Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Frontier Communications SIP Trunking with Avaya Aura® Communication Manager Evolution Server R6.0.1, Avaya Aura® Session Manager R6.1, 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 R6.1, Avaya Aura® Communication Manager Evolution Server R6.0.1, Avaya Aura® Messaging R6.1, 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.

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 R6.1, Avaya Aura® Communication Manager Evolution Server R6.0.1, Avaya Aura® Messaging R6.1, 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 Session Border Controller for Enterprise 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 phone types.
  Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.

- Outgoing PSTN calls from various phone types.
  Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client). Avaya one-X® Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X® Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. 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 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** – When an H.323 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). Consult transfer of similar call to PSTN worked properly (Frontier responded with "202 Accepted" to REFER from the enterprise). 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: Frontier responded to T.38 re-INVITE from the enterprise with "488 Not Acceptable Here". Inbound T.38 faxing worked properly.

- **Call Termination** – In certain call scenarios involving call forward, BYE's from the network would not be passed by Avaya SBC for Enterprise to the next hop (Session Manager), failing proper call termination. This problem was addressed in the compliance test by a special patch to the SBC software version 4.0.5.Q02. Software version later than 4.0.5.Q02 will include this patch.

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 lab test circuit) through a public Internet WAN connection.

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

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

- Avaya S8800 Server running Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Session Manager
- Avaya S8800 Server running System Manager
- Avaya S8800 Server running Avaya SBC for Enterprise
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya 1600-Series IP Telephone (H.323)
- 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
- Avaya S8800 Server running Avaya messaging application

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.

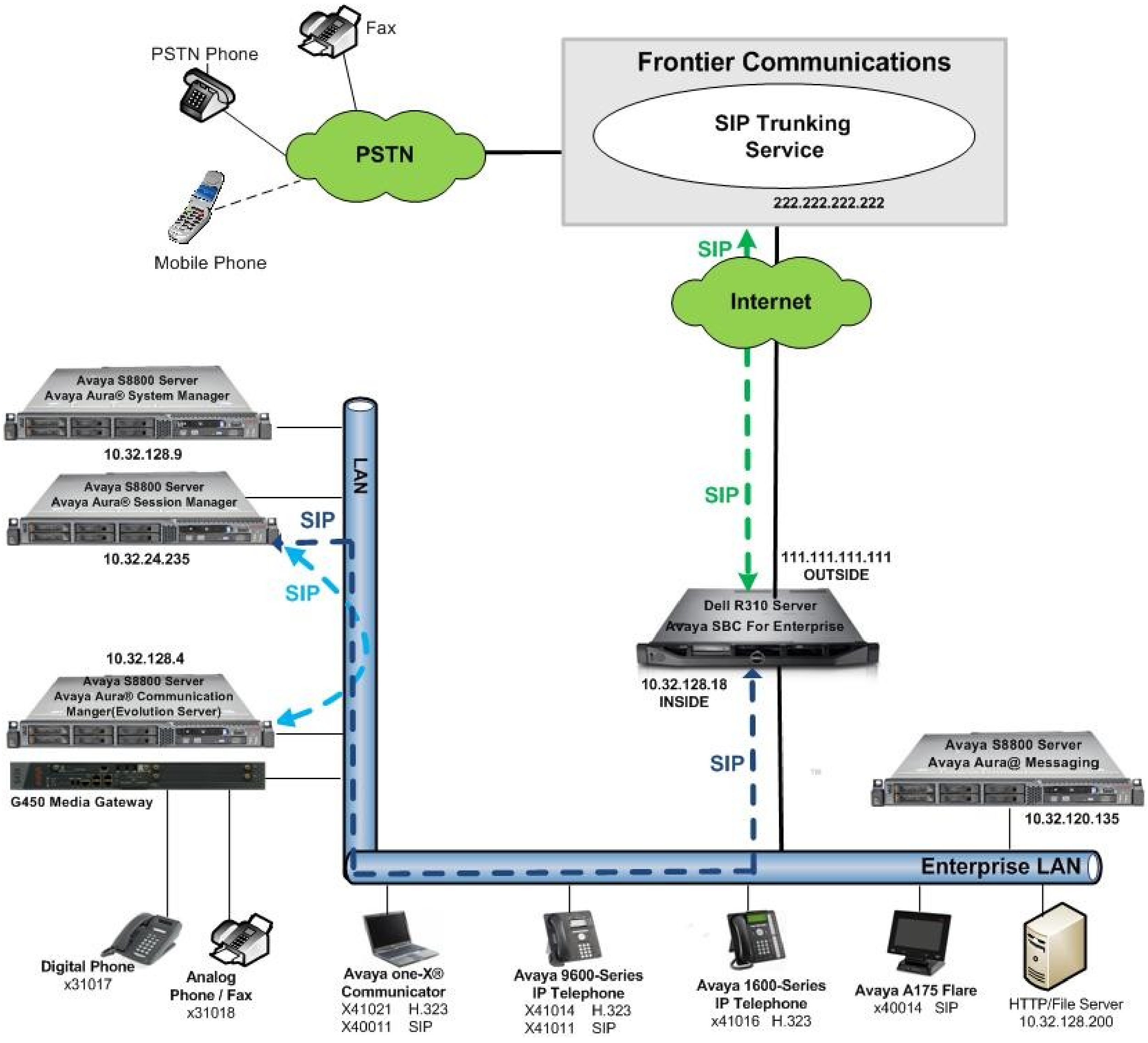


Figure 1: Avaya SIP Enterprise Solution Using Frontier Communications SIP Trunking

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 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 administration of Avaya Aura® Messaging and endpoints on Communication Manager are standard. Since the configuration tasks for Avaya Aura® 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® Communication Manager running on Avaya S8800 Server with Avaya G450 Media Gateway	6.0.1 (R016x.00.1.510.1-19303) 31.20.0
Avaya G450 Media Gateway – ICC – ANA – DCP	31.20.0 HW01 FW001 HW33 FW091 HW07 FW009
Avaya Aura® Session Manager running on Avaya S8800 Server	6.1.5.0.615006
Avaya Aura® System Manager running on Avaya S8800 Server	6.1.0 Build 6.1.0.0.7345-6.1.5.502 Software Update Revision No: 6.1.9.1.1634
Avaya 96xx Series IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1.1
Avaya 96xx Series IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 2.6.6
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 R310 Server	4.0.5.Q02 with special patch
Avaya Aura® Messaging running on Avaya S8800 Server	6.1-11.0
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.

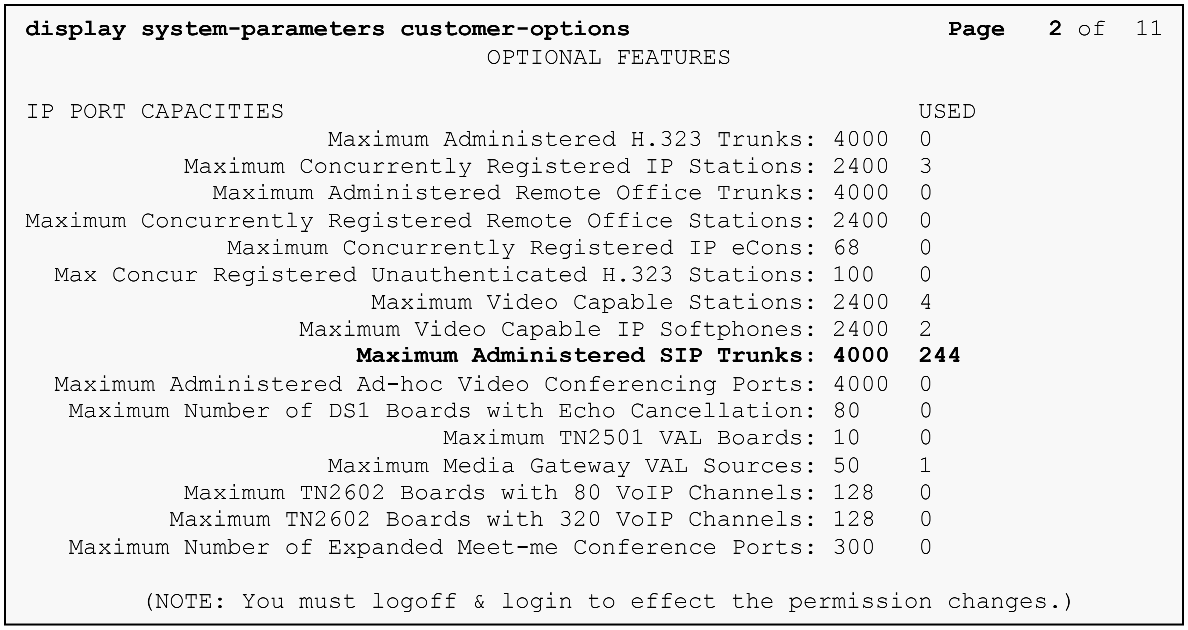
5. Configure Avaya Aura® Communication Manager

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

5.1. Licensing and Capacity

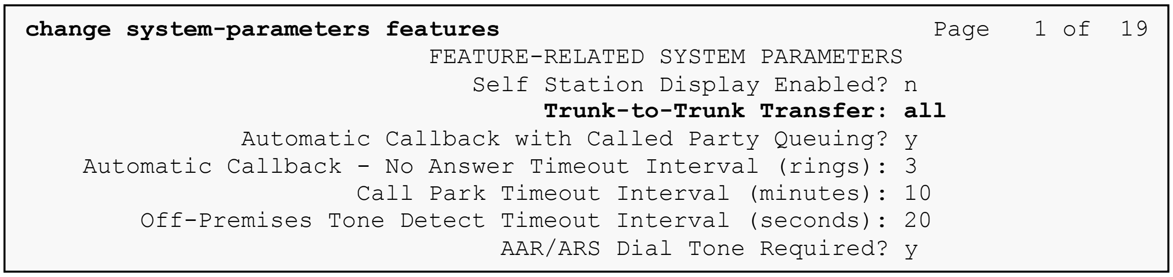
Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 4000 licenses are available and 244 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.



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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  0
           Maximum Concurrently Registered IP Stations: 2400  3
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  4
                   Maximum Video Capable IP Softphones: 2400  2
                       Maximum Administered SIP Trunks: 4000  244
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    1
           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.)
```

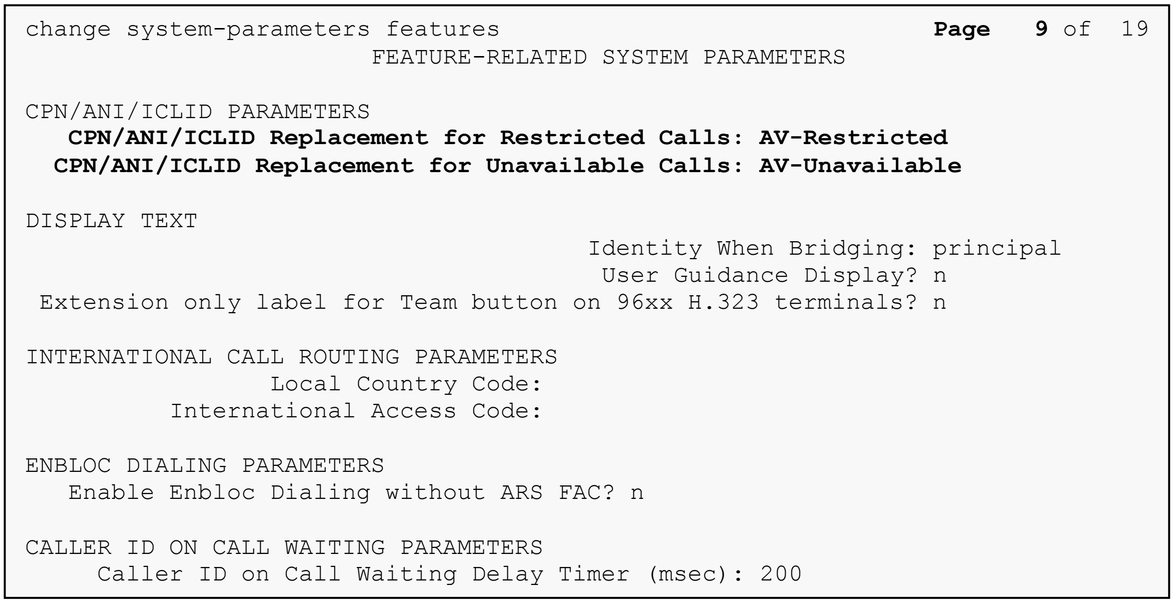
5.2. System Features

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? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? y
    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 ***AV-Restricted*** for restricted calls and ***AV-Unavailable*** for 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: AV-Restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: AV-Unavailable

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:
          International Access Code:

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Avaya S8800 Server running Communication Manager ***(procr***) and for Session Manager (***sessionMgr***). 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
default             0.0.0.0
procr               10.32.128.4
procr6              ::
sessionMgr          10.32.24.235
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. 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 2                                             Page   1 of   2

                          IP Codec Set

    Codec Set: 2

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

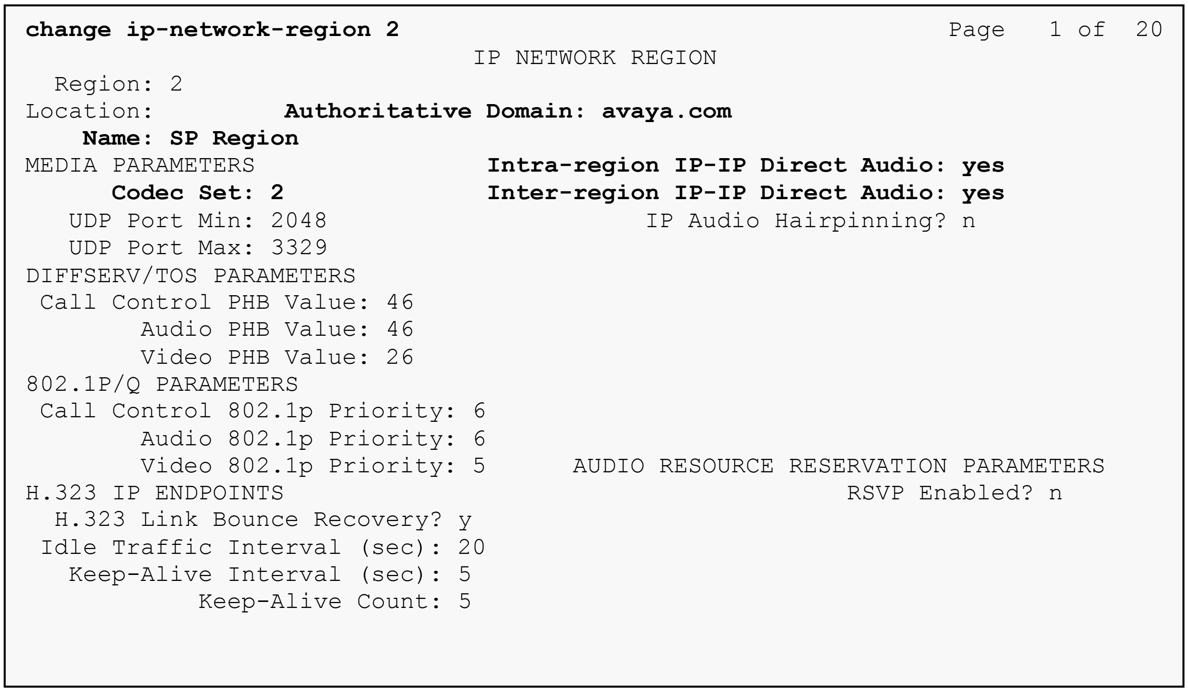
On **Page 2**, set the **Fax Mode** to ***t.38-standard***.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n


                Mode                Redundancy
    FAX         t.38-standard        0
    Modem       off                  0
    TDD/TTY     US                   3
    Clear-channel   n                0
    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 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is ***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 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location:         Authoritative Domain: avaya.com
    Name: SP Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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

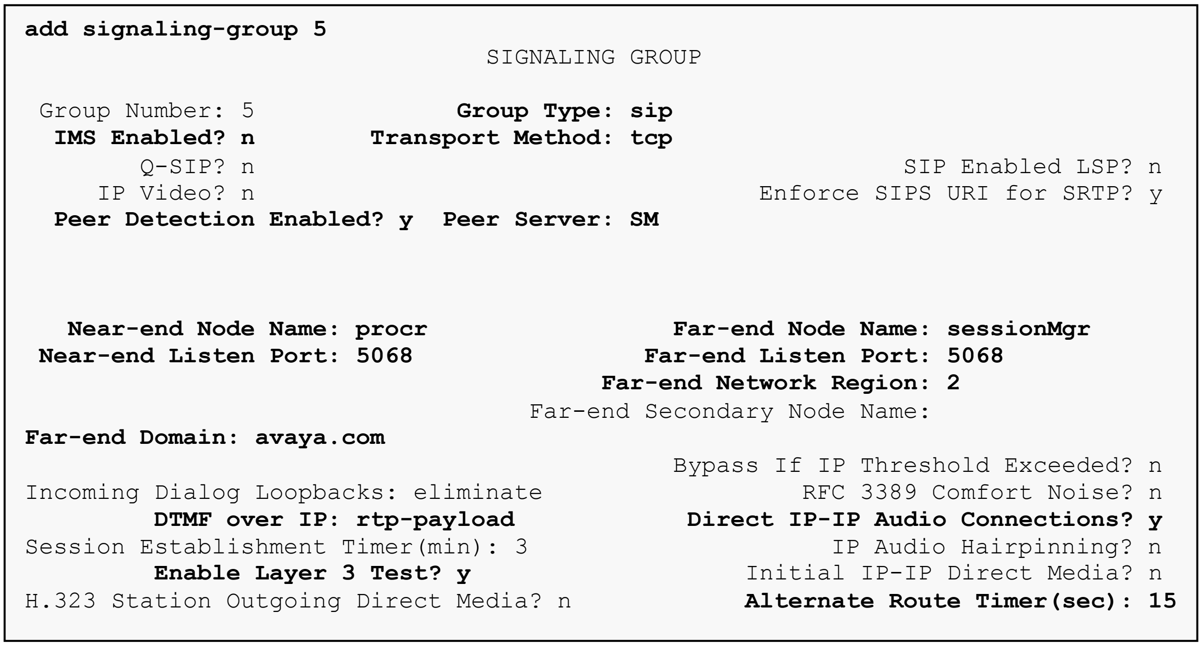
```
change ip-network-region 2                                      Page   4 of  20

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

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 ***tcp*** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to ***tcp*** The transport method specified here is used between Communication Manager and Session Manager.
- Set the **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 ***5068***.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer-Server** field will initially be set to ***Others*** and can not 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 the Avaya S8800 Server running Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***sessionMgr***. 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 completing.
- 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.
- Default values may be used for all other fields.



```
add signaling-group 5
                                SIGNALING GROUP

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



   Near-end Node Name: procr                Far-end Node Name: sessionMgr
 Near-end Listen Port: 5068               Far-end Listen Port: 5068
                                       Far-end Network Region: 2
                                   Far-end Secondary Node Name:
Far-end Domain: 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.

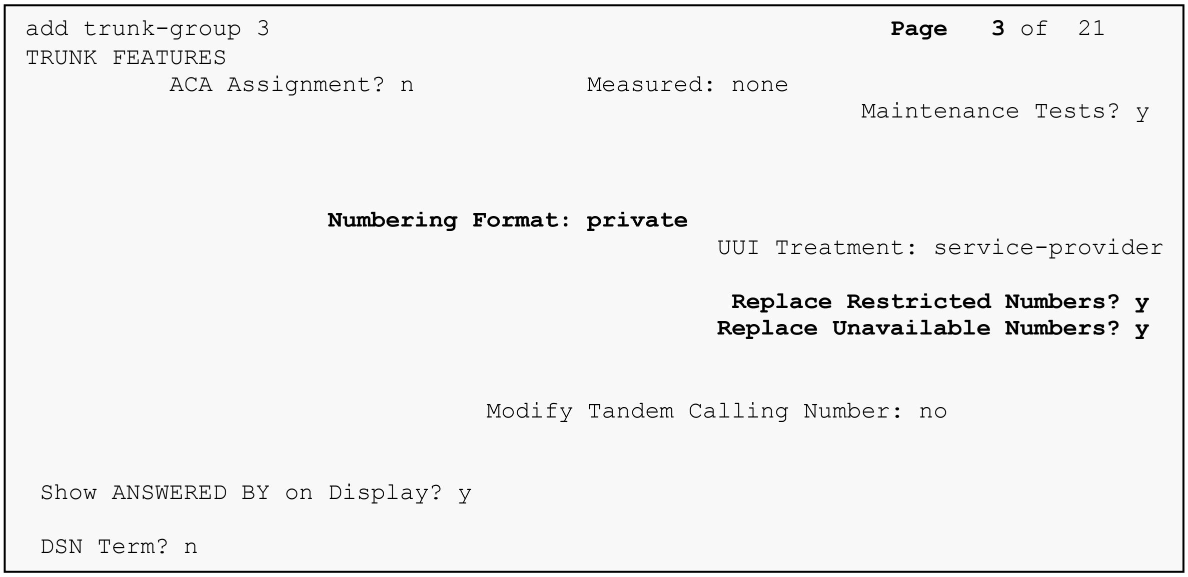
```
add trunk-group 5                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 5                    Group Type: sip           CDR Reports: y
  Group Name: A-SP-Trunk                  COR: 1        TN: 1        TAC: 1005
   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 3                                           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.

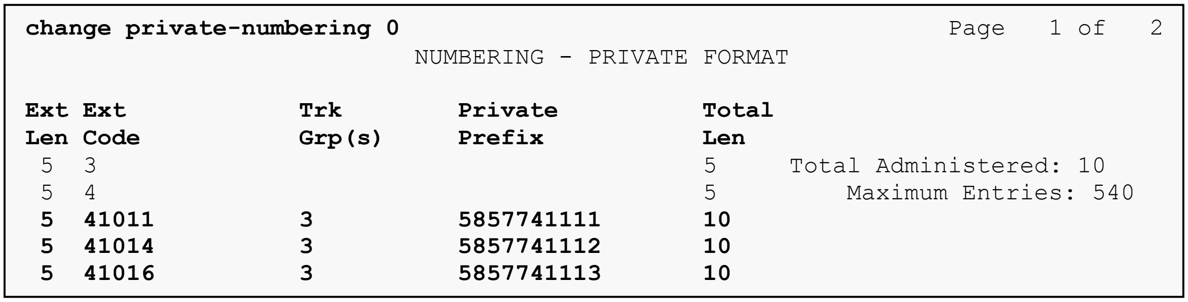
Set the **Telephone Event Payload Type** to ***101***, the value preferred by Frontier.

```
add trunk-group 3                                              Page   4 of  21
                              PROTOCOL VARIATIONS

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


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

5.8. Calling Party Information

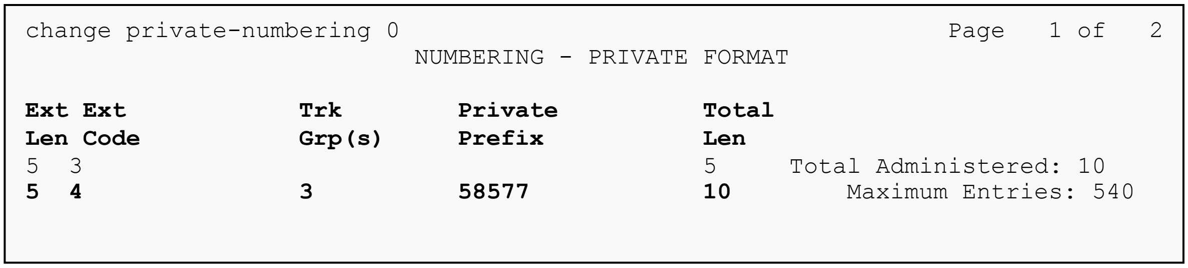
The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are 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 3 numbers were mapped to the 3 enterprise extensions 41011, 41014, and 41016. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 3 extensions.



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

Ext Ext              Trk         Private           Total
Len Code             Grp(s)      Prefix            Len
 5  3                                              5     Total Administered: 10
 5  4                                              5         Maximum Entries: 540
 5  41011            3           5857741111        10
 5  41014            3           5857741112        10
 5  41016            3           5857741113        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 4 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  3                                               5     Total Administered: 10
5  4                 3           58577             10        Maximum Entries: 540
```

Even though private numbering was selected, currently the number used in the SIP Diversion header is derived from the public unknown numbering table and not the private numbering table. As a workaround for this, the entries in the private numbering table must be repeated in the public unknown numbering table.

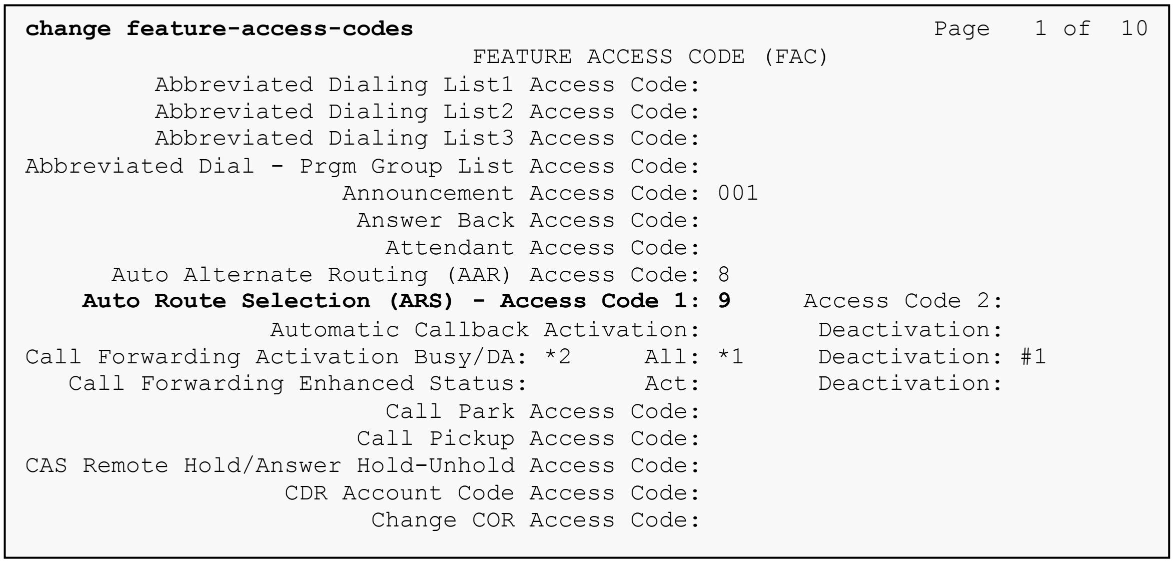
```
change public-unknown-numbering 0                                Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext             Trk       CPN            CPN
Len Code            Grp(s)    Prefix         Len
                                                   Total Administered: 12
 5  3                                        5        Maximum Entries: 240
 5  4                                        5
 5  41012           3         5857741111     10    Note: If an entry applies to
 5  41014           3         5857741112     10    a SIP connection to Avaya to
 5  41016           3         5857741113     10    Aura(tm) Session Manager,
                                                   the resulting number must
                                                   be a complete E.164 number.
```

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**).

