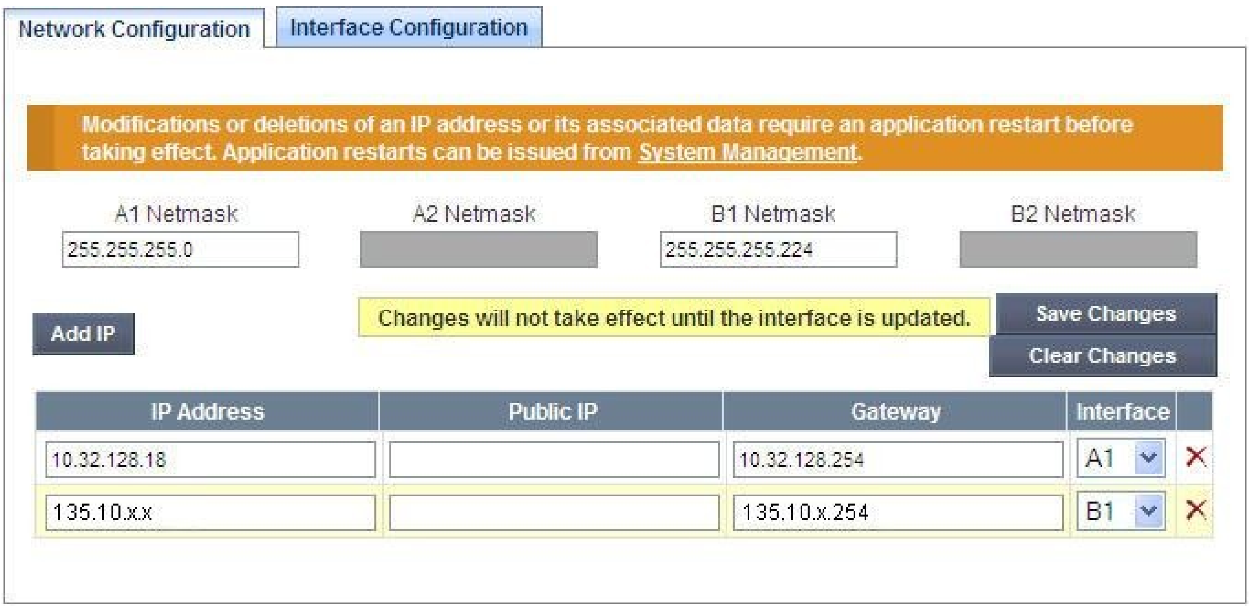


7.10. Device Specific Settings – Network Management

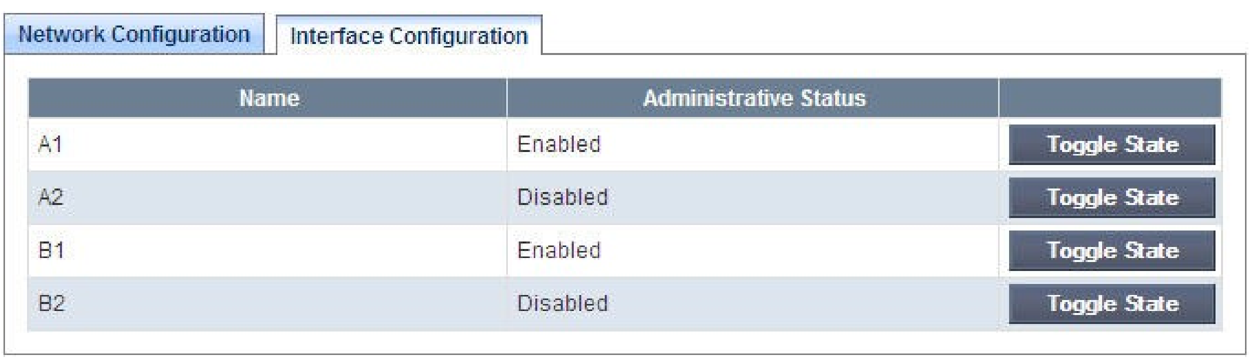
The network information should have been previously specified during installation of the A-SBCE.

Navigate to **Device Specific Setting → Network Management** from the left-side menu.

