Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the MTS SIP Trunking Service with Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.3 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the SIP Trunking Service offered by MTS Inc. and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager Evolution Server 6.3, Avaya Session Border Controller for Enterprise 6.3 and various Avaya endpoints. The Avaya solution connects to the MTS SIP Trunking Service via the public Internet. MTS Inc. is a member of the Avaya DevConnect Service Provider program.

The MTS SIP Trunking Service provides the enterprise with PSTN access via a SIP trunk between the enterprise and the MTS network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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.

©2015 Avaya Inc. All Rights Reserved.

Table of Contents

1. **Introduction** 4
2. **General Test Approach and Test Results** 4
   2.1. Interoperability Compliance Testing 4
   2.2. Test Results 5
   2.3. Support 6
3. **Reference Configuration** 6
4. **Equipment and Software Validated** 9
5. **Configure Avaya Aura® Communication Manager** 10
   5.1. Licensing and Capacity 10
   5.2. System Features 11
   5.3. IP Node Names 12
   5.4. Codecs 12
   5.5. IP Network Region 13
   5.6. Signaling Group 14
   5.7. Trunk Group 16
   5.8. Calling Party Information 21
   5.9. Outbound Routing 22
6. **Configure Avaya Aura® Session Manager** 25
   6.1. Avaya Aura® System Manager Login and Navigation 26
   6.2. Specify SIP Domain 28
   6.3. Add Location 29
   6.4. Add Adaptation Module 30
   6.5. Add SIP Entities 32
   6.6. Add Entity Links 36
   6.7. Add Routing Policies 38
   6.8. Add Dial Patterns 40
   6.9. Add/View Avaya Aura® Session Manager 43
7. **Configure Avaya Session Border Controller for Enterprise** 45
   7.1. Access the Management Interface 45
   7.2. Verify Network Configuration and Enable Interfaces 47
   7.3. Signaling Interface 50
   7.4. Media Interface 51
   7.5. Server Interworking 52
      7.5.1. Server Interworking – Session Manager 53
      7.5.2. Server Interworking – MTS 55
   7.6. Signaling Manipulation 56
   7.7. Server Configuration 58
      7.7.1. Server Configuration – Session Manager 59
      7.7.2. Server Configuration – MTS 61
   7.8. Application Rules 63
   7.9. Media Rules 64

©2015 Avaya Inc. All Rights Reserved.

7.10. Signaling Rules 66
7.10.1. Signaling Rules – Session Manager 67
7.10.2. Signaling Rules – MTS 69
7.11. Endpoint Policy Groups 70
7.11.1. Endpoint Policy Group – Session Manager 71
7.11.2. Endpoint Policy Group – MTS 72
7.12. Routing 73
7.12.1. Routing – Session Manager 74
7.12.2. Routing – MTS 75
7.13. Topology Hiding 76
7.13.1. Topology Hiding – Session Manager 77
7.13.2. Topology Hiding – MTS 78
7.14. End Point Flows 79
7.14.1. End Point Flow – Session Manager 80
7.14.2. End Point Flow – MTS 82
8. **MTS SIP Trunking Service Configuration** 84
9. **Verification Steps** 84
10. **Conclusion** 86
11. **References** 86

©2015 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the MTS SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager Evolution Server 6.3, Avaya Session Border Controller for Enterprise 6.3 (Avaya SBCE) and various Avaya endpoints. In addition, Avaya Aura® System Manager 6.3 is used to configure Avaya Aura® Session Manager. This Avaya solution connects to the MTS SIP Trunking Service via the public Internet.

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

For brevity, the remainder of this document sometimes refers to the MTS SIP Trunking Service or MTS network simply as MTS.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the MTS SIP Trunking Service and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager (administered by System Manager), and Avaya SBCE.

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

2.1. Interoperability Compliance Testing

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

- SIP trunk registration with the MTS SIP Trunking Service.
- SIP OPTIONS queries and responses.
- Incoming calls from the PSTN to H.323 and SIP deskphones at the enterprise. All inbound PSTN calls were routed from the service provider across the SIP trunk to the enterprise.
- Outgoing calls to the PSTN from H.323 and SIP deskphones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Digest Authentication on outbound calls to the PSTN.

©2015 Avaya Inc. All Rights Reserved.

- Inbound and outbound PSTN calls to/from the Avaya one-X® Communicator softphone. Avaya one-X® Communicator can place/receive calls at the local computer or control a hard phone. Both of these modes were tested. Avaya one-X® Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. Each protocol version was tested.
- Inbound and outbound calls to the Avaya Communicator for Windows SIP softphone.
- Various call types including: local, long distance, international, outbound toll-free, and local directory assistance (411).
- Telephony supplementary features such as hold and resume, transfer, and conference.
- Off-net call transfer, conference, forwarding and mobility (extension to cellular – EC500).
- G.711u and G.729a codecs.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk busy or error conditions.
- Voicemail navigation for inbound and outbound calls.
- Voicemail Message Waiting Indicator (MWI)
- T.38 fax
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise extensions.
- Inbound and outbound long-duration call stability.
- Inbound and outbound long-hold call stability.

2.2. Test Results

Interoperability testing of the MTS SIP Trunking Service was completed with successful results for all test cases with the exception of the observations or limitations described below.

- **UPDATE** – The Genband softswitch MTS used for the test circuit did not support the pre-answer UPDATE message without SDP. Consequently, in the case of off-net call forward, when the enterprise issued an UPDATE message to MTS for updating the display information on the PSTN caller, MTS would respond with "488 Not Acceptable Here". During compliance testing, Communication Manager was configured to use re-INVITE instead of UPDATE for display update (see **Section 5.7**).

- **REFER** – MTS informed that an existing bug on the Genband softswitch would fail use of the SIP REFER method in call transfers, therefore Communication Manager was configured to use re-INVITE for call transfers during the compliance test (see **Section 5.7**).

- **Calling Party Number** – The calling party number displayed on the PSTN phone was not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer was completed, the calling party number displayed the number of the transferring party and not the actual connected party. Communication Manager provides the new connected party information by updating the Contact header in an re-

©2015 Avaya Inc. All Rights Reserved.

INVITE message but the far-end phone display was not updated. The PSTN phone display is ultimately controlled by the backbone PSTN carrier, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/MTS solution. It is listed here simply as an observation.

Items not supported or not tested include the following:

- **G.711u Pass-Through Fax –** Fax using the G.711u pass-through mode (treating fax as voice calls with best effort) was not tested. Communication Manager can be configured for G.711u pass-through fax as a fallback from T.38, but the MTS SIP Trunking Service does not allow T.38 disable for a particular enterprise solution. Fax using T.38 is a global setting on the MTS media gateway and gateway controller card.

- **Call Types Not Tested –** Emergency 911 and inbound toll-free calls were not tested.

2.3. Support

For technical support on the MTS SIP Trunking Service, please contact MTS via the following:

- Web: http://www.mts.ca/mts/support
- Phone: 204-225-4BIZ (204-225-4249)

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the MTS SIP Trunking Service. This is the configuration used for the compliance test.

The components used to create the simulated customer site included:

- System Manager
- Session Manager
- Communication Manager
- Avaya G450 Media Gateway
- Avaya SBCE
- Avaya 1600-Series IP Deskphones (H.323)
- Avaya 96x1-Series IP Deskphones (H.323 and SIP)
- Avaya 1100/1200-Series IP Deskphones (SIP)
- One-X® Communicator softphone (H.323 and SIP)
- Avaya Communicator for Windows softphone (SIP)

Located at the edge of the enterprise is the Avaya SBCE. It has a public interface that connects to the external network and a private interface that connects to the internal enterprise network.

©2015 Avaya Inc. All Rights Reserved.

All SIP and RTP traffic entering or leaving the enterprise flows through this Avaya SBCE which can protect the enterprise against any SIP-based attacks. The transport protocol between the Avaya SBCE and MTS across the public IP network is UDP; the transport protocol between the Avaya SBCE and Session Manager across the enterprise IP network is TCP.

For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses in these Application Notes.

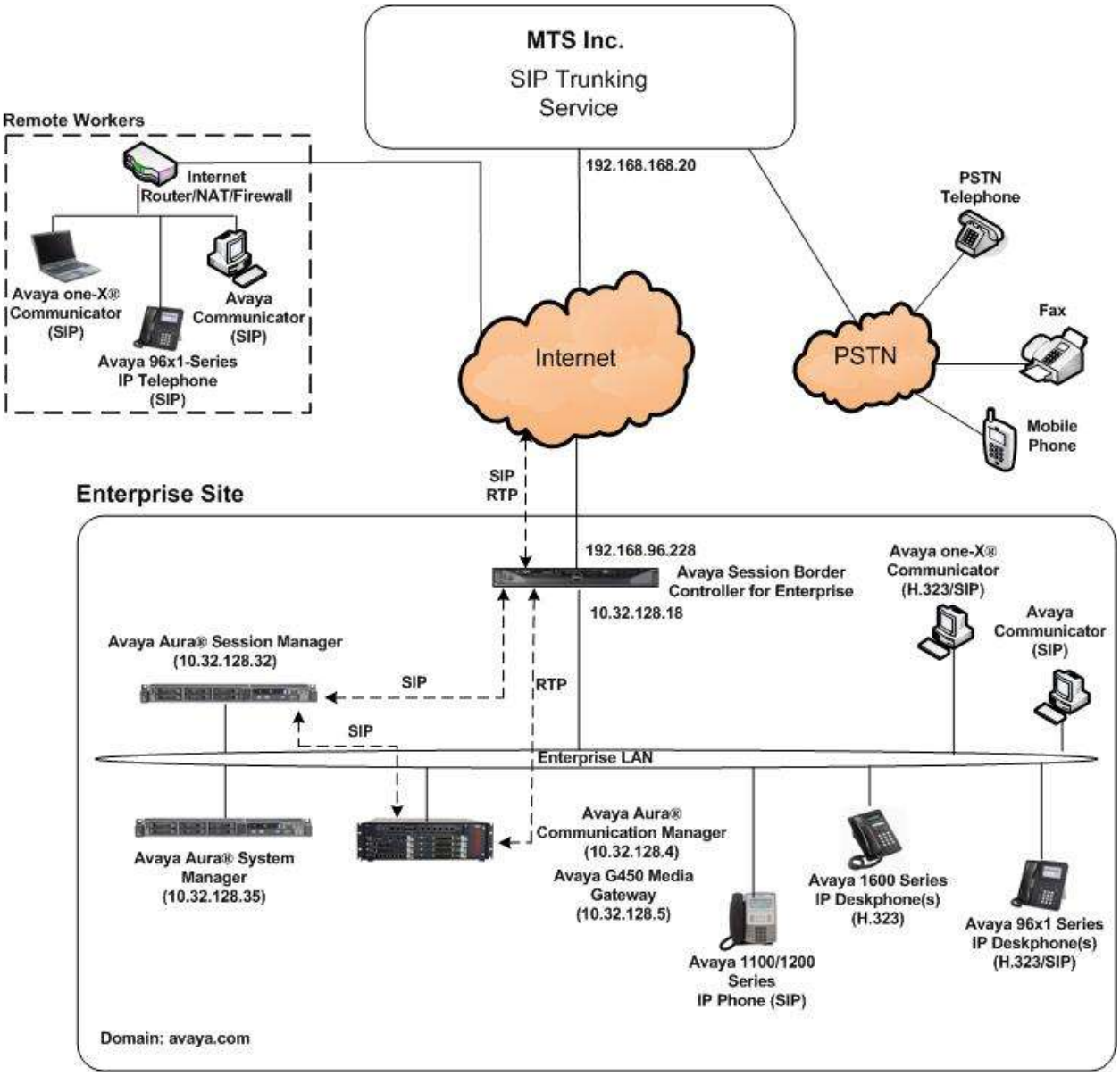


Figure 1: Avaya IP Telephony Network with MTS SIP Trunking Service

©2015 Avaya Inc. All Rights Reserved.

The enterprise endpoints include local extensions that connect to the enterprise network and Remote Worker phones that connect to the public Internet. The same Avaya SBCE was configured to connect to both the service provider network and Remote Worker using separate sets of public/private interfaces (**Figure 1** only shows the public/private interfaces on the Avaya SBCE used for connecting to the service provider network).

A dedicated 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. In addition, this trunk carried both inbound and outbound traffic.

For inbound calls, the calls flow from the service provider to the Avaya SBCE then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case 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) and routing policies to determine the route to the Avaya SBCE for egress to the MTS network.

For outbound calls, the enterprise sends 11 (1+10) digits in the SIP destination headers (Request URI and To). In the SIP source headers (From, Contact, and P-Asserted-Identity), the enterprise sends 10 digits. For inbound calls, MTS sends 10 digits in both the source and destination headers.

The compliance test used Avaya Aura® Communication Manager Messaging (co-resident with Communication Manager) for testing voice mail access/navigation and MWI (Message Waiting Indicator) on Avaya enterprise phones. Other voice messaging applications such as Avaya Aura® Messaging could have been used to satisfy this test purpose.

The administration of Remote Worker via Avaya SBCE, and endpoints on Communication Manager is standard. Since these configuration tasks are not directly related to the inter-operation between the Avaya SIP-enabled enterprise solution and the MTS SIP Trunking Service, they are not included in these Application Notes. See references **[11]** to **[16]** and **[19]** for the detailed information for administration.

©2015 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® System Manager running on an HP® DL360 Server	6.3.14 (Build 6.3.0.8.5682-6.3.8.5304) (Software Update Revision 6.3.14.11.3595) System Platform 6.3.7.0.05001
Avaya Aura® Session Manager running on an HP® DL360 Server	6.3.14 (Release 6.3.14.0.631402)
Avaya Aura® Communication Manager running on an Avaya S8300 Server (installed inside the Avaya G450 Media Gateway)	6.3.11.0- SP11 (R016x.03.0.124.0-22361) System Platform 6.3.7.0.05001
Avaya Aura® Communication Manager Messaging (co-resident with Communication Manager)	6.3-26.0
Avaya G450 Media Gateway	36.12.0 /1
Avaya Session Border Controller for Enterprise running on a Dell® R210 V2 server	6.3.3-08-6224
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP4
Avaya 9611G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.4.0.14
Avaya 9621G IP Deskphone (SIP) running Avaya one-X® Deskphone SIP Edition	6.4.0.14
Avaya 9641G IP Deskphone (SIP) running Avaya one-X® Deskphone SIP Edition	6.4.0.14
Avaya 1140E IP Telephone (SIP)	4.04.20.20
Avaya one-X® Communicator (H.323 and SIP)	6.2.6.03-FP6
Avaya Communicator for Windows	Release 2.1 SP2
MTS SIP Trunking Service Components	
Equipment/Software	Release/Version
Genband A2/Experius	10.3
Genband S3/Q20	V8.3.8.4

Table 1: Equipment and Software Tested

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

©2015 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Communication Manager

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

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged for brevity and clarity in presentation. Note that the IP addresses shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements are not revealed.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that **4000** SIP trunks are available and **80** 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  36
           Maximum Concurrently Registered IP Stations: 2400  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  1
                    Maximum Video Capable IP Softphones: 2400  4
                        Maximum Administered SIP Trunks: 4000  80
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
```


©2015 Avaya Inc. All Rights Reserved.

5.2. System Features

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

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

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

```
change system-parameters features                                Page   9 of  20
                          FEATURE-RELATED SYSTEM PARAMETERS

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

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

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

SCCAN PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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


©2015 Avaya Inc. All Rights Reserved.

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 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
cmm                    10.32.128.4
default                0.0.0.0
procr                  10.32.128.4
procr6                 ::
sessionMgr             10.32.128.32
```

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. The list should include the codecs and preferred order defined by the service provider. For the compliance test, codecs G.711MU and G.729A were tested using ip-codec-set 5. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

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

                          IP Codec Set

    Codec Set: 5

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

On **Page 2**, set the **Fax Mode** to **t.38-standard**, the only fax mode supported by MTS.

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

                         IP CODEC SET

                             Allow Direct-IP Multimedia? n



                                                                    Packet
                         Mode                  Redundancy           Size(ms)
    FAX                  t.38-standard          0            ECM: y
    Modem                off                    0
    TDD/TTY              US                     3
    H.323 Clear-channel  n                      0
    SIP 64K Data         n                      0                   20
```


©2015 Avaya Inc. All Rights Reserved.

5.5. IP Network Region

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

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

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


©2015 Avaya Inc. All Rights Reserved.

On **Page 4**, define the IP codec set to be used for traffic between region 5 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) **1**. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 5 will be used for calls between region 5 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 5 will automatically create a complementary table entry on the IP network region 1 form for destination region 5. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4** (not shown).

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

 Source Region: 5     Inter Network Region Connection Management     I       M
                                                                    G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    5     y    NoLimit                                           n       t
 2
 3
 4
 5    5                                                           all
```

5.6. Signaling Group

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

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the recommended default value of **tls** (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. If TLS is used here, it must also be used on the Session Manager entity link defined in **Section 6.6**.
- Set the **IMS Enabled** field to **n**. This setting directs Communication Manager to serve as an Evolution Server for Session Manager.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the 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 **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). At the time of Session Manager installation, a

©2015 Avaya Inc. All Rights Reserved.

SIP connection between Communication Manager and Session Manager would have been established for use by all Communication Manager SIP traffic using the well-known port value for TLS or TCP. By creating a new signaling group with a separate port value, a separate SIP connection is created between Communication Manager and Session Manager for SIP traffic to and from the service provider. As a result, any signaling group or trunk group settings (**Section 5.7**) will only affect the service provider traffic and not other SIP traffic at the enterprise. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5068**.

- 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.
- 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 that Communication Manager will wait for a response (other than "100 Trying") to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

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

 Group Number: 5              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
       Q-SIP? n
    IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr                Far-end Node Name: sessionMgr
 Near-end Listen Port: 5068               Far-end Listen Port: 5068
                                       Far-end Network Region: 5
                                 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? n                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 15
```


©2015 Avaya Inc. All Rights Reserved.

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 defined 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
```


©2015 Avaya Inc. All Rights Reserved.

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than "100 Trying") to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value equal to the **Alternate Route Timer** on the signaling group form described in **Section 5.6**.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that session-refresh messages must be sent to the remote end to keep the active session alive. For the compliance test, the value of **600** seconds was used.

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

TRUNK PARAMETERS

     Unicode Name: auto

                                          Redirect On OPTIM Failure: 15000

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

 Disconnect Supervision - In? y  Out? y


              XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```


©2015 Avaya Inc. All Rights Reserved.

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. To remove the + sign, the **Numbering Format** was set to **private** and the **Numbering Format** 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 local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
add trunk-group 5                                              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                       SIP ANAT Supported? N
```


©2015 Avaya Inc. All Rights Reserved.

On **Page 4**, set the **Mark Users as Phone** field to **y**. Since MTS does not support use of REFER (see item **REFER** in the observation/limitation list in **Section 2.2**), the **Network Call Redirection** field must be set to **n**. Setting the **Network Call Redirection** flag to **y** enables use of the SIP REFER message for call transfer; otherwise the SIP re-INVITE message will be used as was the case with the compliance test. Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been redirected. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set **Telephone Event Payload Type** to **101**, the value used by MTS.

Set **Always Use re-INVITE for Display Updates** to **y**. This setting directs Communication Manager to use re-INVITE instead of UPDATE (if supported by the remote end) for phone display update in off-net call re-directions (forward and transfer). See the item **UPDATE** in the observation/limitation list in **Section 2.2** for details.

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

                                        Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                    Network Call Redirection? n

                                     Send Diversion Header? y
                                   Support Request History? n
                                Telephone Event Payload Type: 101
                                        Shuffling with SDP? n

                         Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? y
                         Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                               Enable Q-SIP? n
```


©2015 Avaya Inc. All Rights Reserved.

To ensure interoperability with Avaya SIP endpoints, the **Mark Users as Phone** field must also be set to **y** on the SIP trunk used by the SIP endpoints to register and communicate with the Session Manager. In most cases, this will be the trunk created during the initial installation of the Session Manager. In the case of the compliance test, this was trunk-group 1.