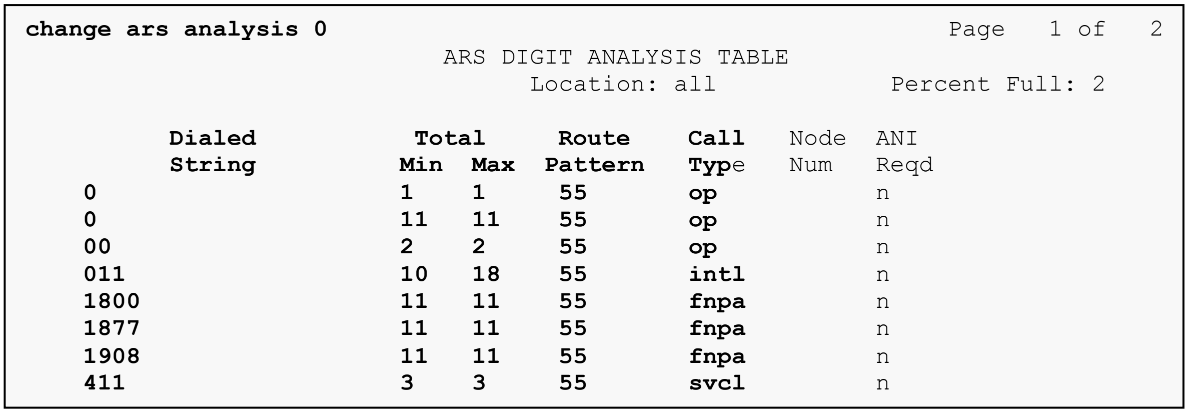
```
change dialplan analysis                                         Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 3

    Dialed    Total  Call      Dialed    Total  Call      Dialed    Total  Call
    String    Length Type      String    Length Type      String    Length Type
   0            1   fac       9           1   fac
   00           3   fac       *           2   fac
   01           3   fac       #           2   fac
   1            3   dac
   2            5   ext
   3            5   ext
   4            5   ext
   44           5   ext
   5            5   ext
   50           4   ext
   6            5   ext
   7            5   ext
   732          10  udp
   777          7   udp
   8            1   fac
```

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



```
change feature-access-codes                                     Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: 001
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *2     All: *1     Deactivation: #1
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
```

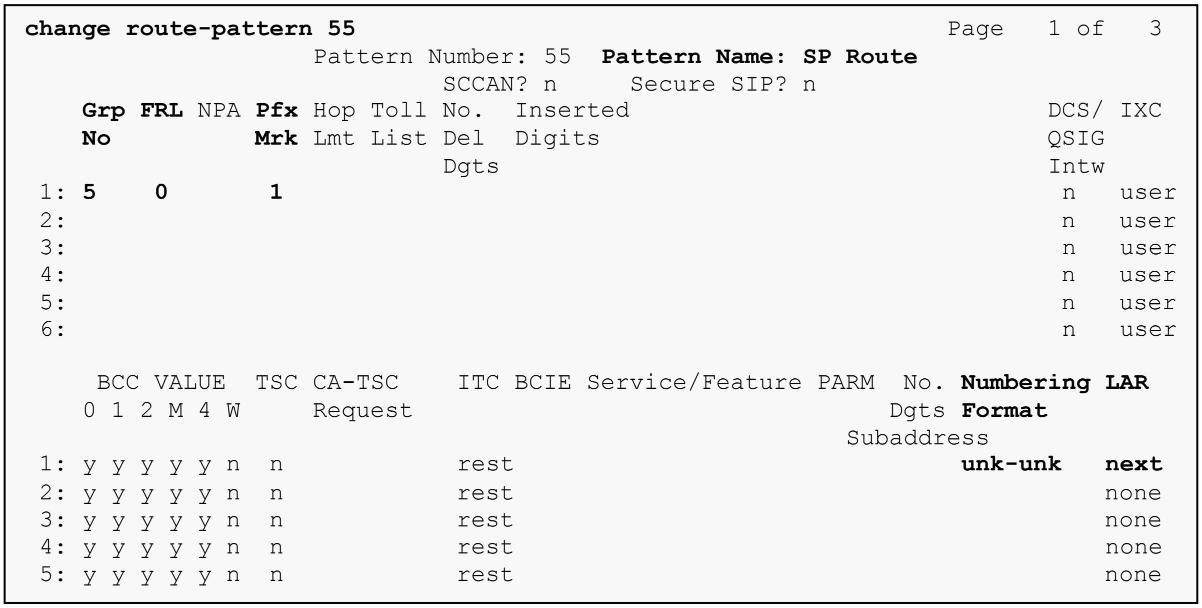
Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 55 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: 2