Under **UC-Sec Devices**, select the device being managed, which was named "sp-ucsec1" in the sample configuration (not shown). The **Network Configuration** tab is shown below. Observe the **IP Address**, **Netmask**, **Gateway**, and **Interface** information previously assigned. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for the external side of the A-SBCE.



Select the **Interface Configuration** tab. The **Administrative Status** can be toggled between **Enabled** and **Disabled** in this screen. The following screen was captured after the interfaces had already been enabled. To enable the interface if it is disabled, click the **Toggle State** button.



When the IP addresses and masks are assigned to the interfaces, these are then configured as signaling and media interfaces.

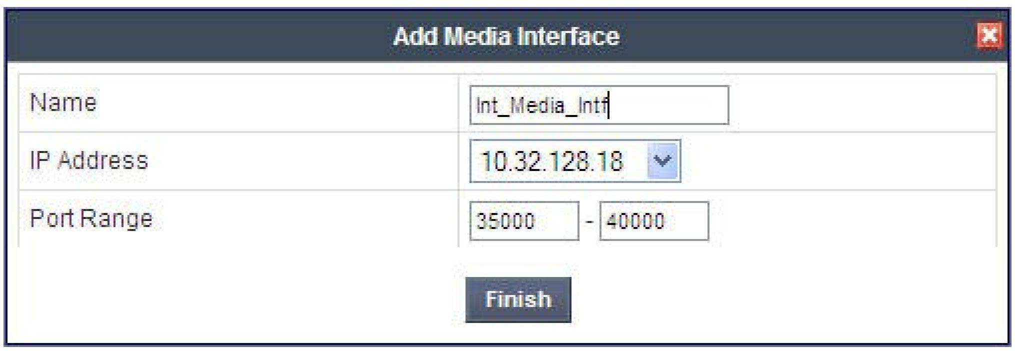
7.11. Device Specific Settings – Media Interface

Media Interfaces are created to adjust the port range assigned to media streams leaving the interfaces of the SBC. The compliance test used the port range 35000 to 40000 for both the private interface and the public interface.

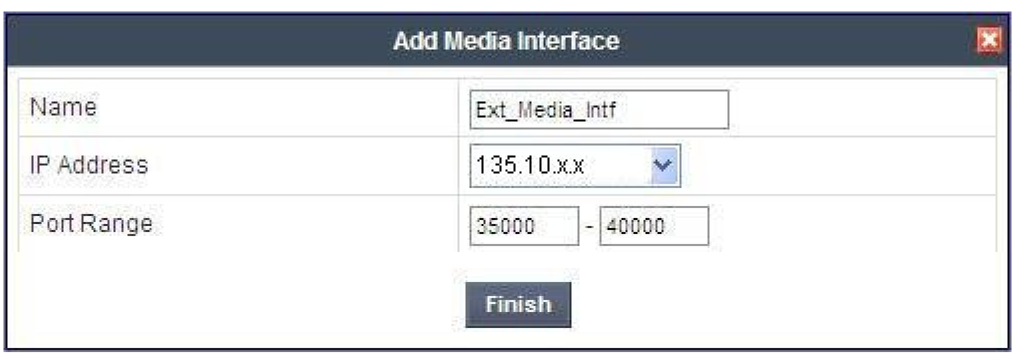
Navigate to **Device Specific Setting → Media Interface** to configure Media Interfaces, one for internal and one for external.

Under **UC-Sec Devices**, select the device being managed, which was named "sp-ucsec1" in the sample configuration (not shown). Select **Add Media Interface**.