```
change trunk-group 1                                          Page   4 of  21
                              PROTOCOL VARIATIONS

                                        Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                      Send Transferring Party Information? n
                                  Network Call Redirection? n

                                    Send Diversion Header? n
                                  Support Request History? y
                               Telephone Event Payload Type:
                                    Shuffling with SDP? n

                         Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                               Enable Q-SIP? n
```


©2015 Avaya Inc. All Rights Reserved.

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 number will be provided by the SIP service provider. It is used to authenticate the caller.

The screen below shows a subset of the DID numbers assigned for testing. These numbers were assigned to the 4 extensions 41015, 41016, 41018 and 41024. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk (trunk group 5) when calls were originated from these extensions.

```
change private-numbering 5                                    Page   1 of   2
                          NUMBERING - PRIVATE FORMAT

Ext Ext            Trk        Private          Total
Len Code           Grp(s)     Prefix           Len
 5  4                                         5     Total Administered: 6
 5  41015          5          2049924610       10       Maximum Entries: 540
 5  41016          5          2049924611       10
 5  41018          5          2049924613       10
 5  41024          5          2049924612       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 3 will send the calling party number as the **Private Prefix** plus the extension number. Note that in the example below, the trunk group 3 is used for the call.

```
change private-numbering 5                                    Page   1 of   2
                          NUMBERING - PRIVATE FORMAT

Ext Ext            Trk        Private      Total
Len Code           Grp(s)     Prefix        Len
 5  3                                      5     Total Administered: 2
 5  3              3          42654         10       Maximum Entries: 540
```


©2015 Avaya Inc. All Rights Reserved.

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
   1           4   dac
   3           5   ext
   4           5   ext
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   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  11
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       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: *01    All: *02    Deactivation: *03
   Call Forwarding Enhanced Status:        Act:        Deactivation:
```


©2015 Avaya Inc. All Rights Reserved.

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: 1

          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
    011                  10   18    55        intl          n
    1609                 11   11    55        natl          n
    1732                 11   11    55        natl          n
    1800                 11   11    55        natl          n
    1877                 11   11    55        natl          n
    1908                 11   11    55        natl          n
    411                  3    3     55        svcl          n
```


©2015 Avaya Inc. All Rights Reserved.

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 route pattern in the following manner. The example below shows the values used for route pattern 55 configured for the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **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.
- **Numbering Format**: Enter **unk-unk**. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR**: **next**

```
change route-pattern 55                                          Page   1 of   3
                   Pattern Number: 55     Pattern Name: A-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                                                              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: y y y y y n  n            rest                                           none
```


©2015 Avaya Inc. All Rights Reserved.

6. Configure Avaya Aura® Session Manager

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

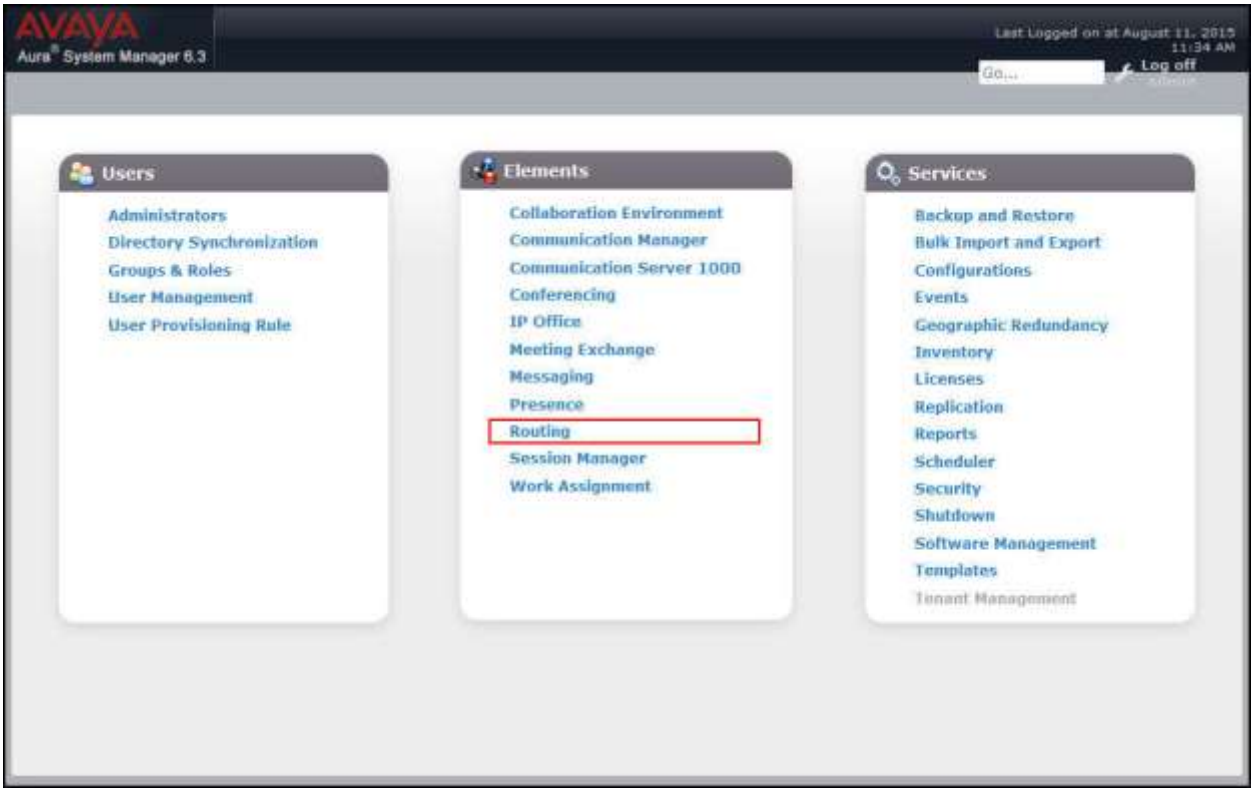
- SIP domain
- Logical/physical Location that can be occupied by SIP entities
- Adaptation module to perform dial plan manipulation
- SIP Entities corresponding to Communication Manager, the Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when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

©2015 Avaya Inc. All Rights Reserved.

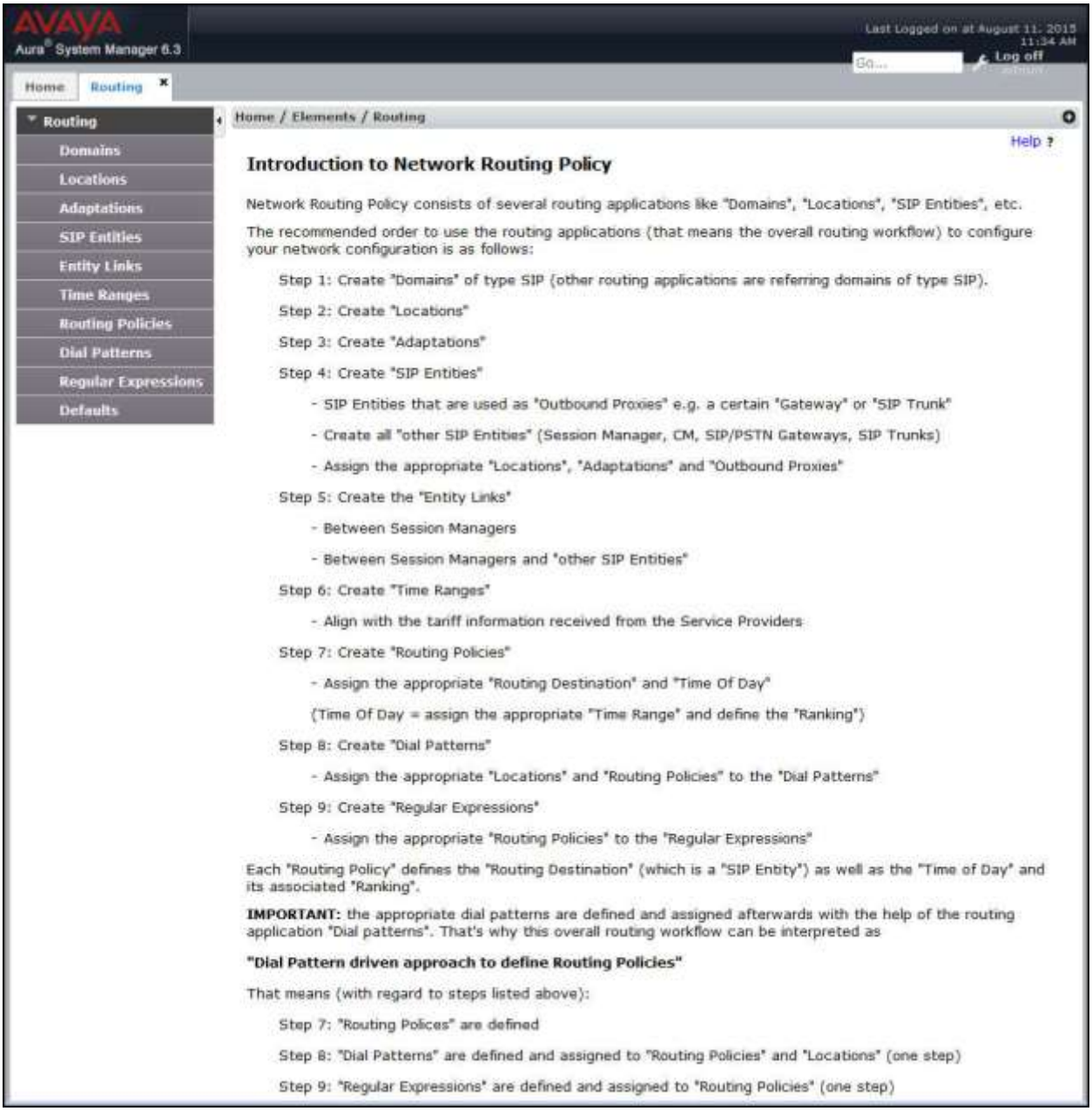
6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **https://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. The **Home** page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located using the **Elements → Routing** link highlighted below.



©2015 Avaya Inc. All Rights Reserved.

Clicking the **Elements → Routing** link to display the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.



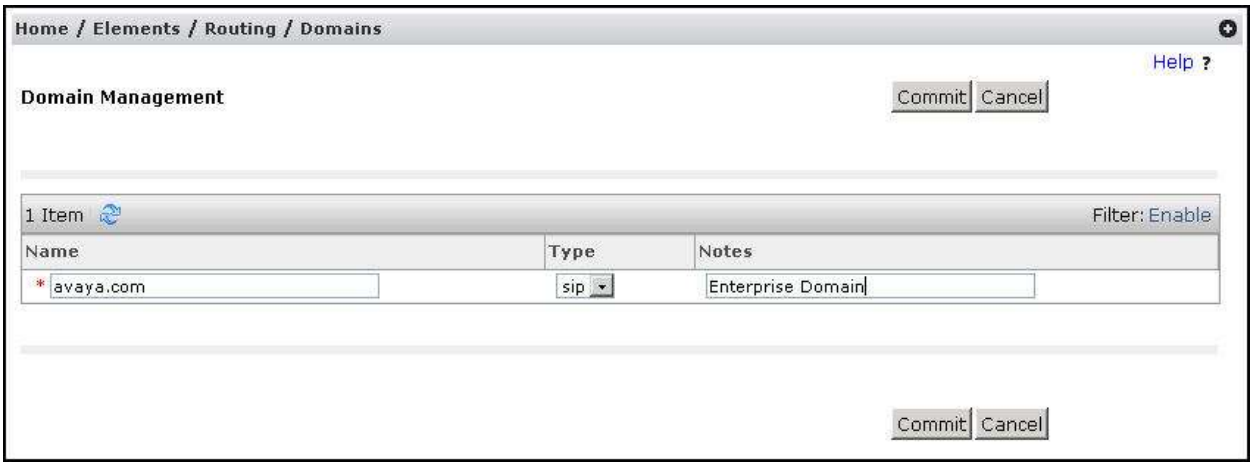
©2015 Avaya Inc. All Rights Reserved.

6.2. Specify SIP Domain

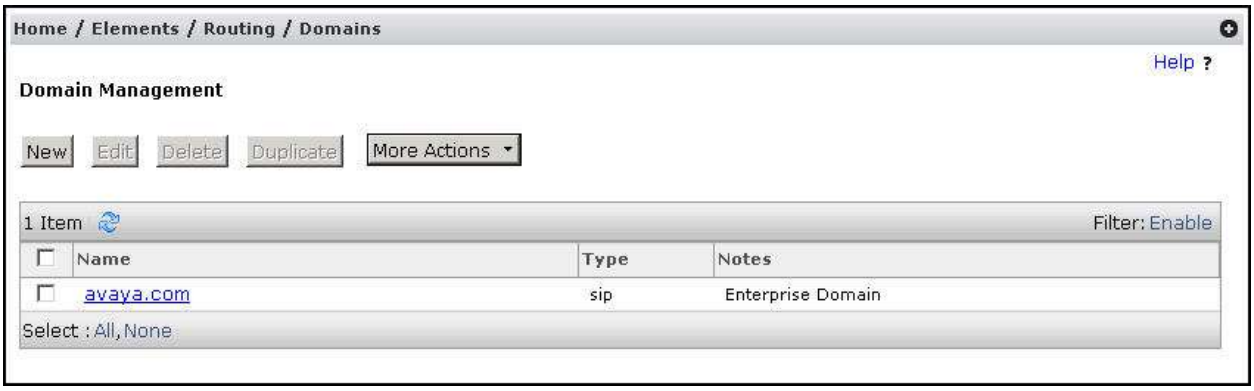
Create a SIP domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avaya.com**). Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the **Domain Management** 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** to save.



The screen below shows the configured entry for the enterprise domain.



©2015 Avaya Inc. All Rights Reserved.

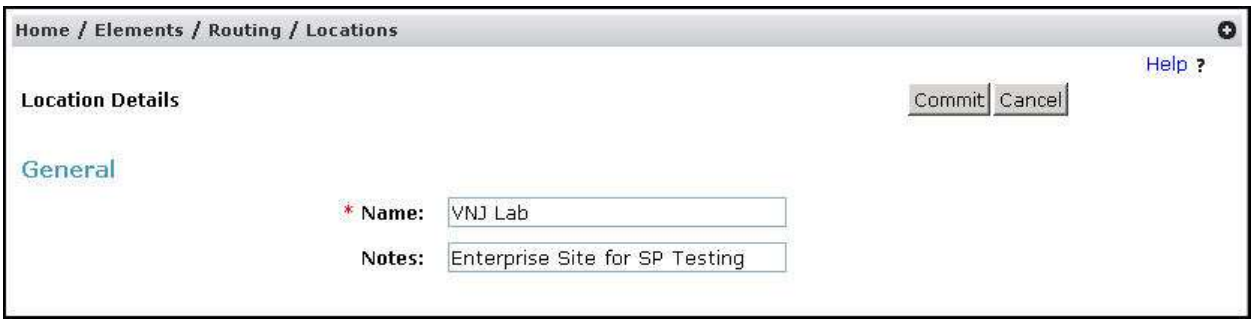
6.3. Add Location

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

To add a location, navigate to **Routing → Locations** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the **Location Details** right pane that appears (shown below), fill in the following:

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

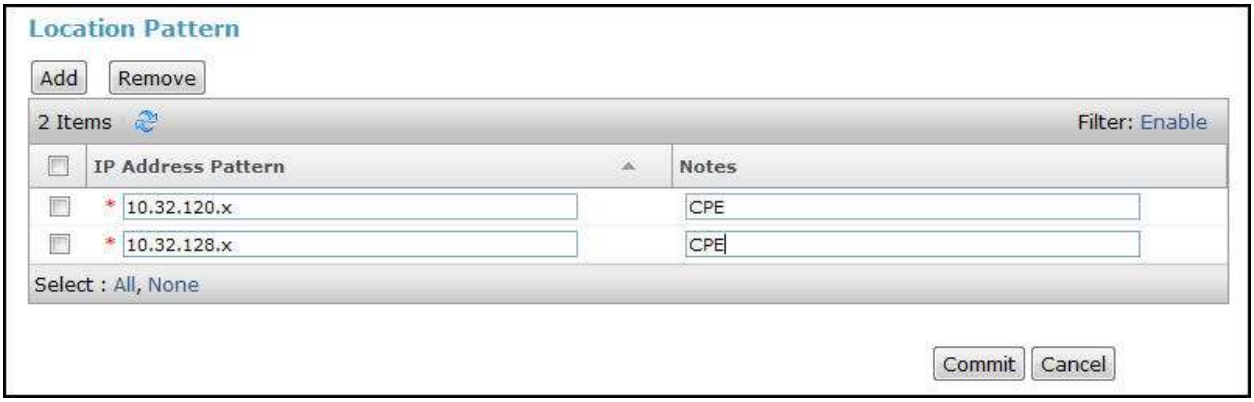
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).



Scroll down to the **Location Pattern** section. Click **Add** and enter the following values. Use default values for all remaining fields.

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

Click **Commit** to save.



©2015 Avaya Inc. All Rights Reserved.

6.4. Add Adaptation Module

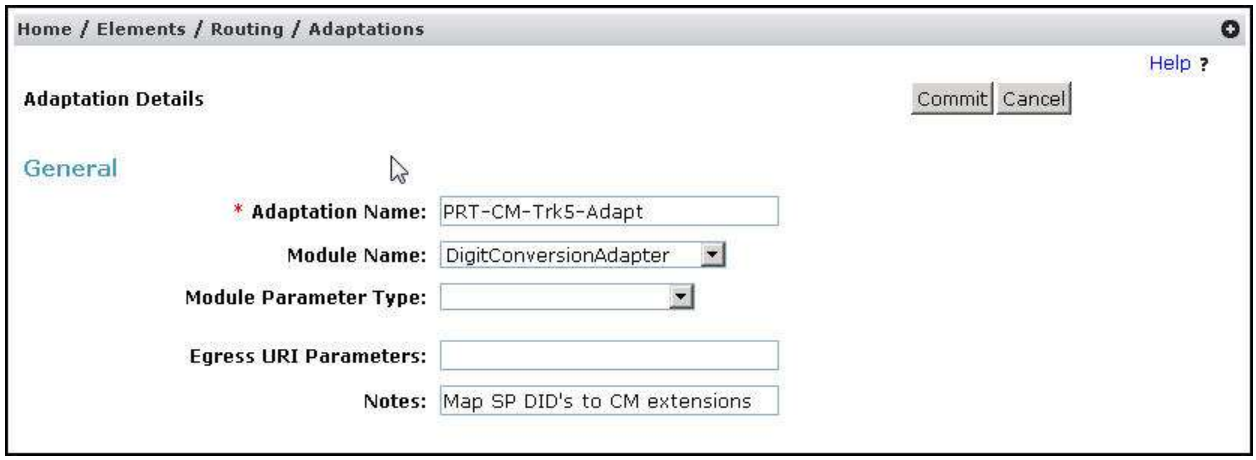
Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules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

For the compliance test, one adaptation was created for Communication Manager. The adaptation mapped inbound DID numbers from MTS to local Communication Manager extensions.

To create the adaptation that will be applied to the Communication Manager SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the **Adaption Details** right pane that appears (shown below), fill in the following:

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

- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter or select **DigitConversionAdapter**.
- **Notes:** Enter a description (optional).