          Dialed          Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
    0                    1    1      55      op           n
    0                    11   11     55      op           n
    00                   2    2      55      op           n
    011                  10   18     55      intl         n
    1800                 11   11     55      fnpa         n
    1877                 11   11     55      fnpa         n
    1908                 11   11     55      fnpa         n
    411                  3    3      55      svcl         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 55 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**: ***1*** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **LAR**: ***next***



```
change route-pattern 55                                         Page   1 of   3
                    Pattern Number: 55  Pattern Name: 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   next
 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. Configure Avaya Aura® Session Manager

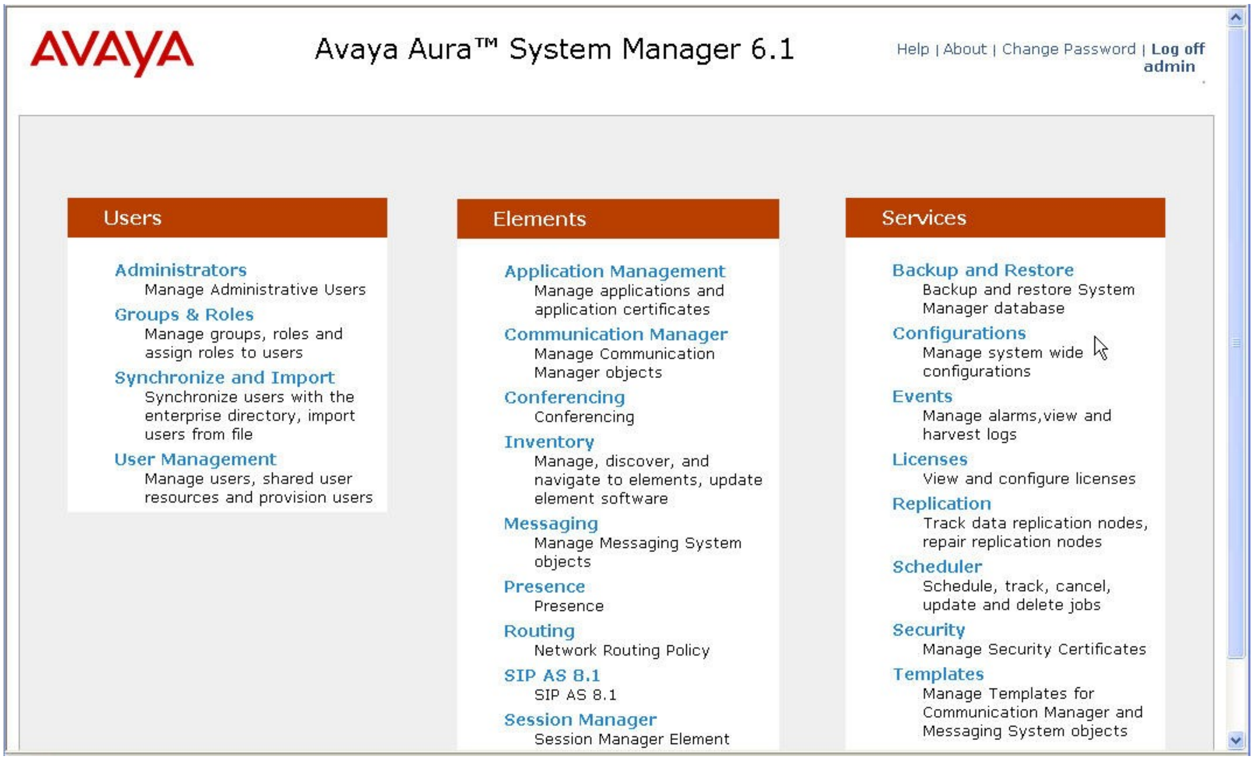
This section provides the procedures for configuring Session Manager. The procedures include the following items:

- Specify SIP domain
- Add Logical/physical Location that can be occupied by SIP Entities
- 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.



Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Users

Administrators
Manage Administrative Users

Groups & Roles
Manage groups, roles and assign roles to users

Synchronize and Import
Synchronize users with the enterprise directory, import users from file

User Management
Manage users, shared user resources and provision users

Elements

Application Management
Manage applications and application certificates

Communication Manager
Manage Communication Manager objects

Conferencing
Conferencing

Inventory
Manage, discover, and navigate to elements, update element software

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

SIP AS 8.1
SIP AS 8.1

Session Manager
Session Manager Element

Services

Backup and Restore
Backup and restore System Manager database

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

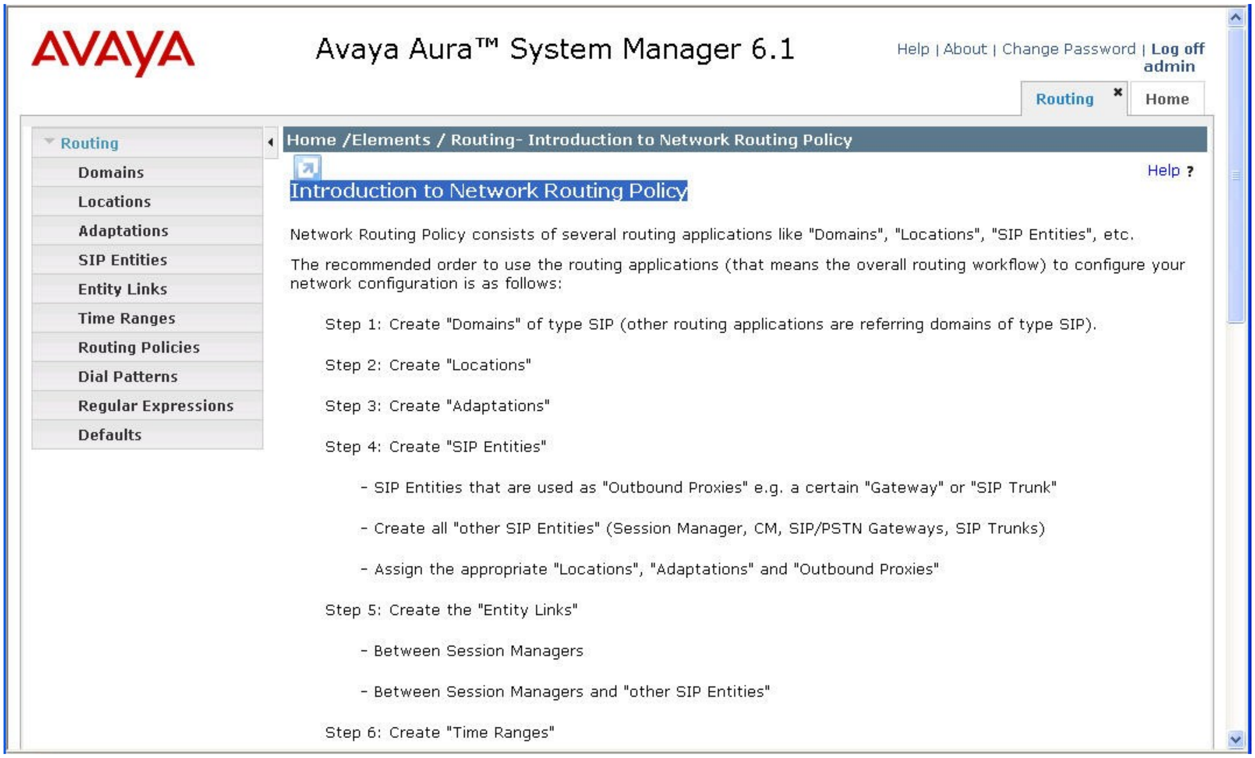
Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager and Messaging System objects

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.



Introduction to Network Routing Policy

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

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

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

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

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

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

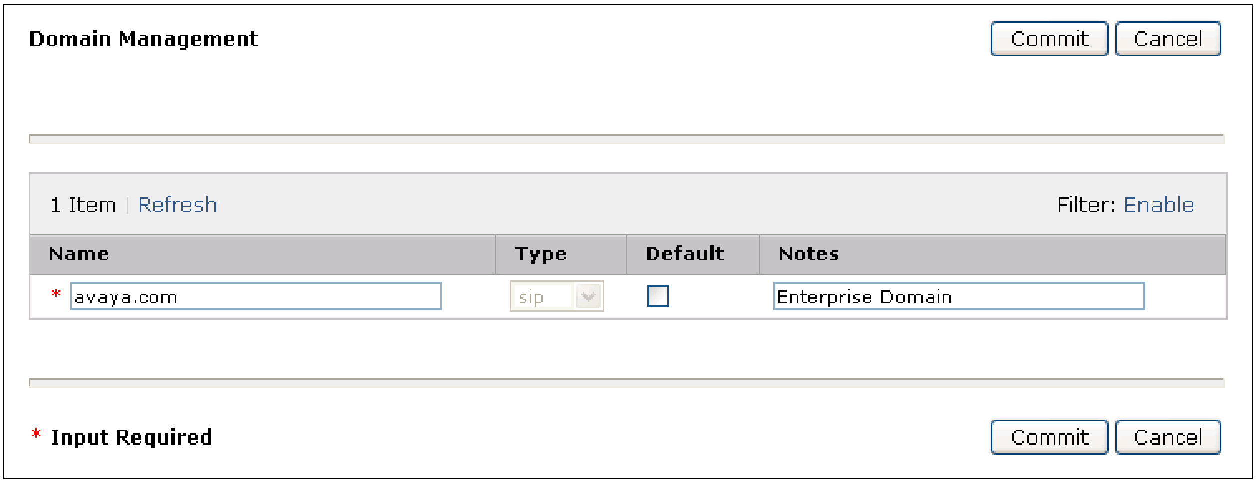
Step 6: Create "Time Ranges"

6.2. Specify SIP Domain

Create a SIP domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (***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.



Domain Management

Name	Type	Default	Notes
* avaya.com	sip	□	Enterprise Domain

* Input Required

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).

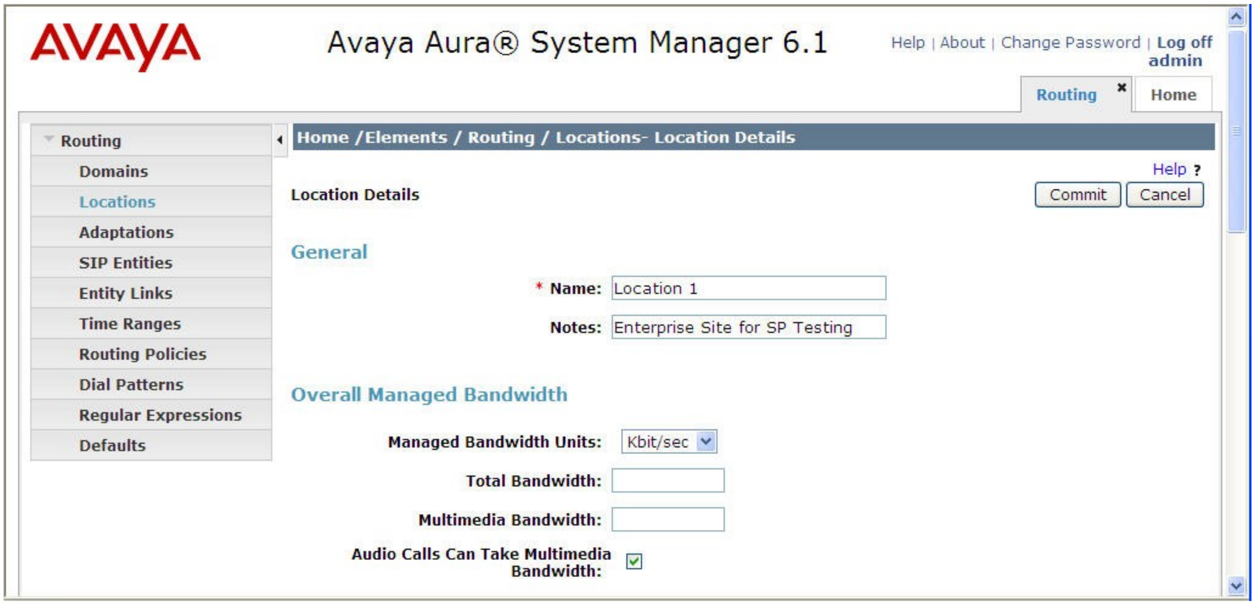
In the **General** section, enter the following values:

- **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 **Location 1** Location, which includes all equipment on the enterprise network including Communication Manager and the Session Manager itself. Click **Commit** to save.



Location Details

General

* Name: Location 1

Notes: Enterprise Site for SP Testing

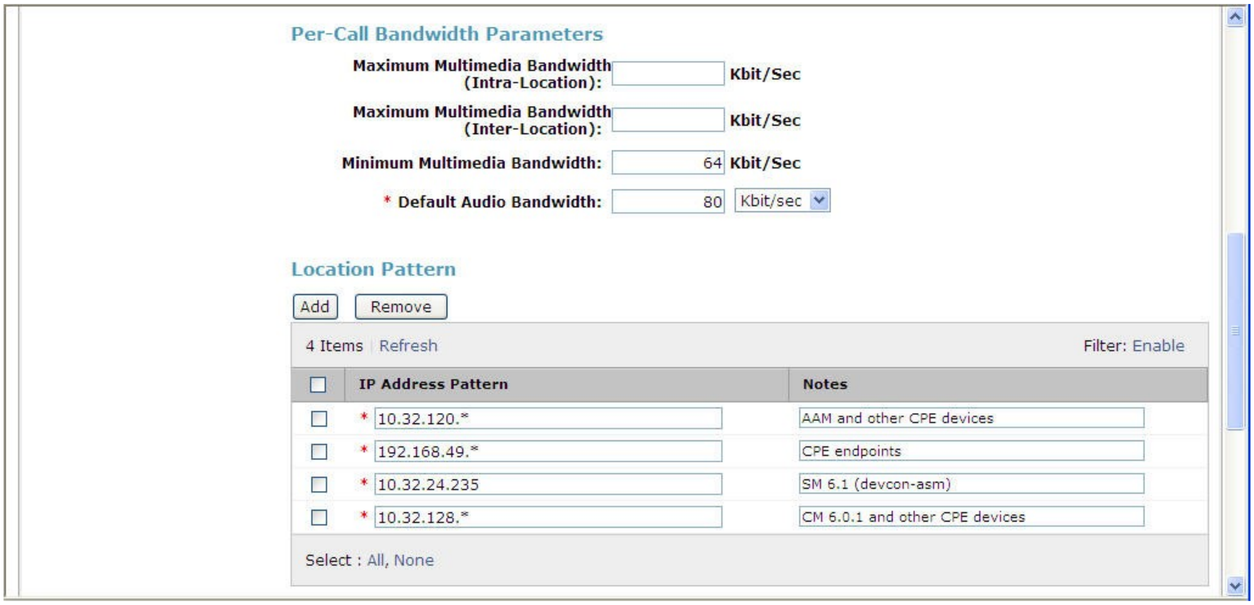
Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑



Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

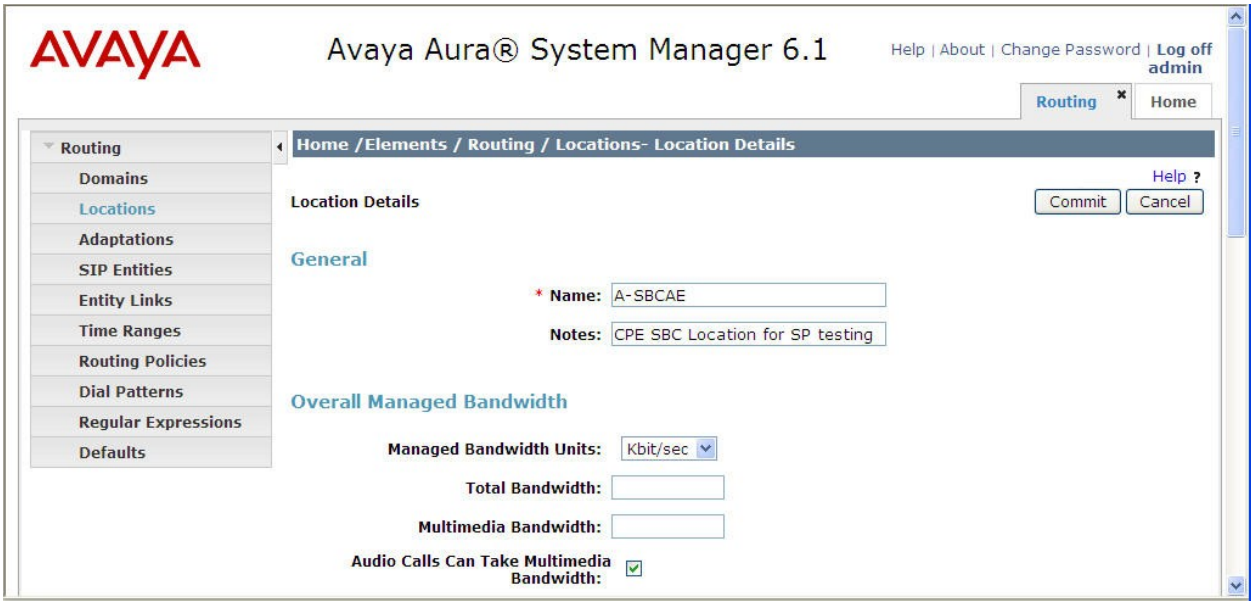
Location Pattern

4 Items

□	IP Address Pattern	Notes
□	* 10.32.120.*	AAM and other CPE devices
□	* 192.168.49.*	CPE endpoints
□	* 10.32.24.235	SM 6.1 (devcon-asm)
□	* 10.32.128.*	CM 6.0.1 and other CPE devices

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

Repeat the preceding procedure to create a separate Location for Avaya SBC for Enterprise. Displayed below are the top and bottom halves of the screen for addition of the **A-SBCAE** Location, which specifies the specific inside IP address for the SBC. Click **Commit** to save.



Home /Elements / Routing / Locations- Location Details

Location Details

General

* Name: A-SBCAE

Notes: CPE SBC Location for SP testing

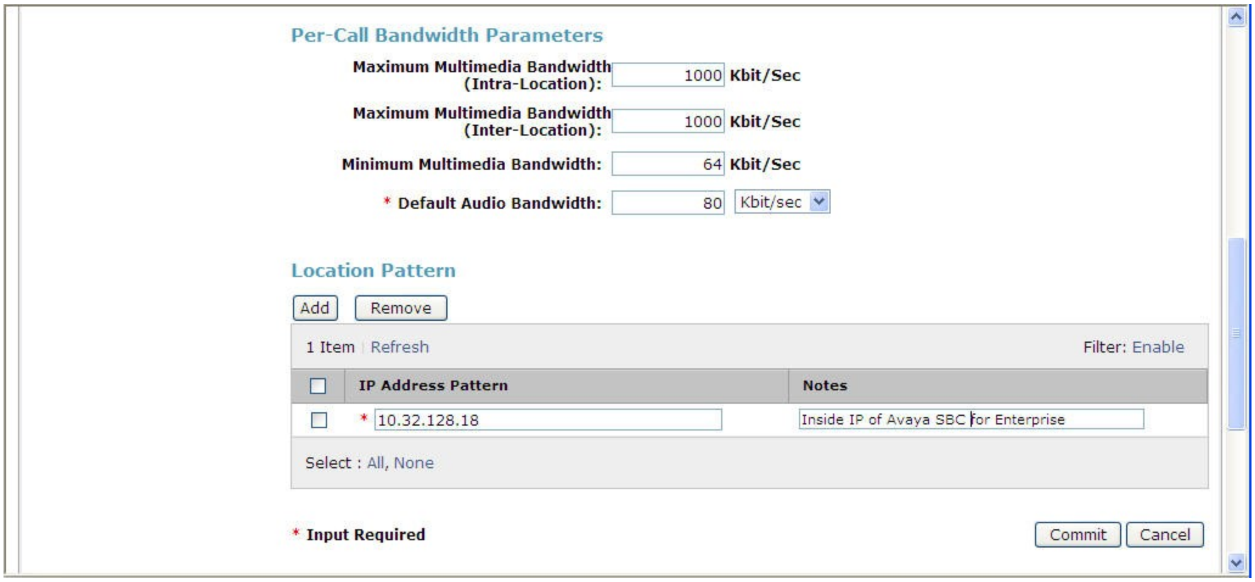
Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑



Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

□	IP Address Pattern	Notes
□	* 10.32.128.18	Inside IP of Avaya SBC for Enterprise

Select : All, None

* Input Required

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.

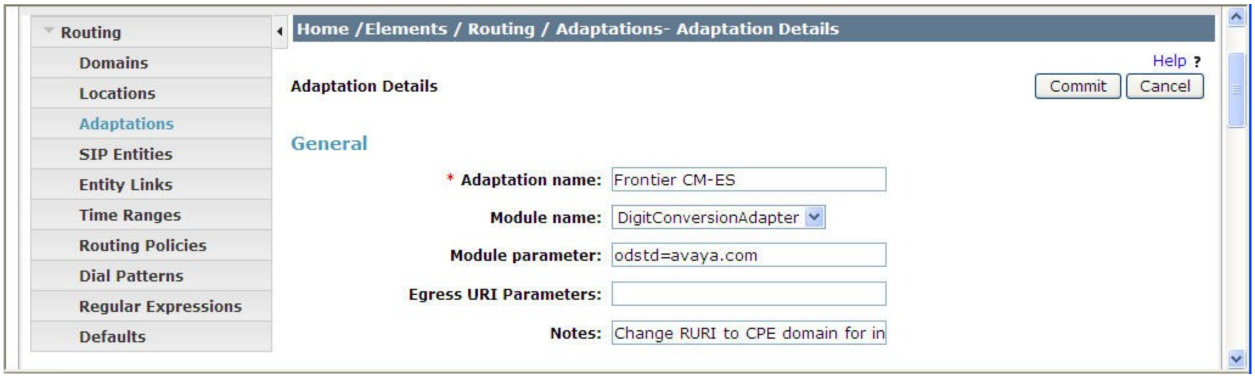
For interoperability with Frontier SIP Trunking, two adaptations are needed. The first adaptation is applied to the Communication Manager SIP entity and maps inbound DID numbers from Frontier to local Communication Manager extensions. The second adaptation is applied to the Avaya SBC for Enterprise SIP entity and converts the domain part of the outbound Request URI from Session Manager containing the enterprise domain to the Frontier SIP proxy IP address.

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

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

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter ***DigitConversionAdapter***
- **Module parameter:** Enter ***odstd=avaya.com***. This is the OverrideDestinationDomain parameter. This parameter replaces the domain in the Request URI with the given value for outbound only.

This adaptation uses the **DigitConversionAdapter** and specifies the **odstd=avaya.com** parameter to adapt the outbound destination domain to the domain expected by Communication Manager. More specifically, this configuration enables the destination domain to be overwritten with **avaya.com** for calls that egress to a SIP entity using this adapter. For example, for inbound PSTN calls from Frontier to the enterprise, the Request-URI sent to Communication Manager will contain **avaya.com** as expected by Communication Manager.



Adaptation Details

General

* Adaptation name: Frontier CM-ES

Module name: DigitConversionAdapter

Module parameter: odstd=avaya.com

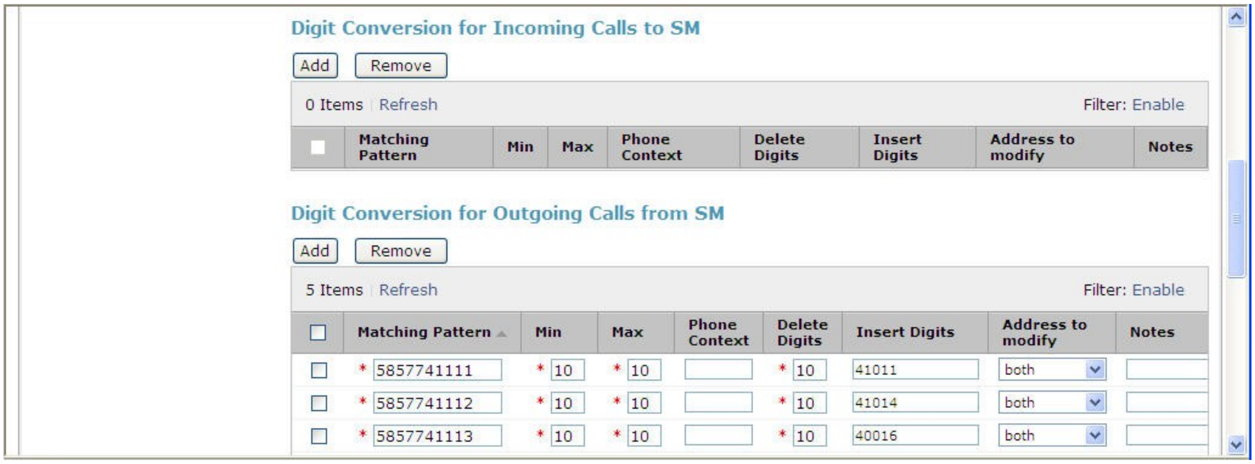
Egress URI Parameters:

Notes: Change RURI to CPE domain for in

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 **both**.

Click **Commit** to save.



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	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	Notes
□	* 5857741111	* 10	* 10		* 10	41011	both	
□	* 5857741112	* 10	* 10		* 10	41014	both	
□	* 5857741113	* 10	* 10		* 10	40016	both	

In the example shown above, if a user on the PSTN dials 585-774-1112, Session Manager will convert the number to 41014 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 was configured with an entry to convert 41012 to 5857741112 before sending the call on the trunk group to Session Manager (as shown in **Section 5.8**).

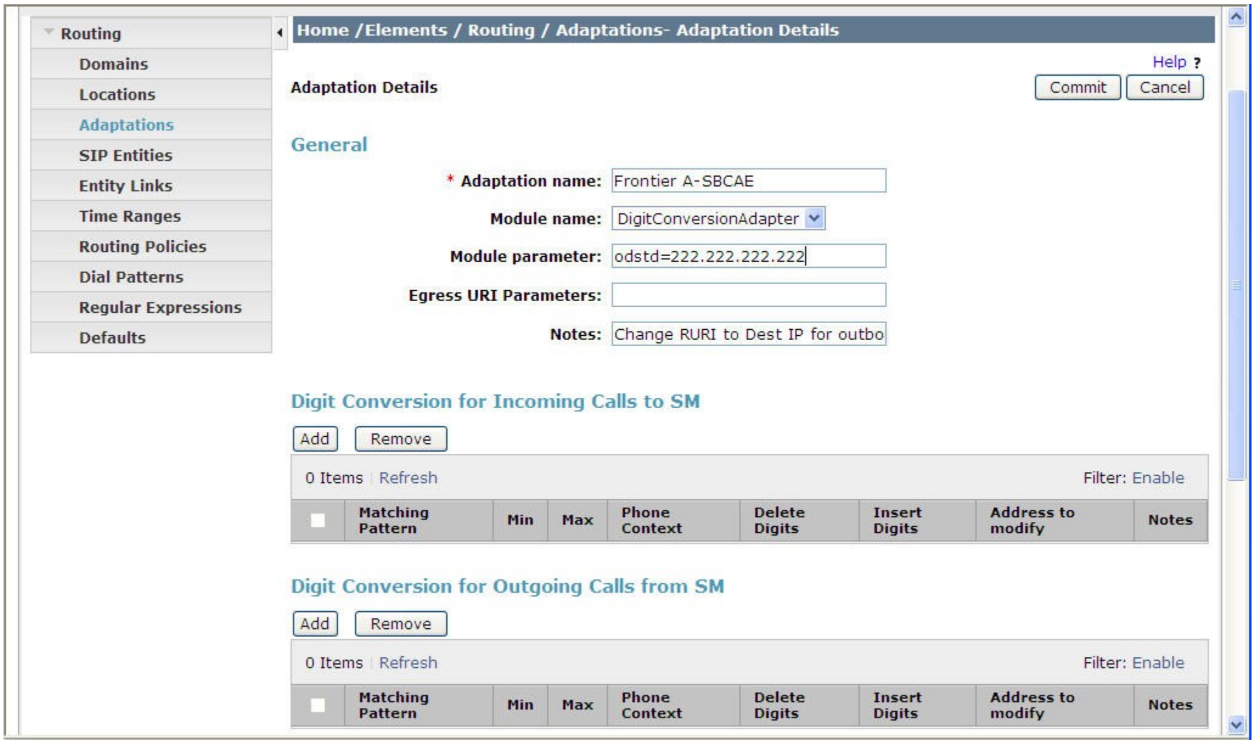
During the compliance test, the digit conversions (or number mappings) in Session Manager **adaptation** as well as in **private-numbering** and **public-unknown-numbering** tables (see **Section 5.8**) were varied to route inbound calls to various destinations (including Communication Manager Vector Directory Numbers) for different test cases.

To create the adaptation that will be applied to the Avaya SBC for Enterprise SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

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

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter ***DigitConversionAdapter***.