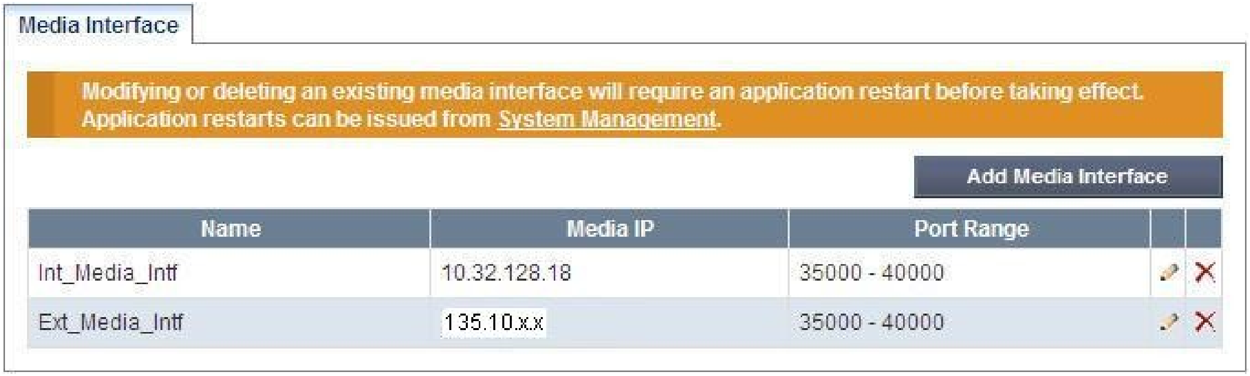
Enter an appropriate **Name** for the Media Interface facing the enterprise and select the inside private IP Address from the **IP Address** drop-down menu. In the sample configuration, ***Int_Media_Intf*** is chosen as the name, and the inside IP Address of the SBC is ***10.32.128.18***. For the **Port Range**, default values are shown. Click **Finish**.



An external Media Interface facing the network was similarly created with name ***Ext_Media_Intf*** and the outside IP Address of the SBC ***135.10.x.x*** as shown below. Same **Port Range** setting was used as for the internal Media Interface.



The resultant Media Interface configuration used in the sample configuration is shown below.