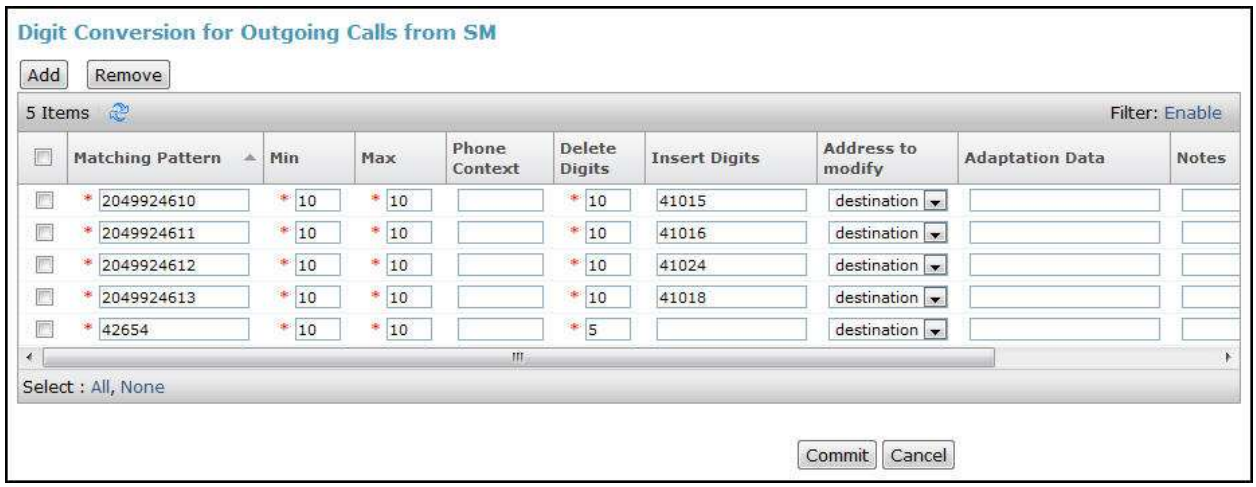


©2015 Avaya Inc. All Rights Reserved.

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

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

Click **Commit** to save.



In the above screen, the top 4 rows specify the DID numbers to be converted to the 4 enterprise local extensions. Note that the mappings configured in the adaptation shown here should match those specified in the Communication Manager private numbering form in **Section 5.8**.

In a real customer environment, often the DID number is comprised of the local extension plus a prefix. If this is true, then a single digit conversion entry can be created for all extensions. In the example above, the 5th row specifies a 5 digit prefix that is deleted from each incoming 10-digit DID number starting with "42654" leaving a 5 digit extension to be routed by Session Manager.

©2015 Avaya Inc. All Rights Reserved.

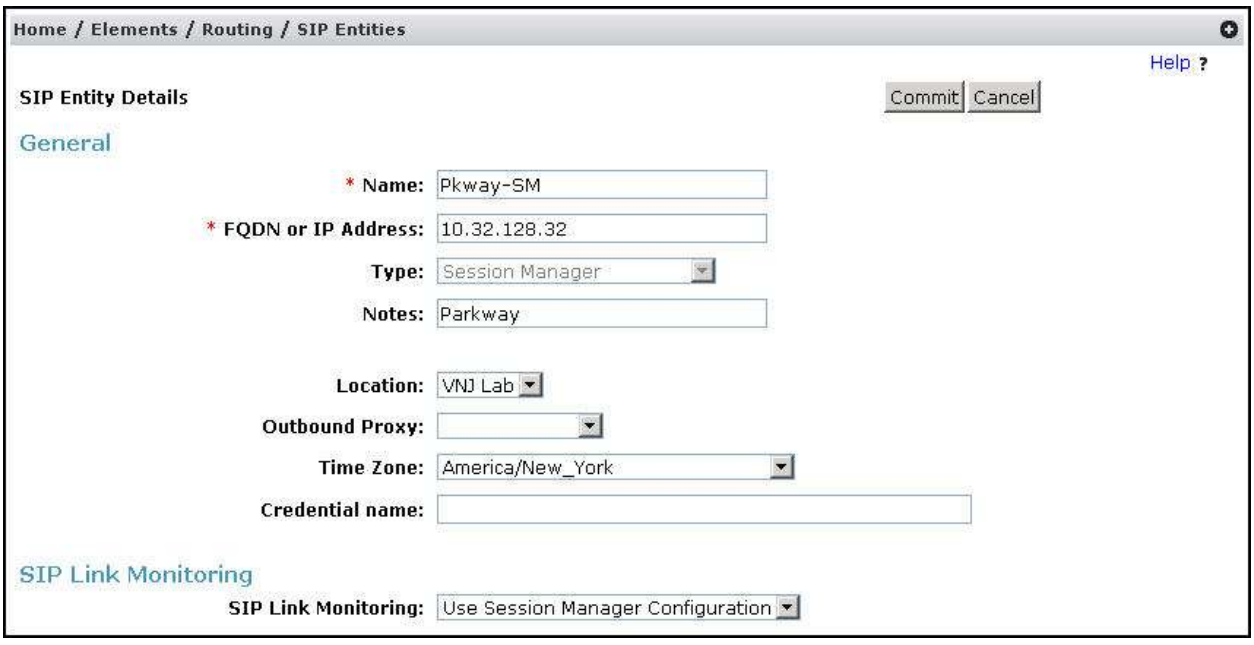
6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the **SIP Entity Details** right pane that appears (shown below), fill in the following:

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate adaptation created in **Section 6.4** that will be applied to this entity.
- **Location:** Select the location that applies to the SIP entity being created. For the compliance test, all components were located in the **VNJ Lab** location.
- **Time Zone:** Select the time zone for the location above.

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



©2015 Avaya Inc. All Rights Reserved.

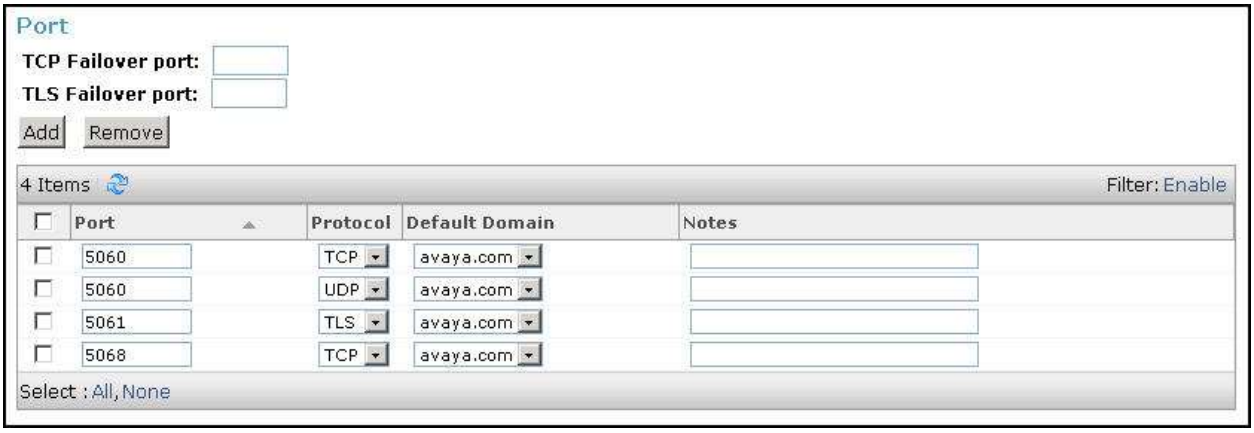
To define the ports used by Session Manager, scroll down to the **Port** section. This section is only present for **Session Manager** SIP entities.

In the **Port** section, click **Add** and enter the following values:

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

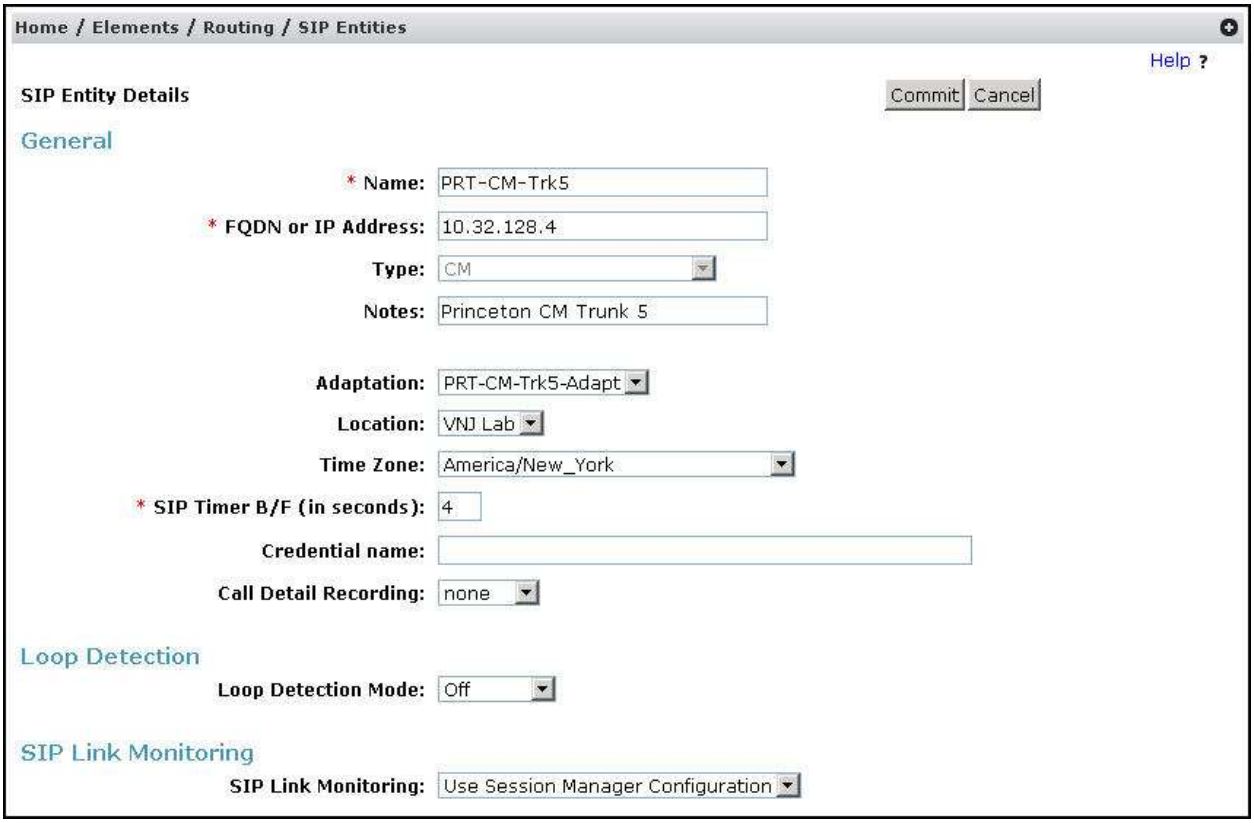
Click **Commit** on the top and bottom of the **SIP Entity Details** screen to save.

For the compliance test, four port entries were used. The first three are the standard ports used for SIP traffic: port 5060 for UDP/TCP and port 5061 for TLS. In addition, port 5068 defined in **Section 5.6** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list.



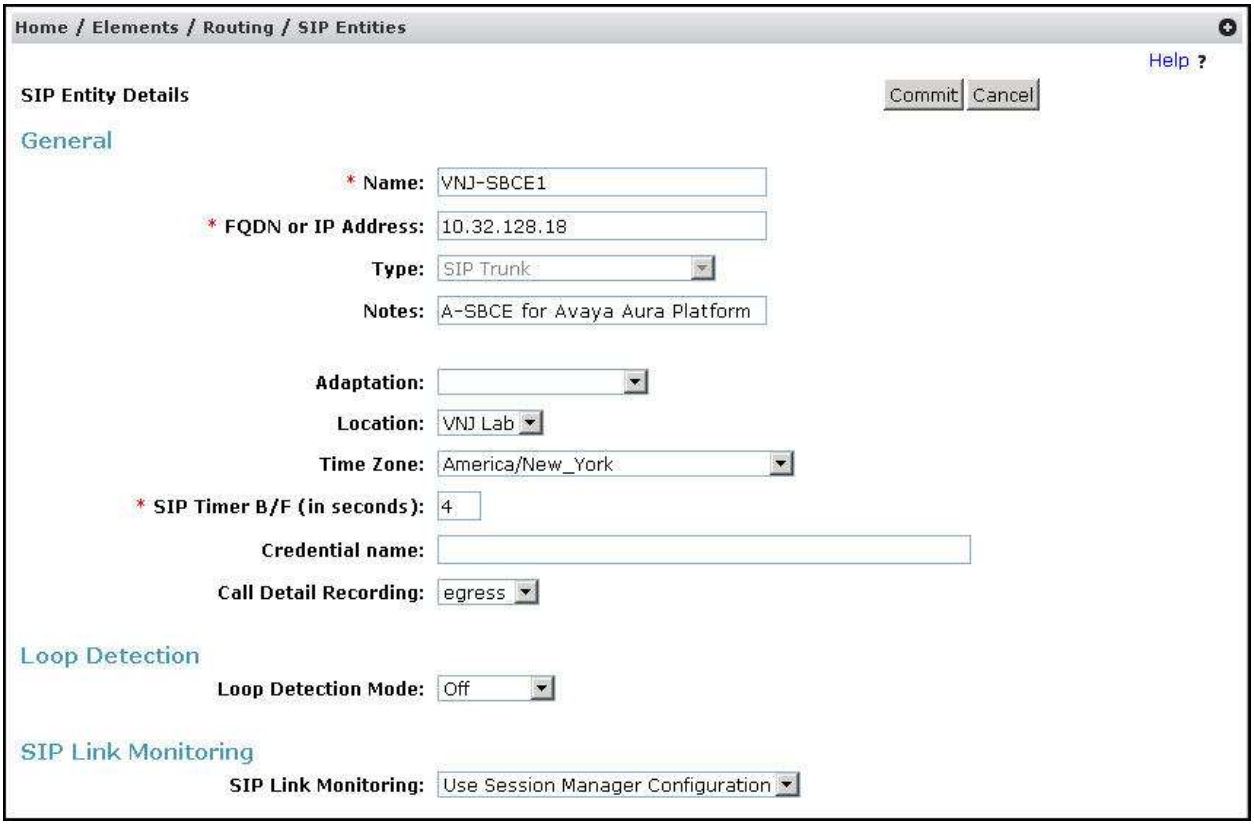
©2015 Avaya Inc. All Rights Reserved.

The following screen shows the addition of Communication Manager SIP entity. In order for Session Manager to send SIP service provider traffic on a dedicated entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This specific Communication Manager SIP entity is separate from the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of Communication Manager. For **Type**, **CM** is selected. For the **Adaptation** field, select the adaptation module previously defined for dial digit manipulation in **Section 6.4**. The **Location** field is set to **VNJ Lab** which is the location defined for the subnet where Communication Manager resides.



©2015 Avaya Inc. All Rights Reserved.

The following screen shows the addition of the Avaya SBCE SIP entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). For **Type**, **SIP Trunk** is selected. The **Location** field is set to **VNJ Lab** which is the location defined for the subnet where the Avaya SBCE resides.



©2015 Avaya Inc. All Rights Reserved.

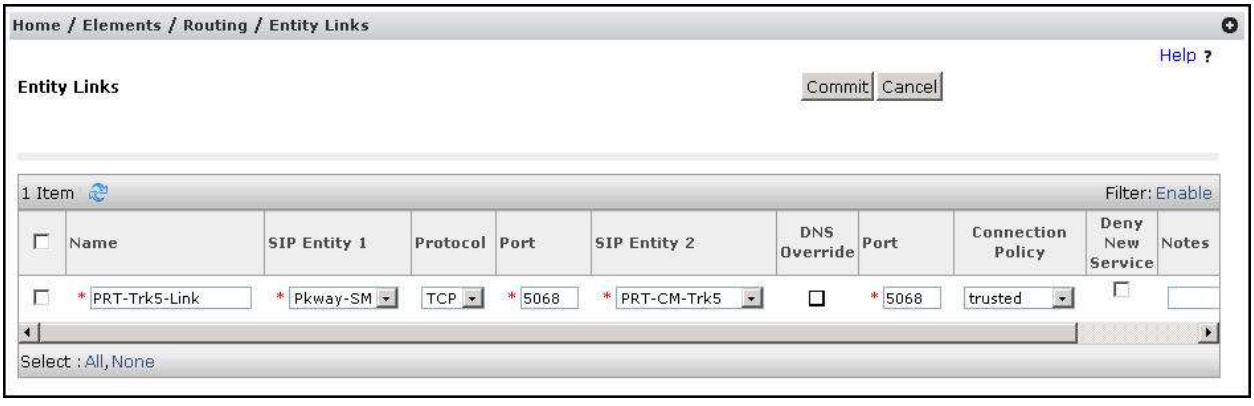
6.6. Add Entity Links

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 one to the Avaya SBCE. To add an entity link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the **Entity Links** right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link. This must match the protocol used in the Communication Manager signaling group in **Section 5.6**.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager entity link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager entity link, 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 the Communication Manager entity link, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Connection Policy:** Select **Trusted** from pull-down menu.

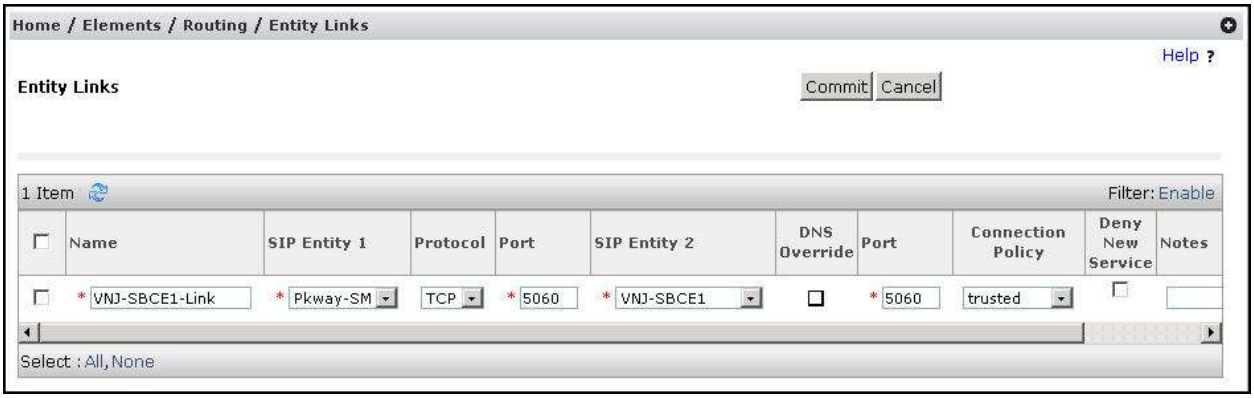
Click **Commit** to save.

The following screen illustrates the entity link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. For the compliance test, the TCP protocol was used (for ease in troubleshooting traces) but the recommended configuration is to use TLS.



©2015 Avaya Inc. All Rights Reserved.

The following screen illustrates the entity link to the Avaya SBCE.



©2015 Avaya Inc. All Rights Reserved.

6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP entities (as route destinations) specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the **Routing Policy Details** right pane that appears (shown below), fill in the following:

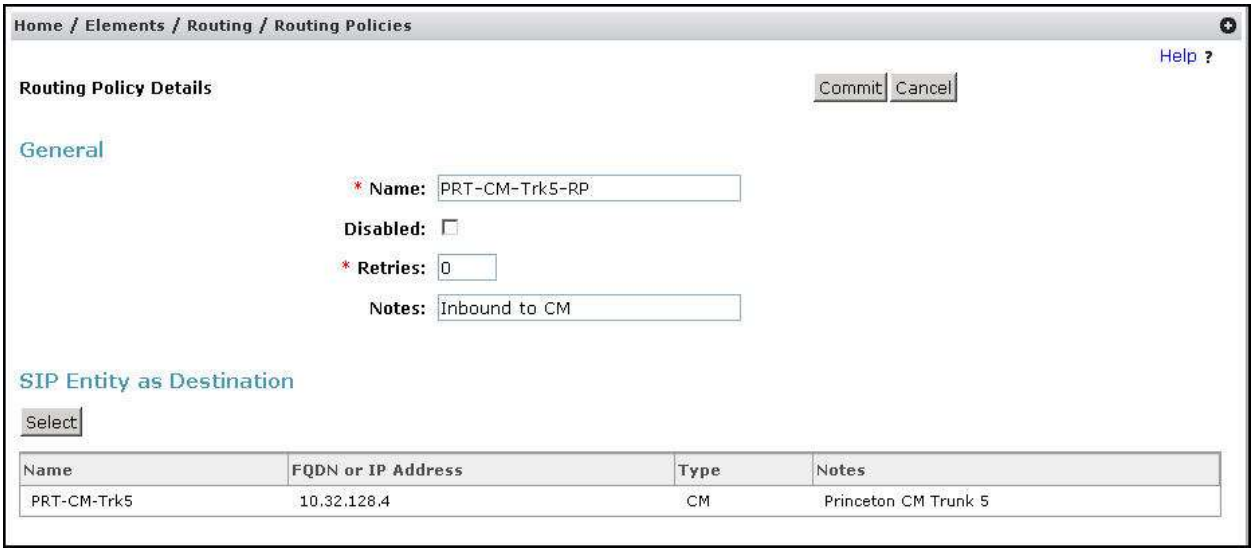
In the **General** section, enter the following values. Use default values for all remaining fields.