- **Module parameter:** Enter ***odstd=2222.222.222.222***, the IP address for accessing the Frontier SIP Trunking network. This is the OverrideDestinationDomain parameter. This parameter replaces the domain in the Request URI header with the given value for outbound only.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.



Home /Elements / Routing / Adaptations- Adaptation Details

Adaptation Details

General

* Adaptation name: Frontier A-SBCAE

Module name: DigitConversionAdapter

Module parameter: odstd=222.222.222.222

Egress URI Parameters:

Notes: Change RURI to Dest IP for outbo

Digit Conversion for Incoming Calls to SM

0 Items

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

Digit Conversion for Outgoing Calls from SM

0 Items

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

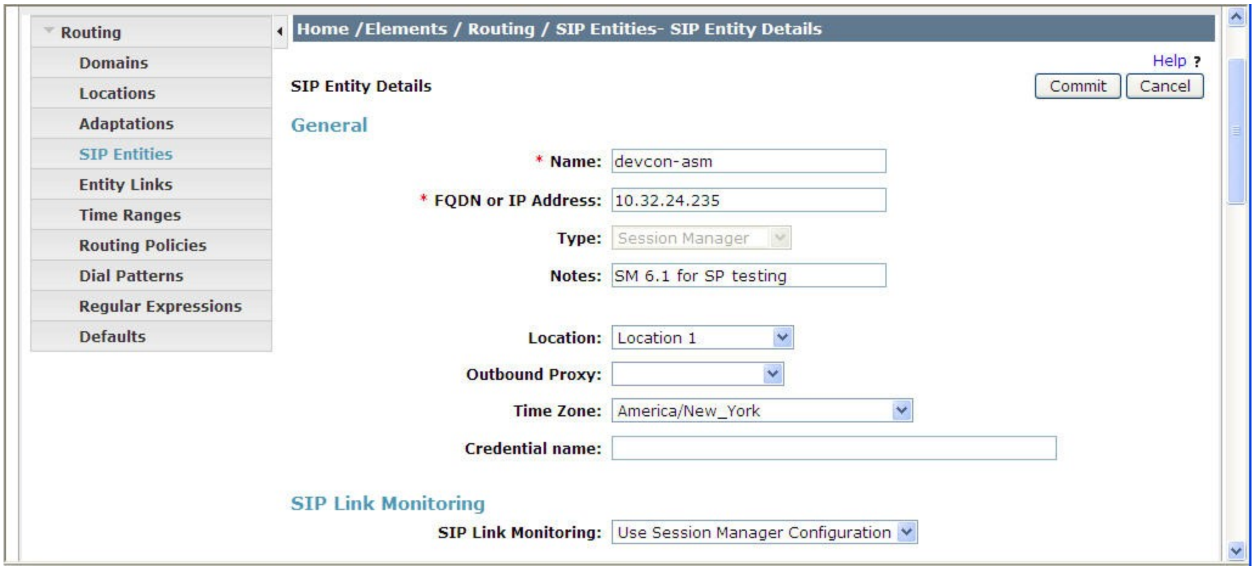
6.5. Add SIP Entities

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 one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

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



SIP Entity Details

General

* Name: devcon-asm

* FQDN or IP Address: 10.32.24.235

Type: Session Manager

Notes: SM 6.1 for SP testing

Location: Location 1

Outbound Proxy:

Time Zone: America/New_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

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

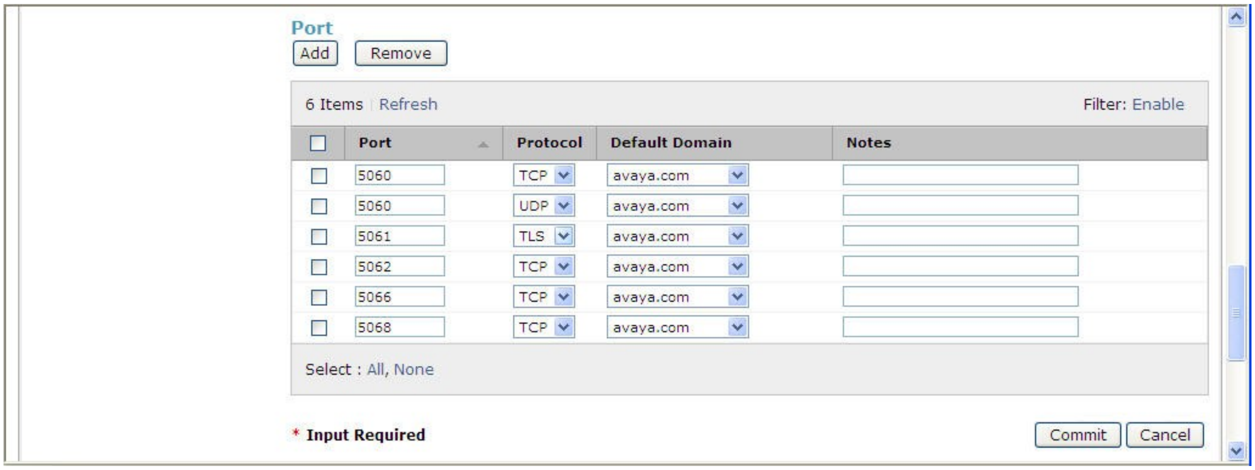
- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

The compliance test used 2 **Port** entries:

– **5060** with **TCP** for connecting to Avaya SBC for Enterprise
– **5068** with **TCP** for connecting to Communication Manager

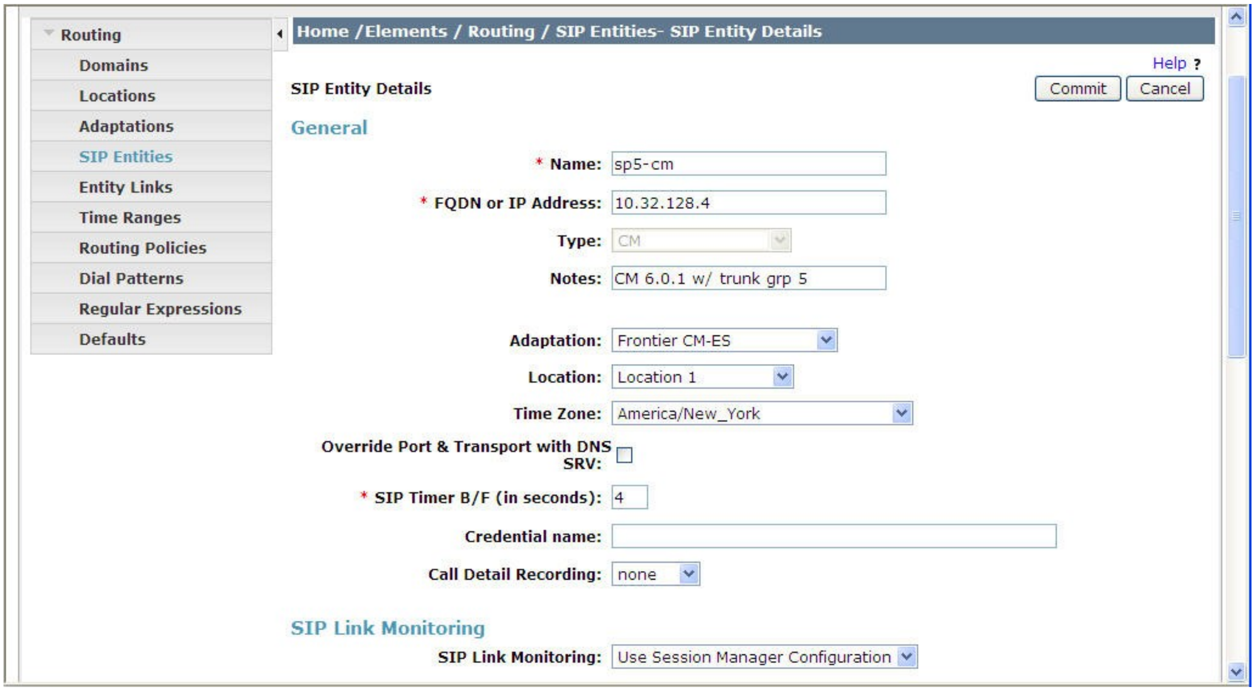
In addition, port 5060 with TCP was also used by a separate SIP Link between Session Manager and Communication Manager for Avaya SIP telephones and SIP soft clients. This SIP Link was part of the standard configuration on Session Manager and was not directly relevant to the inter-operability with Frontier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



6 Items | Refresh

☐	Port	Protocol	Default Domain	Notes
☐	5060	TCP	avaya.com	
☐	5060	UDP	avaya.com	
☐	5061	TLS	avaya.com	
☐	5062	TCP	avaya.com	
☐	5066	TCP	avaya.com	
☐	5068	TCP	avaya.com	

The following screen shows the addition of Communication Manager SIP Entity. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created at Session Manager installation for use with all other SIP traffic 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**.



Home /Elements / Routing / SIP Entities- SIP Entity Details

SIP Entity Details

General

* Name: sp5-cm

* FQDN or IP Address: 10.32.128.4

Type: CM

Notes: CM 6.0.1 w/ trunk grp 5

Adaptation: Frontier CM-ES

Location: Location 1

Time Zone: America/New_York

Override Port & Transport with DNS SRV: □

* SIP Timer B/F (in seconds): 4

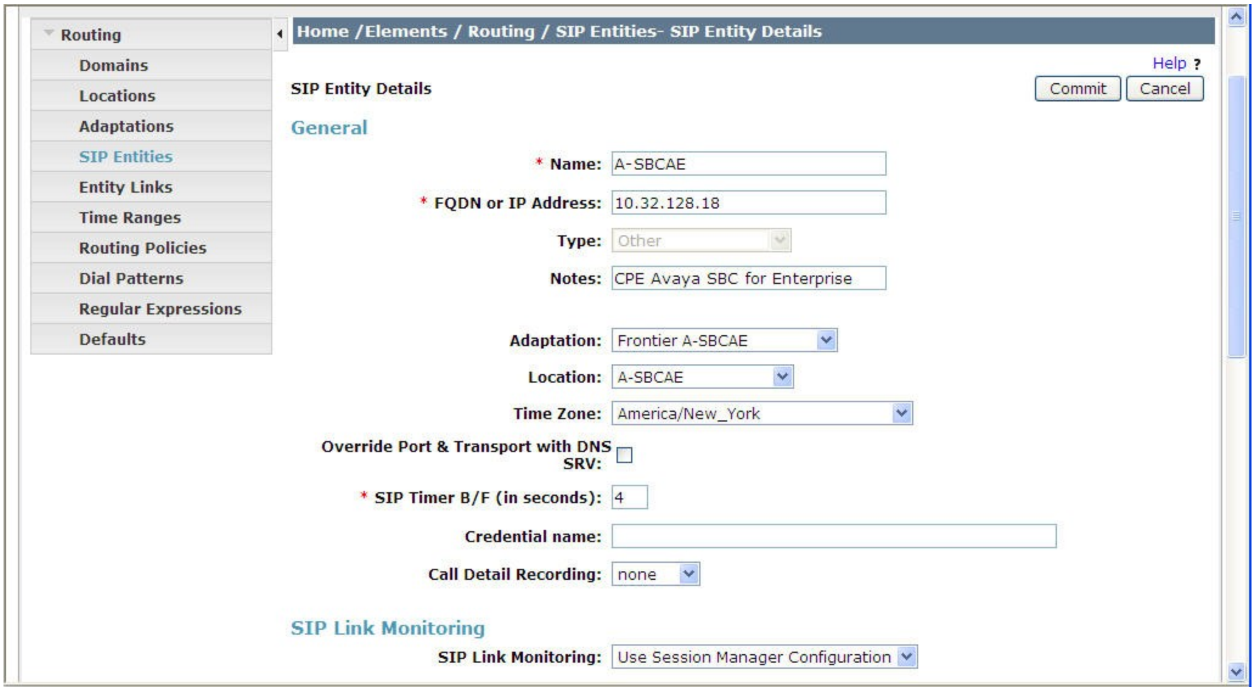
Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the 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**).



SIP Entity Details

General

* Name:	A-SBCAE
* FQDN or IP Address:	10.32.128.18
Type:	Other
Notes:	CPE Avaya SBC for Enterprise
Adaptation:	Frontier A-SBCAE
Location:	A-SBCAE
Time Zone:	America/New_York
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

6.6. Add Entity Links

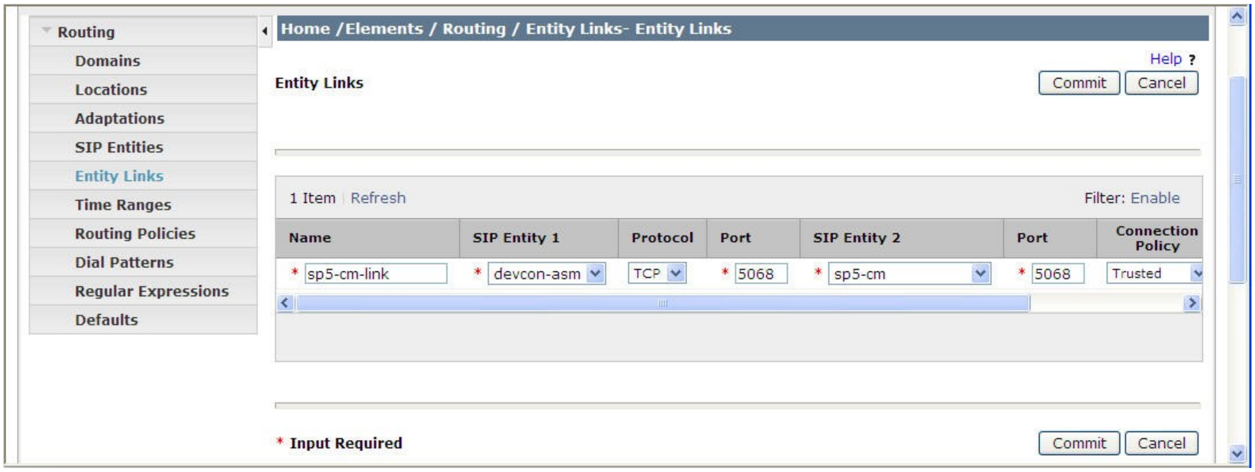
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to Communication Manager for use only by service provider traffic and the other to Avaya SBC for Enterprise. To add an Entity Link, navigate to **Routing → Entity Links** in the 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. For the compliance test, TCP was used to aid in troubleshooting since the signaling traffic would not be encrypted. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.

Entity Link to Communication Manager:



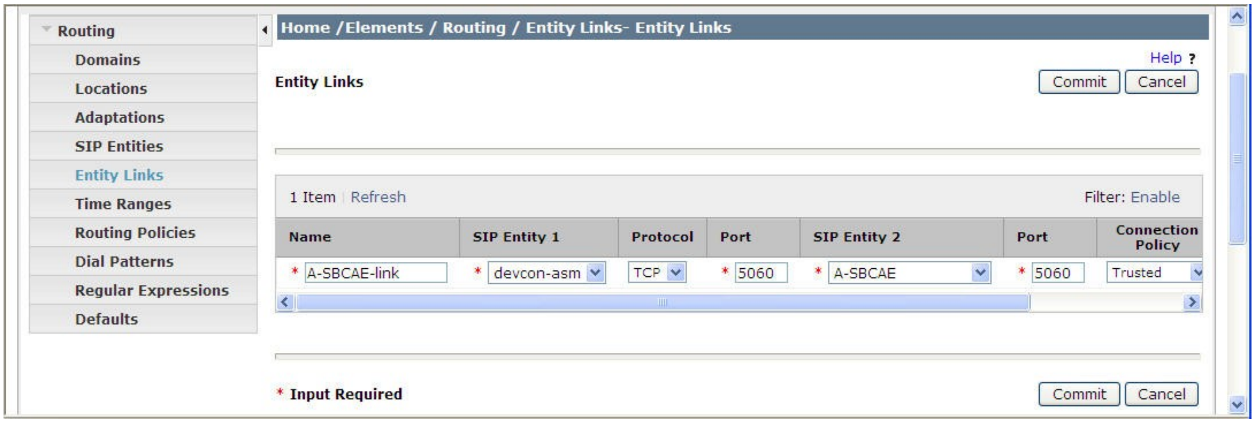
Entity Links

1 Item | Refresh   Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* sp5-cm-link	* devcon-asm	TCP	* 5068	* sp5-cm	* 5068	Trusted

* Input Required

Entity Link to Avaya SBC for Enterprise:



Entity Links

1 Item | Refresh   Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* A-SBCAE-link	* devcon-asm	TCP	* 5060	* A-SBCAE	* 5060	Trusted

* Input Required

Note that a separate Entity Link existed between Communication Manager and Session Manager (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 Avaya Aura® 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:

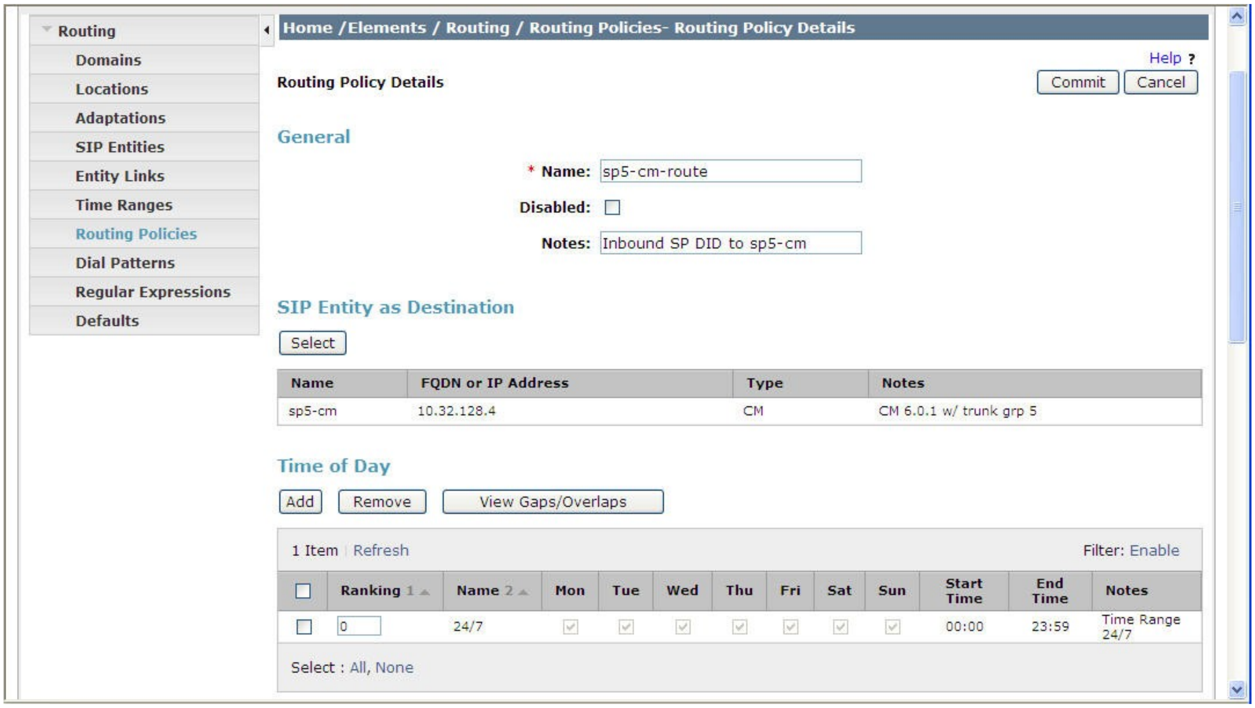
In the **General** section, enter the following values. Use default values for all remaining fields:

- **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.

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

Routing Policy for Communication Manager:



Routing Policy Details

General

* Name: sp5-cm-route

Disabled: □

Notes: Inbound SP DID to sp5-cm

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
sp5-cm	10.32.128.4	CM	CM 6.0.1 w/ trunk grp 5

Time of Day

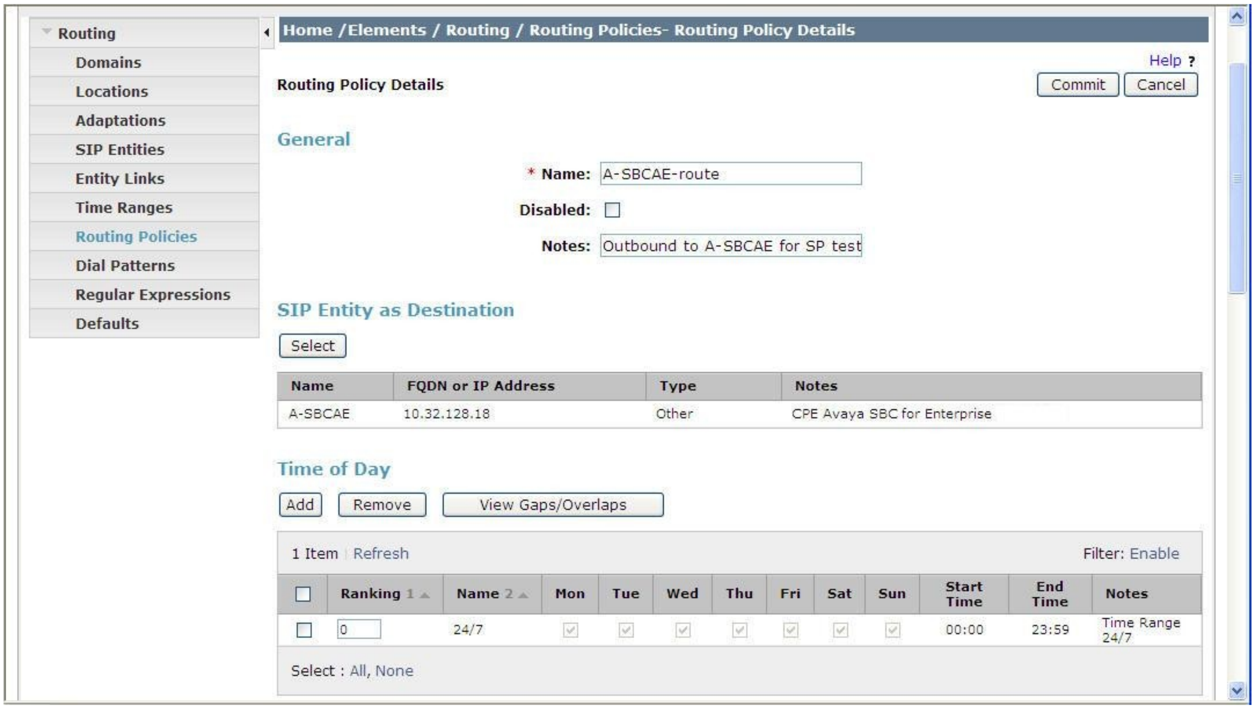
Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Routing Policy for Avaya SBC for Enterprise:



Routing Policy Details

General

* Name: A-SBCAE-route

Disabled: □

Notes: Outbound to A-SBCAE for SP test

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
A-SBCAE	10.32.128.18	Other	CPE Avaya SBC for Enterprise

Time of Day

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

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

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

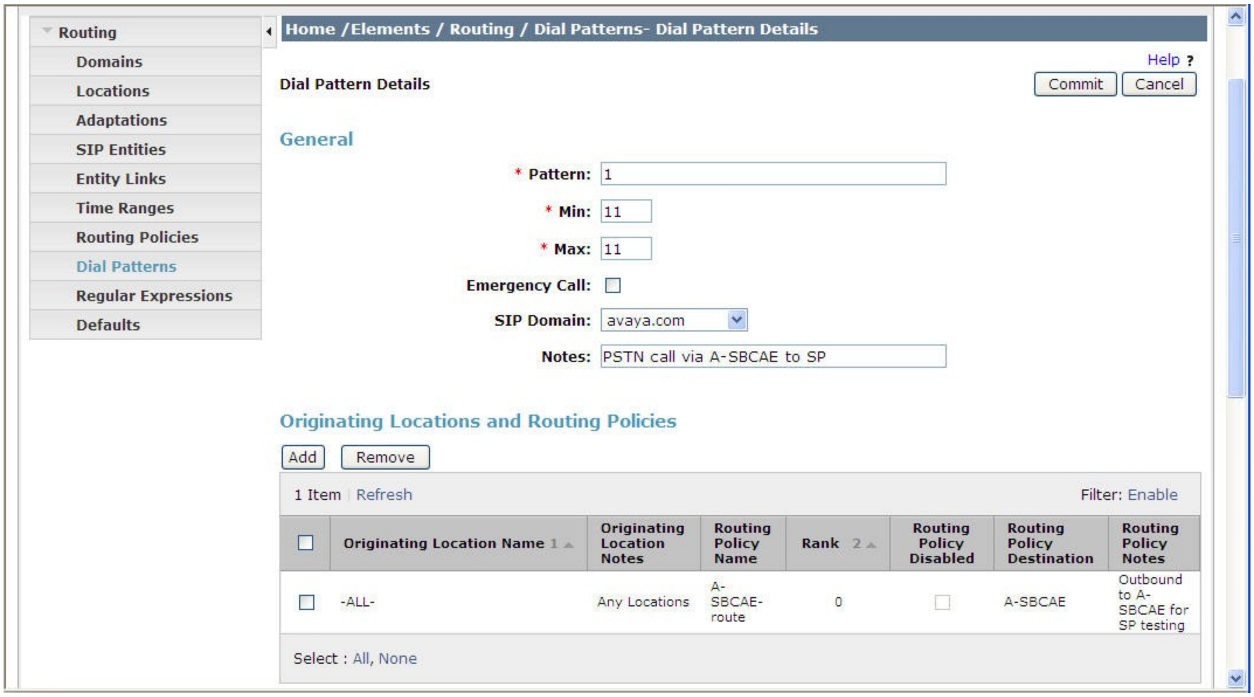
- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:**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

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

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

Two examples of the dial patterns used for the compliance test are shown below, 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 domain of ***avaya.com*** (to be adapted to the destination IP address by the "Frontier A-SBCAE" adaptation defined in **Section 6.4**) uses route policy ***A-SBCAE-route*** as defined in **Section 6.7**.



Home /Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details

General

* Pattern: 1

* Min: 11

* Max: 11

Emergency Call: □

SIP Domain: avaya.com

Notes: PSTN call via A-SBCAE to SP

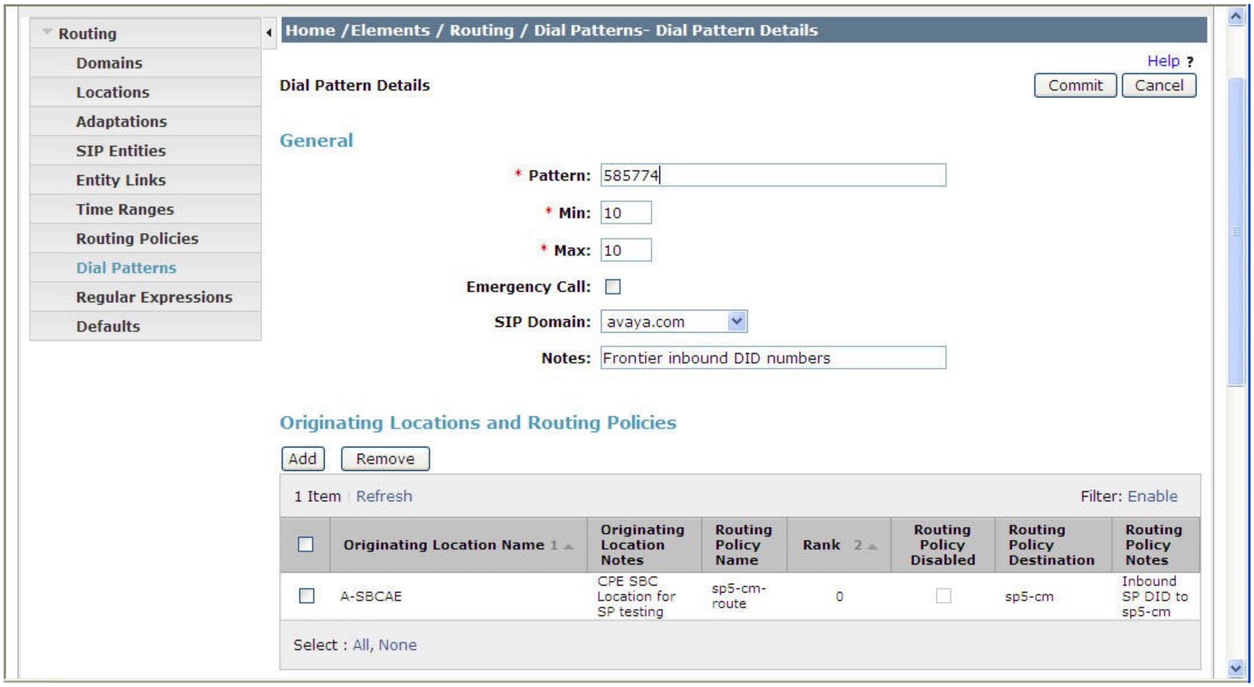
Originating Locations and Routing Policies

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	A-SBCAE-route	0	□	A-SBCAE	Outbound to A-SBCAE for SP testing

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 Pattern 1908, 1732, etc. with 11 digits) per customer business policies.

Also note that ***–ALL-*** was selected for Originating Location. This selection was 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 ***Location 1*** could have been selected.

The second example shows that inbound 10-digit numbers that start with ***585774*** uses route policy ***sp5-cm-route*** as defined in **Section 6.7**. This dial pattern matches the DID numbers assigned to the enterprise by Frontier. Location ***A-SBCAE*** was selected as the originating location to indicate these calls come via Avaya SBC for Enterprise.



Dial Pattern Details

General

* Pattern:	585774
* Min:	10
* Max:	10
Emergency Call:	□
SIP Domain:	avaya.com
Notes:	Frontier inbound DID numbers

Originating Locations and Routing Policies

1 Item | Refresh   Filter: Enable

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	A-SBCAE	CPE SBC Location for SP testing	sp5-cm-route	0	□	sp5-cm	Inbound SP DID to sp5-cm

Select : All, None

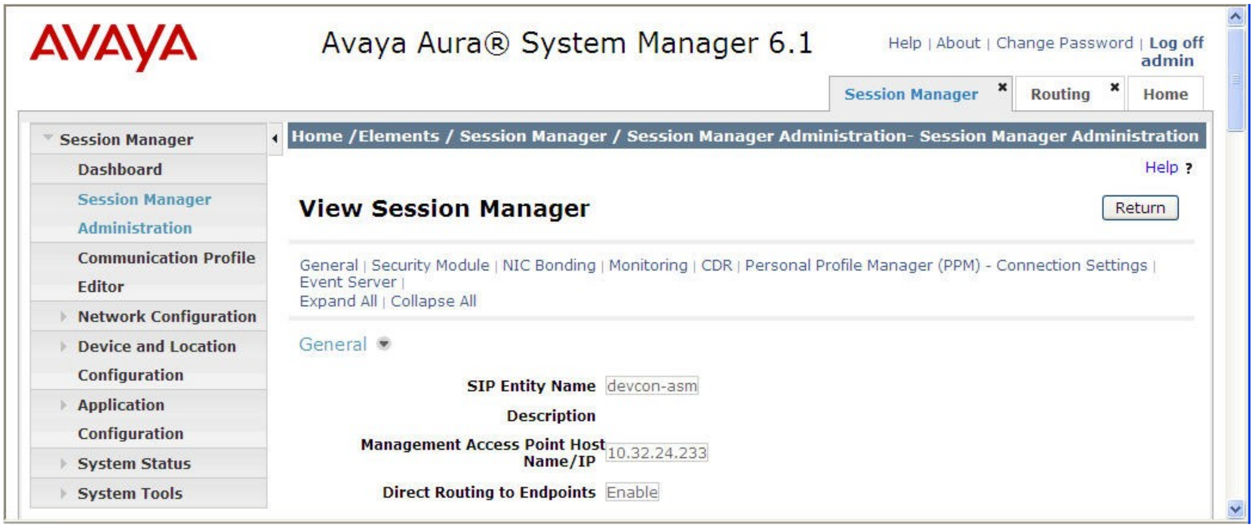
6.9. Add/View Session Manager

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, 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 IP address of the Session Manager management interface.