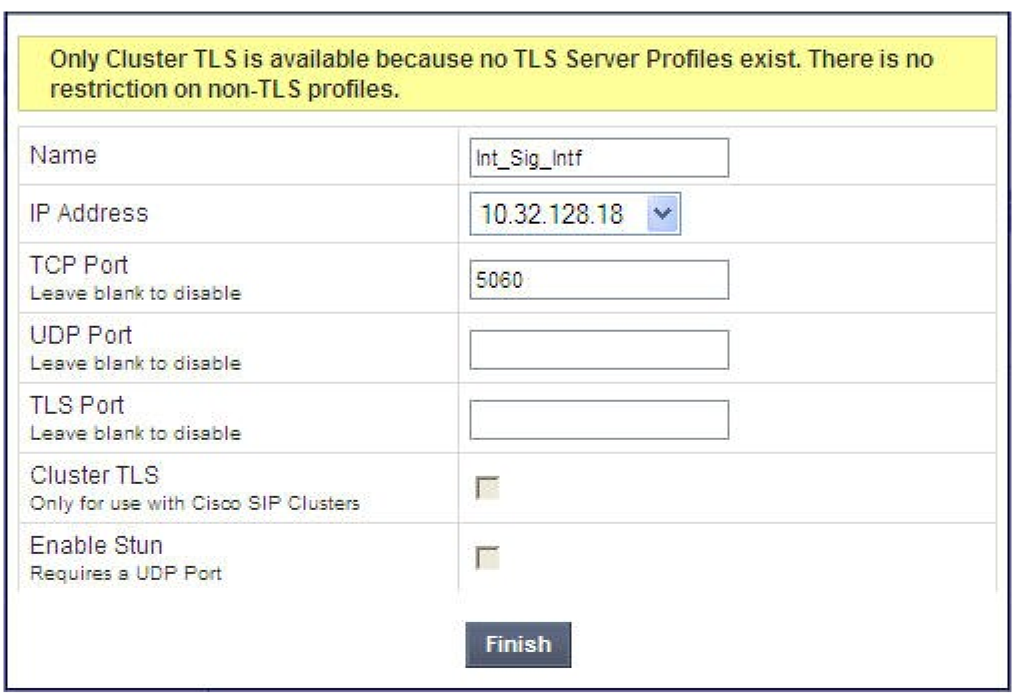


7.12. Device Specific Settings – Signaling Interface

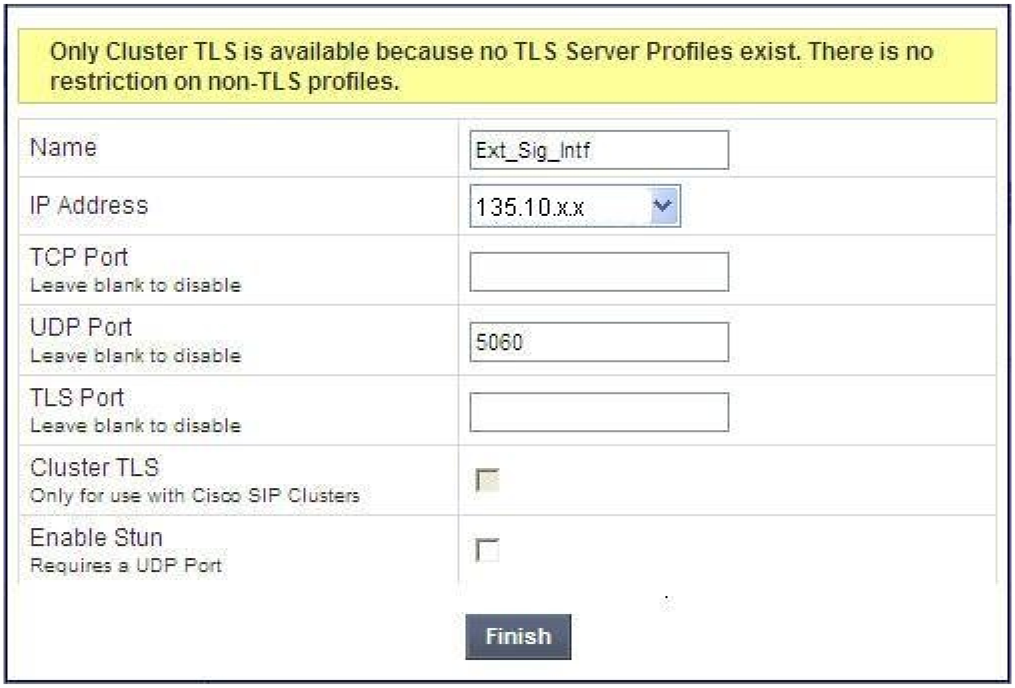
Navigate to **Device Specific Setting → Signaling Interface** to configure Signaling Interfaces, one for internal and one for external.

Under **UC-Sec Devices**, select the device being managed, which was named "sp-ucsec1" in the sample configuration (not shown). Select **Add Signaling Interface**.

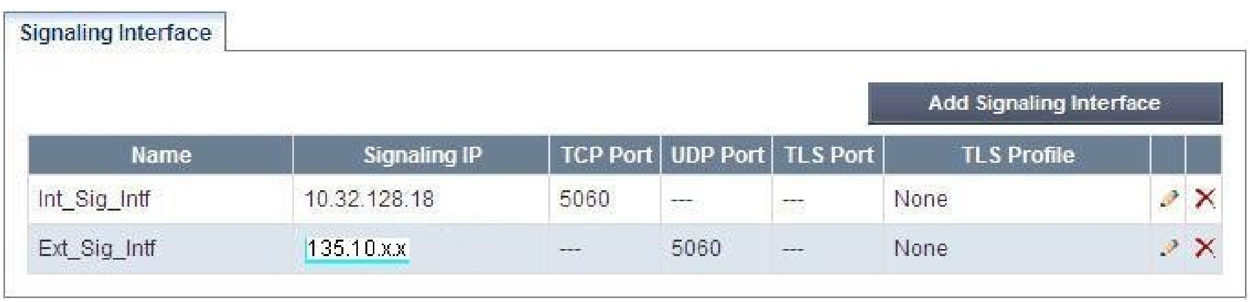
In the **Add Signaling Interface** screen, enter an appropriate **Name** (e.g., ***Int_Sig_Intf***) for the inside interface, and choose the private inside IP Address from the **IP Address** drop-down menu. Enter ***5060*** for **TCP Port** since TCP and port 5060 is used between Session Manager and the SBC in the sample configuration. Click **Finish**.