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

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

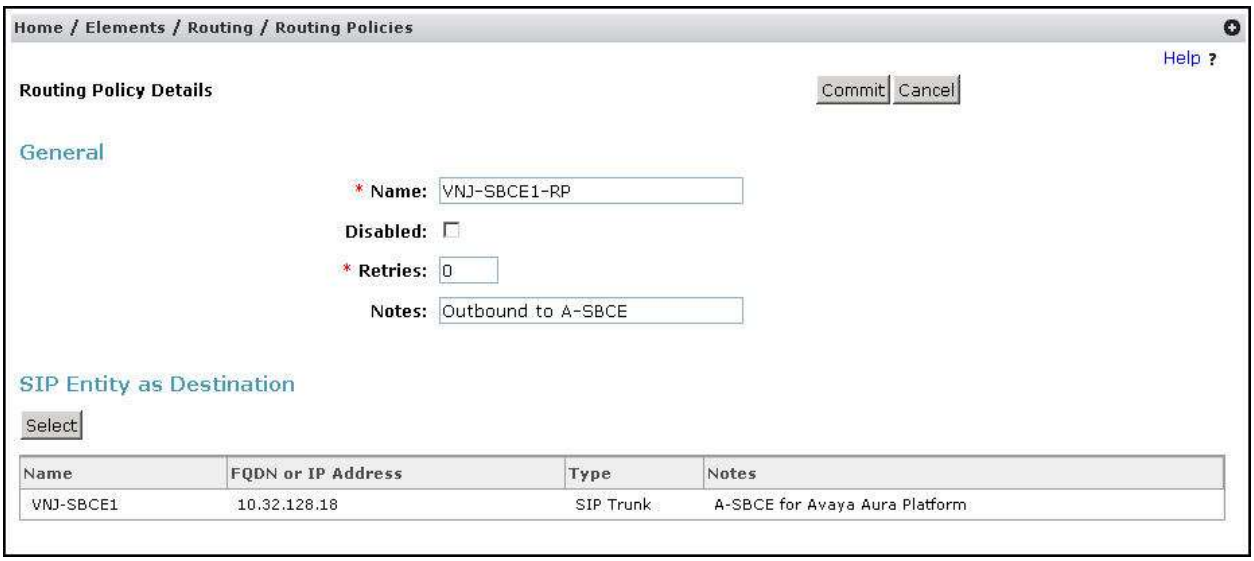
Click **Commit** to save.

The following screen shows the routing policy for Communication Manager.



©2015 Avaya Inc. All Rights Reserved.

The following screen shows the routing policy for the Avaya SBCE.



©2015 Avaya Inc. All Rights Reserved.

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 MTS 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 (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the **Dial Patterns Details** right pane that appears (shown below), fill in the following:

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

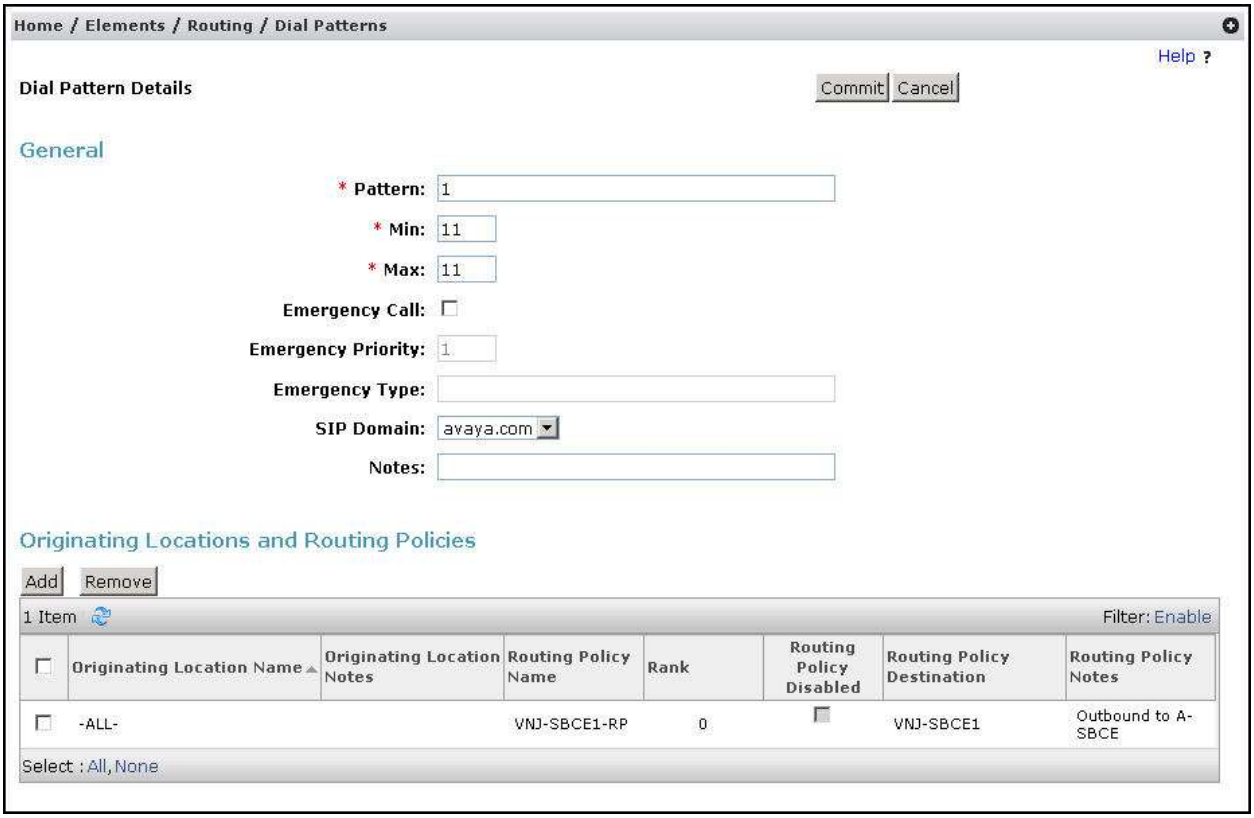
- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:**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

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

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

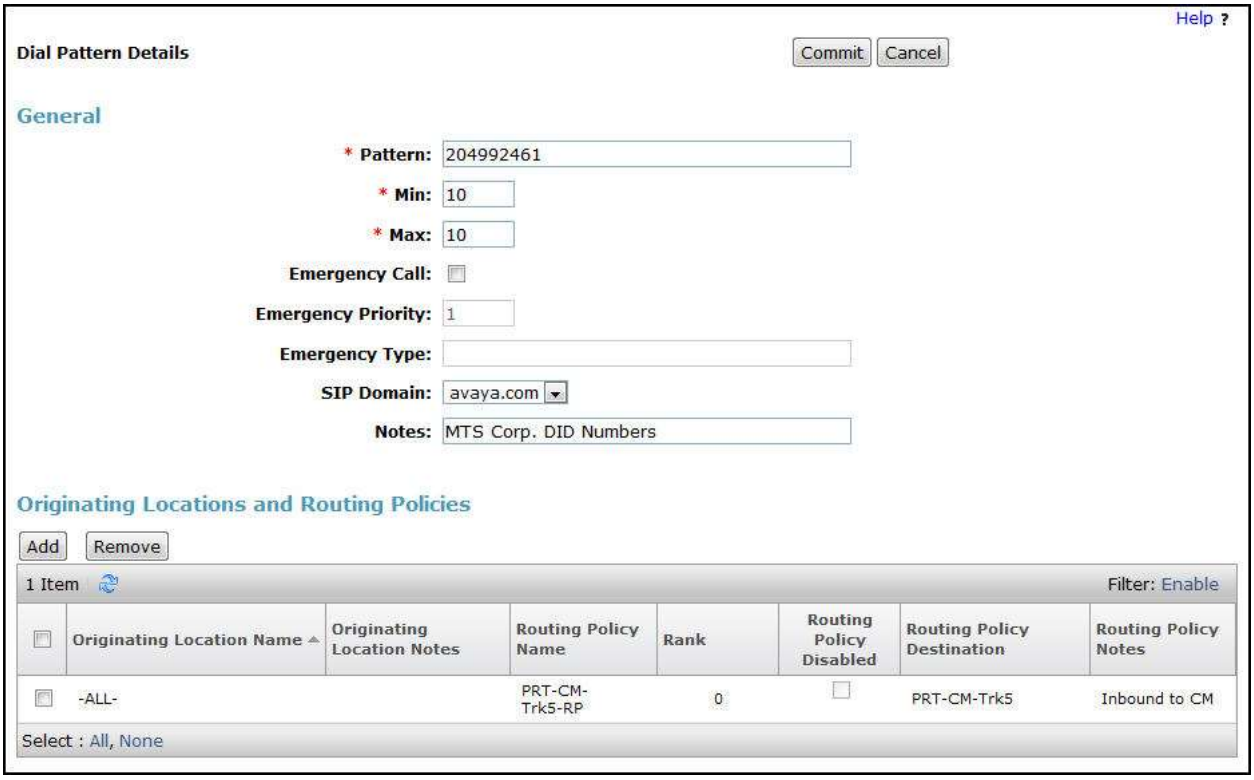
©2015 Avaya Inc. All Rights Reserved.

Two examples of the dial patterns used for the compliance test are shown below. The first example is for routing outbound calls and shows that **11**-digit numbers that begin with **1** and have a destination domain of **avaya.com** from **ALL** locations use route policy **VNJ-SBCE1-RP**.



©2015 Avaya Inc. All Rights Reserved.

The second example is for routing inbound calls and shows that **10**-digit numbers that start with **204992461** to domain **avaya.com** and originating from **ALL** locations use route policy **PRT-CM-Trk5-RP**. These are the DID numbers assigned to the enterprise from MTS. All other dial patterns used as part of the compliance test were configured in a similar manner.



©2015 Avaya Inc. All Rights Reserved.

6.9. Add/View Avaya Aura® 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, from the **Home** page, navigate to **Elements** → **Session Manager** → **Session Manager Administration** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the **Session Manager Instances** section on the right pane (not shown). If the Session Manager already exists, select the appropriate Session Manager and 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/verify the following values:

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

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

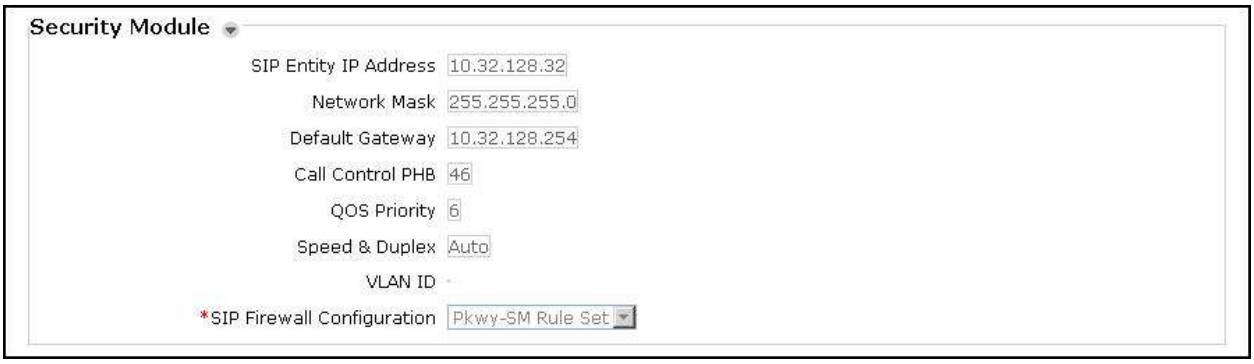


©2015 Avaya Inc. All Rights Reserved.

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name in the above screen. 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.



©2015 Avaya Inc. All Rights Reserved.

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (e.g., A1 and B1). If the management interface has not been configured on a separate subnet, then contact your Avaya representative for guidance in correcting the configuration.

On all screens described in this section, it is to be assumed that parameters are left at their default values unless specified otherwise.

7.1. Access the Management Interface

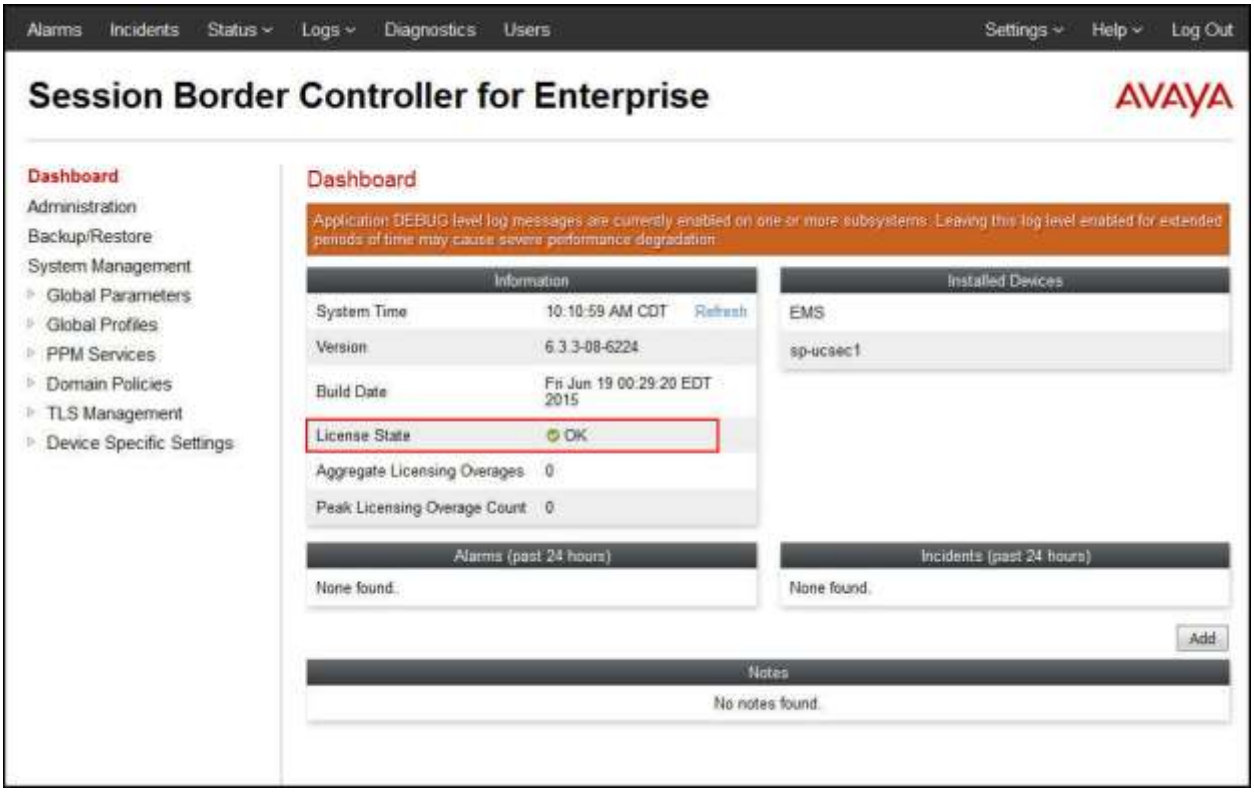
Use a web browser to access the administration web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. The Avaya SBCE login page will appear as shown below. Log in with the appropriate credentials.



©2015 Avaya Inc. All Rights Reserved.

After logging in, the Dashboard screen will appear as shown below. Verify that **License State** is **OK** as highlighted. The Avaya SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license if necessary.

All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.



©2015 Avaya Inc. All Rights Reserved.

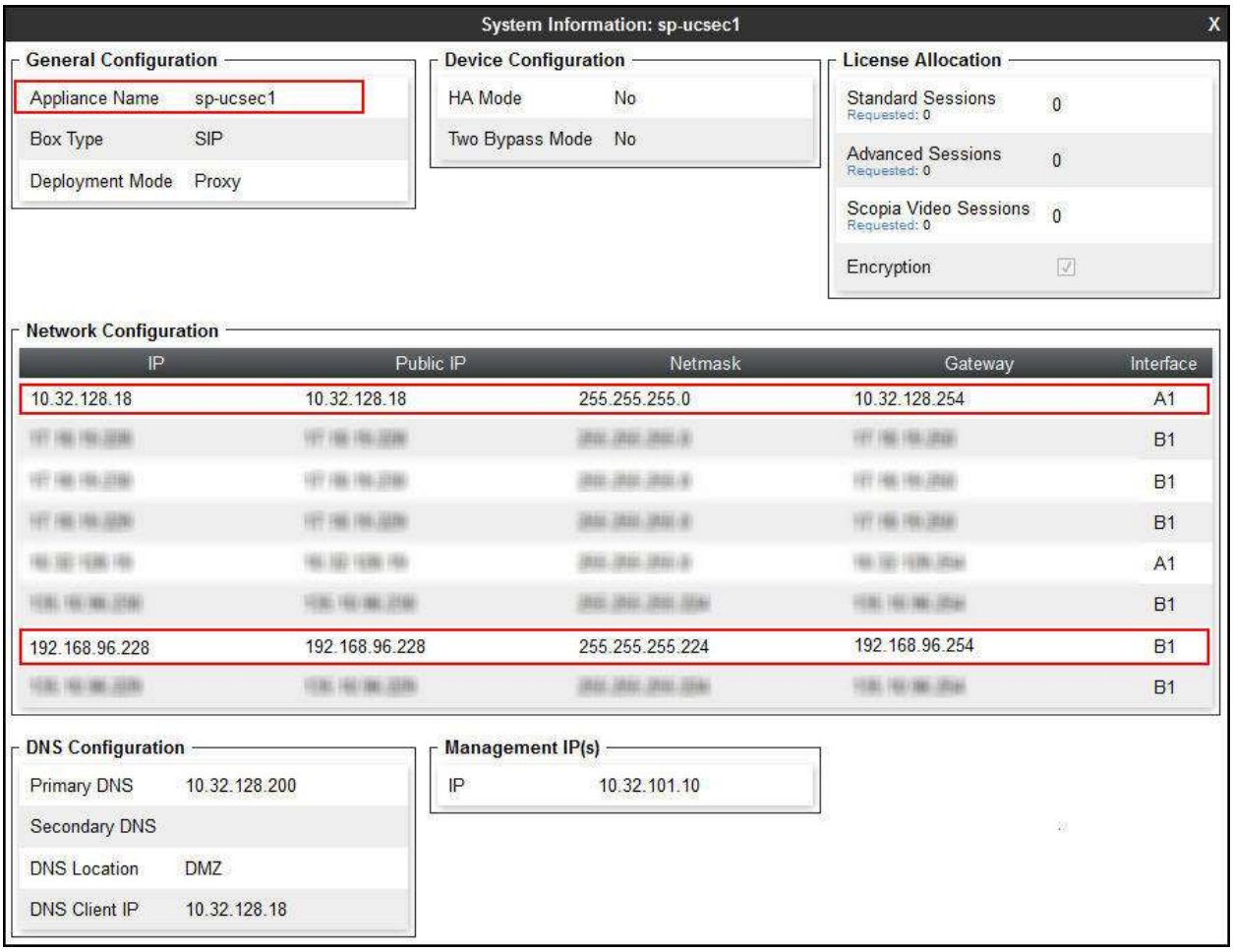
7.2. Verify Network Configuration and Enable Interfaces

To view the network information provided during installation, navigate to **System Management**. In the right pane, click **View** highlighted below.