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


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Routing
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Help ?
Return
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

Home /Elements / Session Manager / Session Manager Administration- Session Manager Administration

View Session Manager

General

SIP Entity Name: devcon-asm

Description:

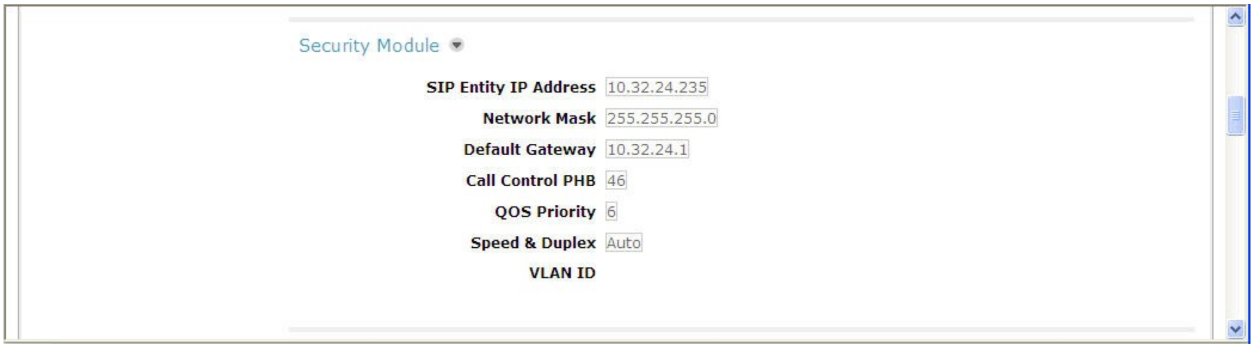
Management Access Point Host Name/IP: 10.32.24.233

Direct Routing to Endpoints: Enable

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.

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.



SIP Entity IP Address	10.32.24.235
Network Mask	255.255.255.0
Default Gateway	10.32.24.1
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	

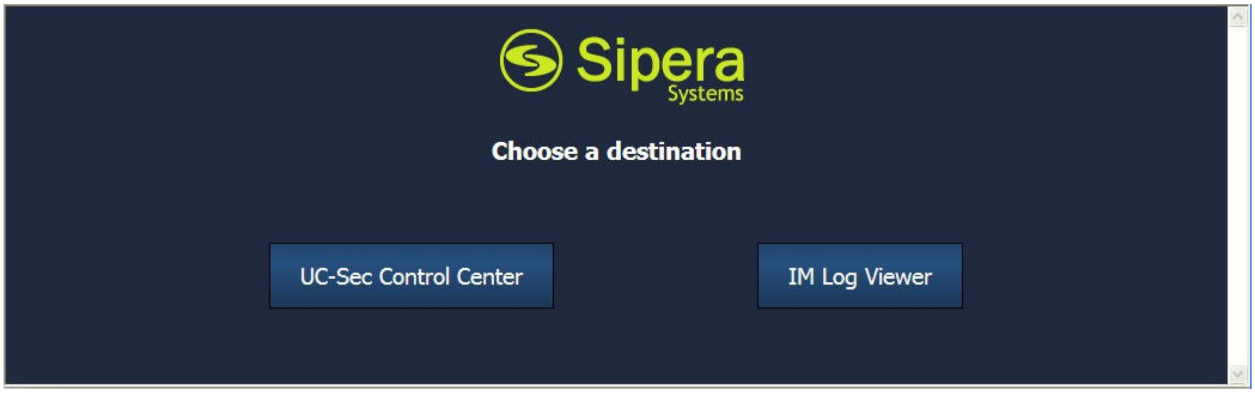
7. Configure Avaya Session Border Controller for Enterprise

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

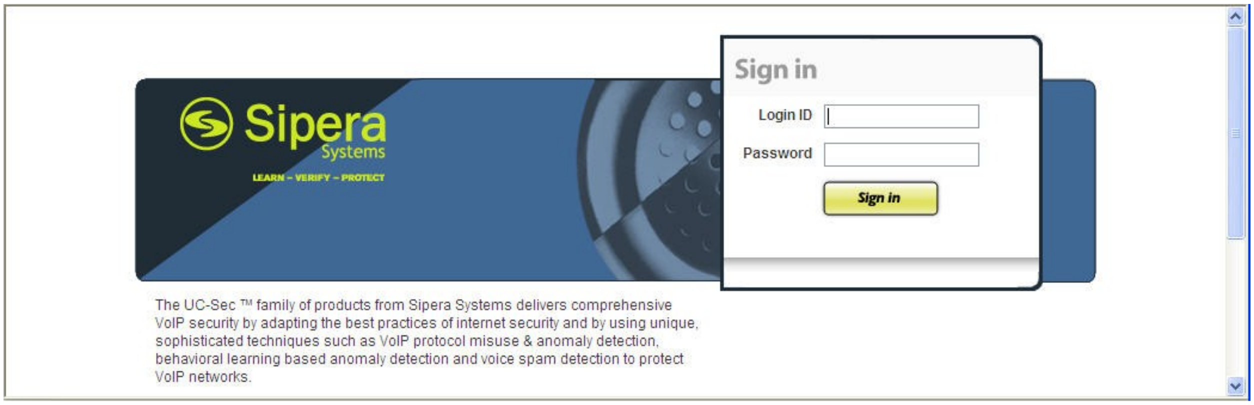
These Application Notes assume that the installation of the SBC and the assignment of a management IP Address have already been completed.

7.1. Access the Management Interface

Use a WEB browser to access the web management interface web interface by entering URL https://<ip-addr>, where <ip-addr> is the management LAN IP address of assigned during installation. Select **UC-Sec Control Center** on the displayed web page.

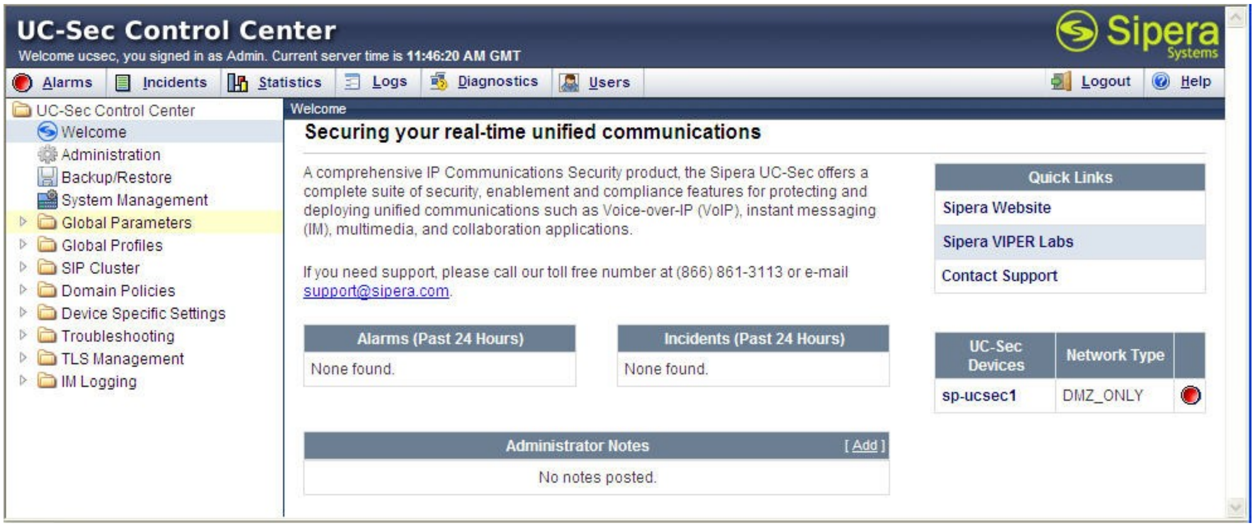


A log in screen is presented. Enter an appropriate **Login ID** and **Password**.



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

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.



Welcome ucsec, you signed in as Admin. Current server time is 11:46:20 AM GMT

Securing your real-time unified communications

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

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

Quick Links
Sipera Website
Sipera VIPER Labs
Contact Support

Alarms (Past 24 Hours)
None found.

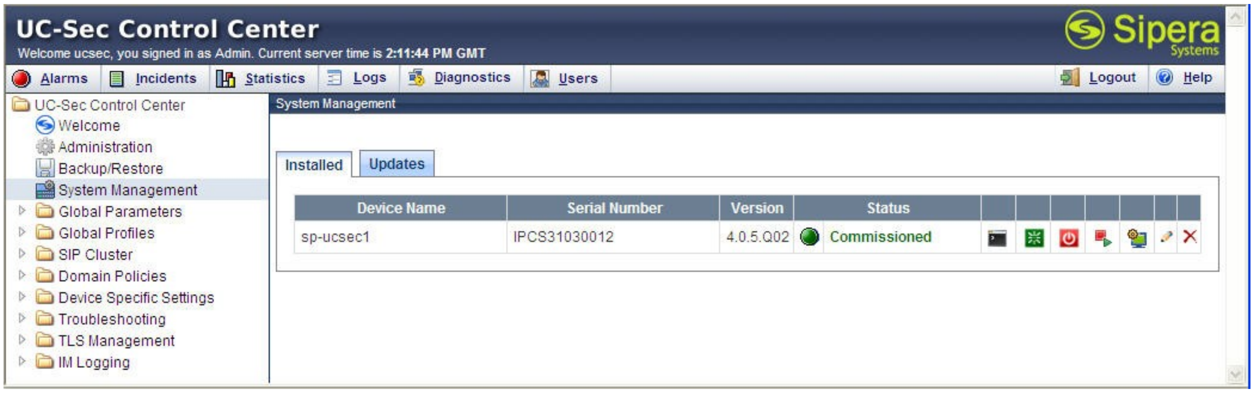
Incidents (Past 24 Hours)
None found.

UC-Sec Devices	Network Type	
sp-ucsec1	DMZ_ONLY	●

Administrator Notes [Add]
No notes posted.

7.2. System Status

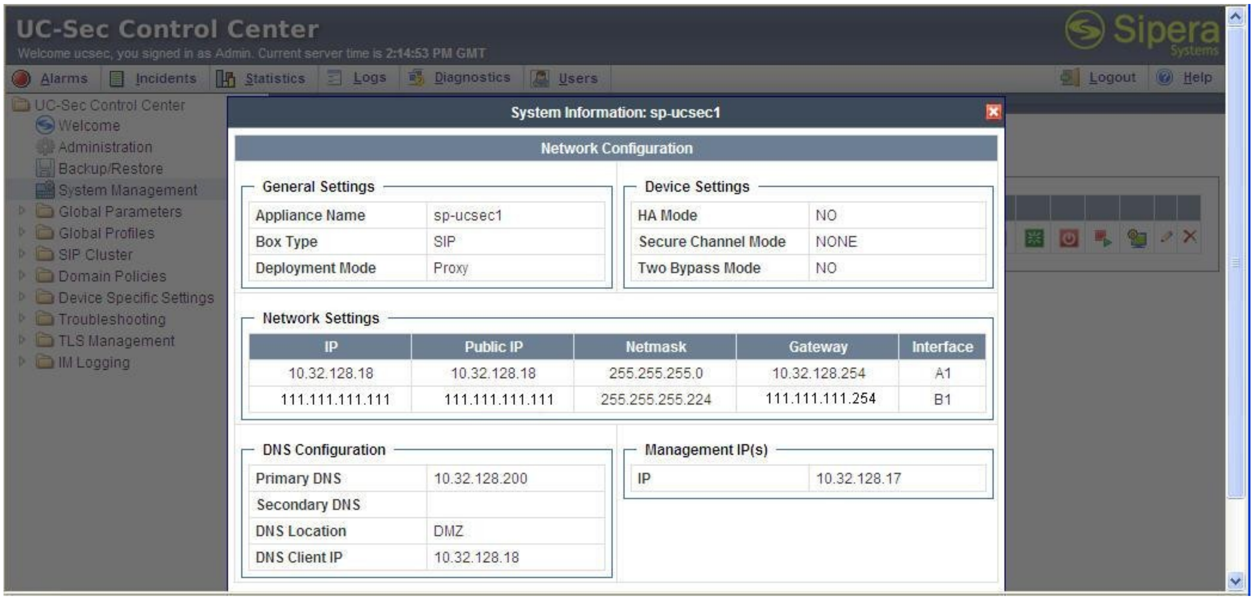
Navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named ***sp-ucsec1*** is shown. Device **Status** "Commissioned" should be displayed as shown below.



Welcome ucsec, you signed in as Admin. Current server time is 2:11:44 PM GMT

Device Name	Serial Number	Version	Status
sp-ucsec1	IPCS31030012	4.0.5.Q02	● Commissioned

To view the network information of this device specified 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 Avaya SBC for Enterprise as shown in **Figure 1**.



Welcome ucsec, you signed in as Admin. Current server time is 2:14:53 PM GMT

System Information: sp-ucsec1

Network Configuration

General Settings

Appliance Name	sp-ucsec1
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	NO
Secure Channel Mode	NONE
Two Bypass Mode	NO

Network Settings

IP	Public IP	Netmask	Gateway	Interface
10.32.128.18	10.32.128.18	255.255.255.0	10.32.128.254	A1
111.111.111.111	111.111.111.111	255.255.255.224	111.111.111.254	B1

DNS Configuration

Primary DNS	10.32.128.200
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.32.128.18

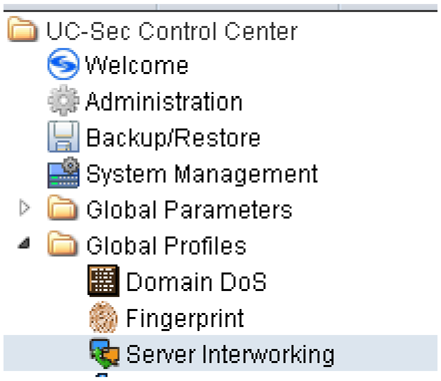
Management IP(s)

IP	10.32.128.17

7.3. Global Profiles – Server Interworking

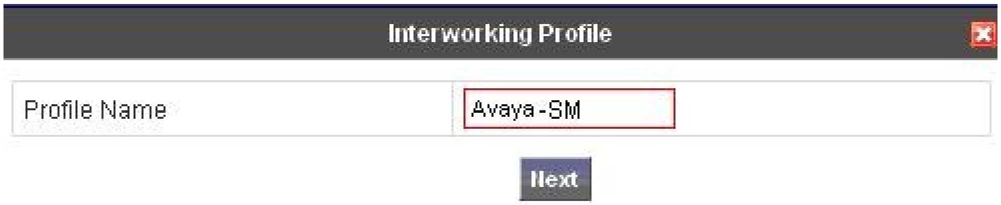
Server interworking is defined for each server connected to Avaya SBC for Enterprise. For the compliance test, the Frontier network-edge SBC serves as the Trunk Server and the Session Manager serves as the Call Server.

Select **Global Profiles → Server Interworking** from the left-side menu as shown below.



7.3.1. Server Interworking: Avaya-SM

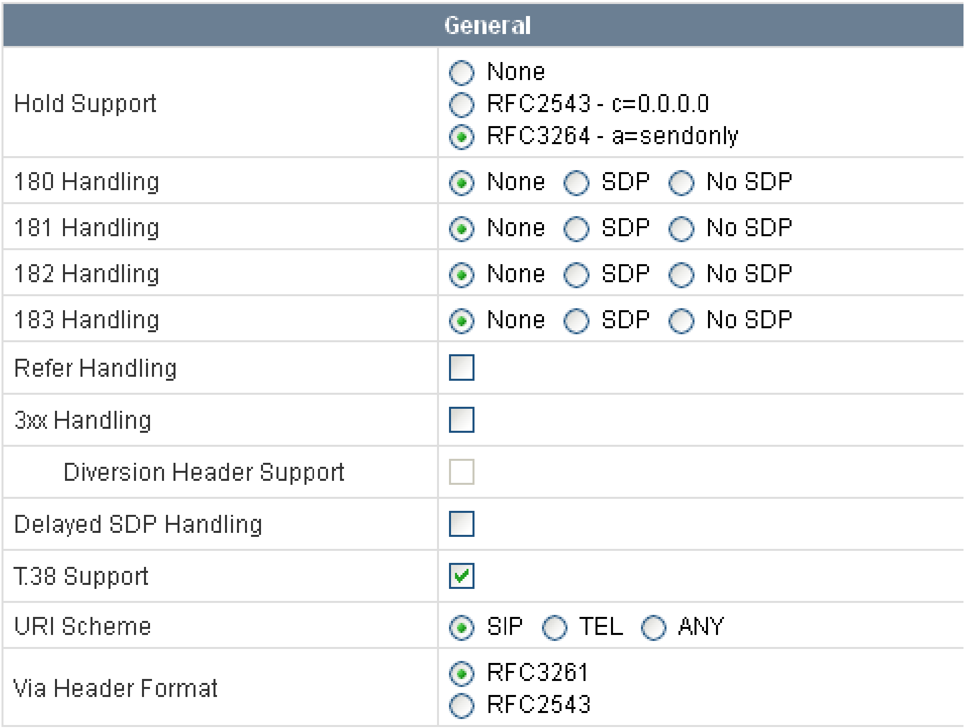
Click the **Add Profile** button (not shown) to add a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as "Avaya-SM" shown below. Click **Next**.



Interworking Profile

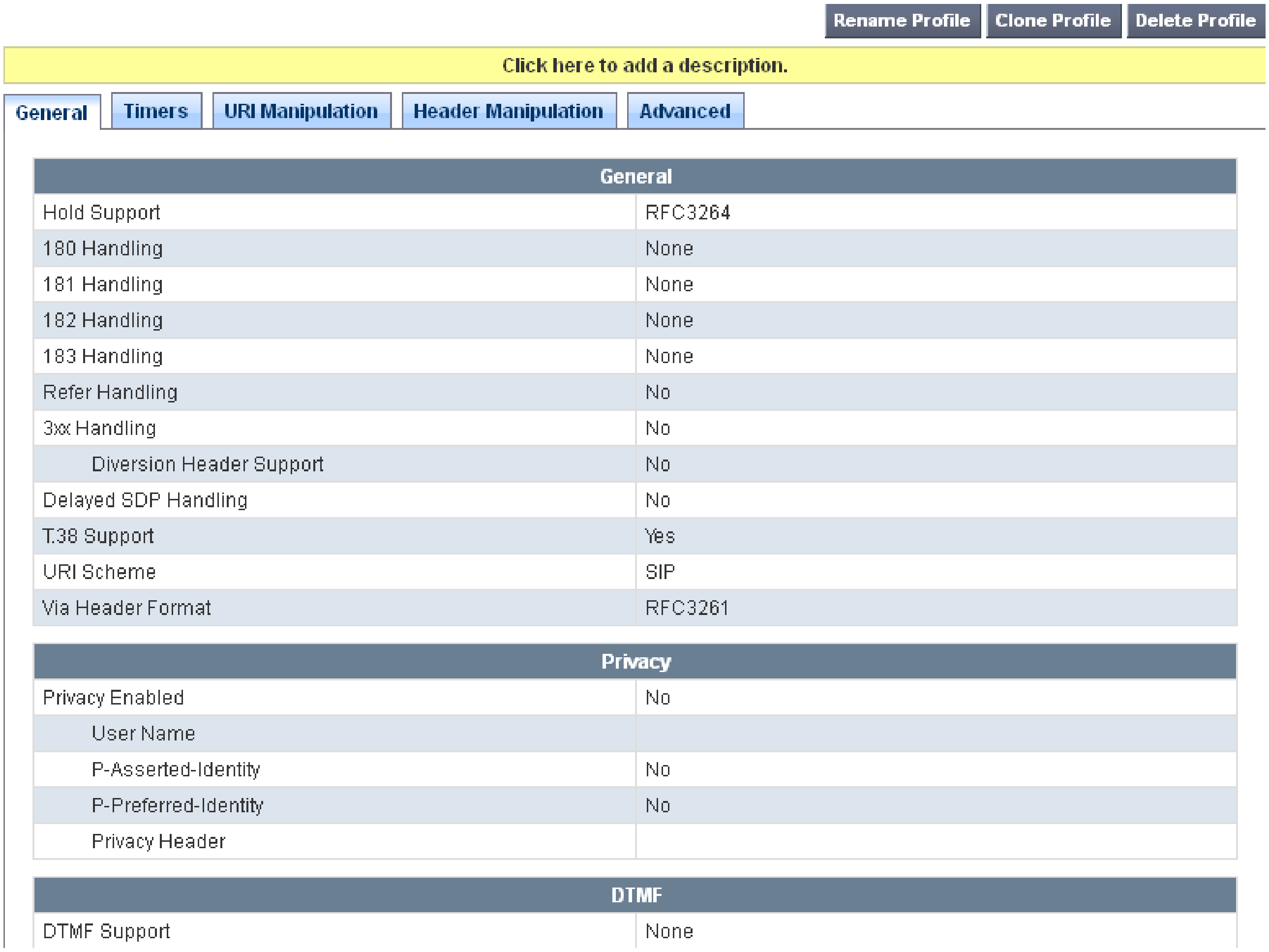
Profile Name	Avaya-SM

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 interworking profile named "Avaya-SM"

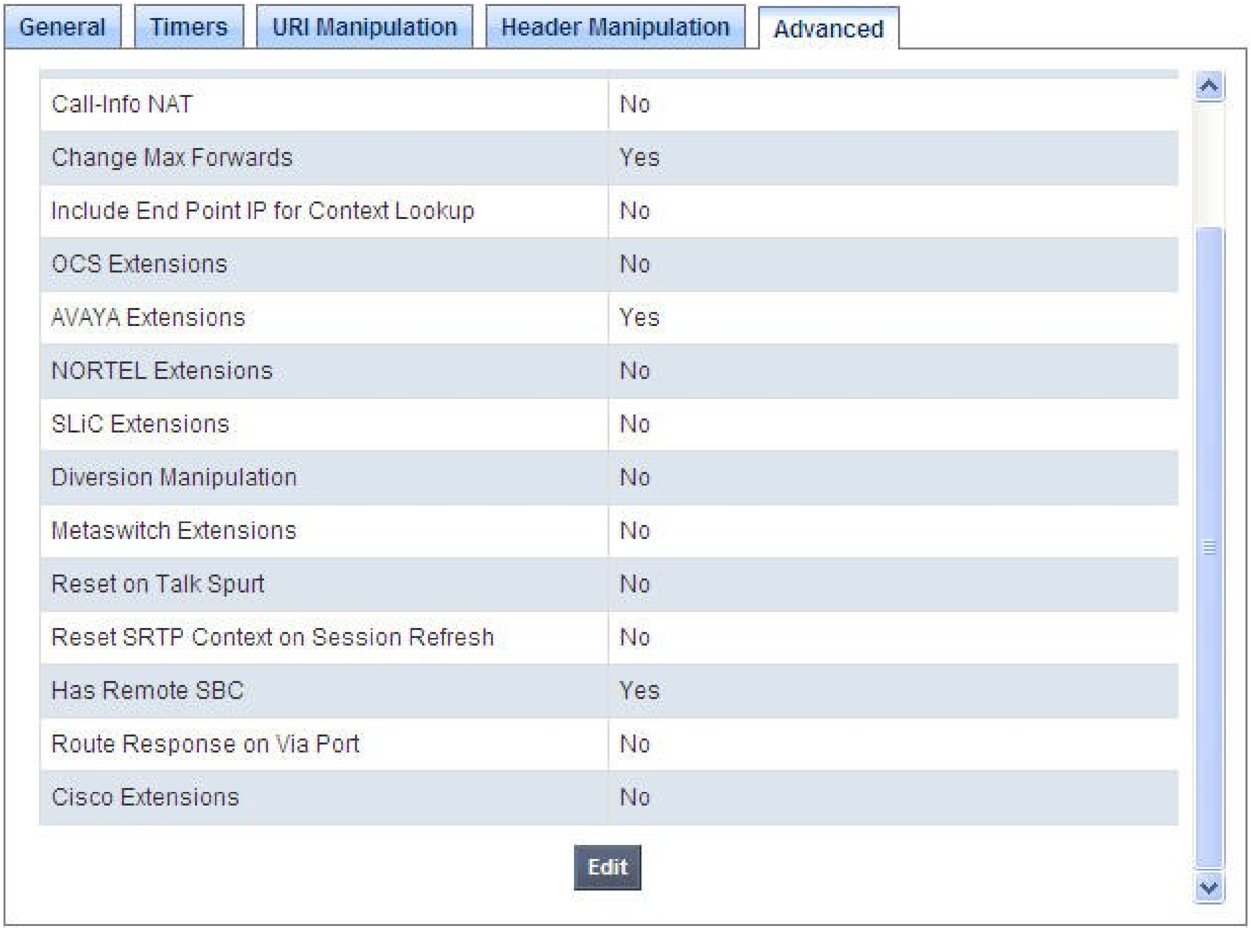


General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

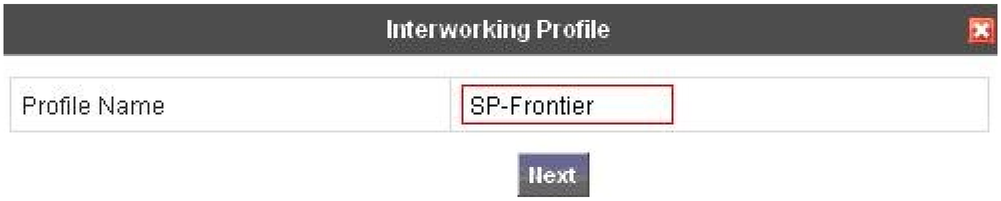
The following screen illustrates the **Advanced Settings** configuration. All parameters shown are default values.



Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
SLiC Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No

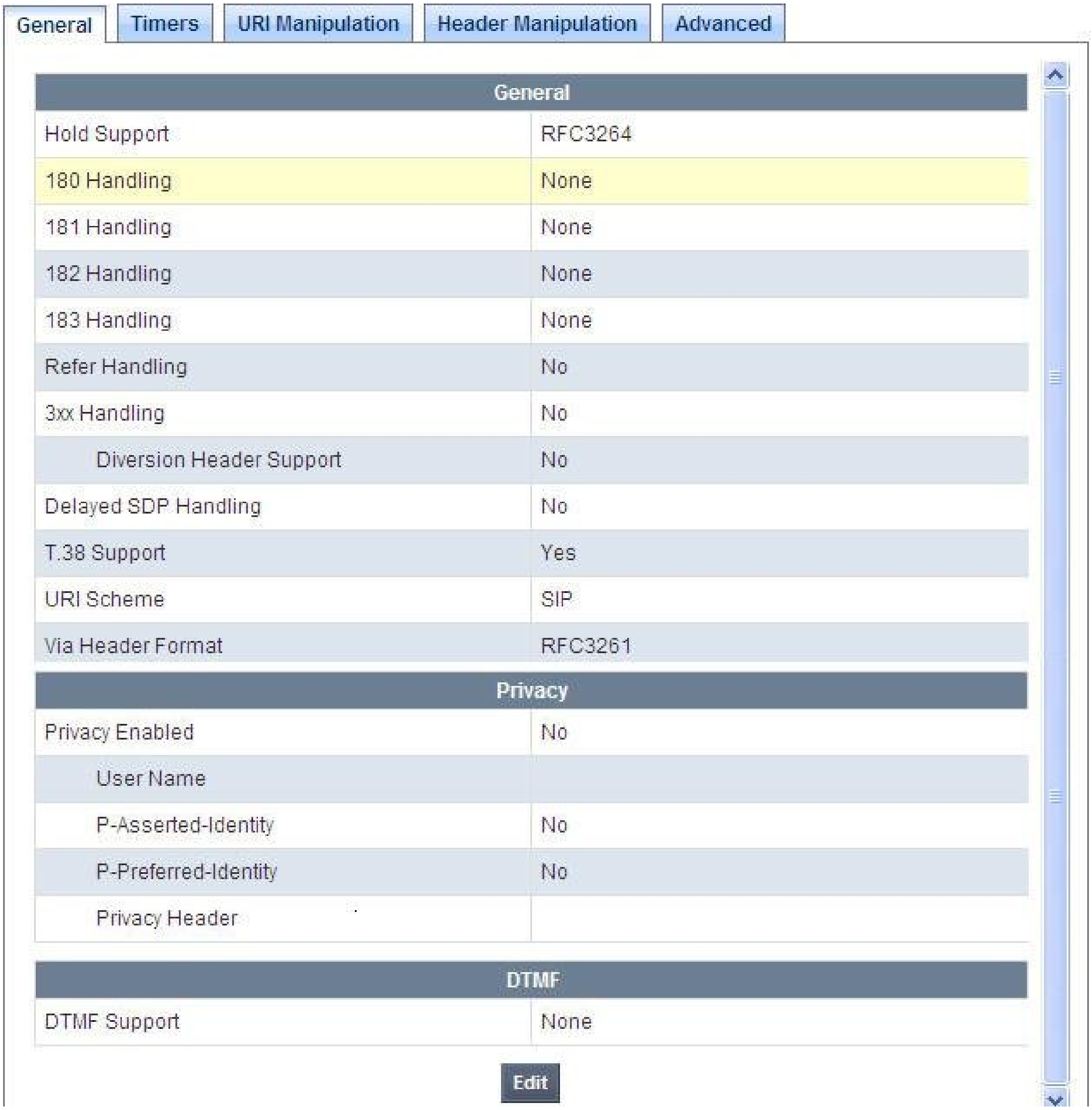
7.3.2. Server Interworking: SP-Frontier

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



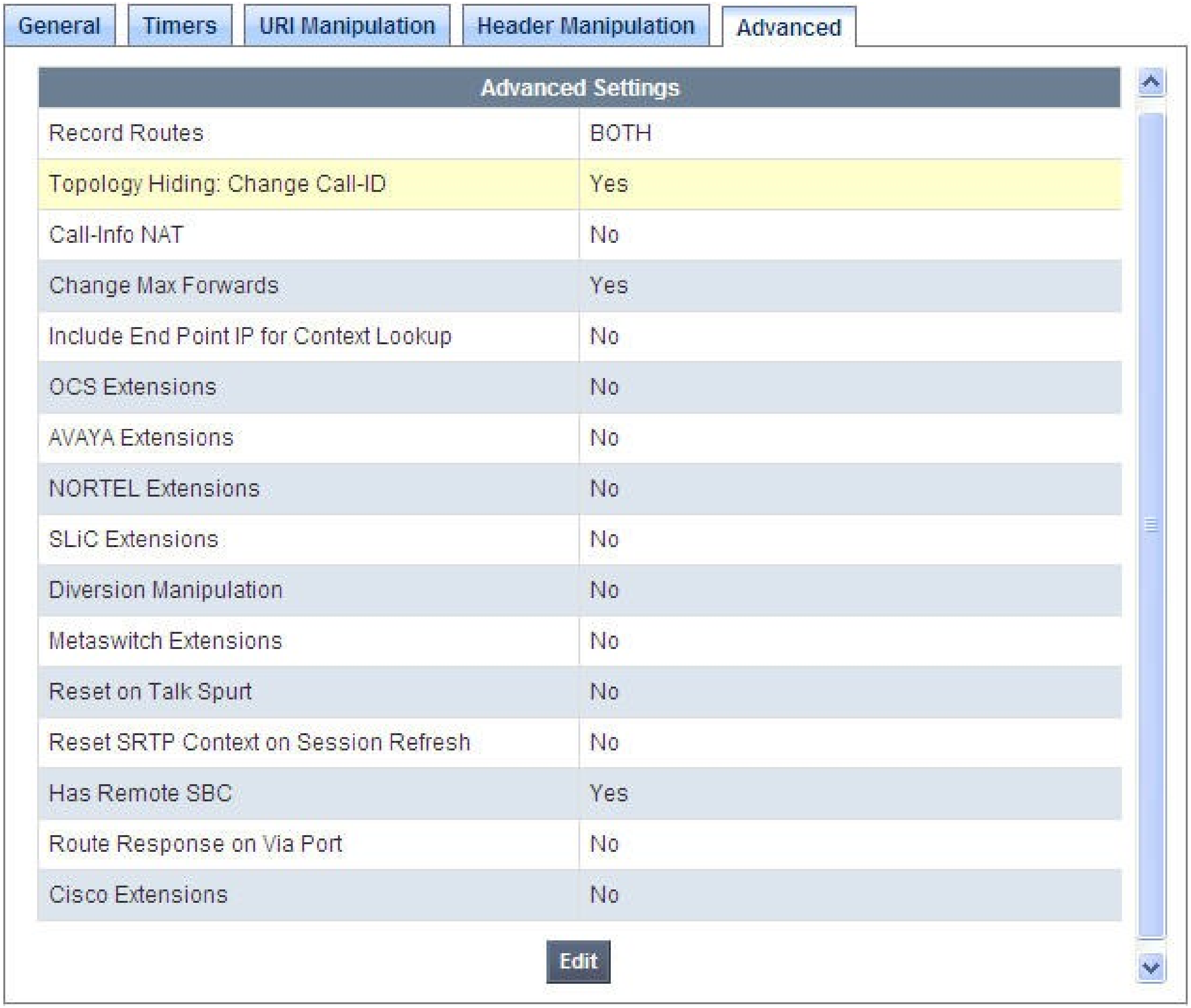
Profile Name: SP-Frontier

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



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

The following screen illustrates the **Advanced Settings** configuration. All parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.

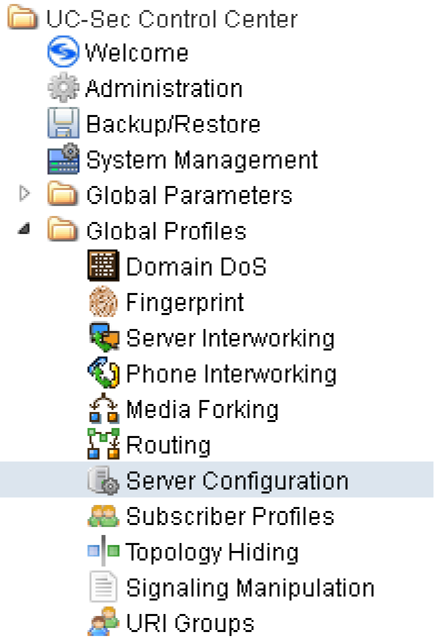


Advanced Settings	
Record Routes	BOTH
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
NORTEL Extensions	No
SLiC Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No

7.4. Global Profiles – Server Configuration

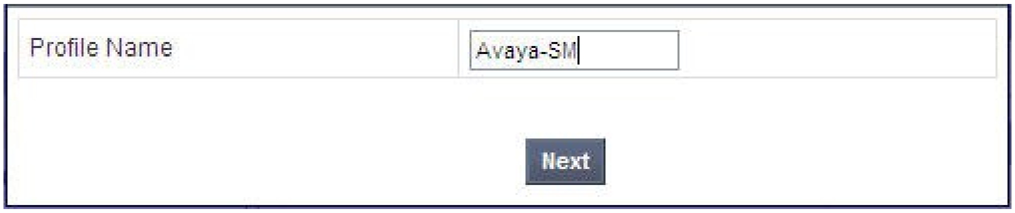
In the compliance test, the Frontier network-edge SBC is connected as the Trunk Server and the enterprise Session Manager is connected as the Call Server.

Select **Global Profiles → Server Configuration** from the left-side menu as shown below.



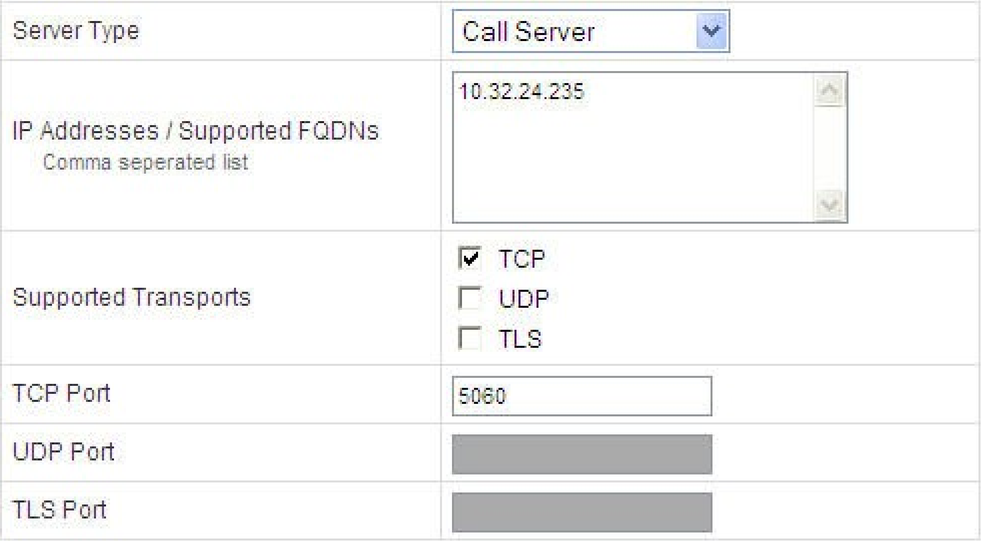
7.4.1. Server Configuration for Session Manager

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 "Avaya_SM" shown below. Click **Next**.



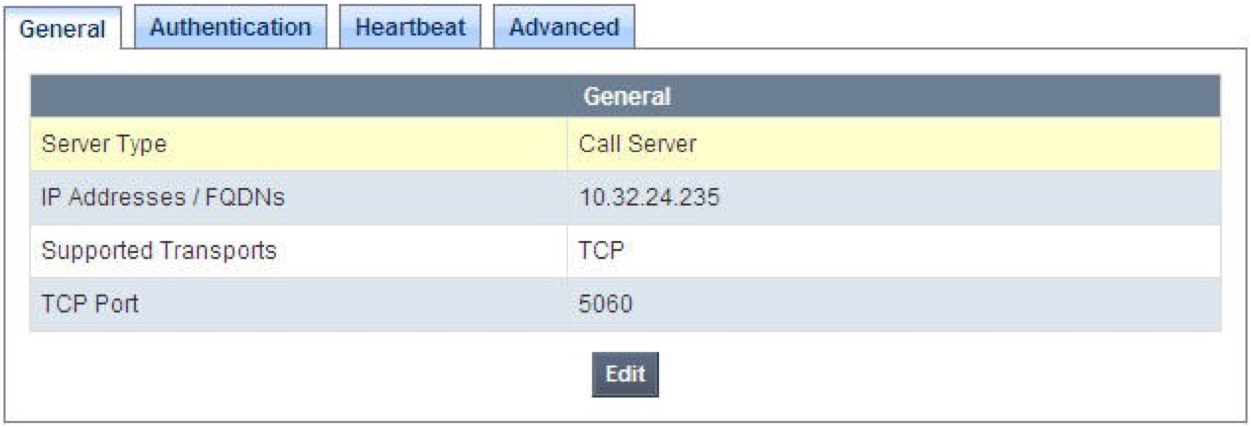
Profile Name	Avaya-SM

The following screens illustrate the Server Configuration with Profile name "Avaya-SM". In the "General" parameters, select ***Call Server*** from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the IP Address of the Session Manager SIP signaling interface in the sample configuration is entered. In the **Supported Transports** area, ***TCP*** is selected, and the **TCP Port** is set to ***5060***. This configuration corresponds with the Session Manager Entity Link configuration for the Entity Link connecting to the SBC. If adding a new profile, click **Next**. If editing an existing profile, click **Finish**.



Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.32.24.235
Supported Transports	☑ TCP ☐ UDP ☐ TLS
TCP Port	5060
UDP Port	
TLS Port	

Once configuration is completed, the **General** tab for "Avaya_SM" will appear as shown below.

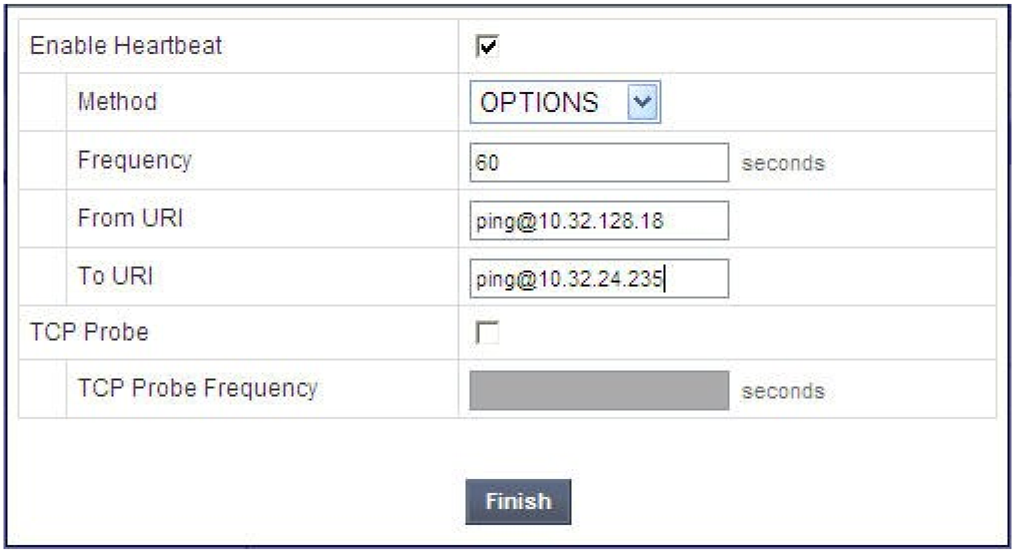


General	
Server Type	Call Server
IP Addresses / FQDNs	10.32.24.235
Supported Transports	TCP
TCP Port	5060

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.

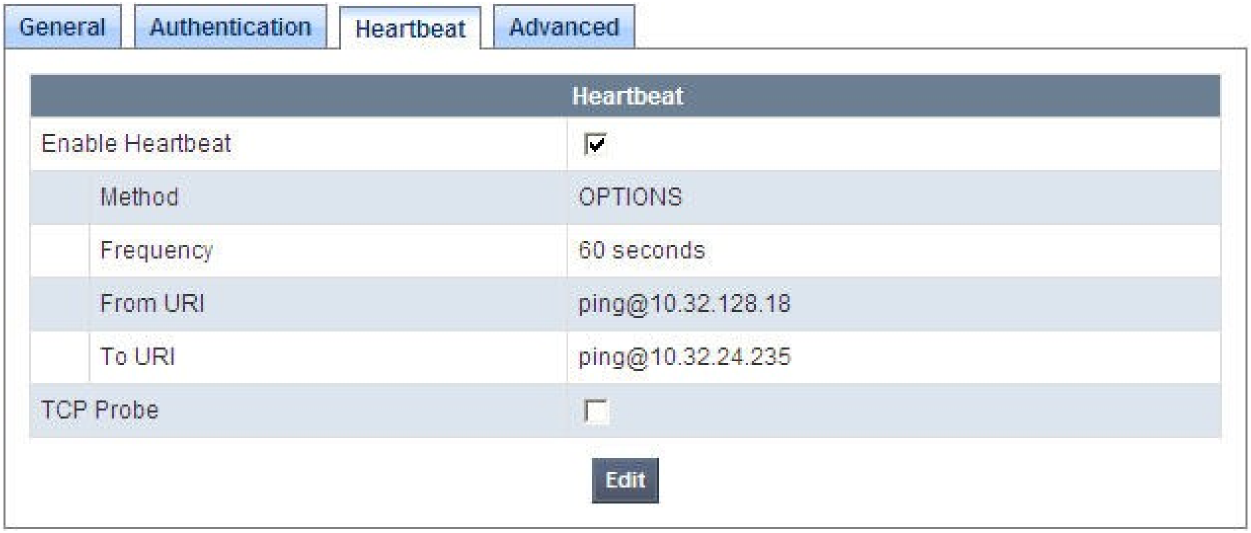
The SBC can be configured to source "heartbeats" in the form of SIP OPTIONS. In the sample configuration, with one Session Manager, this configuration is optional.

If SBC-sourced OPTIONS messages are desired, check the **Enable Heartbeat** box. Select “OPTIONS” from the **Method** drop-down menu. Select 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**.



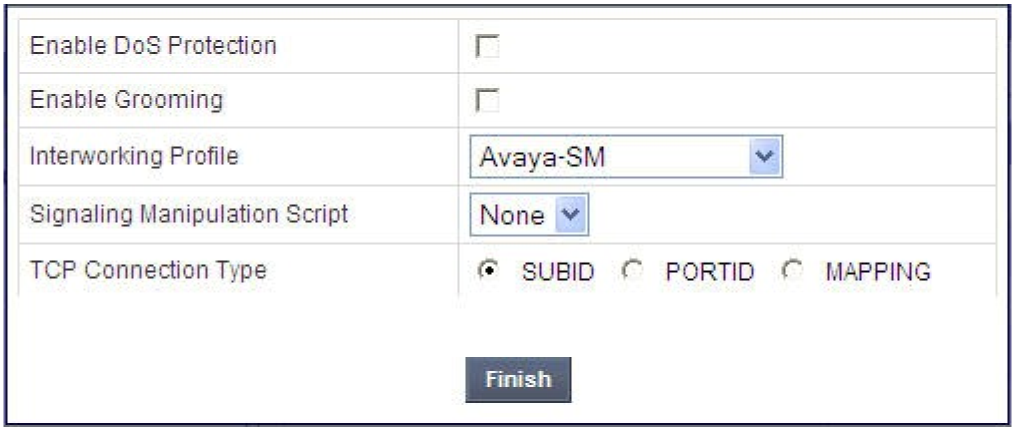
Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	ping@10.32.128.18
To URI	ping@10.32.24.235
TCP Probe	□
TCP Probe Frequency	seconds

If SBC sourced OPTIONS are configured, the **Heartbeat** tab for “Avaya_SM” will appear as shown below.



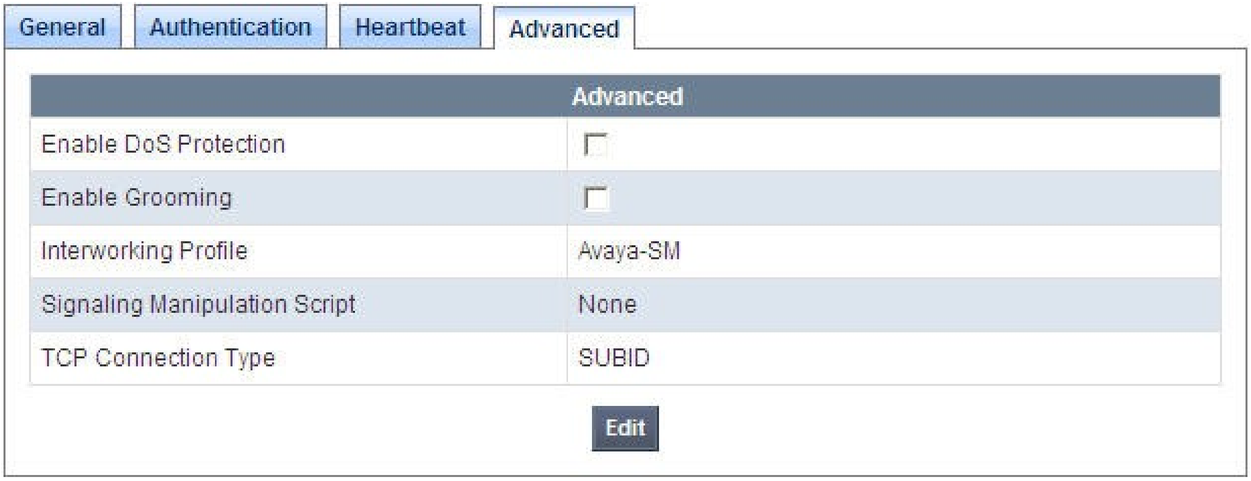
Heartbeat	
Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	ping@10.32.128.18
To URI	ping@10.32.24.235