An external Signaling Interface facing the network was similarly created with name ***Ext_Sig_Intf*** and the outside IP Address of the SBC ***135.10.x.x*** as shown below. Note that ***5060*** was specified for **UDP Port** since UDP was used between the SBC and the Frontier network.



The following screen shows the Signaling Interfaces defined for the sample configuration.



Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Int_Sig_Intf	10.32.128.18	5060	---	---	None		
Ext_Sig_Intf	135.10.x.x	---	5060	---	None		

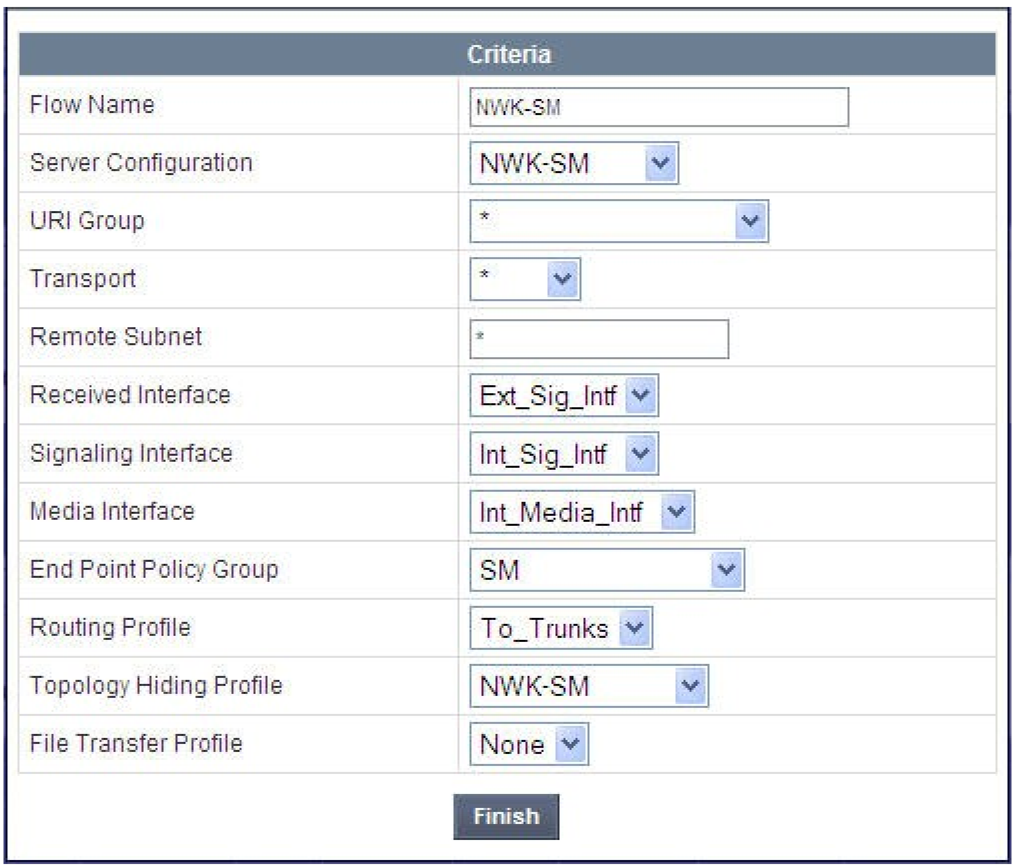
7.13. Device Specific Settings – End Point Server Flows

End Point Server Flows combine the previously defined profiles into an outgoing flow from the Call Server (Session Manager) to the Trunk Server (service provider network) and an incoming flow from the Trunk Server to the Call Server. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to the service provider network and vice versa.

Select **Device Specific Setting → End Point Flows** to configure End Point Flows.