©2015 Avaya Inc. All Rights Reserved.

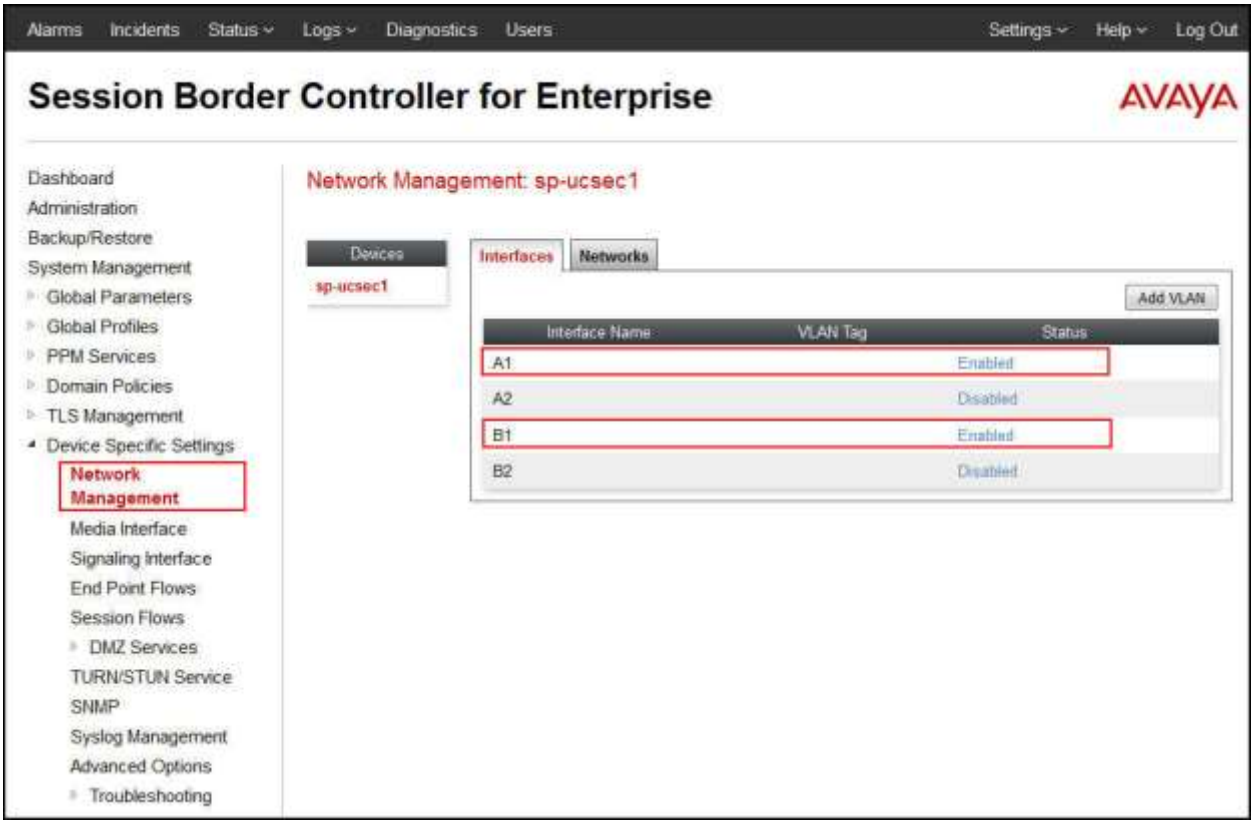
A System Information page will appear showing the information provided during installation. In the **Appliance Name** field is the name of the device (**sp-ucsec1**). This name will be referenced in other configuration screens. The two **Network Configuration** entries highlighted below are the only two IP addresses that are directly related to the SIP trunking solution described in these Application Notes. Interfaces **A1** and **B1** represent the private (or internal) and public (or external) interfaces of the Avaya SBCE. Each of these interfaces must be enabled after installation. Note that the **Management IP** is on a different subnet than either the A1 or B1 interfaces.



Entries masked in the above screen are for Remote Worker setup or for other test environments.

©2015 Avaya Inc. All Rights Reserved.

To enable the interfaces, first navigate to **Device Specific Settings → Network Management** in the left pane and select the device being managed in the center pane. In the right pane, click on the **Interfaces** tab. Verify the **Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click on **Disabled** and confirm in the pop-up confirmation window to toggle to **Enabled**.



©2015 Avaya Inc. All Rights Reserved.

7.3. Signaling Interface

A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear for configuring the name of the new interface as well as the interface parameters. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int_Sig_Intf** was created for the Avaya SBCE internal interface and signaling interface **Ext_Sig_Intf** was created for the Avaya SBCE external interface. Both completed configurations are highlighted below.

In the pop-up interface configuration window (not shown), configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the **IP Address** field, select the A1 interface and the IP address associated with the interface shown in **Section 7.2**. For the external signaling interface, select the B1 interface and the IP address associated with the interface shown in **Section 7.2**.
- In the **UDP Port**, **TCP Port** and **TLS Port** fields, enter the port the Avaya SBCE will listen on for each transport protocol. For the internal interface, the Avaya SBCE was configured to listen for TCP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP or TCP on port 5060. Since the MTS SIP Trunking Services uses UDP, it would have been sufficient to simply configure the Avaya SBCE for UDP.



©2015 Avaya Inc. All Rights Reserved.

7.4. Media Interface

A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings → Media Interface** in the left pane. In the center pane, select the Avaya SBCE device to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear for configuring the name of the new interface as well as the interface parameters. Once complete, the settings are shown in the far right pane.

For the compliance test, media interface **Int_Media_Intf** was created for the Avaya SBCE internal interface and media interface **Ext_Media_Intf** was created for the Avaya SBCE external interface. Both completed configurations are highlighted below.

In the pop-up interface configuration window (not shown), configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the **IP Address** field, select the A1 interface and the IP address associated with the interface shown in **Section 7.2**. For the external media interface, select the B1 interface and the IP address associated with the interface shown in **Section 7.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the far-end. For the compliance test, the default port range was used for both interfaces.



©2015 Avaya Inc. All Rights Reserved.

7.5. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create separate server interworking profiles for Session Manager and the service provider SIP server. These profiles will be applied to the appropriate server in **Section 7.7.1** and **7.7.2**.

To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

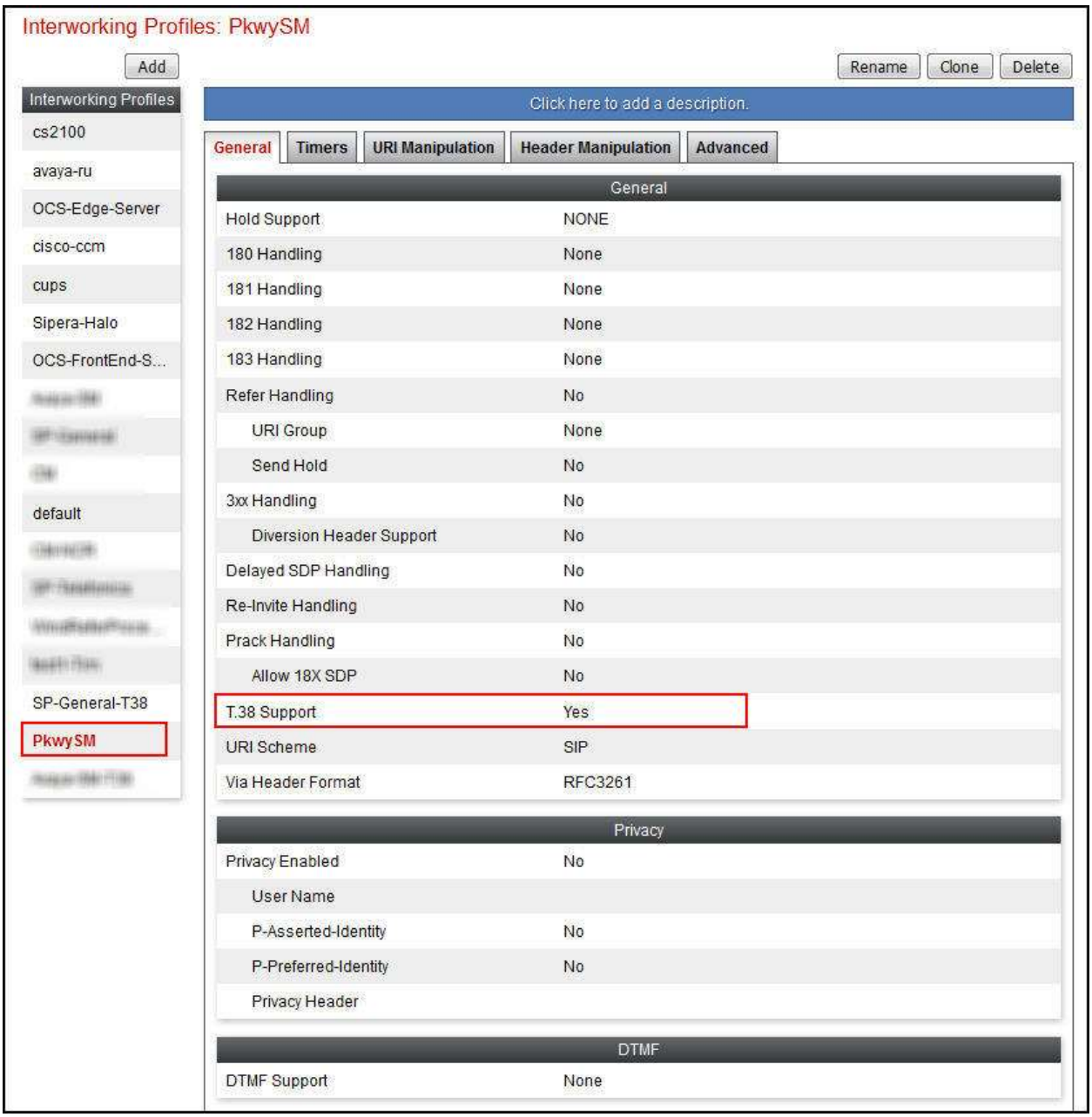
The screen below shows the GUI elements described above before the server interworking profiles were added for the compliance test.



©2015 Avaya Inc. All Rights Reserved.

7.5.1. Server Interworking – Session Manager

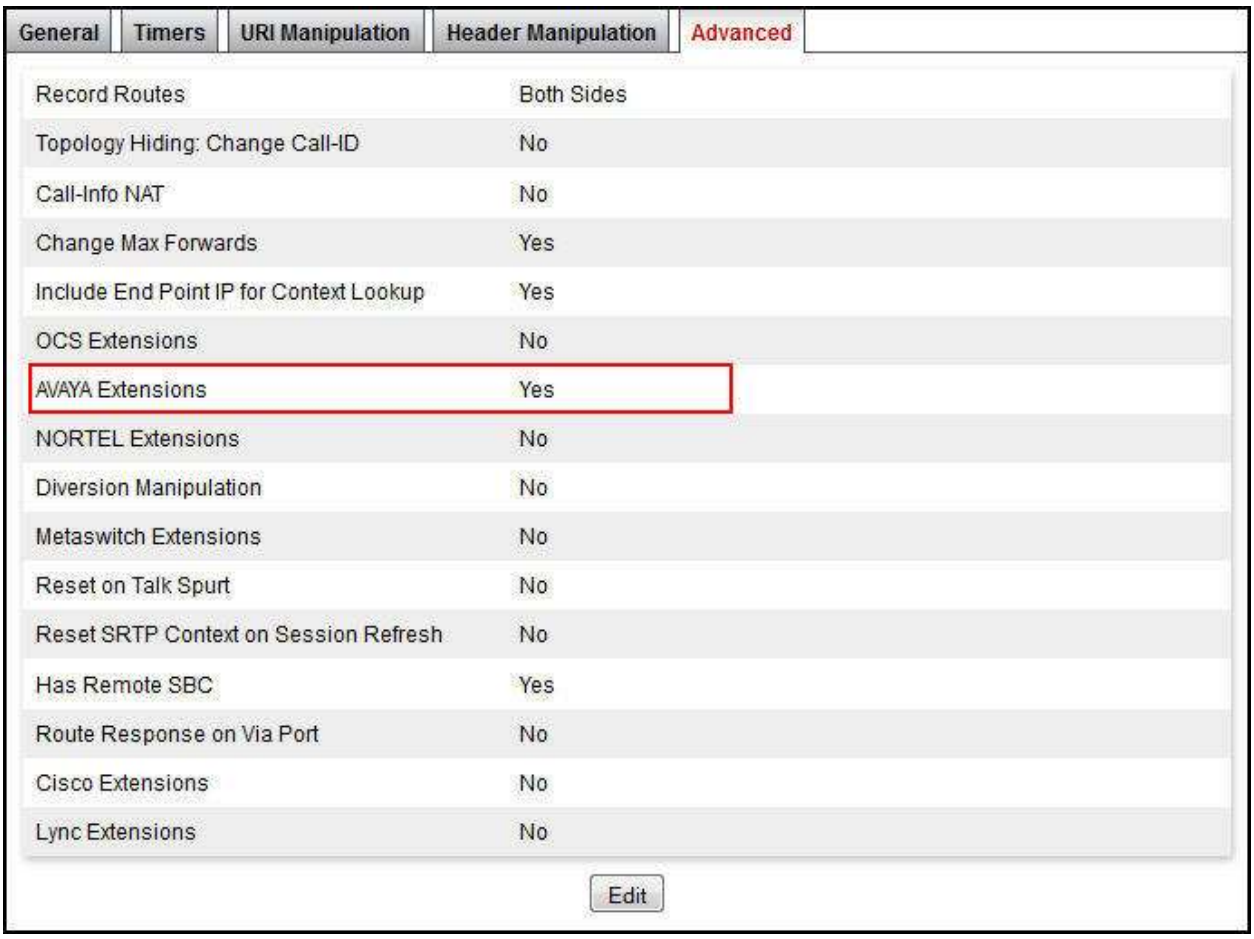
For the compliance test, server interworking profile **PkwySM** was created for Session Manager by cloning the existing profile **avaya-ru**. The **General** tab parameters are shown below. Note that **T.38 Support** is set to **Yes**.



The **Timers**, **URI Manipulation** and **Header Manipulation** tabs have no entries.

©2015 Avaya Inc. All Rights Reserved.

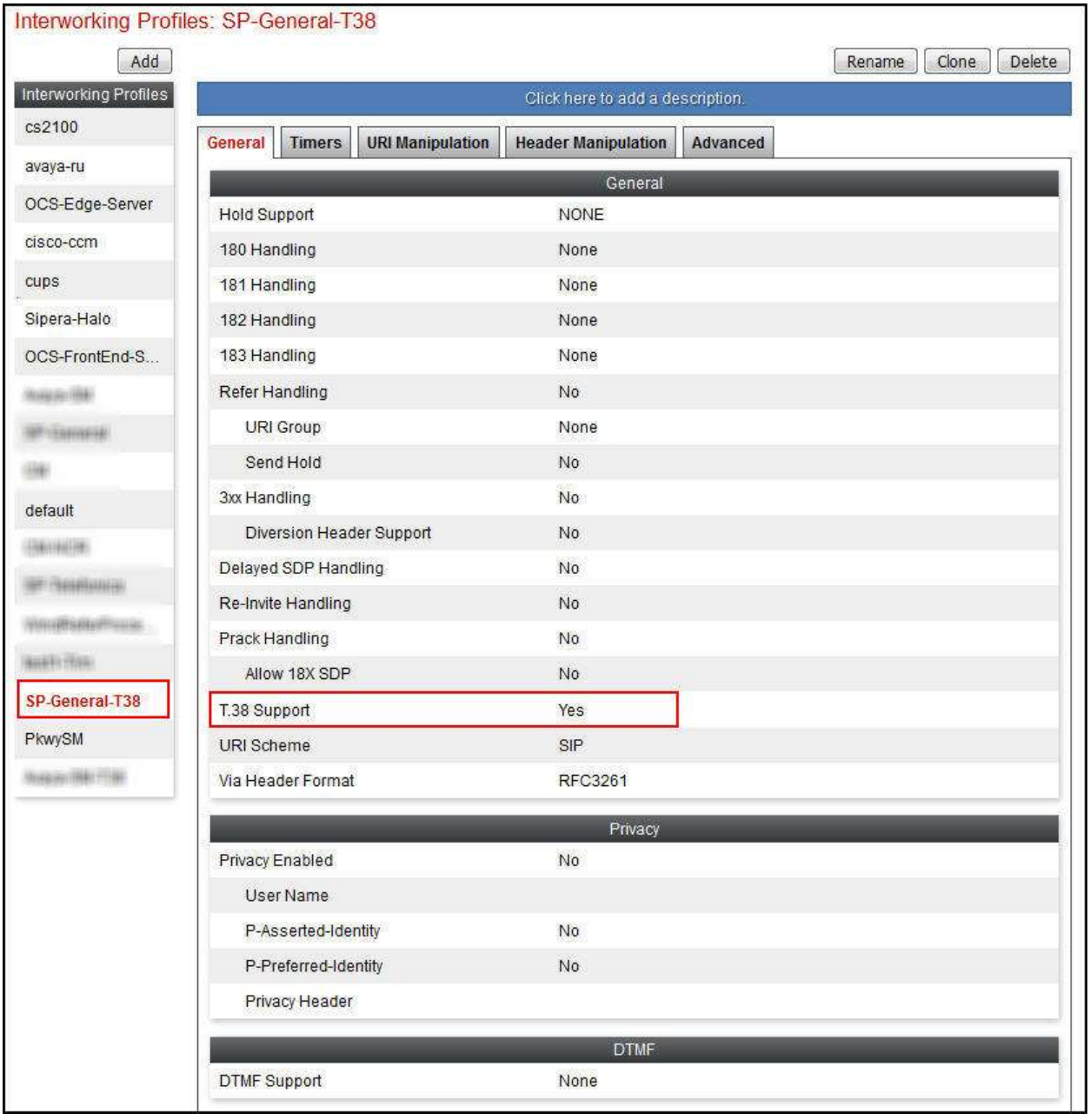
The **Advanced** tab parameters are shown below. Note that **AVAYA Extensions** is set to **Yes**.



©2015 Avaya Inc. All Rights Reserved.