TCP Probe	□

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



Enable DoS Protection	☐
Enable Grooming	☐
Interworking Profile	Avaya-SM
Signaling Manipulation Script	None
TCP Connection Type	● SUBID ○ PORTID ○ MAPPING

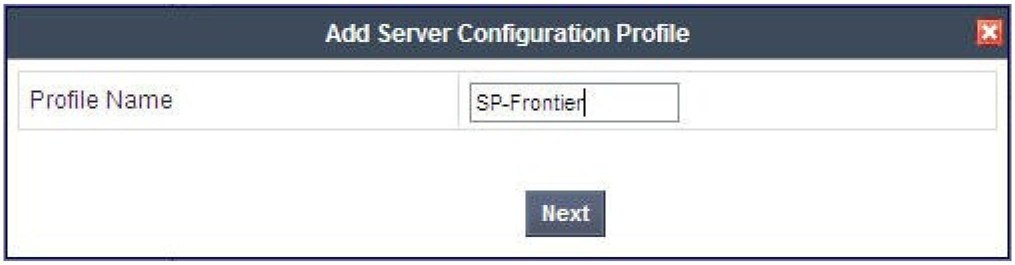
Once configuration is completed, the **Advanced** tab for the call server "Avaya_SM" will appear as shown below.



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

7.4.2. Server Configuration for Frontier SIP Trunking

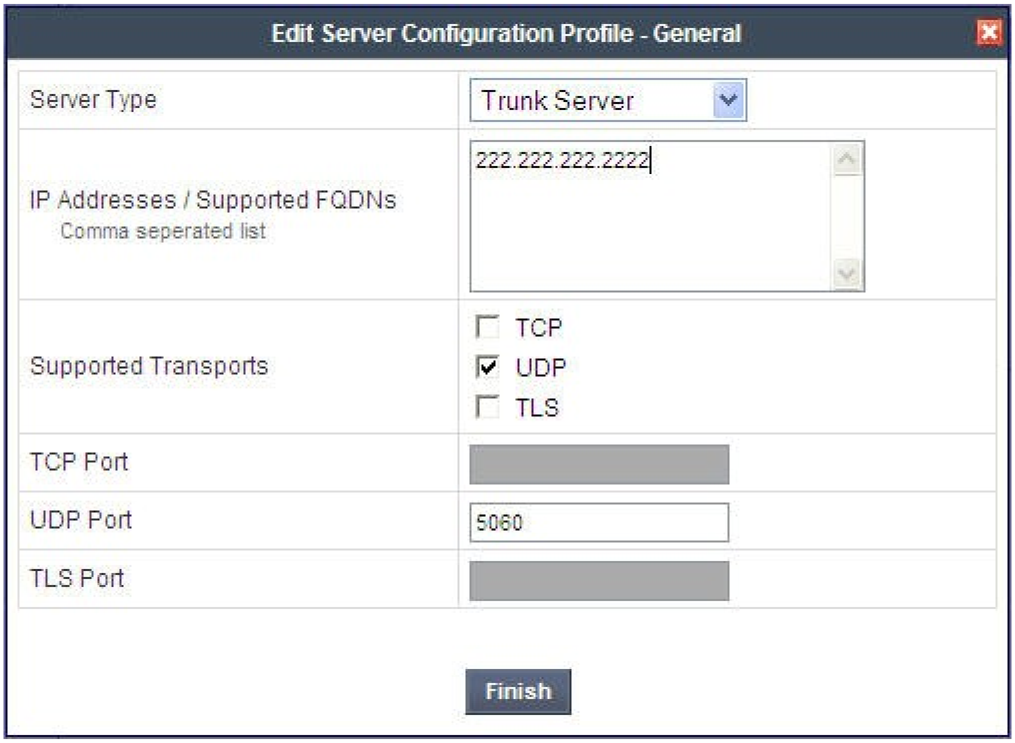
Click the **Add Profile** button (not shown) to add a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate Profile Name such as "SP-Frontier" shown below. Click **Next**.



Add Server Configuration Profile

Profile Name	SP-Frontier

The following screens illustrate the Server Configuration with Profile name “SP-Frontier”. In the “General” parameters, select “Trunk Server” from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the Frontier-provided SIP Trunking service network IP Address is entered. In the **Supported Transports** area, UDP is selected, and the **UDP Port** is set to 5060.



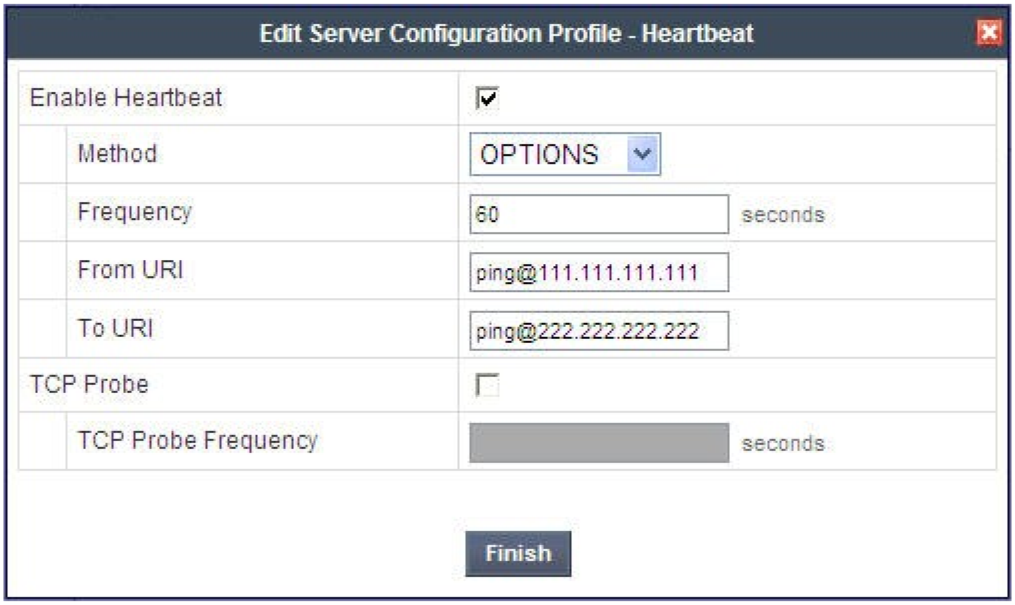
Edit Server Configuration Profile - General

Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma seperated list	222.222.222.2222
Supported Transports	□ TCP ☑ UDP □ TLS
TCP Port	
UDP Port	5060
TLS Port	

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 SIP 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 SIP OPTIONS to the inside private IP Address of the SBC, the SBC will send SIP OPTIONS to Frontier. When Frontier responds, the SBC will pass the response to Session Manager.

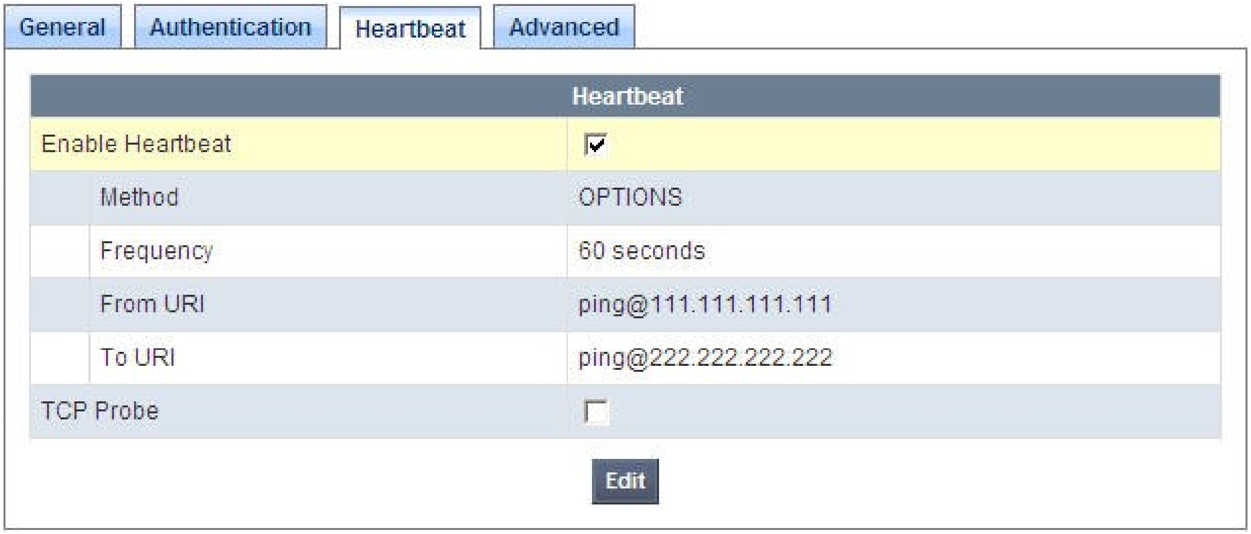
If SBC-sourced OPTIONS are desired, select "OPTIONS" from the **Method** drop-down menu. Select the desired frequency that the SBC will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the SBC. If adding a new profile,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



Edit Server Configuration Profile - Heartbeat

Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	ping@111.111.111.111
To URI	ping@222.222.222.222
TCP Probe	□
TCP Probe Frequency	seconds

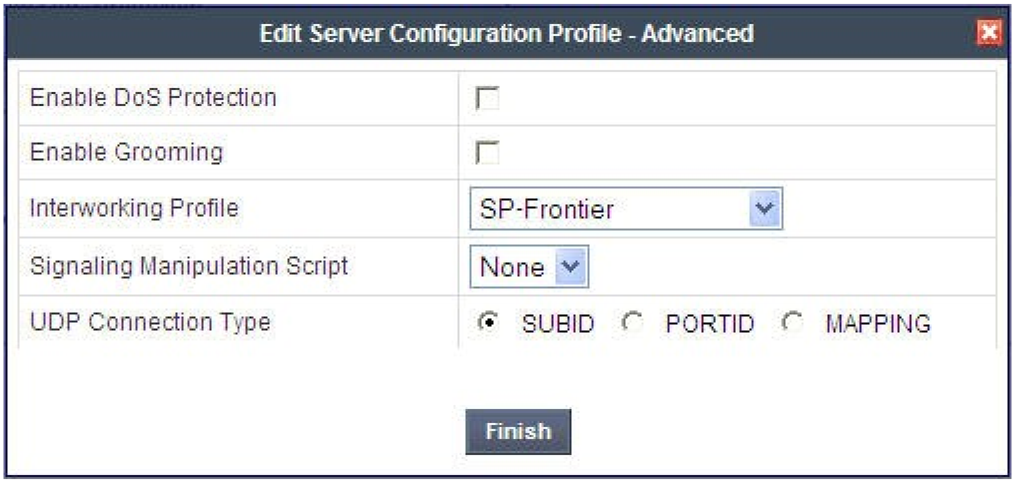
If the optional SBC sourced OPTIONS configuration is completed, the **Heartbeat** tab for "SP-Frontier" will appear as shown below.



Heartbeat

Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	ping@111.111.111.111
To URI	ping@222.222.222.222
TCP Probe	□

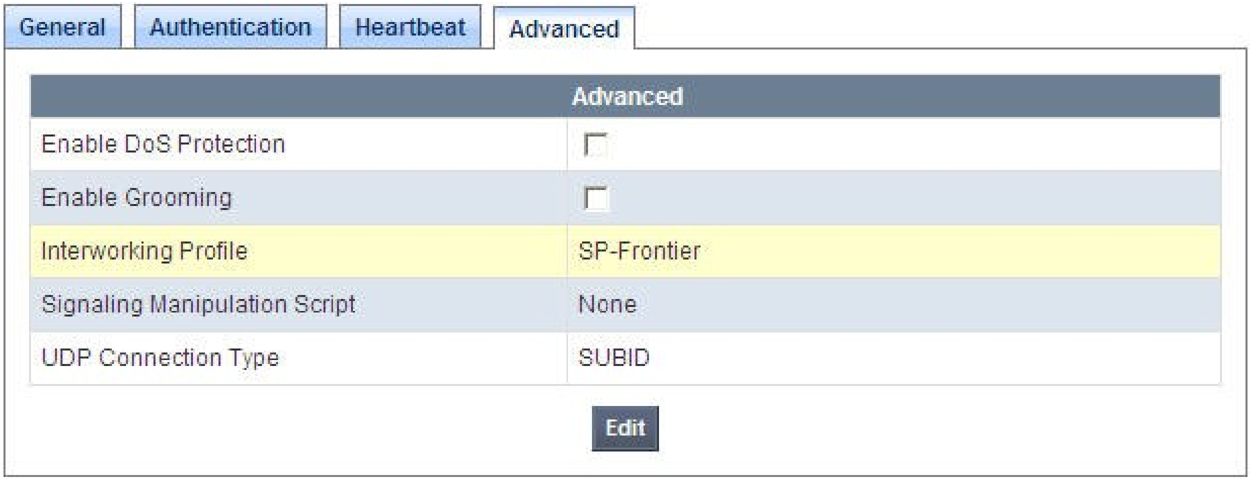
If adding a profile, click **Next** to continuing to the "Advanced" settings. If editing an existing profile, select the **Advanced** tab and **Edit**. In the resultant screen, select the **Interworking Profile** "SP-Frontier" created in **Section 7.3.2**. Other SBC features, such as DoS Protection and Grooming, can be configured according to customer preference. Click **Finish**.



Edit Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	SP-Frontier
Signaling Manipulation Script	None
UDP Connection Type	● SUBID ○ PORTID ○ MAPPING

Once configuration is completed, the **Advanced** tab for "VZ-IPCC" will appear as shown below.

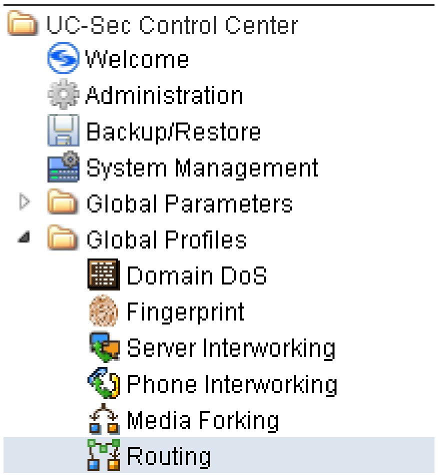


Advanced	
Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	SP-Frontier
Signaling Manipulation Script	None
UDP Connection Type	SUBID

7.5. Global Profiles – Routing

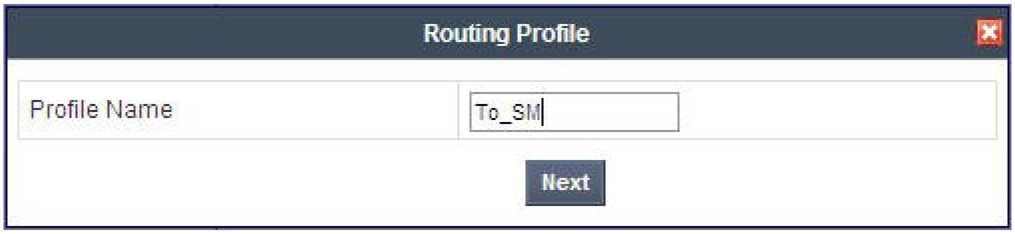
Routing information is required for routing to Session Manager on the internal side and Frontier on the external side. The IP addresses and ports defined here will be used as the destination addresses for signaling. If no port is specified, default 5060 is used.

Select **Global Profiles → Routing** from the left-side menu as shown below.



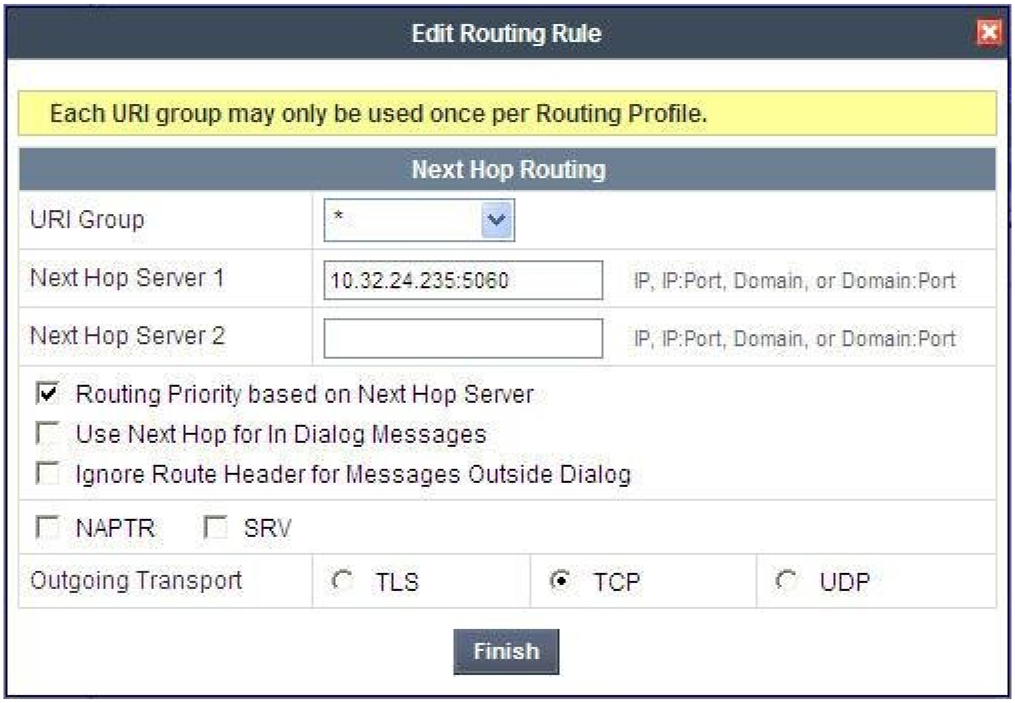
7.5.1. Routing Configuration for Session Manager

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**.



Profile Name: To_SM

For the **Next Hop Routing**, enter the IP Address of the Session Manager SIP signaling interface as **Next Hop Server 1**, as shown below. Check **Routing Priority based on Next Hop Server**. Choose **TCP** for **Outgoing Transport**.



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

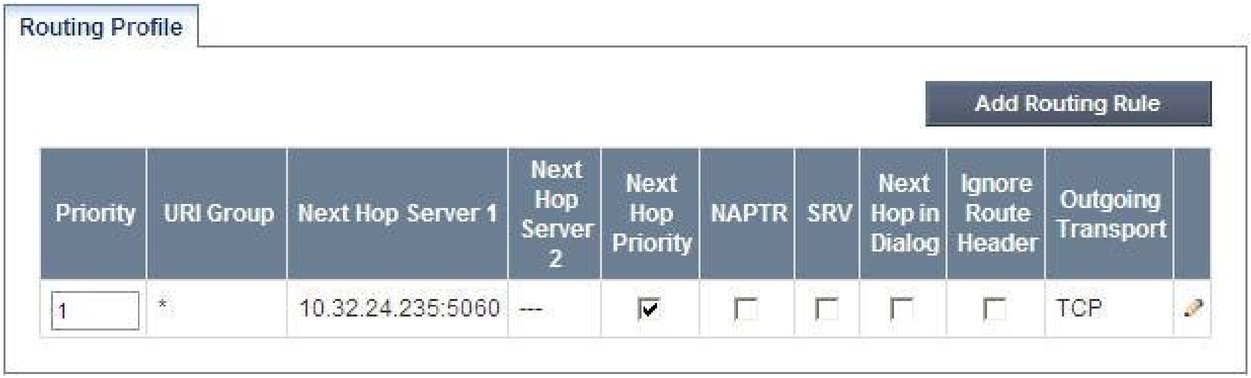
Next Hop Routing

URI Group	*		
Next Hop Server 1	10.32.24.235:5060	IP, IP:Port, Domain, or Domain:Port	
Next Hop Server 2		IP, IP:Port, Domain, or Domain:Port	
Outgoing Transport	○ TLS	● TCP	○ UDP

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

☐ NAPTR ☐ SRV

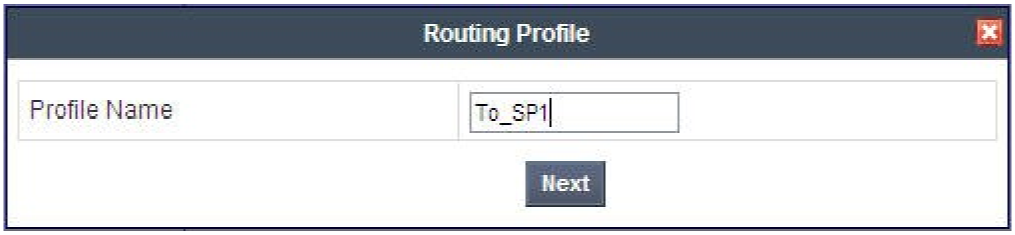
Once configuration is completed, the **Routing Profile** for "To_SM" will appear as follows.



Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport	
1	*	10.32.24.235:5060	---	☑	☐	☐	☐	☐	TCP	✎

7.5.2. Routing Configuration for Frontier SIP Trunking

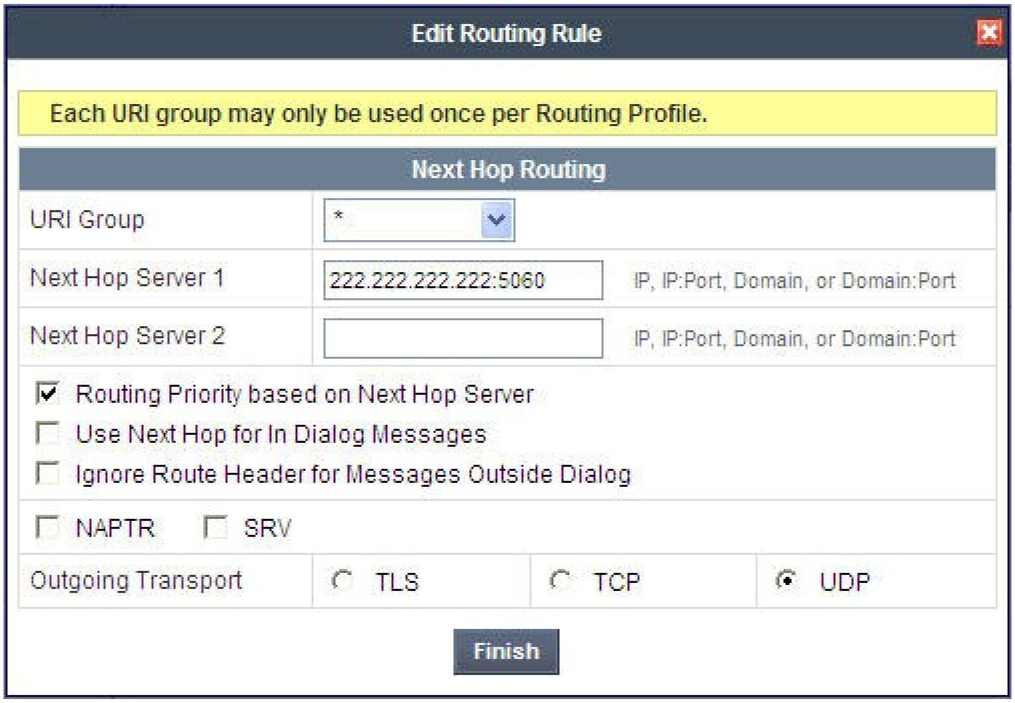
Click the **Add Profile** button (not shown) to add a new profile, or select an existing routing profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as "To_SP1" shown below. Click **Next**.



Routing Profile

Profile Name	To_SP1

For the **Next Hop Server 1**, enter the IP Address of the Frontier SIP Trunking service, a colon, and the port to be used as shown in the screen below. Check **Routing Priority based on Next Hop Server**. Choose **UDP** for **Outgoing Transport**.



Edit Routing Rule

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

Next Hop Routing

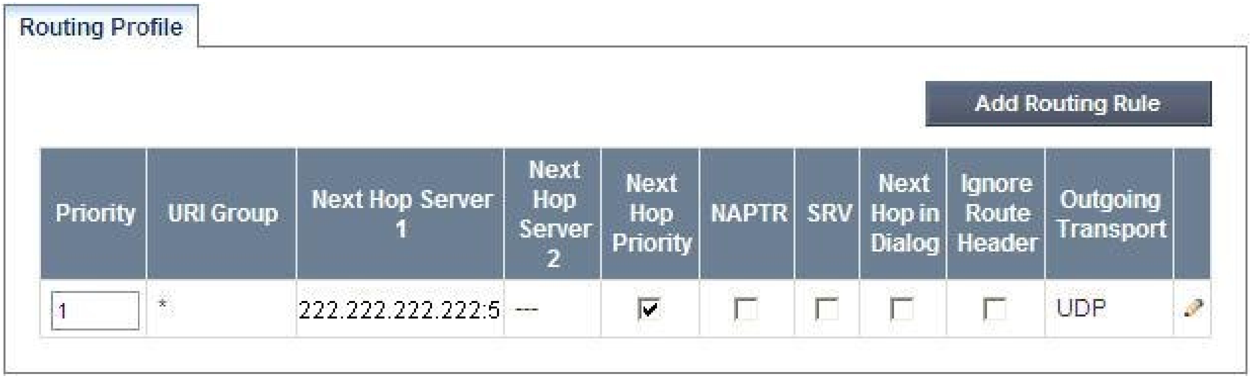
URI Group	*	
Next Hop Server 1	222.222.222.222:5060	IP, IP:Port, Domain, or Domain:Port
Next Hop Server 2		IP, IP:Port, Domain, or Domain:Port

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

☐ NAPTR ☐ SRV

Outgoing Transport: ○ TLS ○ TCP ● UDP

Once configuration is completed, the **Routing Profile** for “VZ-IPCC” will appear as follows.



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	*	222.222.222.222:5	---	☑	□	□	□	□	UDP	

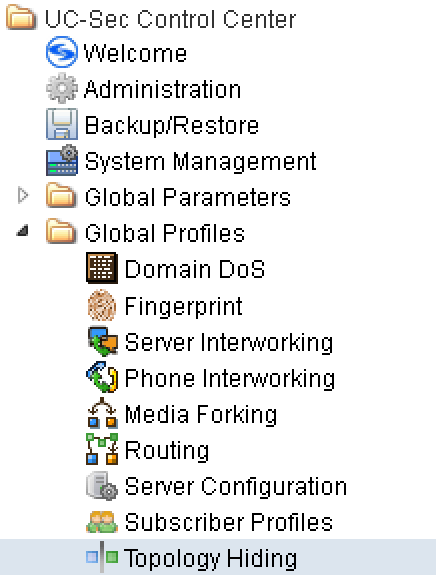
7.6. Global Profiles – Topology Hiding

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.

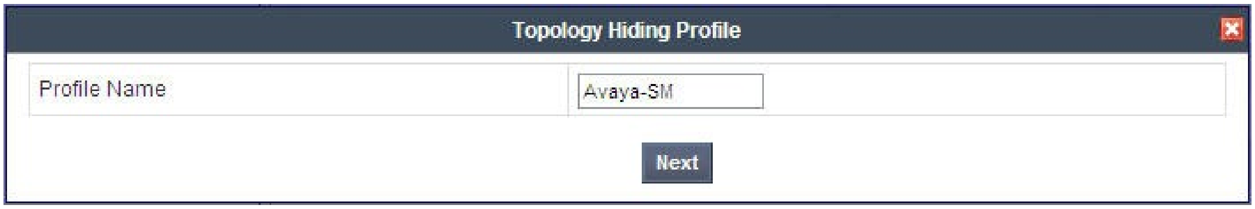
For the compliance test, only the minimum configuration required to achieve interoperability was performed.

Select **Global Profiles → Topology Hiding** from the left-side menu as shown below.



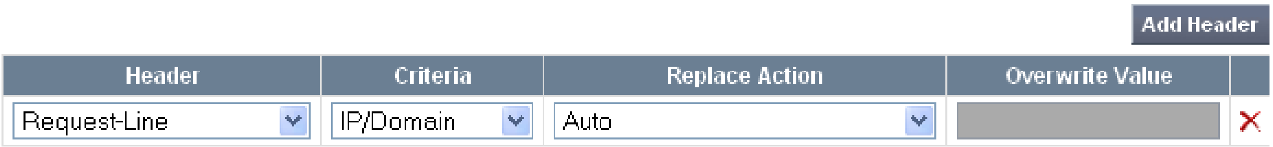
7.6.1. Topology Hiding for Session Manager

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 "Avaya-SM" shown below. Click **Next**.


Topology Hiding Profile

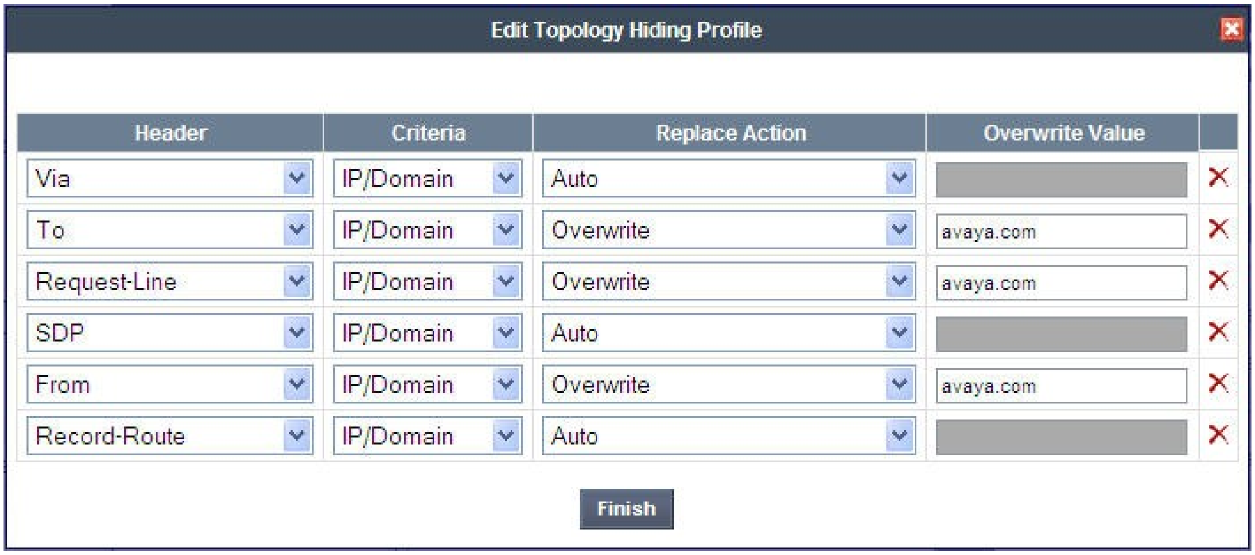
Profile Name	Avaya-SM

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



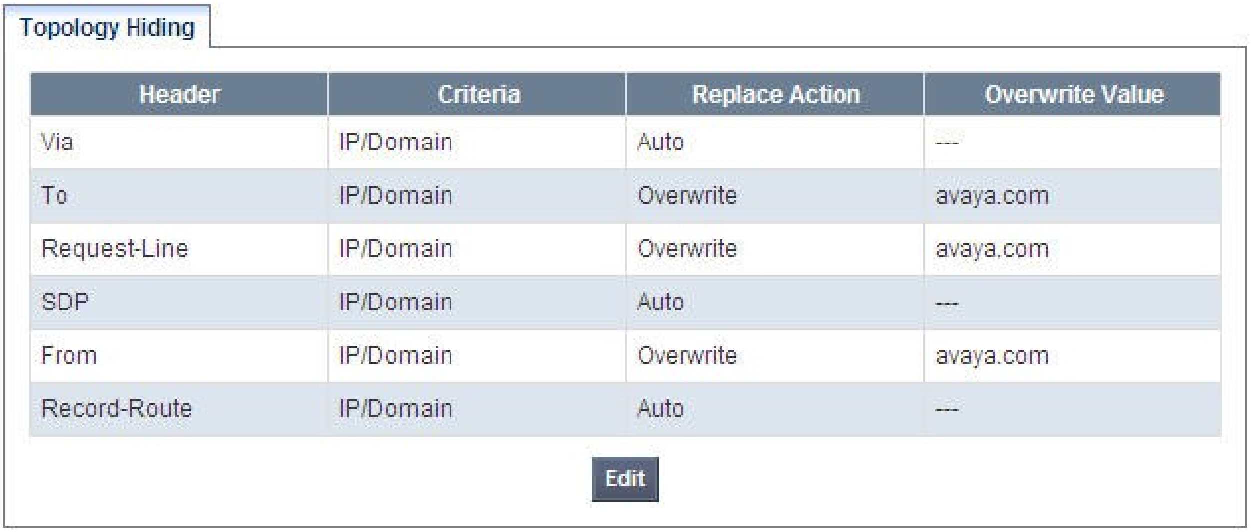
Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Auto		✕

If it is desired 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 "avaya.com". Click **Finish**.


Edit Topology Hiding Profile

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

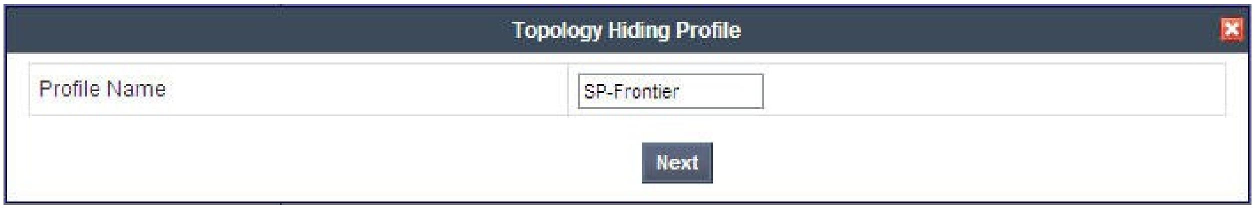
After configuration is completed, the Topology Hiding for profile "Avaya-SM" will appear as follows.



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

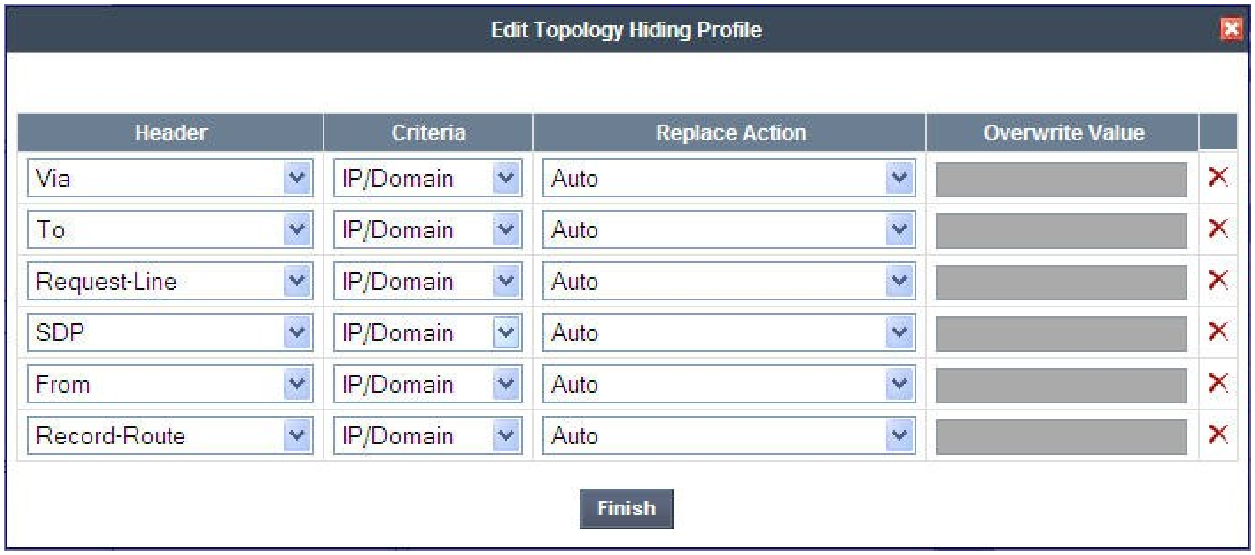
7.6.2. Topology Hiding for Frontier SIP Trunking

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 "SP-Frontier" shown below. Click **Next**.



Profile Name	SP-Frontier

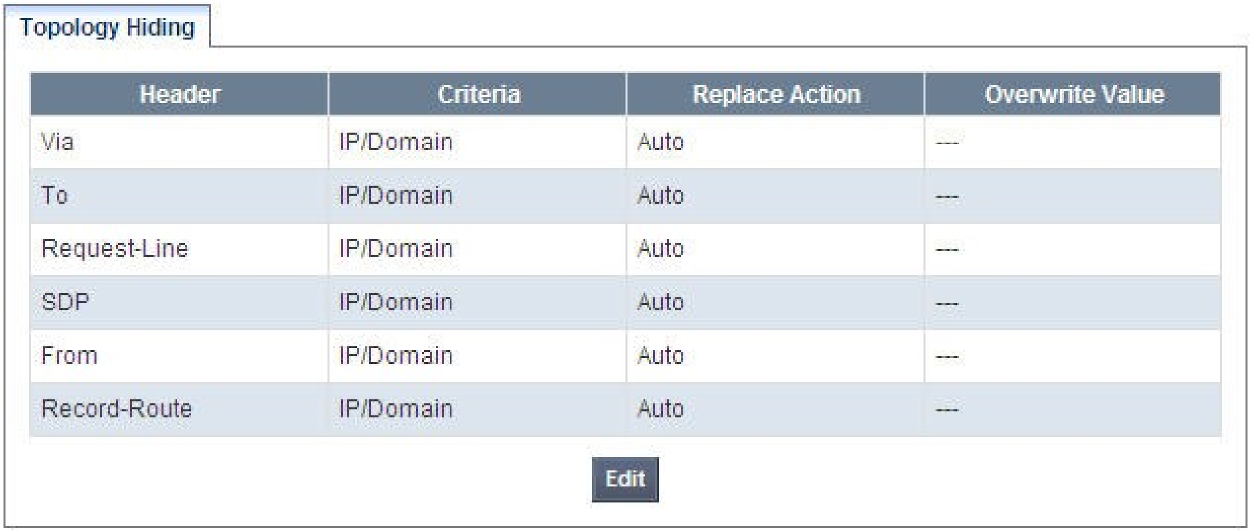
In the resultant screen, click the **Add Header** button in the upper right to reveal additional headers until the final screen appears as follows. The default "Auto" behaviors are sufficient. Click **Finish**.



Edit Topology Hiding Profile

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		✕

After configuration is completed, the **Topology Hiding** for profile "SP-Frontier" will appear as follows.