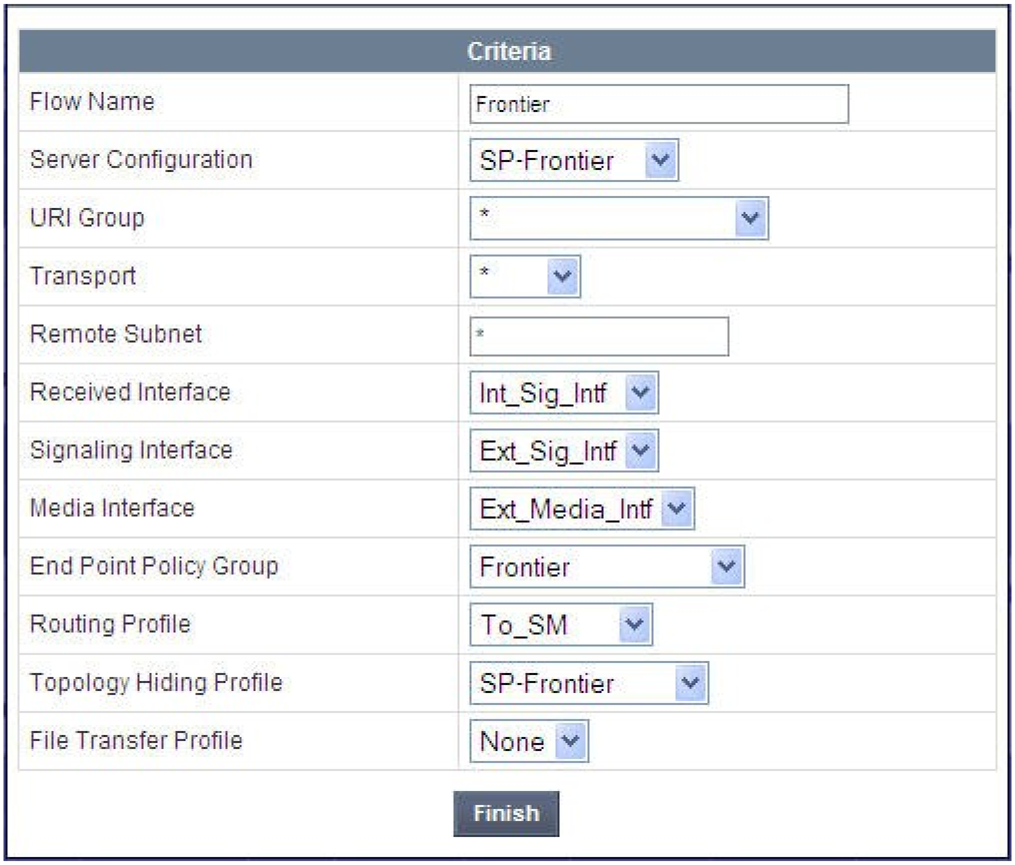
Under **UC-Sec Devices**, select the device being managed, which was named "sp-ucsec1" in the sample configuration (not shown). Select the **Server Flows** tab. Select **Add Flow**.

The following screen shows the flow named ***NWK-SM*** being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection which is the reverse route of the flow. Click **Finish**.



Once again, select the **Server Flows** tab. Select **Add Flow**.

The following screen shows the flow named ***Frontier*** being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection which is the reverse route of the flow. Click **Finish**.



The following 2 screens (at different scroll positions of the **Server Flows** tab) summarize the Server Flows configured in the sample configuration.

Subscriber Flows | Server Flows

Server Configuration: NWK-SM

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

Server Configuration: SP-Allstream

Subscriber Flows | Server Flows

Server Configuration: SP-Frontier

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

8. Frontier SIP Trunking Configuration

To use Frontier SIP Trunking, a customer must request the service from Frontier using the established sales and provisioning processes. The process can be started by contacting Frontier via the corporate web site at http://www.frontier.com and requesting information via the online sales links or telephone numbers.

During the signup process, Frontier will require that the customer provide the public IP address used to reach the SBC at the edge of the enterprise and information related to SIP configuration supported by the enterprise. Frontier will provide the IP address of the Frontier SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the configurations of Communication Manager, Session Manager, and Avaya SBC for Enterprise discussed in the previous sections.

The configuration between Frontier SIP Trunking and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the Frontier network.