7.5.2. Server Interworking – MTS

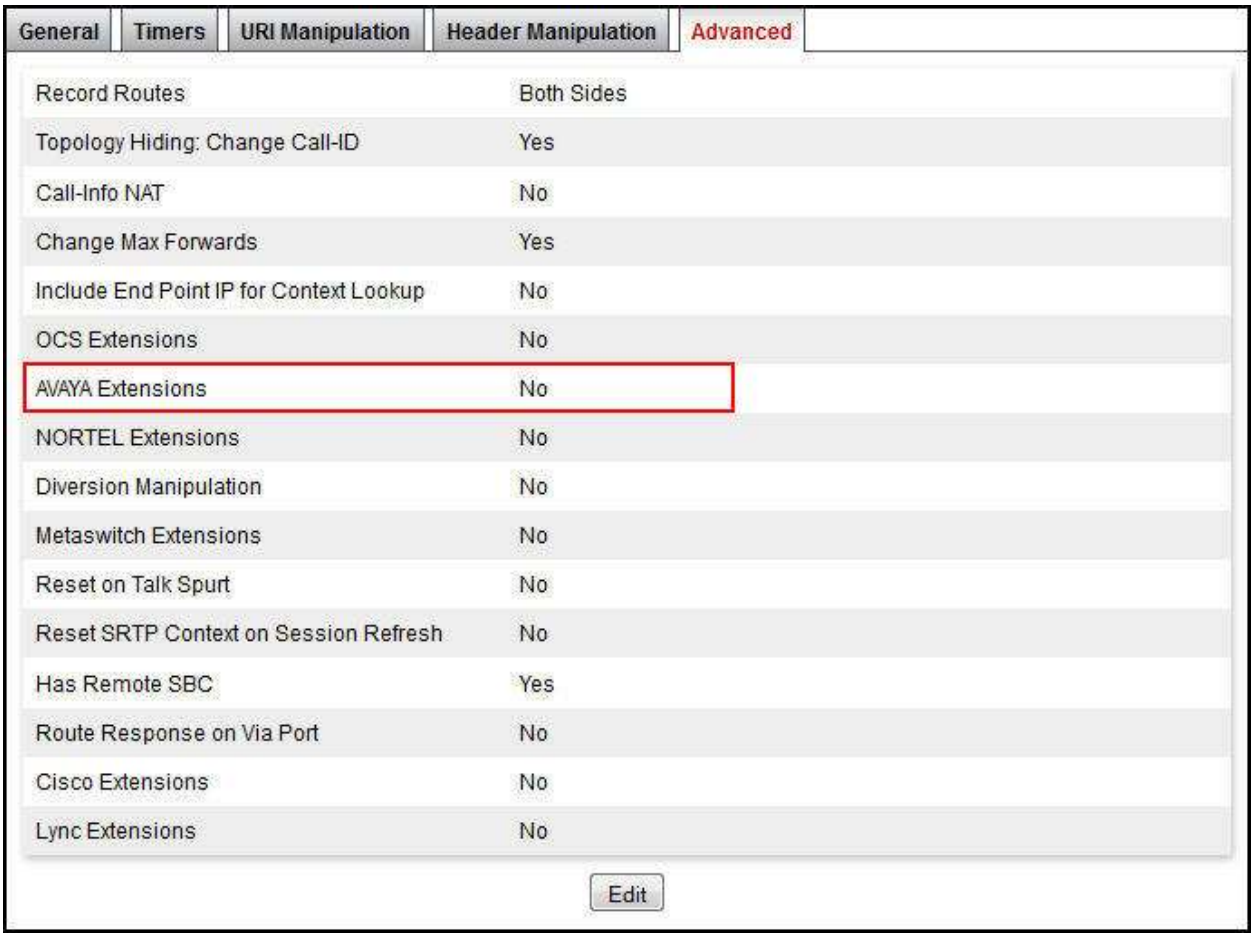
For the compliance test, server interworking profile **SP-General-T38** was created for the MTS SIP server. The **General** tab parameters are shown below. Note the setting for **T.38 Support**.



The **Timers**, **URI Manipulation**, **Header Manipulation** tabs have no entries.

©2015 Avaya Inc. All Rights Reserved.

The **Advanced** tab parameters are shown below. Note that **AVAYA Extensions** is set to **No**.



7.6. Signaling Manipulation

Signaling manipulation scripts provides for the manipulation of SIP messages which cannot be achieved by other configuration within the Avaya SBCE.

The compliance test used a signaling manipulation script to modify some header contents in the OPTIONS messages sent by MTS. These header modifications were necessary for Session Manager to accept the MTS-sourced OPTIONS and send the proper response back.

To create a signaling manipulation script, navigate to **Global Profiles → Signaling Manipulation** (see 2nd screen below). Click on **Add** in the center pane. In the pop-up **Signaling Manipulation Editor** window, type in a script title and enter the script statements/commands.

Save the script by clicking on **Save**.

©2015 Avaya Inc. All Rights Reserved.

For the compliance test, a script named **ChgRUI-OPTIONS** was created as shown below.



The screen below shows the saved script listed on the Avaya SBCE.



©2015 Avaya Inc. All Rights Reserved.

The **ChgRUI-OPTIONS** script is tied to the **Pkwy-SM** server in server configuration (**Section 7.7.1**).

Note that use of Signaling Manipulation scripts demands higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should be used with care and only in cases where the use of Signaling Rules (**Section 7.10**) does not meet the desired result. Refer to **[17]** for information on the Avaya SBCE scripting language.

7.7. Server Configuration

A server configuration profile defines the attributes of the physical server. Create a server configuration profile for Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Server Configuration** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before the server profiles were added for the compliance test.



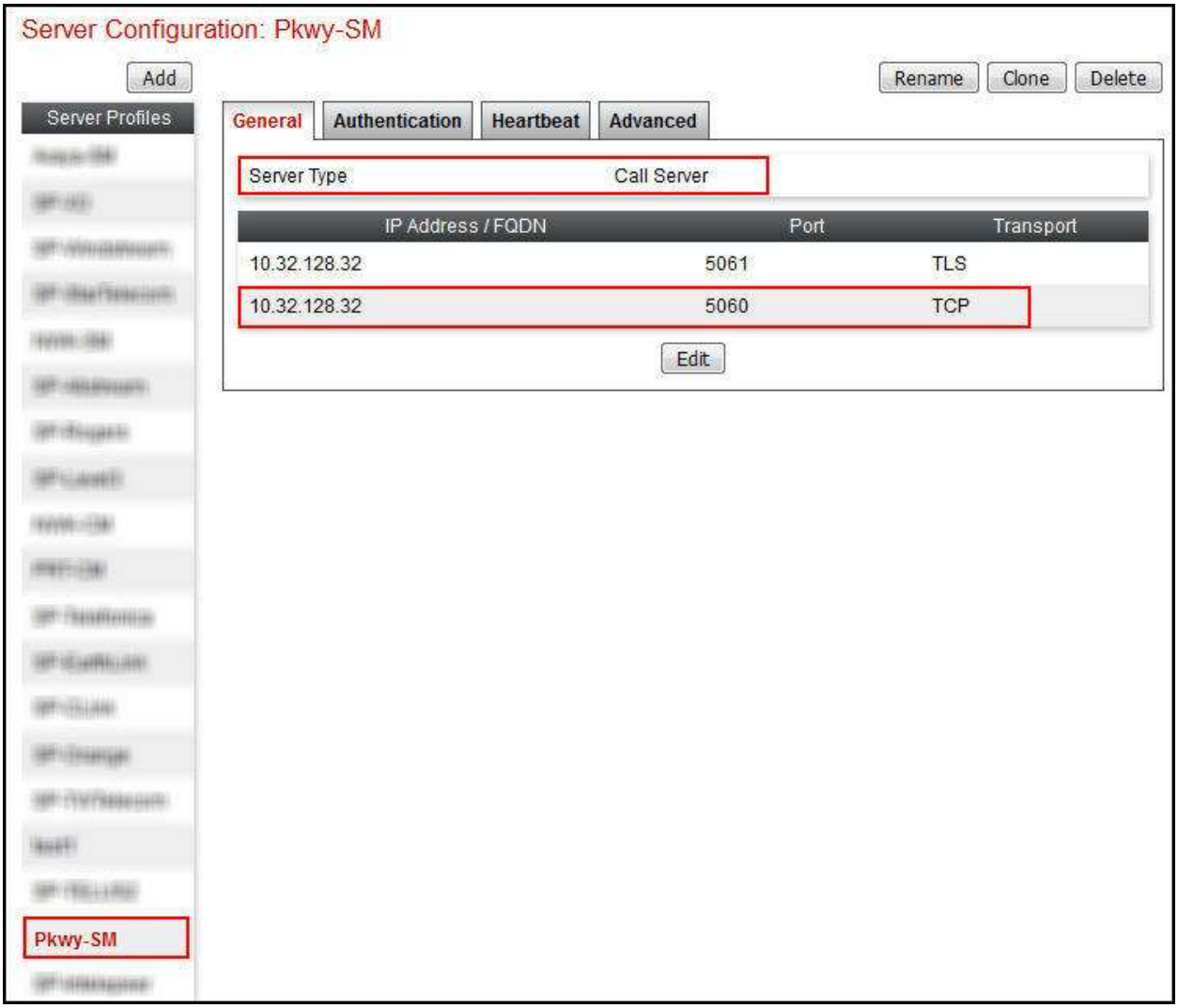
©2015 Avaya Inc. All Rights Reserved.

7.7.1. Server Configuration – Session Manager

For the compliance test, server configuration profile **Pkwy-SM** was created for Session Manager. When creating the profile, configure the **General** tab parameters as follows:

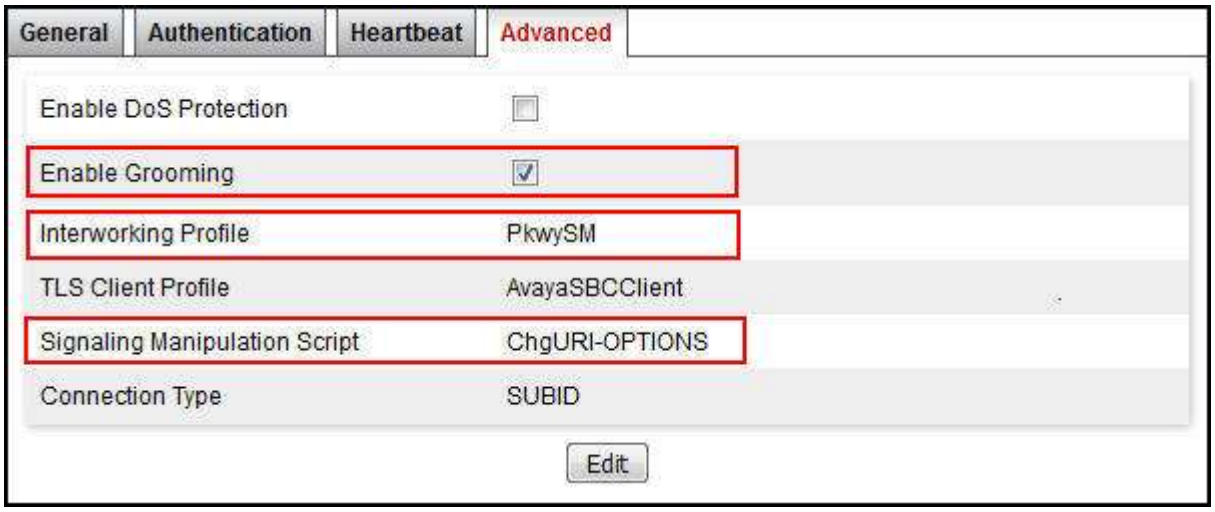
- Set **Server Type** to **Call Server.**
- Set **IP Addresses / FQDNs** to the IP address of the Session Manager signaling interface.
- Set **Transports** to **TCP**, the transport protocol used for SIP signaling between Session Manager and the Avaya SBCE.
- Set the **Port** to the port Session Manager will listen on for SIP requests from the Avaya SBCE.

Note that TLS was also set in the screen below, which is configured for Remote Worker setup.



©2015 Avaya Inc. All Rights Reserved.

On the **Advanced** tab, check **Enable Grooming**, set **Interworking Profile** to the interworking profile for Session Manager defined in **Section 7.5.1**, and select the **Signaling Manipulation Script** created in **Section 7.6**.

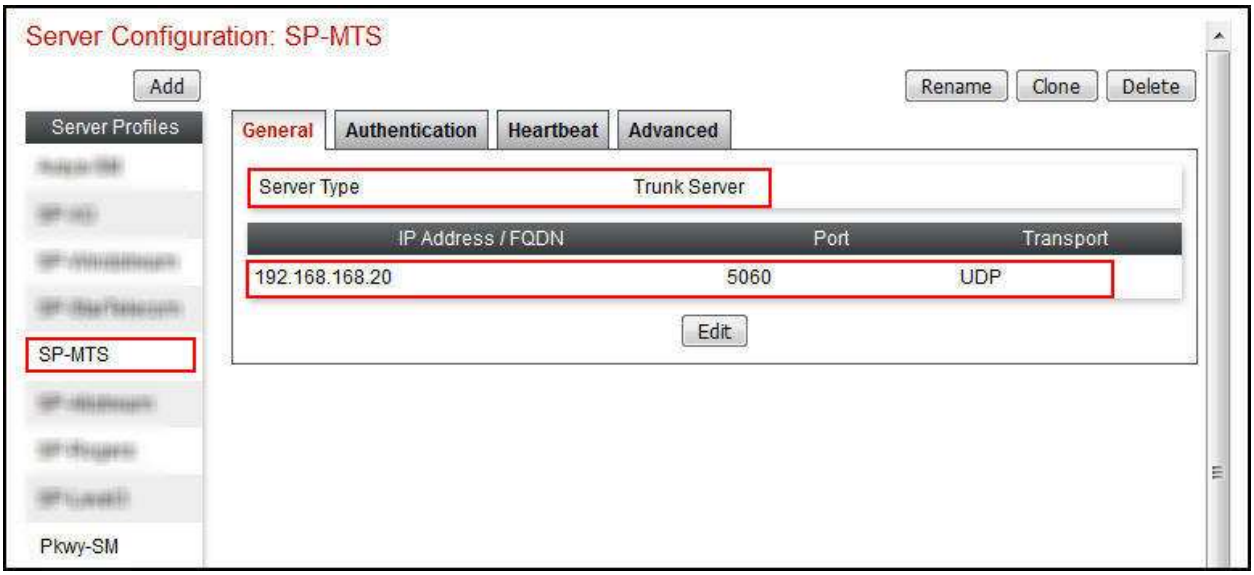


©2015 Avaya Inc. All Rights Reserved.

7.7.2. Server Configuration – MTS

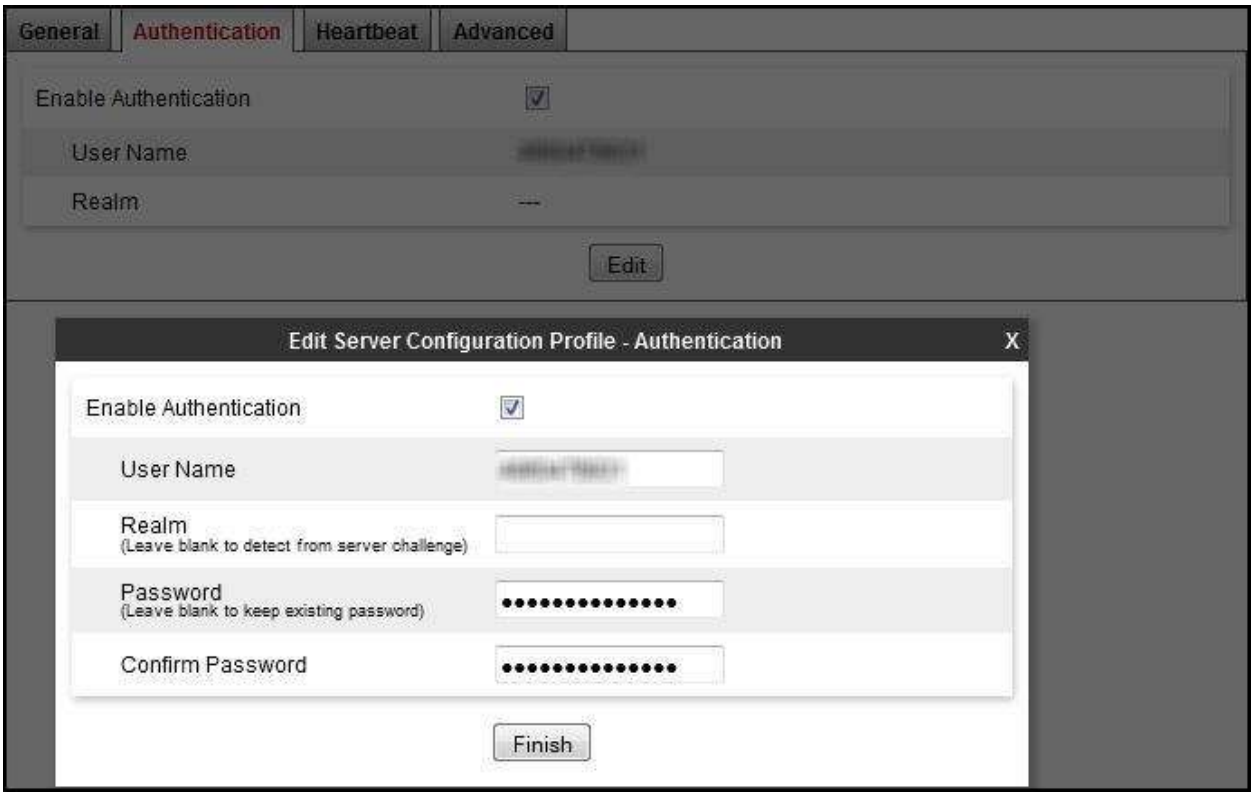
For the compliance test, server configuration profile **SP-MTS** was created for MTS. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Trunk Server.**
- Set **IP Addresses / FQDNs** to the IP address of the MTS network access interface as shown in **Figure 1** in **Section 3**.
- Set **Transports** to the transport protocol used for SIP signaling between MTS and the Avaya SBCE. In the compliance test, **UDP** was tested.
- Set the **Port** to the standard SIP port of 5060. This is the port the remote end will listen on for SIP requests from the Avaya SBCE.

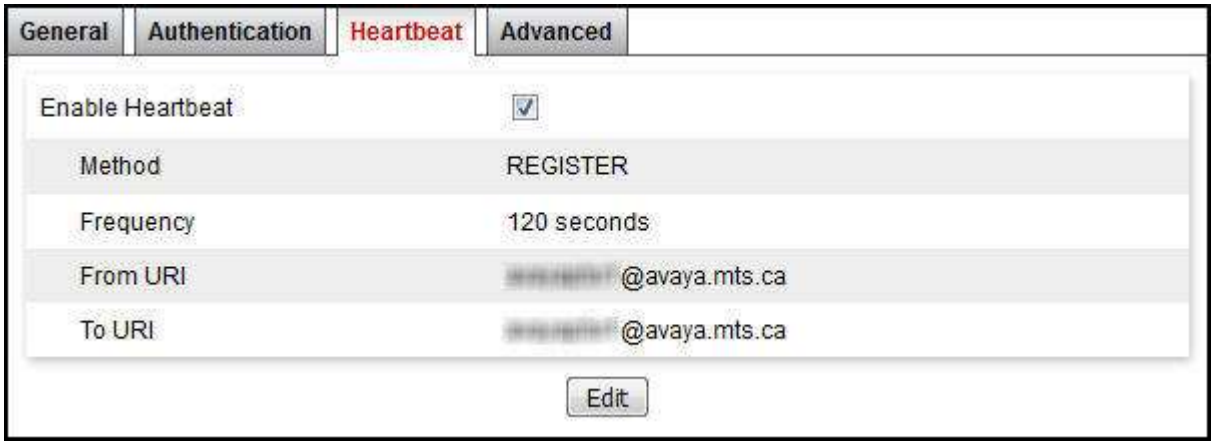


©2015 Avaya Inc. All Rights Reserved.

In the **Authentication** tab, check the **Enable Authentication** option box, and enter the SIP credentials (provided by MTS) for **User Name** and **Password**.

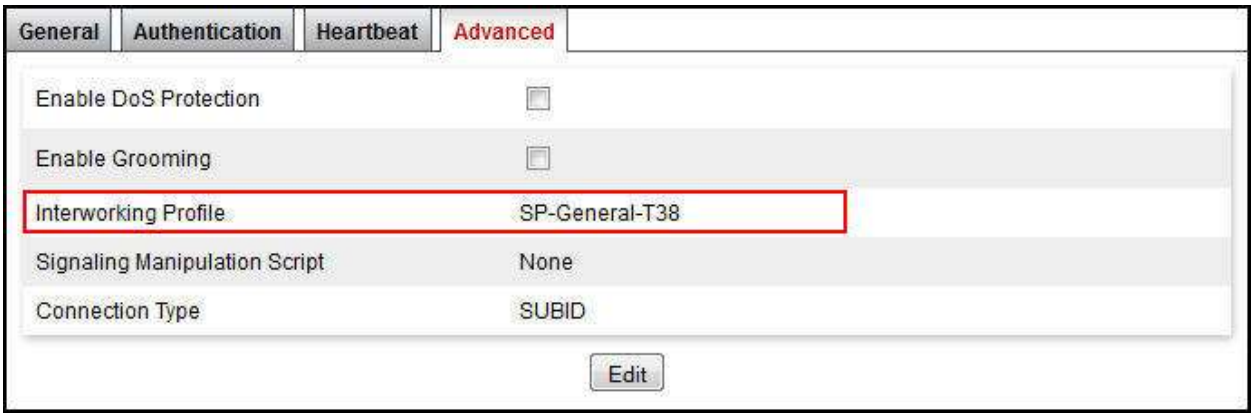


In the **Heartbeat** tab, check the **Enable Heartbeat** option box. Select **REGISTER** for **Method**, and enter the desired **Frequency** setting for the time interval at which the REGISTER message will be issued from the enterprise site. Finally enter the **From URI** and **To URI** settings: the user part of the URIs is the user name credential provided by the service provider for SIP trunk registration; the domain in the URIs is the domain for the MTS SIP Trunking Service as provided by MTS.