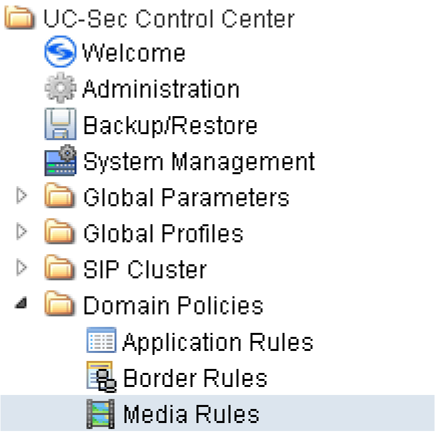
Topology Hiding

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	---

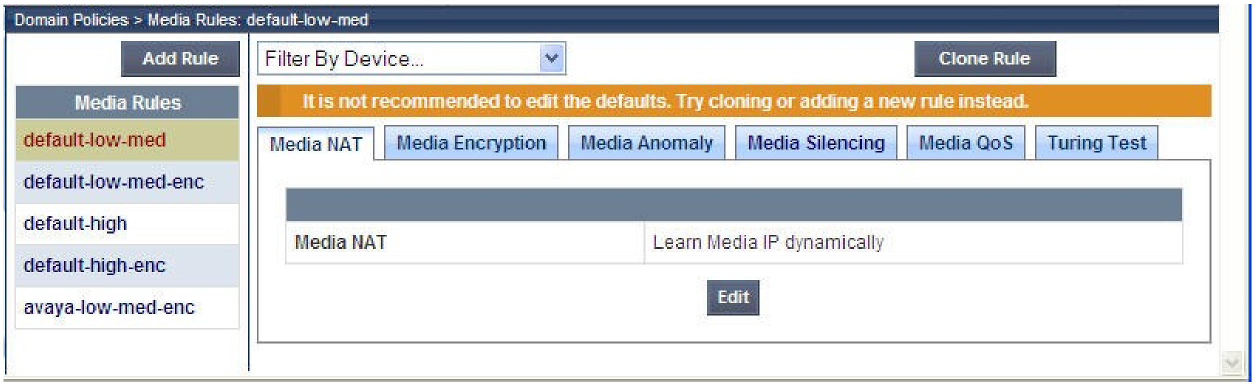
7.7. Domain Policies – Media Rules

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.

Select **Domain Policies → Media Rules** from the left-side menu as shown below.



In the sample configuration, a single media rule was used: the default rule named "default-low-med". This default rule is sufficient for the compliance test. The screen below shows the selection of the "default-low-med" media rule.



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

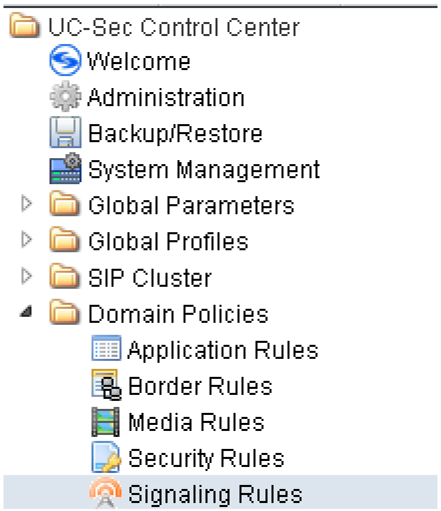
Media NAT	Learn Media IP dynamically

7.8. Domain Policies – Signaling Rules

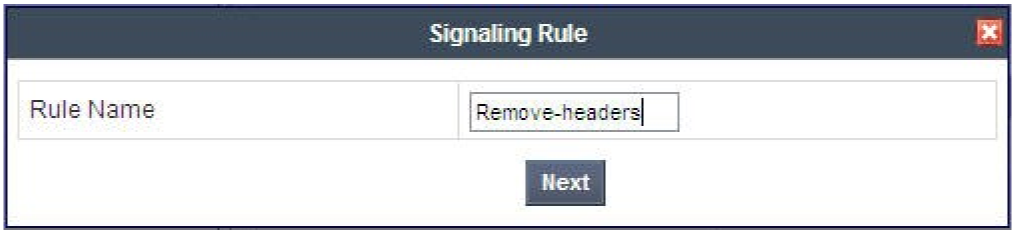
Signaling Rules define the actions to be taken (*Allow*, *Block*, *Block with Response*, etc.) on signaling request and response messages. They also allow the control of the Quality of Service of the signaling packets

The P-Location and P-Charging-Vector headers are sent in SIP messages from the 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 requests and responses. In addition, the Route header in certain SIP messages inbound from the service provider network was also removed to ensure interoperability.

Select **Domain Policies → Signaling Rules** from the left-side menu as shown below.



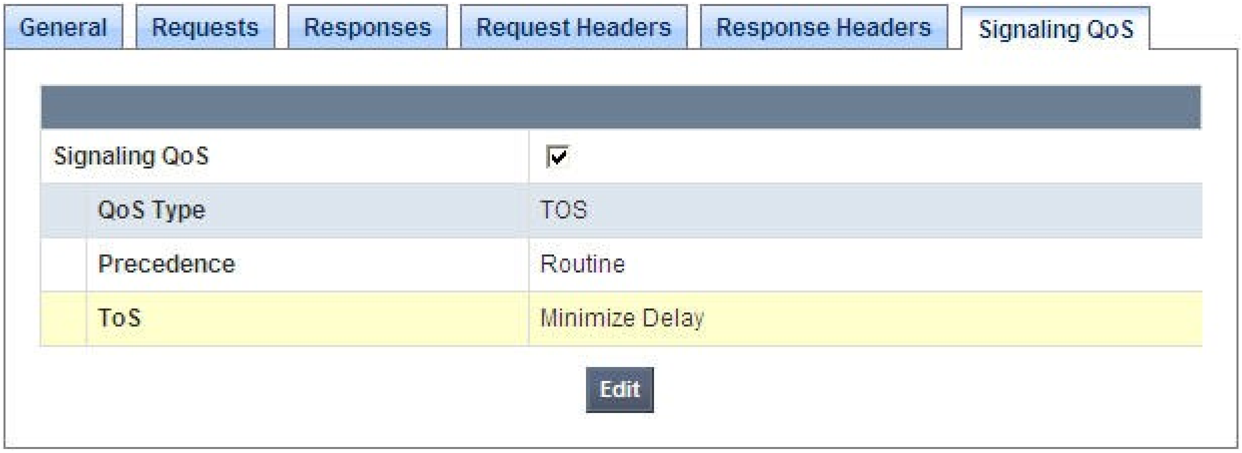
Click the Add Rule button to add a new signaling rule. In the Rule Name field, enter an appropriate name, such as “Remove-headers”.



Rule Name: Remove-headers

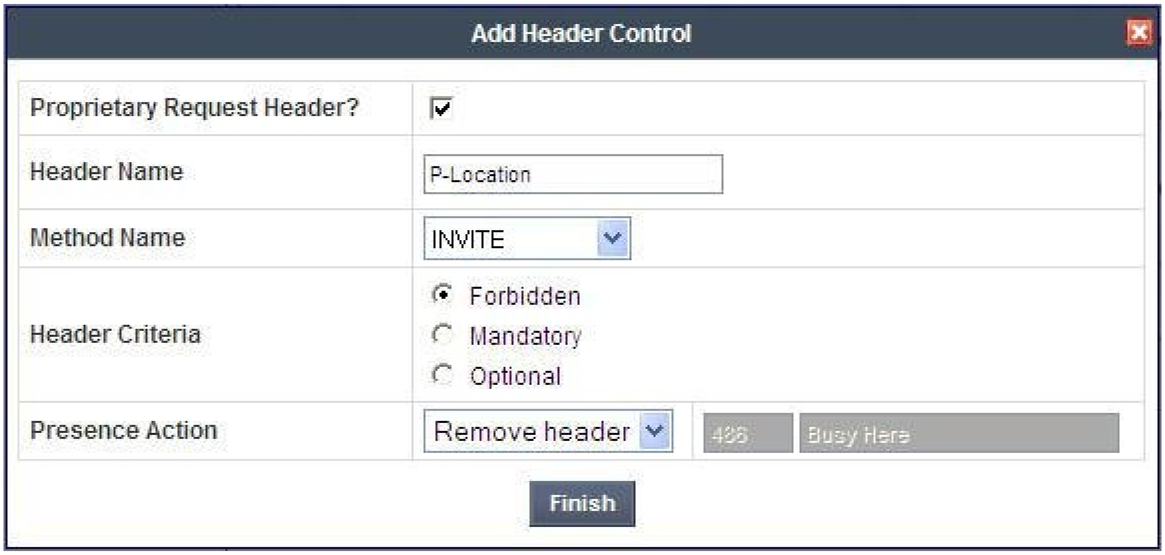
In the subsequent screen (not shown), click **Next** to accept defaults. In the Signaling QoS screen, click **Finish** (not shown).

After this configuration, the new “Remove-headers” rule will appear as follows.



Signaling QoS	☑
QoS Type	TOS
Precedence	Routine
ToS	Minimize Delay

Select the **Request Headers** tab, and select the **Add Out Header Control** button. Check the **Proprietary Request Header?** checkbox. In the **Header Name** field, type “P-Location”. Select “INVITE” as the **Method Name**. In the Header Criteria, select **Forbidden**. Retain **Presence Action** “Remove header”. The intent is to remove the P-Location header which is inserted by Session Manager, but not needed by Frontier SIP Trunking service. This configuration is optional in that the P-Location header does not cause any user-perceivable problem if presented to Frontier.

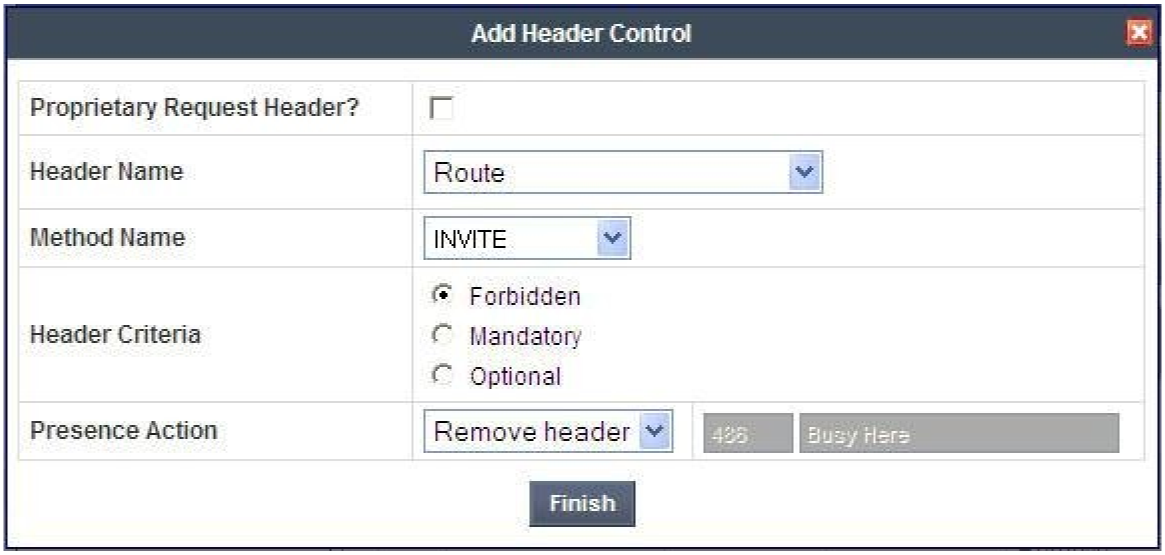


Proprietary Request Header?	☑
Header Name	P-Location
Method Name	INVITE
Header Criteria	● Forbidden ○ Mandatory ○ Optional
Presence Action	Remove header 486 Busy Here

Similarly, configure additional header control rules to

- Remove the P-Charging-Vector header in the outbound INVITE
- Remove the P-Charging-Vector header in the outbound UPDATE

In the **Request Headers** tab, select the **Add In Header Control** button. In the displayed **Add Header Control** window, select "Route" as **Header Name** and "INVITE" as **Method Name**. In the Header Criteria, select **Forbidden**. Retain **Presence Action** "Remove header". The intent is to remove the Route header in inbound INVITE that caused interoperability problem during compliance testing. This configuration was necessary due to the Frontier test circuit configuration for shared use.

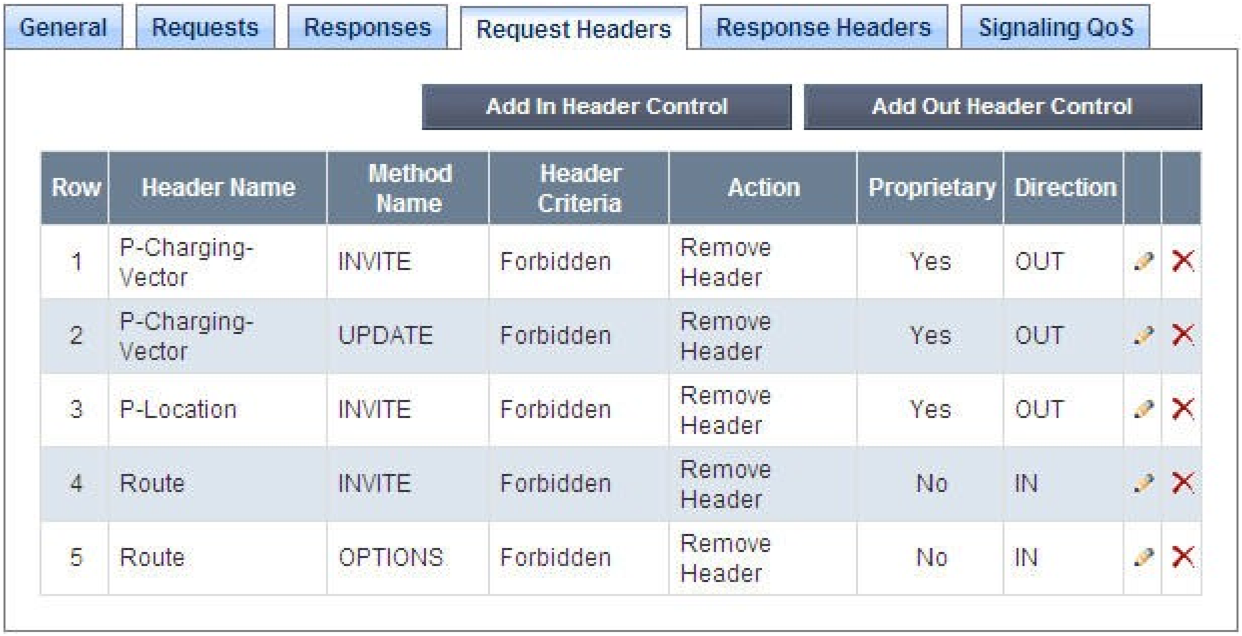


Add Header Control

Proprietary Request Header?	□
Header Name	Route
Method Name	INVITE
Header Criteria	● Forbidden ○ Mandatory ○ Optional
Presence Action	Remove header 486 Busy Here

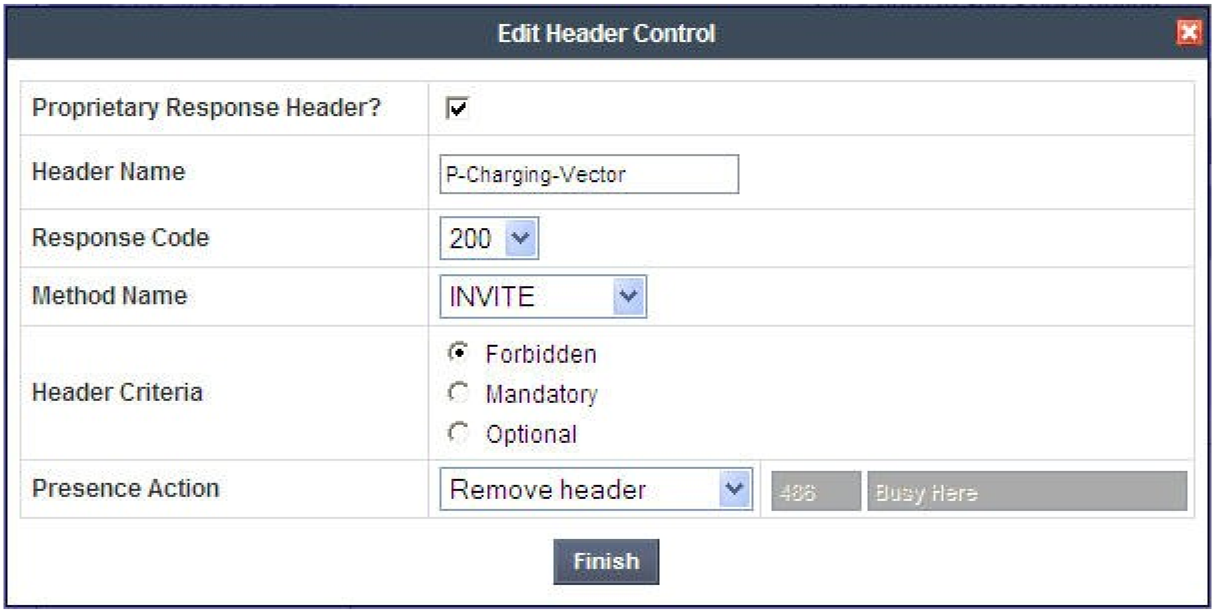
Similarly, configure an additional header control rules to remove the Route header in the inbound OPTIONS message.

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



Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	P-Charging-Vector	INVITE	Forbidden	Remove Header	Yes	OUT	✎	✗
2	P-Charging-Vector	UPDATE	Forbidden	Remove Header	Yes	OUT	✎	✗
3	P-Location	INVITE	Forbidden	Remove Header	Yes	OUT	✎	✗
4	Route	INVITE	Forbidden	Remove Header	No	IN	✎	✗
5	Route	OPTIONS	Forbidden	Remove Header	No	IN	✎	✗

Select the **Response Headers** tab, and select the **Add In Header Control** button. Check **Proprietary Response Header?** In the **Header Name** field, type "P-Location". Select "INVITE" as the **Method Name,** and "200" from the **Response Code** drop-down. In the Header Criteria, select **Forbidden**. Retain **Presence Action** "Remove header". The intent is to remove the P-Location header from 200 OK responses. This configuration is optional in that the P-Location header does not cause any user-perceivable problem if presented to Frontier. Click **Finish**.

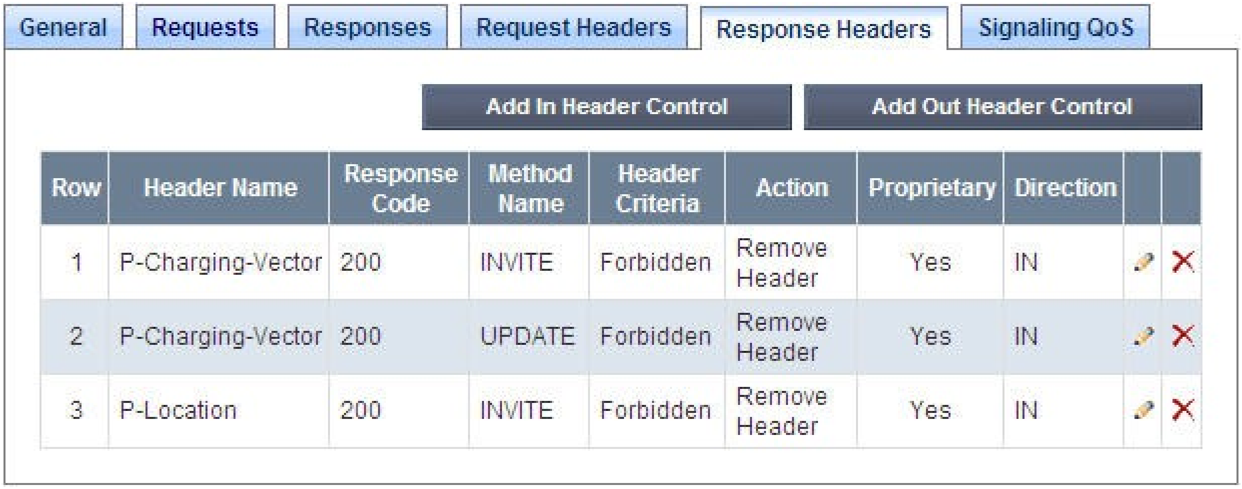


Proprietary Response Header?	☑
Header Name	P-Charging-Vector
Response Code	200
Method Name	INVITE
Header Criteria	● Forbidden ○ Mandatory ○ Optional
Presence Action	Remove header 486 Busy Here

Similarly, configure additional header control rules to

- Remove the P-Charging-Vector header in the 200 OK response to INVITE
- Remove the P-Charging-Vector header in the 200 OK response to UPDATE
- Remove the P-Location header in the 200 OK response to INVITE

Once configuration is complete, the **Response Headers** tab for the "Remove-headers" signaling rule will appear as follows.

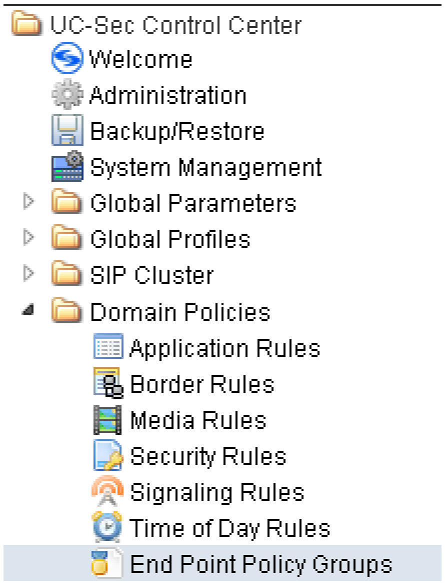


Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	P-Charging-Vector	200	INVITE	Forbidden	Remove Header	Yes	IN	✎	✕
2	P-Charging-Vector	200	UPDATE	Forbidden	Remove Header	Yes	IN	✎	✕
3	P-Location	200	INVITE	Forbidden	Remove Header	Yes	IN	✎	✕

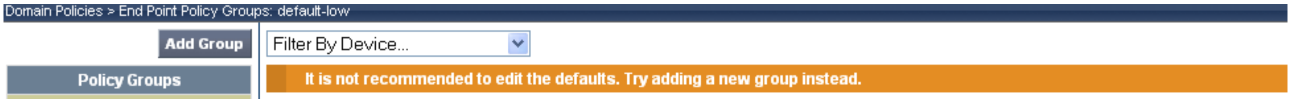
7.9. Domain Policies – End Point Policy Groups

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.

Select **Domain Policies → End Point Policy Groups** from the left-side menu as shown below.



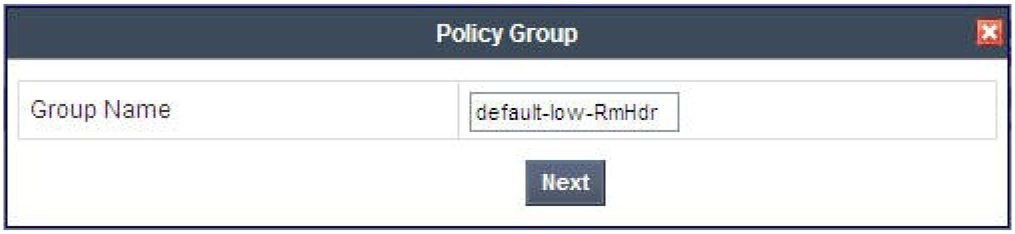
Select the **Add Group** button.



Domain Policies > End Point Policy Groups: default-low

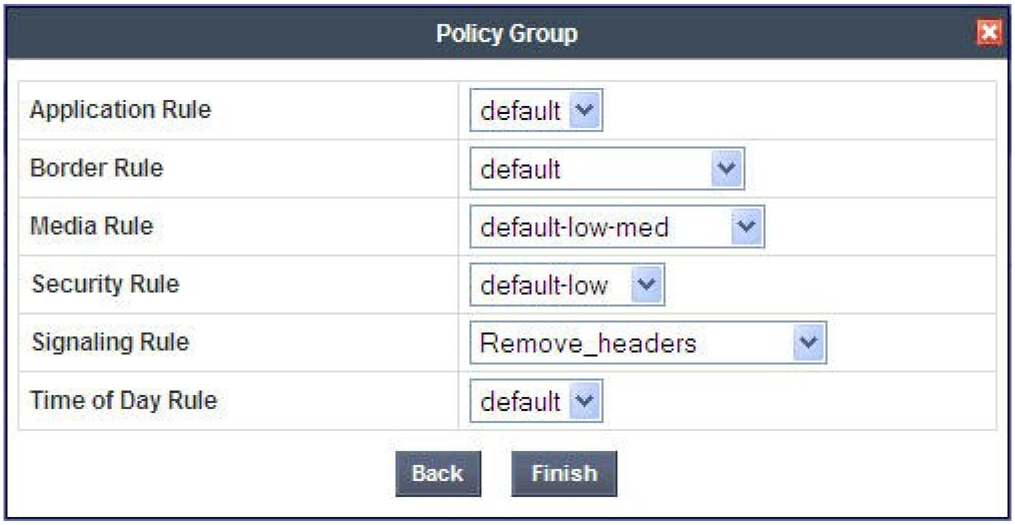
It is not recommended to edit the defaults. Try adding a new group instead.

Enter a name in the **Group Name** field, such as “default-low-RmHdr” as shown below. Click **Next**.



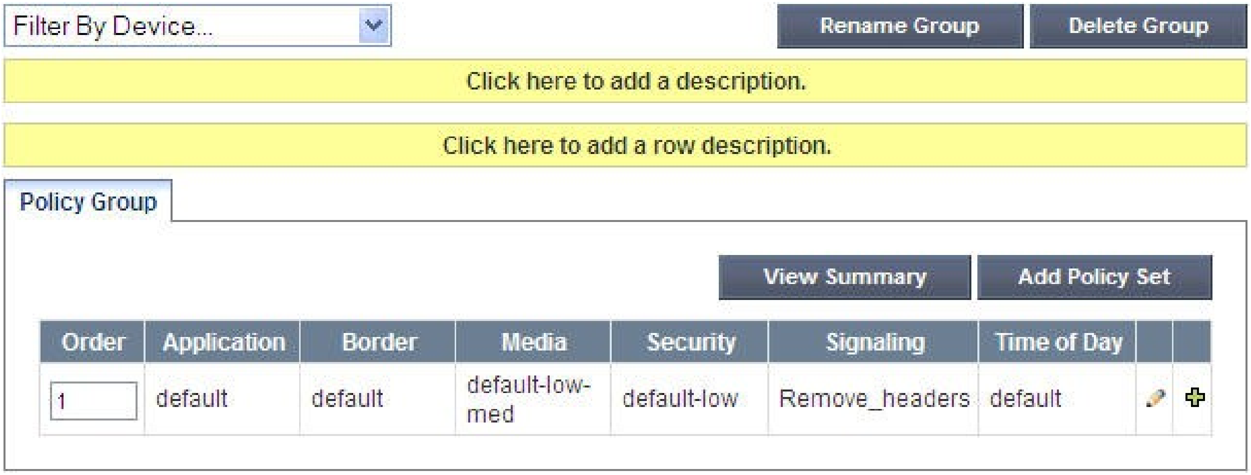
Group Name	default-low-RmHdr

In the sample configuration, defaults were selected for all fields, with the exception of the **Signaling Rule**, which was set to the “Remove-headers” signaling rule as defined in **Section 7.8** as shown below. Note that the default “default-low-med” media rule was used for the compliance test as stated in **Section 7.7**. Click **Finish**.



Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	Remove_headers
Time of Day Rule	default

Once configuration is completed, the "default-low-RmHdr" policy group will appear as follows.

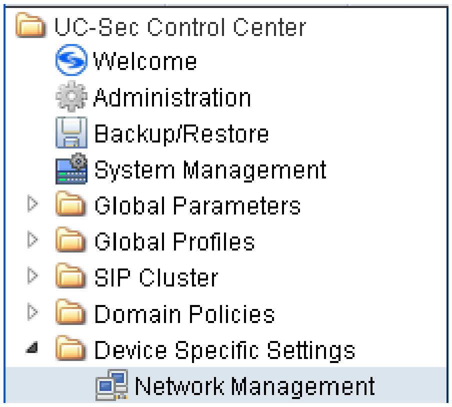


Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default	default	default-low-med	default-low	Remove_headers	default	✎	✚

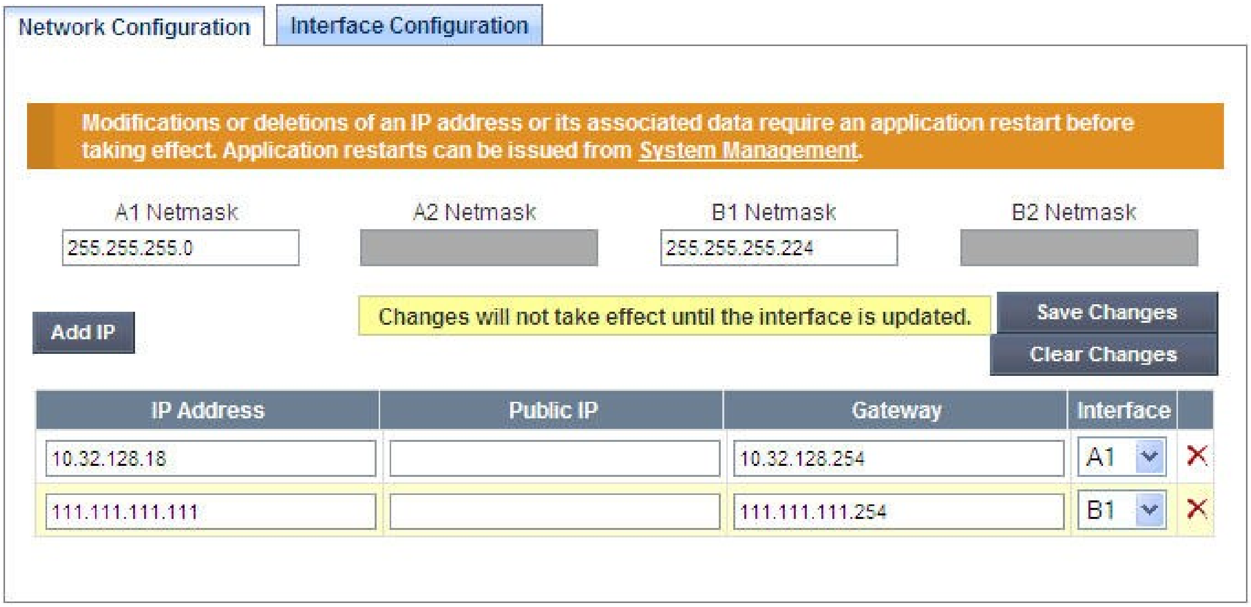
7.10. Device Specific Settings - Network Management

The network information should have been previously specified during installation of Avaya SBC for Enterprise.

Select **Device Specific Setting → Network Management** from the left-side menu as shown below.



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 Avaya SBC for Enterprise.



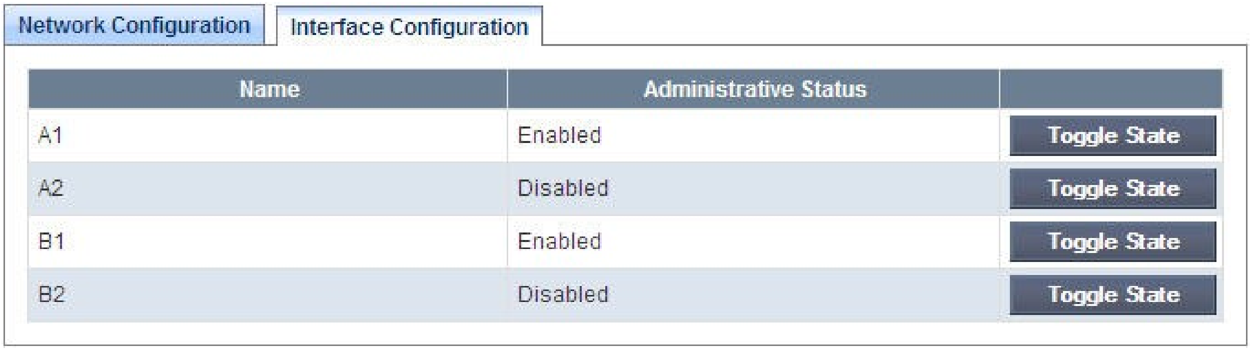
Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.0		255.255.255.224	

Changes will not take effect until the interface is updated.

IP Address	Public IP	Gateway	Interface	
10.32.128.18		10.32.128.254	A1	✕
111.111.111.111		111.111.111.254	B1	✕