9. Verification and Troubleshooting

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

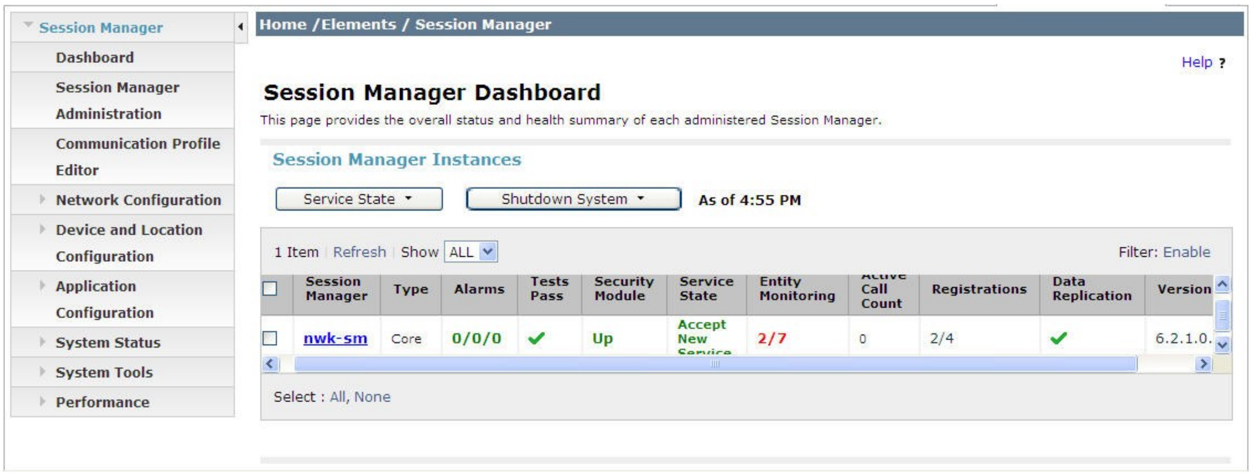
Verification Steps:

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active with 2-way audio path.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active with 2-way audio path.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Troubleshooting:

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

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



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

3. Avaya SBC for Enterprise
    - **OPTIONS** - Disable the SBC-sourced OPTIONS to the trunk server (see **Section 7.4.2**) and use a network sniffer like Wireshark to verify that the service provider network will receive OPTIONS forwarded by the SBC from the enterprise site as a result of the SIP Entity Monitoring configured for Session Manager. Reversely, when the service provider network responds to the OPTIONS from Session Manager, the SBC will pass the response to Session Manager.
    - **Incidents** – From the admin web interface of A-SBCE, open the Incidents report by clicking the **Incidents** menu button in the menu bar. Verify that no abnormal incidents are listed

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.2, Avaya Aura® Session Manager R6.2 and Avaya Session Border Controller for Enterprise R4.0.5 to Frontier Communications SIP Trunking service. Frontier SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Frontier SIP Trunking provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. References

The Avaya product documentation is available at http://support.avaya.com unless otherwise noted.

Avaya Aura® Solution for Midsize Enterprise

[1] *Avaya Aura® Solution for the Midsize Enterprise (ME) 6.2 Intelligent Workbook*, Workbook Version 1.3, April 2012

[2] *Implementing Avaya Aura® Solution for Midsize Enterprise*, Release 6.2, Issue 4.1, May 2012

Avaya Aura® Session Manager/System Manager

[3] *Administering Avaya Aura® Session Manager*, Document ID 03-603324, Release 6.2, February 2012

[4] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Doc ID 03-603325, Release 6.2, February 2012

[5] *Administering Avaya Aura® System Manager*, Release 6.2, March 2012

Avaya Aura® Communication Manager

[6] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509, Release 6.2, Issue 7.0, February 2012

[7] *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010

Avaya one-X™ IP Phones

[8] *Avaya one-X™ Deskphone SIP 9621G/9641G User Guide for 9600 Series IP Telephones*, Document ID 16-603596, Issue 1, May 2011

[9] *Avaya one-X™ Deskphone H.323 9608 and 9611G User Guide*, Document ID 16-603593, Issue 3, February 2012

[10] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide,* Document ID 16-601944, Release 2.6, June 2010

[11] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* Document ID 16-300698, Release 3.1, November 2009

[12] *Administering Avaya one-X® Communicator,* April 2011

Avaya Session Border Controller for Enterprise

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

[14] *Sipera Systems E-SBC Administration Guide, Release 4.0.5,* November 2011

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.