©2015 Avaya Inc. All Rights Reserved.

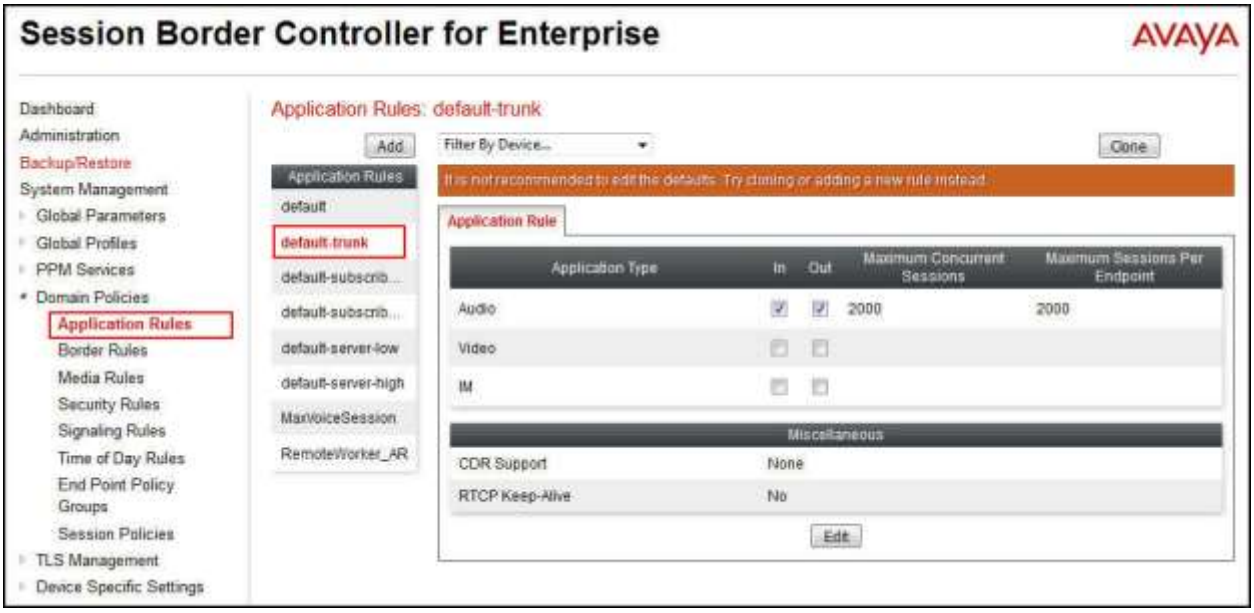
In the **Advanced** tab, set the **Interworking Profile** field to the interworking profile for MTS defined in **Section 7.5.2**.



7.8. Application Rules

An application rule defines the allowable SIP applications and associated parameters. An application rule is one component of the larger endpoint policy group defined in **Section 7.11**. For the compliance test, the predefined **default-trunk** application rule (shown below) was used for both Session Manager and the MTS SIP server.

To view an existing rule, navigate to **Domain Policies → Application Rules** in the left pane. In the center pane, select the rule (e.g., **default-trunk**) to be viewed.



©2015 Avaya Inc. All Rights Reserved.

7.9. Media Rules

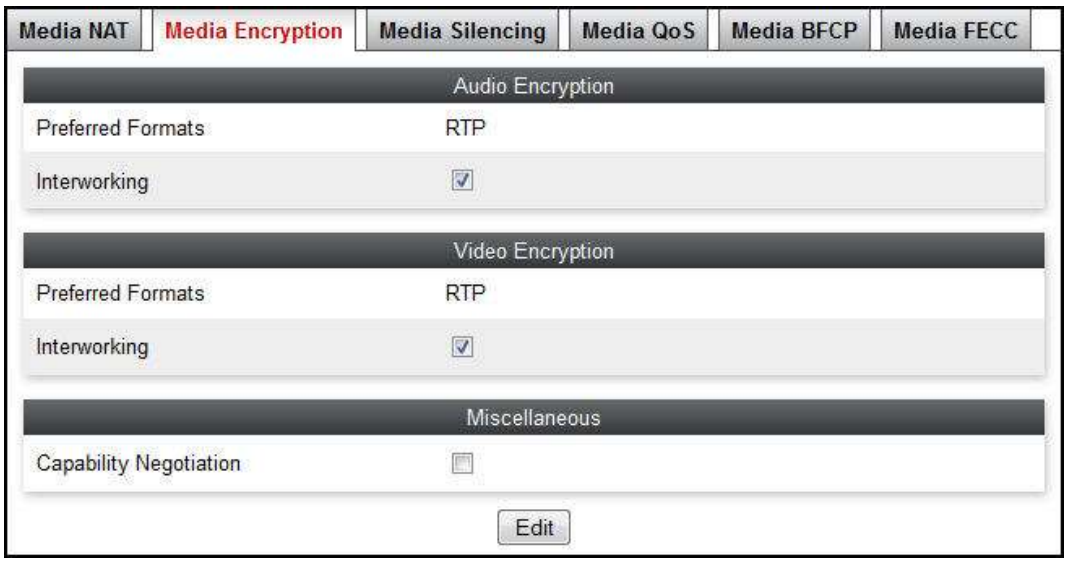
A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 7.11**. For the compliance test, the predefined **default-low-med** media rule (shown below) was used for both Session Manager and the MTS SIP server.

To view an existing rule, navigate to **Domain Policies → Media Rules** in the left pane. In the center pane, select the rule (e.g., **default-low-med**) to be viewed. Each of the tabs of the **default-low-med** media rule containing data is shown below.

The **Media NAT** tab has no entries.



The **Media Encryption** tab indicates that no encryption was used.



©2015 Avaya Inc. All Rights Reserved.

The **Media Silencing** tab shows **Media Silencing** was disabled.



The **Media QoS** tab is shown below.



The **Media BFCP** tab is shown below.



The **Media FECC** tab is shown below.



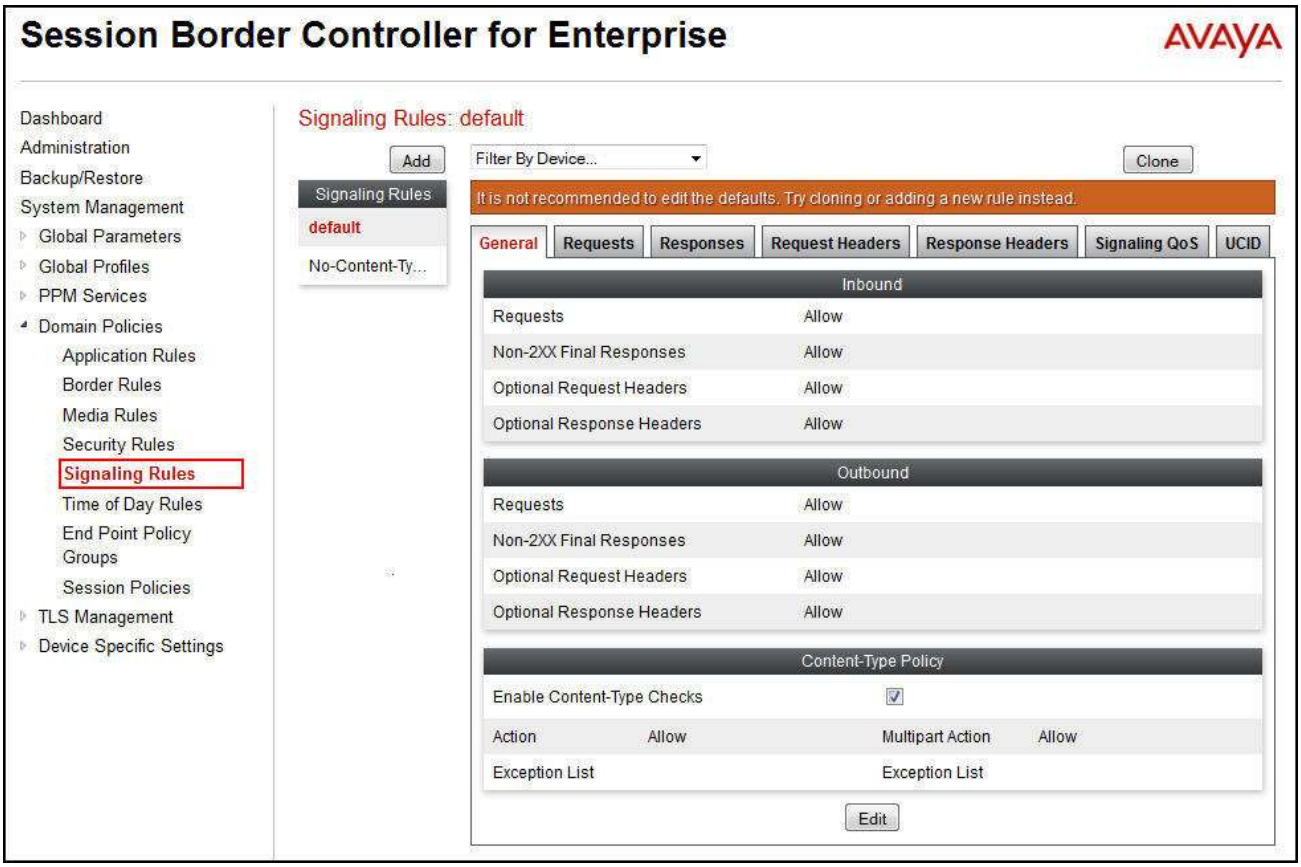
©2015 Avaya Inc. All Rights Reserved.

7.10. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 7.11**. A specific signaling rule was created for Session Manager. The MTS SIP server used the **default** rule.

To create a new rule, navigate to **Domain Policies → Signaling Rules** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by a series of pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above.



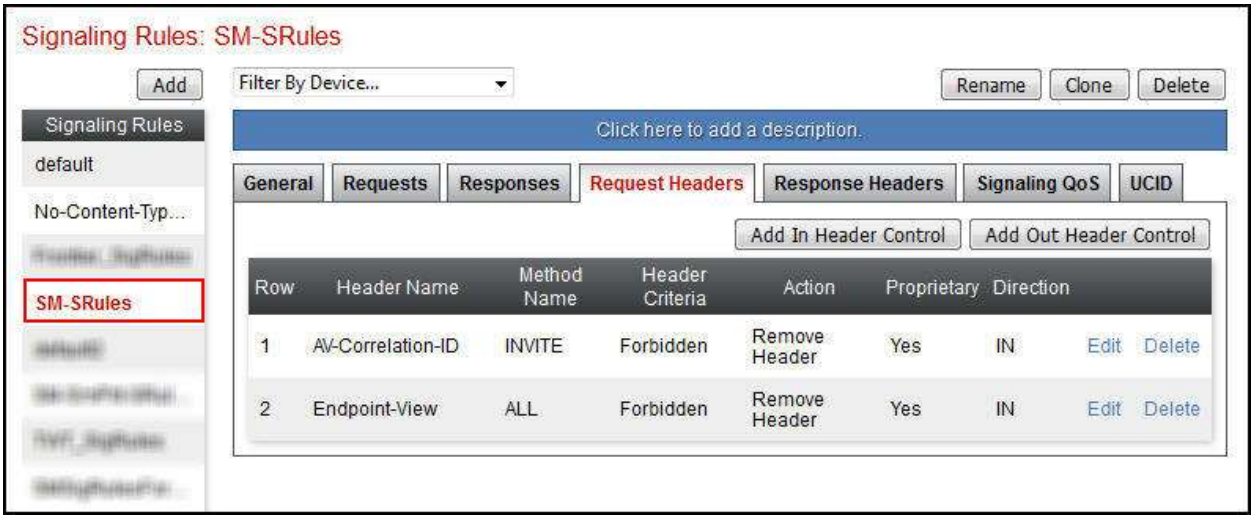
©2015 Avaya Inc. All Rights Reserved.

7.10.1. Signaling Rules – Session Manager

For the compliance test, signaling rule **SM-SRules** was created for Session Manager to prevent proprietary headers in the SIP messages sent from the Session Manager from being propagated to MTS. These headers may contain internal addresses or other information about the internal network.

Click **Add** to create the rule. Keep the default values on all tabs. After the signaling rule is created, select the **Request Headers** tab to create the manipulations performed on request messages such as INVITE. An entry is created by clicking the **Add In Header Control** or **Add Out Header Control** button depending on the direction (relative to the Avaya SBCE) of the message to be modified. Entries were created to perform the following actions:

1. Removes the **AV-Correlation-ID** header from **INVITE** messages in the **IN** direction (Session Manager to Avaya SBCE).
2. Removes the **Endpoint-View** header from **ALL** messages in the **IN** direction.



©2015 Avaya Inc. All Rights Reserved.

Similarly, manipulations can be performed on SIP response messages. These can be created by selecting the **Response Headers** tab as shown below. Entries were created in the same manner as was done on the **Request Headers** tab. The entries shown below perform the following actions:

1. Removes the **Endpoint-View** header from any **2XX** response to **ALL** messages in the **IN** direction (Session Manager to Avaya SBCE).
2. Removes the **Endpoint-View** header from any **1XX** response to **INVITE** messages in the **IN** direction.



The **Requests**, **Responses**, and **UCID** tabs have no entries.

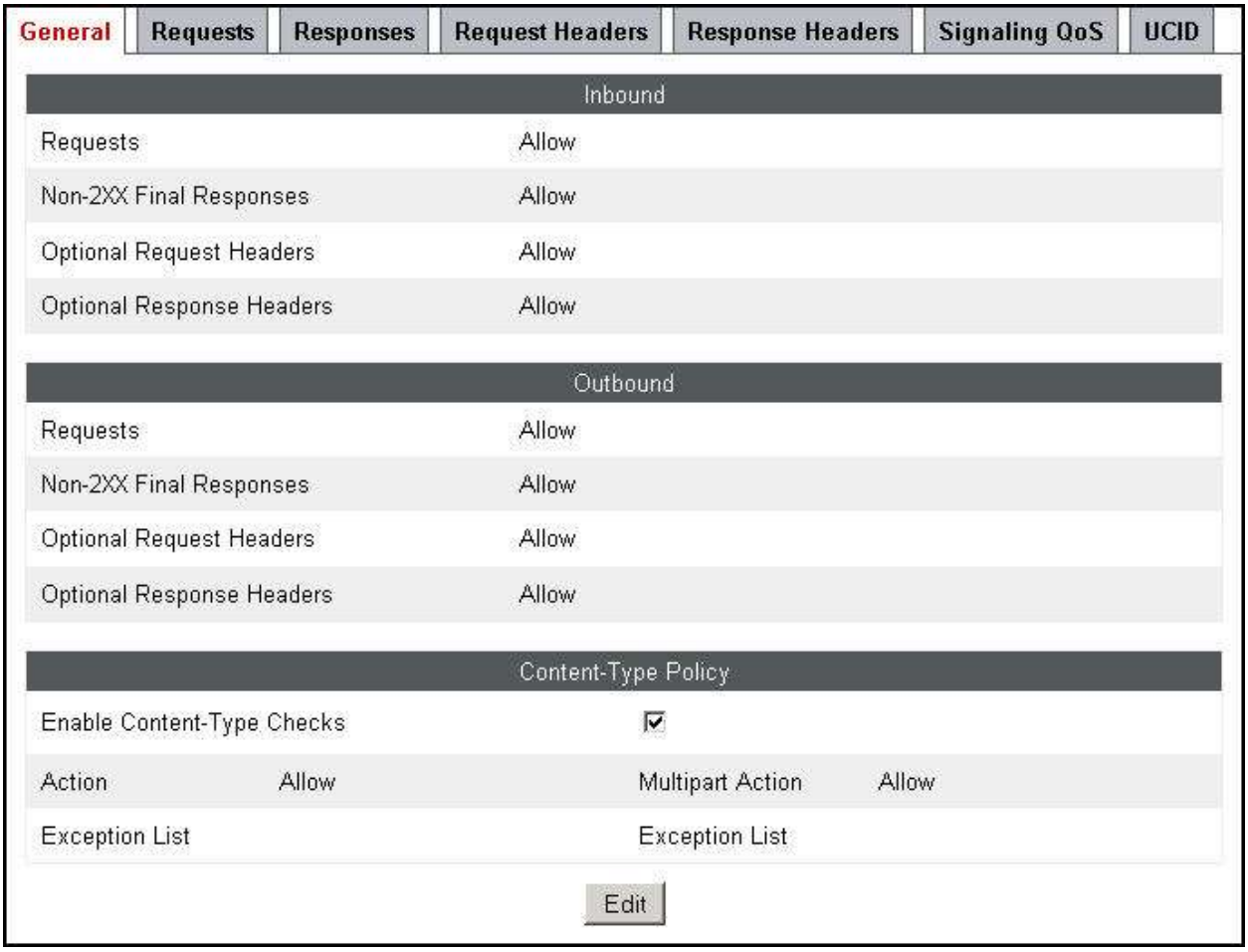
The **Signaling QoS** tab is shown below.



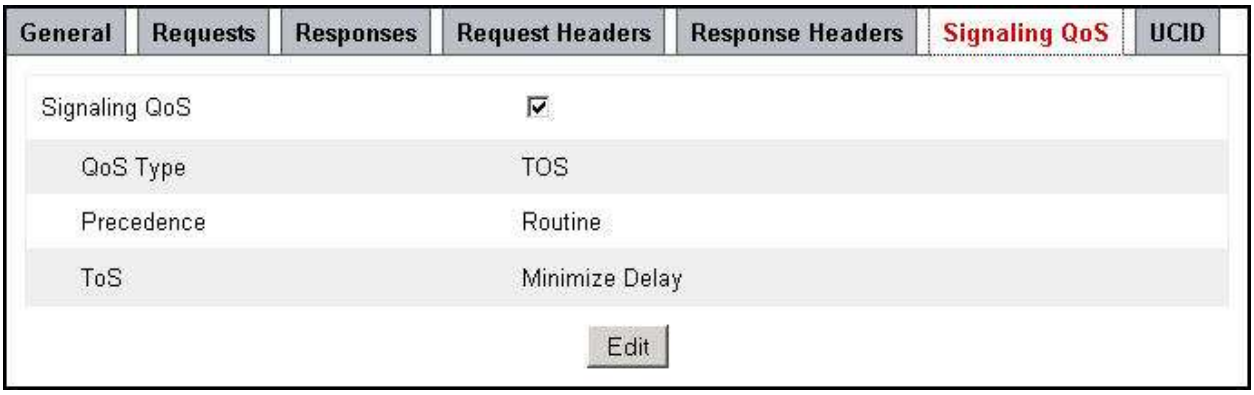
©2015 Avaya Inc. All Rights Reserved.

7.10.2. Signaling Rules – MTS

The predefined **default** signaling rule (shown below) was used for the MTS SIP server. The **General** tab settings are shown below.



The **Requests**, **Responses**, **Request Headers**, **Response Headers** and **UCID** tabs have no entries. The **Signaling QoS** tab is shown below.



©2015 Avaya Inc. All Rights Reserved.

7.11. Endpoint Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, an endpoint policy group must be created for Session Manager and the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.14**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by a **Policy Group** window in which the group parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before specific endpoint policy groups were added for the compliance test.



©2015 Avaya Inc. All Rights Reserved.

7.11.1. Endpoint Policy Group – Session Manager

For the compliance test, the endpoint policy group **SM** was created for Session Manager as shown below. For **Application**, enter the application rule described in **Section 7.8**. For **Media**, enter the media rule described in **Section 7.**9. For **Signaling**, enter the signaling rule created in **Section 7.10.1**.



©2015 Avaya Inc. All Rights Reserved.