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.



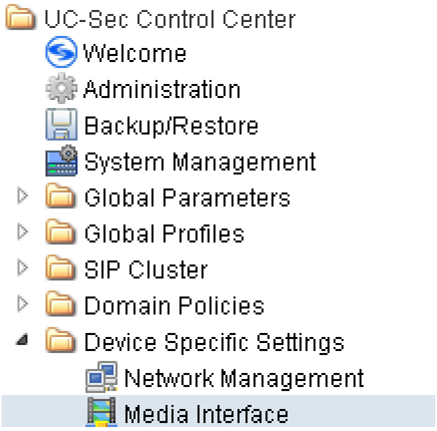
Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

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

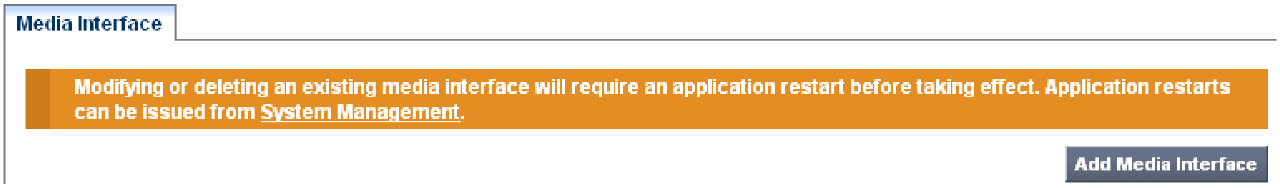
7.11. Device Specific Settings – Media Interface

Media Interfaces were 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.

Select **Device Specific Setting → Media Interface** from the left-side menu as shown below.

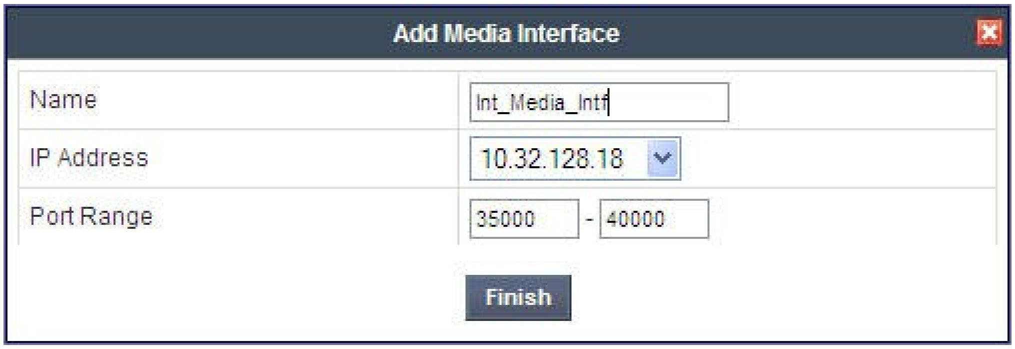


Under **UC-Sec Devices**, select the device being managed, which was named "sp-ucsec1" in the sample configuration (not shown). Select **Add Media Interface**.



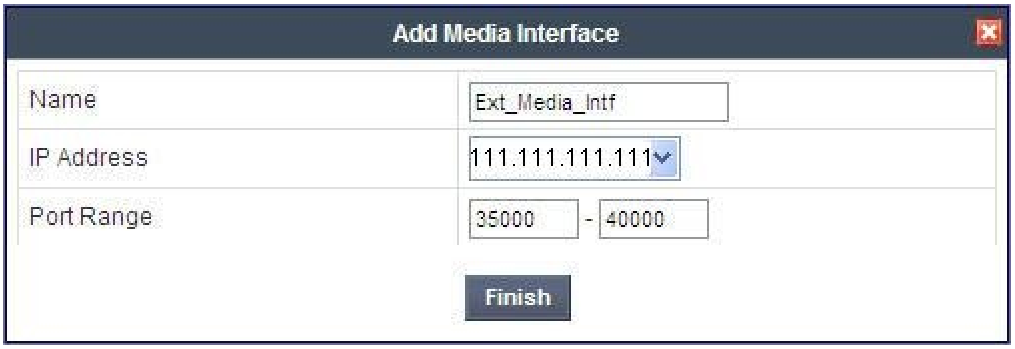
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Enter an appropriate **Name** for the media interface for the Avaya CPE 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**.



Name	Int_Media_Intf
IP Address	10.32.128.18
Port Range	35000 - 40000

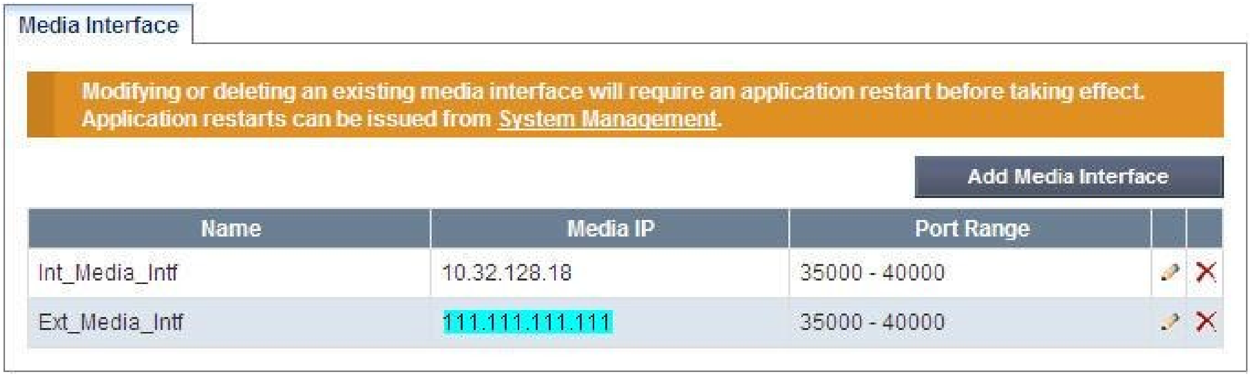
Once again, select **Add Media Interface**. Enter an appropriate **Name** for the media interface for the public "outside" of the SBC, and select the outside public IP Address from the **IP Address** drop-down menu. In the sample configuration, "Ext_Media_Intf" is chosen as the name, and the "outside" public IP Address of the SBC is "111.111.111.111". For the **Port Range**, default values are shown. Click **Finish**.



Add Media Interface

Name	Ext_Media_Intf
IP Address	111.111.111.111
Port Range	35000 - 40000

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

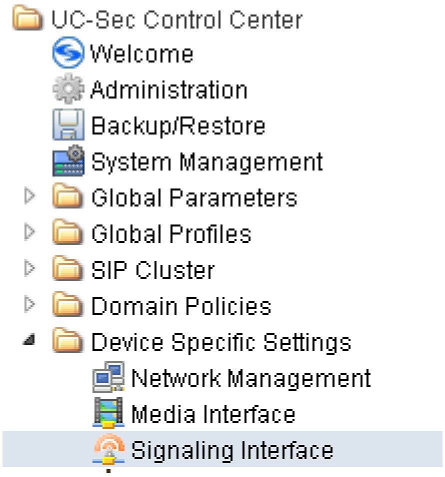


Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

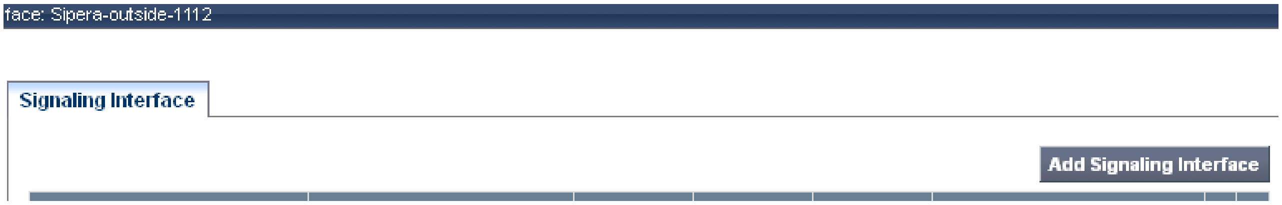
Name	Media IP	Port Range		
Int_Media_Intf	10.32.128.18	35000 - 40000		
Ext_Media_Intf	111.111.111.111	35000 - 40000		

7.12. Device Specific Settings – Signaling Interface

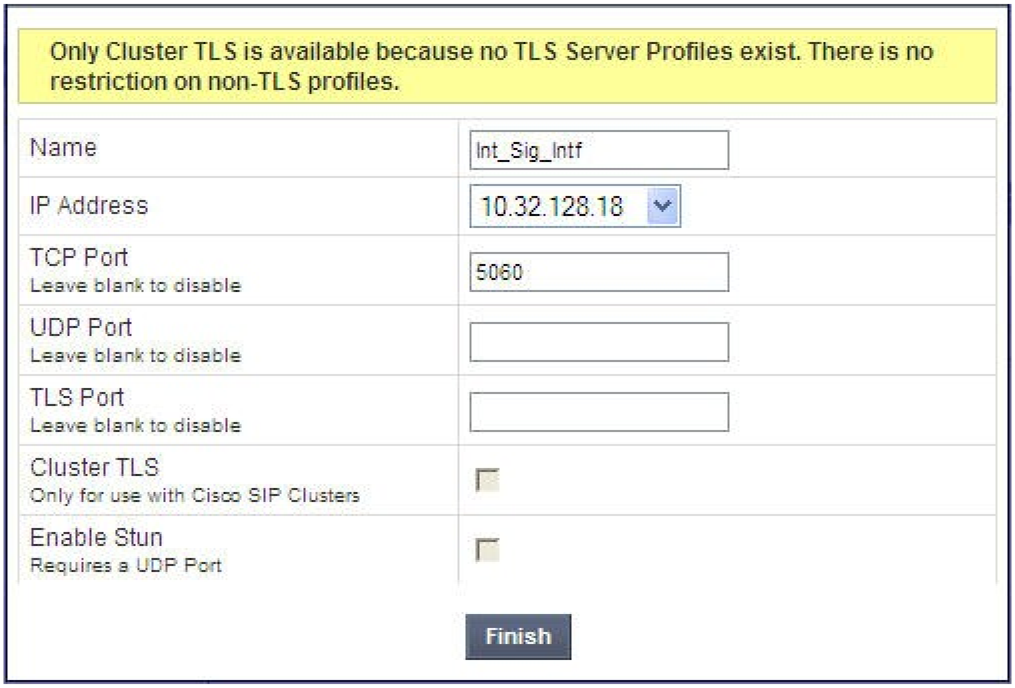
Select **Device Specific Setting → Signaling Interface** from the left-side menu as shown below.



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



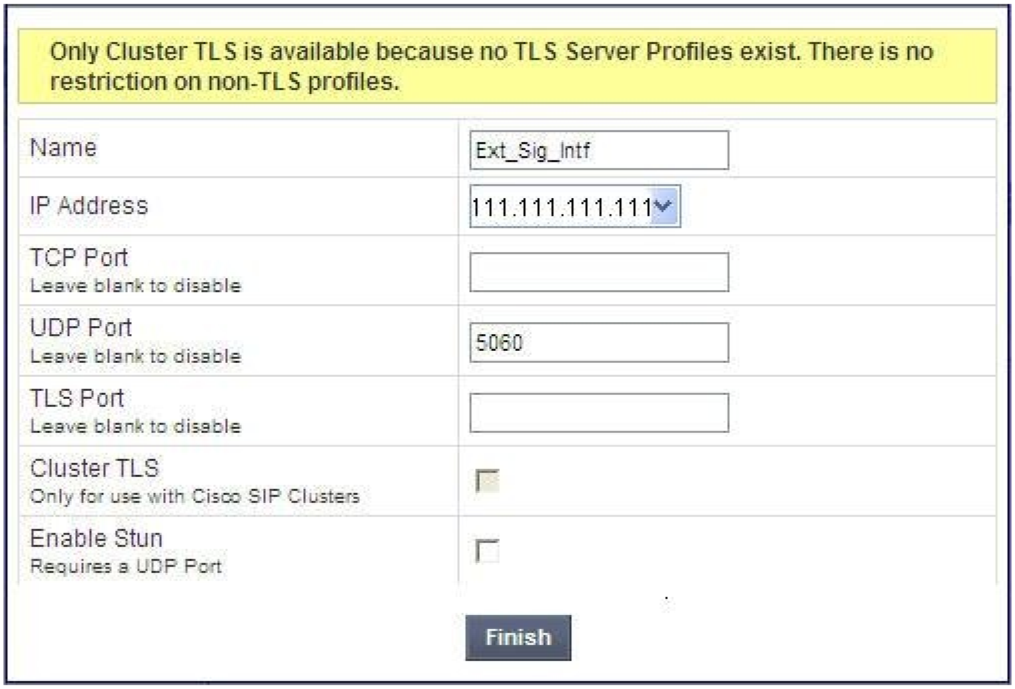
In the Add Signaling Interface screen, enter an appropriate **Name** (e.g., "Int_Sig_Intf") for the "inside" private interface, and choose the private inside IP Address from the **IP Address** drop-down menu.   Choose **TCP Port** "5060" since TCP and port 5060 is used between Session Manager and the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



Only Cluster TLS is available because no TLS Server Profiles exist. There is no restriction on non-TLS profiles.

Name	Int_Sig_Intf
IP Address	10.32.128.18
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	
Cluster TLS Only for use with Cisco SIP Clusters	□
Enable Stun Requires a UDP Port	□

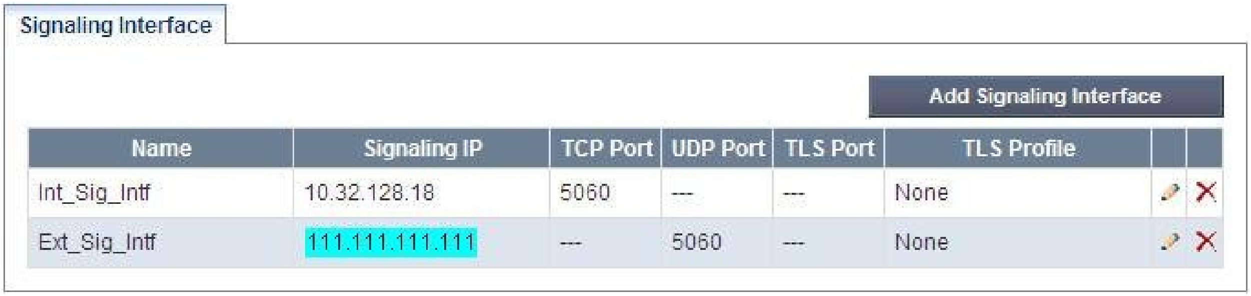
Once again, select **Add Signaling Interface**. In the Add Signaling Interface screen, enter an appropriate **Name** (e.g., "Ext_Sig_Intf") for the "outside" public interface, and choose the public IP Address from the **IP Address** drop-down menu. Choose **UDP Port** "5060". In the sample configuration, Frontier SIP Trunking will send SIP signaling using UDP to the CPE IP Address 111.111.111.111 and to UDP Port 5060. Click **Finish**.



Only Cluster TLS is available because no TLS Server Profiles exist. There is no restriction on non-TLS profiles.

Name	Ext_Sig_Intf
IP Address	111.111.111.111
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	
Cluster TLS Only for use with Cisco SIP Clusters	□
Enable Stun Requires a UDP Port	□

The following screen shows the signaling interfaces defined for the sample configuration.

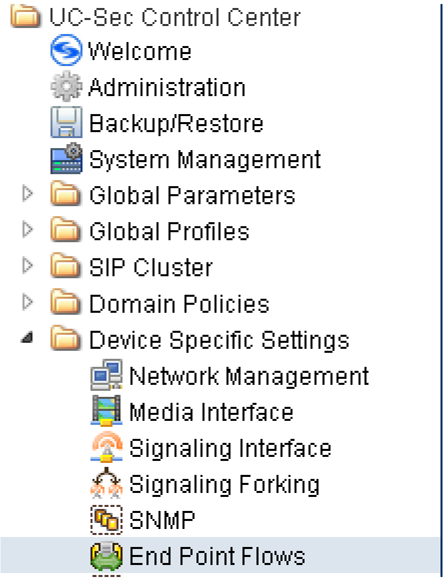


Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Int_Sig_Intf	10.32.128.18	5060	---	---	None	✎	✕
Ext_Sig_Intf	111.111.111.111	---	5060	---	None	✎	✕

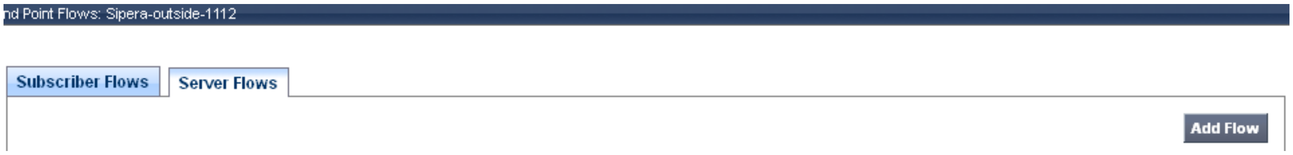
7.13. Device Specific Settings – End Point Server Flows

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.

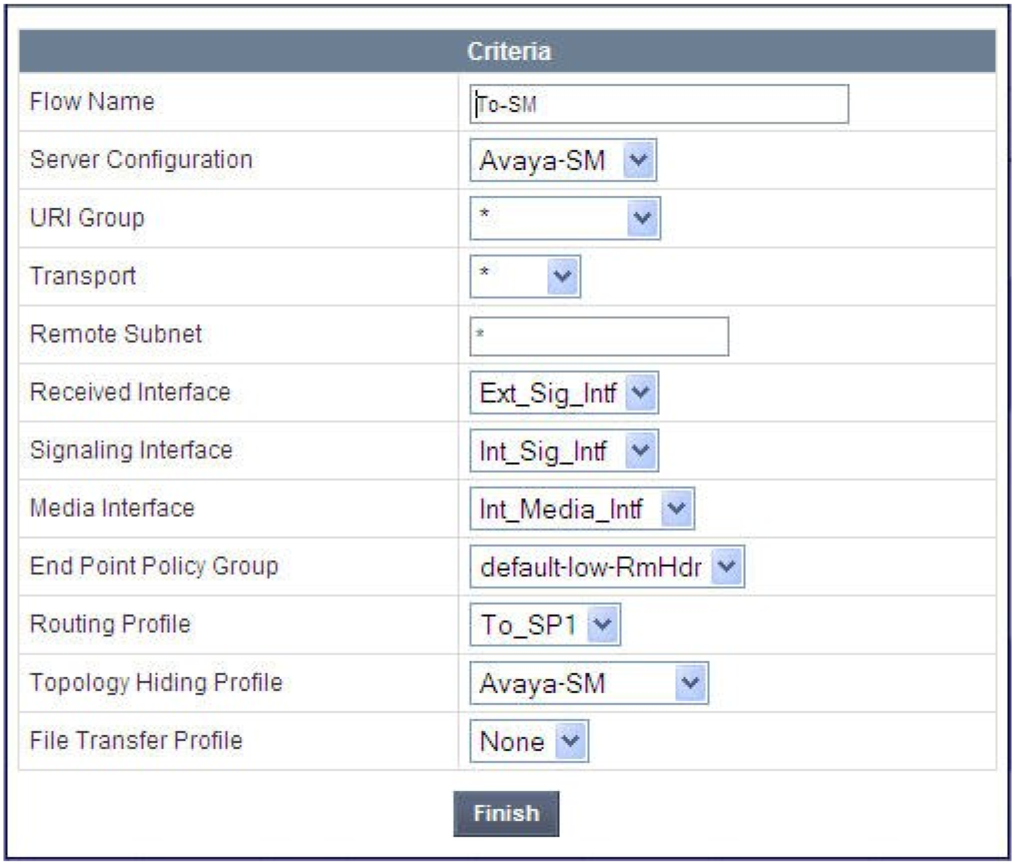
Select **Device Specific Setting → End Point Flows** from the left-side menu as shown below.



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**.



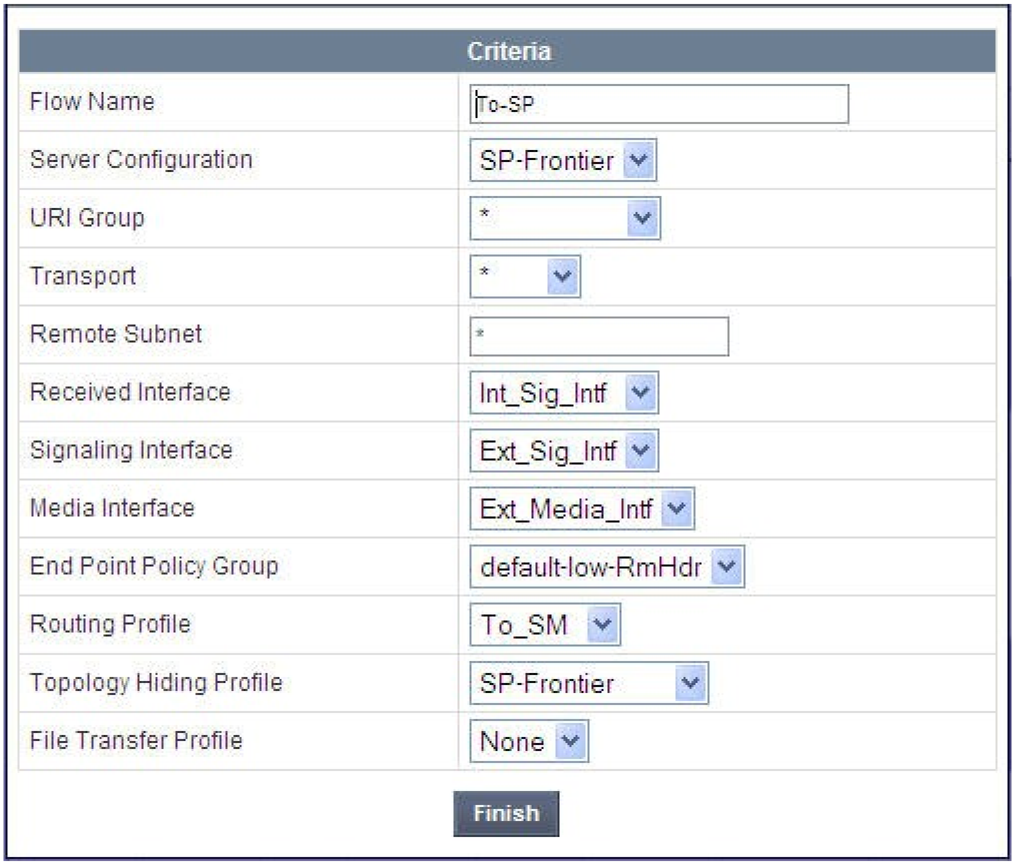
The following screen shows the flow named "To-SM" being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection which is the reverse route of the flow. Click **Finish**.



Criteria	
Flow Name	To-SM
Server Configuration	Avaya-SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig_Intf
Signaling Interface	Int_Sig_Intf
Media Interface	Int_Media_Intf
End Point Policy Group	default-low-RmHdr
Routing Profile	To_SP1
Topology Hiding Profile	Avaya-SM
File Transfer Profile	None

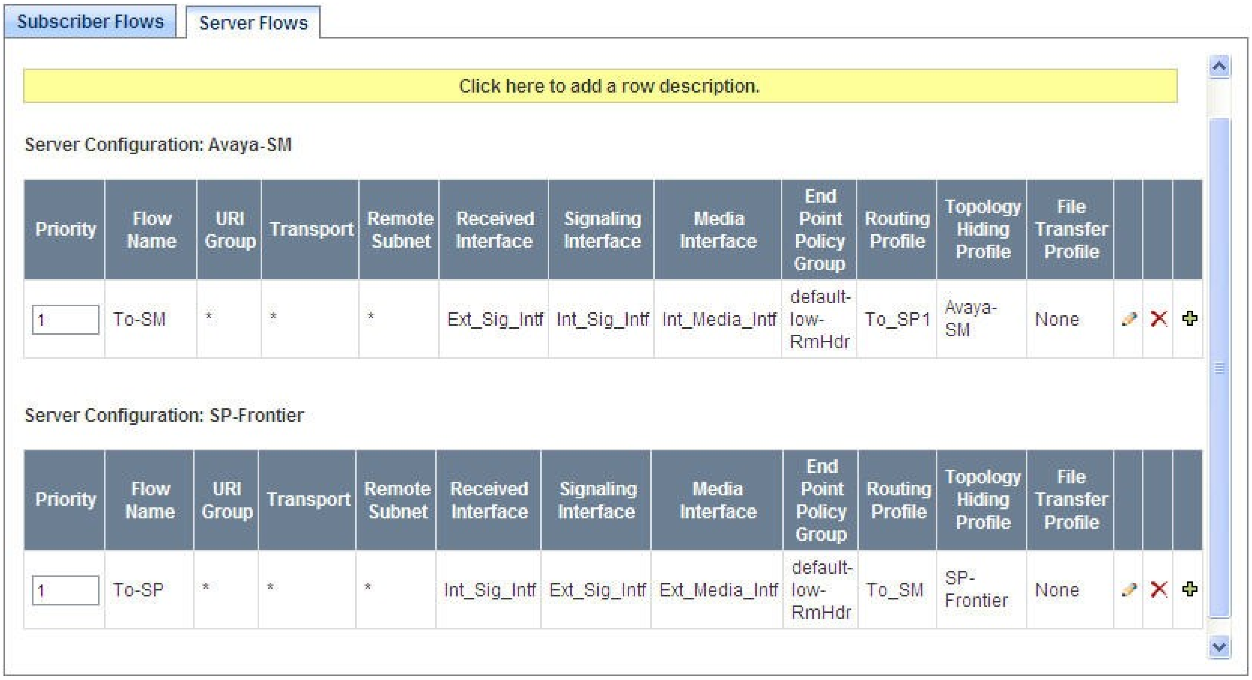
Once again, select the **Server Flows** tab. Select **Add Flow**.

The following screen shows the flow named "To-SP" 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**.



Criteria	
Flow Name	To-SP
Server Configuration	SP-Frontier
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig_Intf
Signaling Interface	Ext_Sig_Intf
Media Interface	Ext_Media_Intf
End Point Policy Group	default-low-RmHdr
Routing Profile	To_SM
Topology Hiding Profile	SP-Frontier
File Transfer Profile	None

The following screen summarizes the Server Flows configured in the sample configuration.



Server Configuration: Avaya-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	To-SM	*	*	*	Ext_Sig_Intf	Int_Sig_Intf	Int_Media_Intf	default-low-RmHdr	To_SP1	Avaya-SM	None	✎	✕	✚

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	To-SP	*	*	*	Int_Sig_Intf	Ext_Sig_Intf	Ext_Media_Intf	default-low-RmHdr	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.

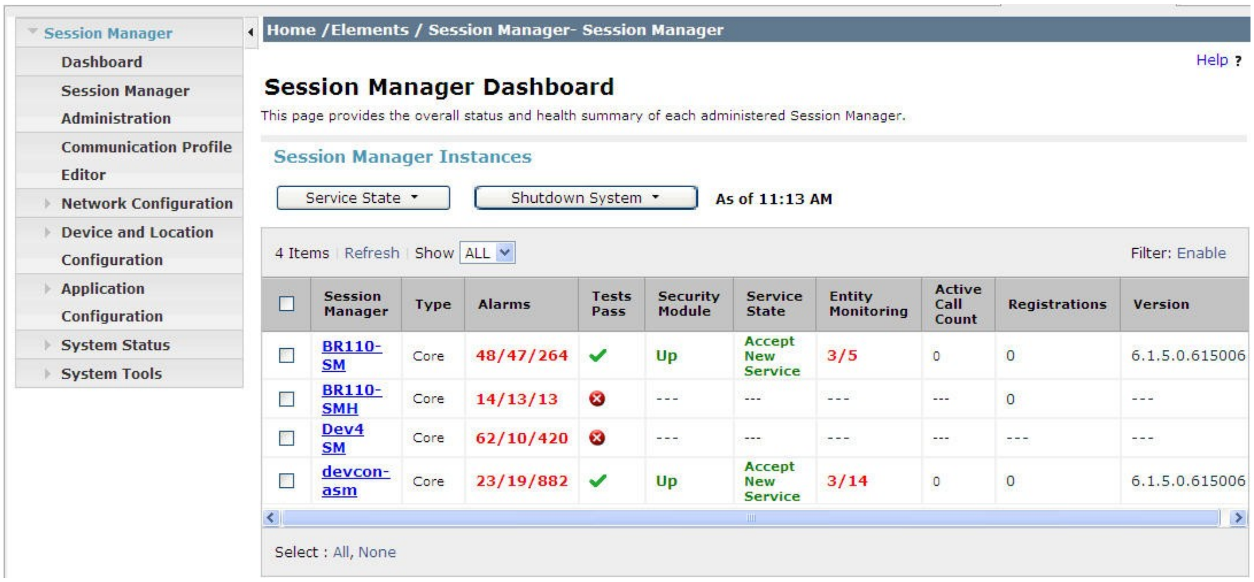
Verification Steps:

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**.



Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Help ?
Service State
Shutdown System

Home /Elements / Session Manager- Session Manager

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

As of 11:13 AM

4 Items | Refresh | Show ALL

Filter: Enable

□	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
□	BR110-SM	Core	48/47/264	✓	Up	Accept New Service	3/5	0	0	6.1.5.0.615006
□	BR110-SMH	Core	14/13/13	☒	---	---	---	---	0	---
□	Dev4 SM	Core	62/10/420	☒	---	---	---	---	---	---
□	devcon-asm	Core	23/19/882	✓	Up	Accept New Service	3/14	0	0	6.1.5.0.615006

Select : All, None

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.0.1, Avaya Aura® Session Manager R6.1 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® Session Manager/System Manager

[1] *Administering Avaya Aura® Session Manager*, Document ID 03-603324, Issue 1.1, Release 6.1, October 2011

[2] *Installing and Configuring Avaya Aura® Session Manager*, Doc ID 03-603473 Issue 2.2, April 2011

[3] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Doc ID 03-603325, Issue 4.1, March 2011

[4] *Administering Avaya Aura® System Manager*, Document Number 03-603324, June 2010

Avaya Aura® Communication Manager

[5] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509, Issue 6.0, Release 6.0, August 2010

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

Avaya Aura® Messaging

[7] *Administering Avaya Aura® Messaging 6.1*, CID: 151610, December 2011

[8] *Implementing Avaya Aura® Messaging 6.1*, CID: 150976, October 2011

Avaya Session Border Controller for Enterprise

Product documentation for UC-Sec can be obtained from Sipera using the link at http://www.sipera.com.

[9] *E-SBC 1U Installation Guide, Release 4.0.5,* Part Number: 101-5225-405v1.00, Release Date: November 2011

[10] *E-SBC Administration Guide, Release 4.0.5,* Part Number: 010-5424-405v1.00, Release Date: 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.