7.11.2. Endpoint Policy Group – MTS

For the compliance test, the endpoint policy group **General-SP** was created for the MTS SIP server as shown below. For **Application**, enter the application rule described in **Section 7.8**. The details of the default settings for **Media** and **Signaling** are showed in **Section 7.9** and **Section 7.10.2** respectively.



©2015 Avaya Inc. All Rights Reserved.

7.12. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 7.14**. Create separate routing profiles for Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a **Routing Profile** window in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane.

The screen below shows the GUI elements described above before specific routing profiles were added for the compliance test.

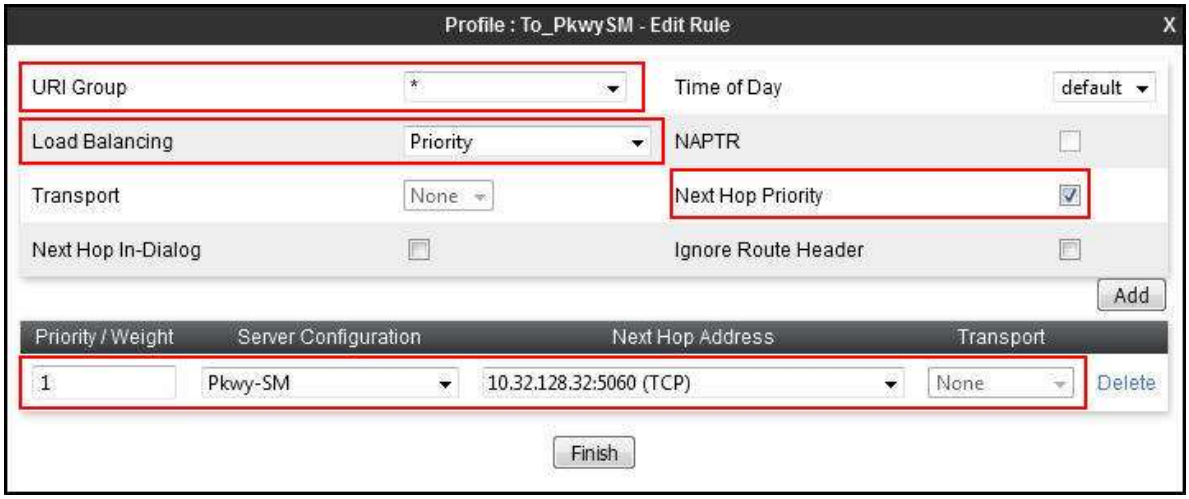


©2015 Avaya Inc. All Rights Reserved.

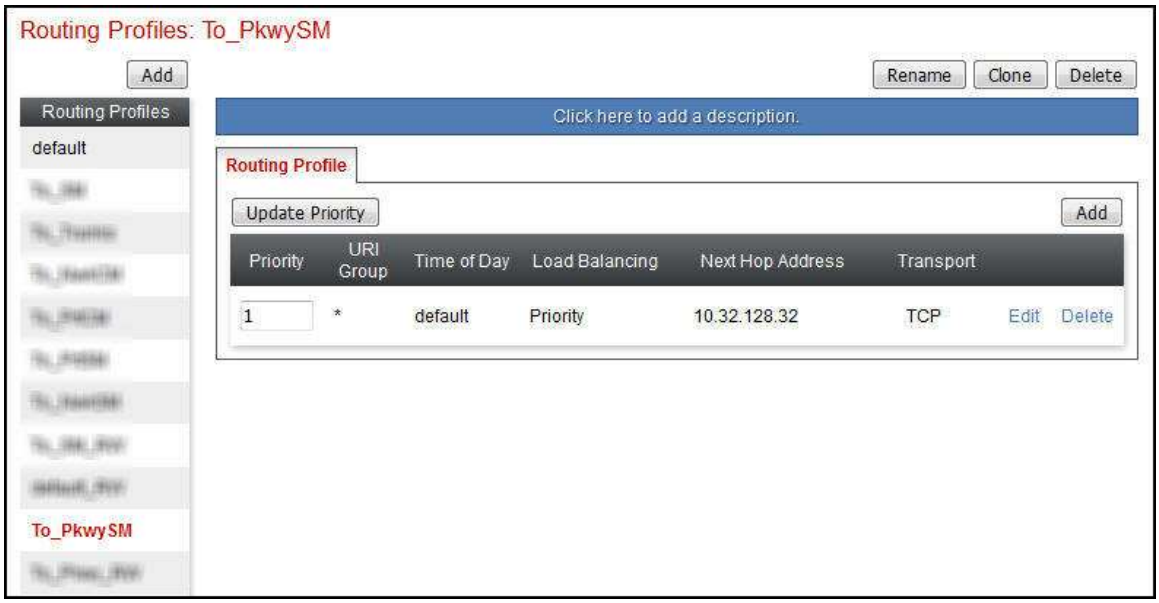
7.12.1. Routing – Session Manager

For the compliance test, routing profile **To-PkwySM** was created for Session Manager. When creating the profile, configure the parameters as follows:

- Set **URI Group** to the wild card ***** to match on any URI.
- Select **Priority** for **Load Balancing**.
- Enable **Next Hop Priority**.
- When adding an entry for routing destination (Next Hop Address)
  - Enter **1** for **Priority/Weight**.
  - For **Server Configuration**, select the Server for Session Manager as configured in **Section 7.7.1**. The selection will automatically populate **Next Hop Address**.



The following screen shows the routing profile for Session Manager when configured.

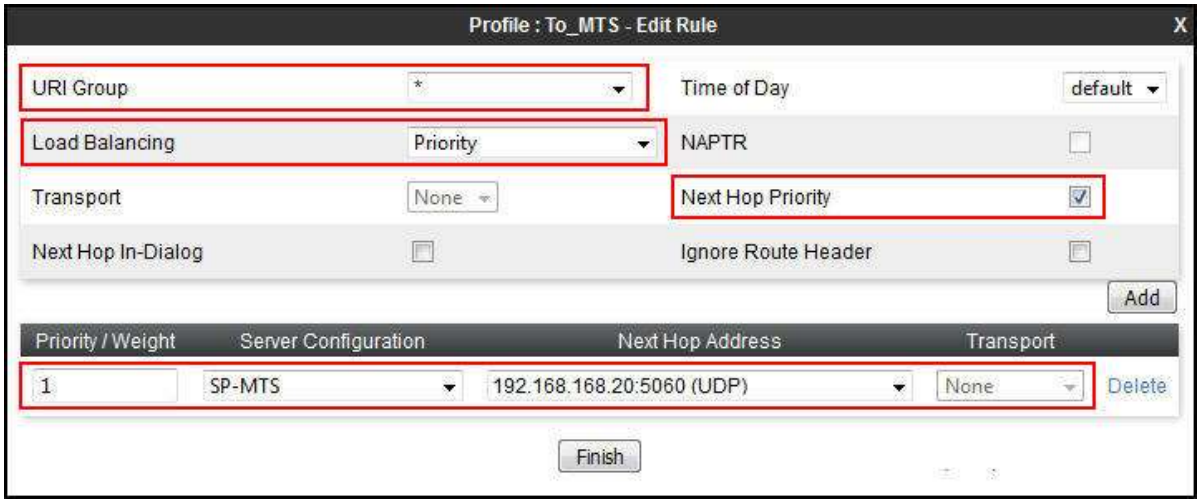


©2015 Avaya Inc. All Rights Reserved.

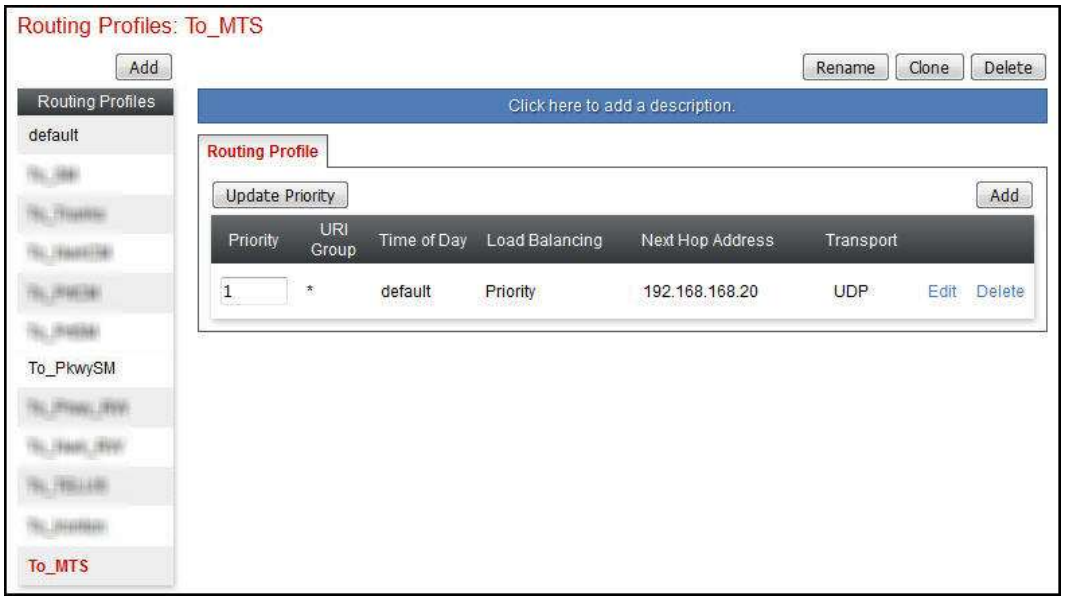
7.12.2. Routing – MTS

For the compliance test, routing profile **To_MTS** was created for MTS. When creating the profile, configure the parameters as follows:

- Set **URI Group** to the wild card ***** to match on any URI.
- Select **Priority** for **Load Balancing**.
- Enable **Next Hop Priority**.
- When adding an entry for routing destination (Next Hop Address)
  - Enter **1** for **Priority/Weight**.
  - For **Server Configuration**, select the Server for MTS as configured in **Section 7.7.2**. The selection will automatically populate **Next Hop Address**



The following screen shows the routing profile for MTS when configured.



©2015 Avaya Inc. All Rights Reserved.

7.13. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 7.14**.

To create a new profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a **Topology Hiding Profile** window in which the profile parameters can be configured. Additional headers can be added in this window. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile (e.g., **default**), select the profile from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before specific topology hiding profiles were added for the compliance test.



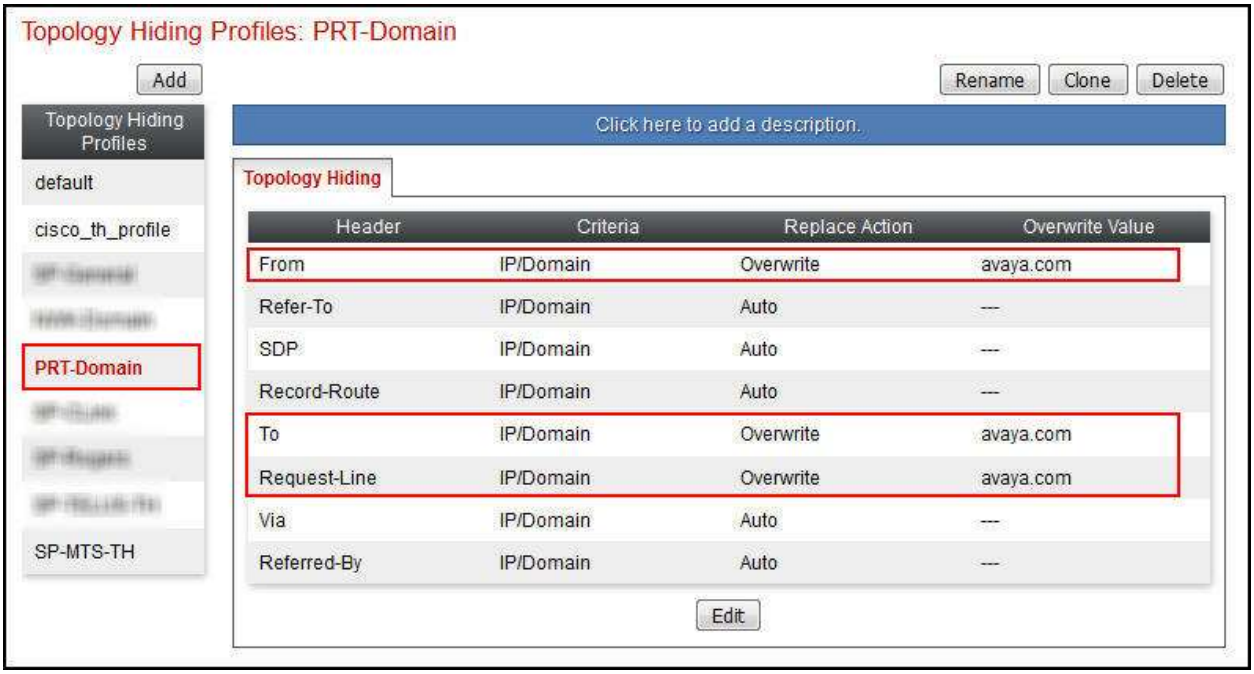
©2015 Avaya Inc. All Rights Reserved.

7.13.1. Topology Hiding – Session Manager

For the compliance test, the topology hiding profile **PRT-Domain** was created for Session Manager. This profile will be applied to traffic from the Avaya SBCE to Session Manager. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line**, **From** and **To** which should be set to **Overwrite**.
- For those headers to be overwritten, the **Overwrite Value** is set to the enterprise domain (**avaya.com**).

The following screen shows the configured topology hiding profile for Session Manager:



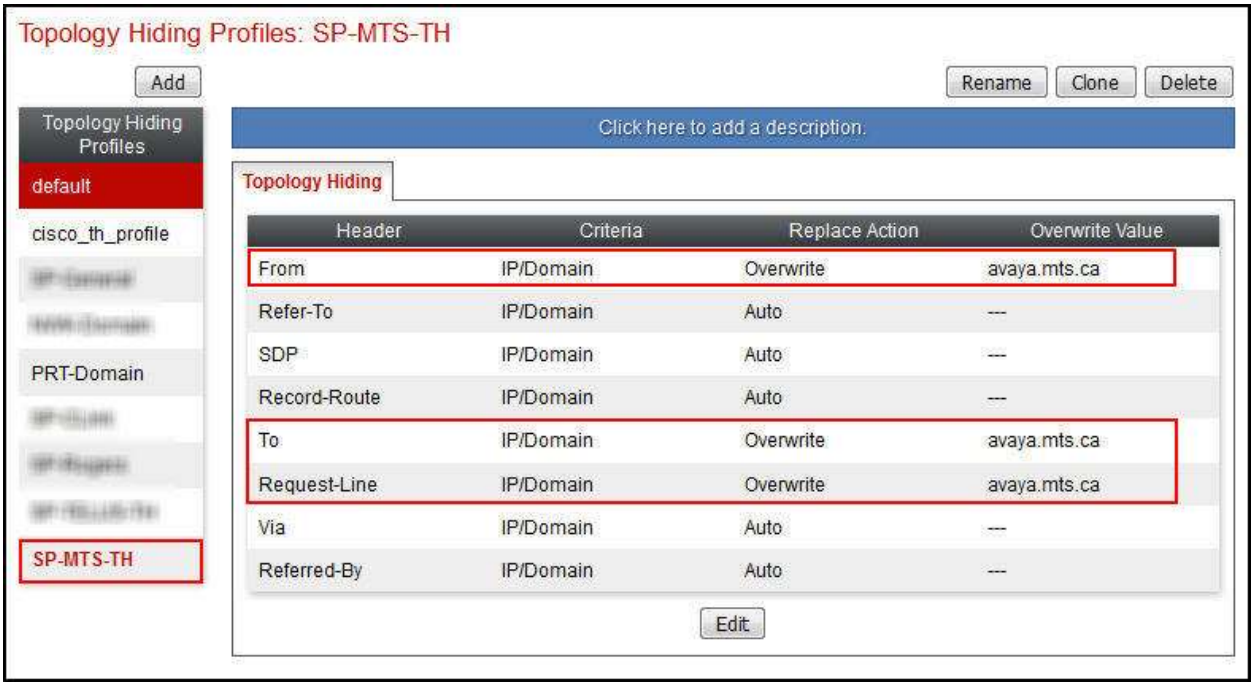
©2015 Avaya Inc. All Rights Reserved.

7.13.2. Topology Hiding – MTS

For the compliance test, the topology hiding profile **SP-MTS-TH** was created for MTS. This profile will be applied to traffic from the Avaya SBCE to MTS. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line**, **From** and **To** which should be set to **Overwrite**.
- For those headers to be overwritten, the **Overwrite Value** is set to the MTS SIP Trunking Service domain (**avaya.mts.ca**).

The following screen shows the configured topology hiding profile for MTS:



©2015 Avaya Inc. All Rights Reserved.

7.14. End Point Flows

Endpoint flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.,) is used to determine which flow it matches. Once the flow is determined, the flow points to policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of the compliance test, the signaling endpoints are Session Manager and the service provider SIP server.

To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device to be managed. In the right pane, select the **Server Flows** tab and click the **Add** button (not shown) on top of the far right pane . A pop-up window (not shown) will appear requesting the name of the new flow and settings for the flow parameters. Once complete, the settings are shown in the far right pane under the server name listed by the **Server Configuration** heading, as shown below.

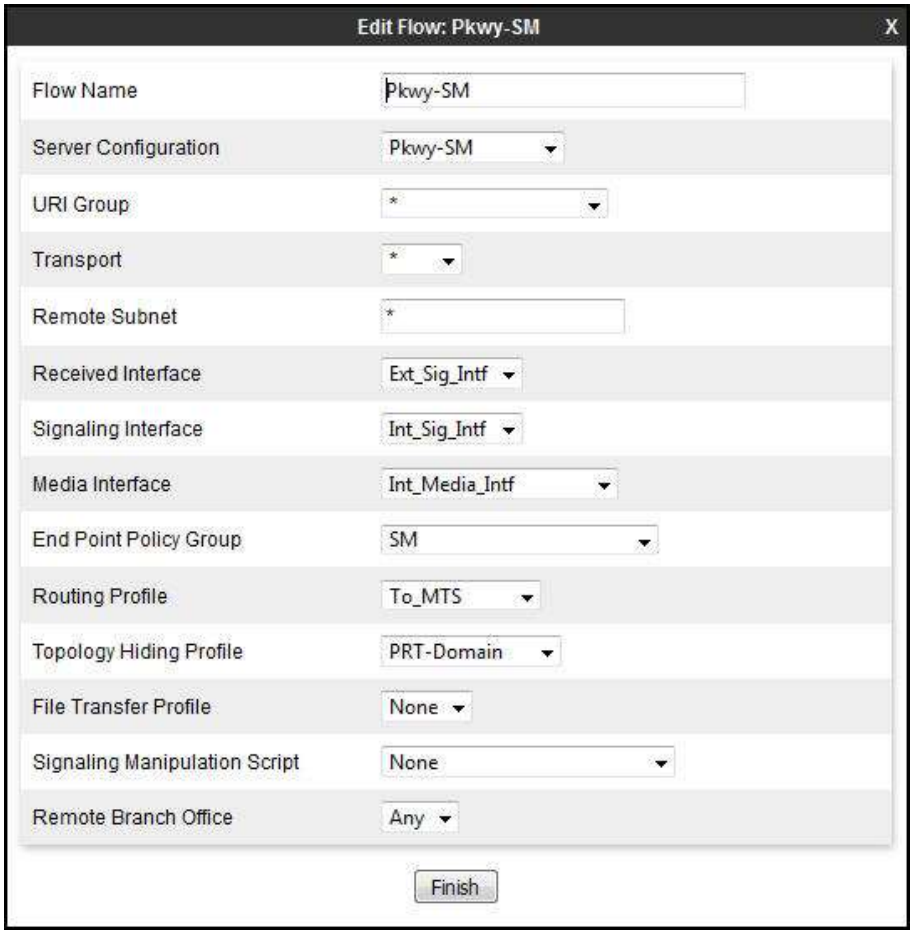


©2015 Avaya Inc. All Rights Reserved.

7.14.1. End Point Flow – Session Manager

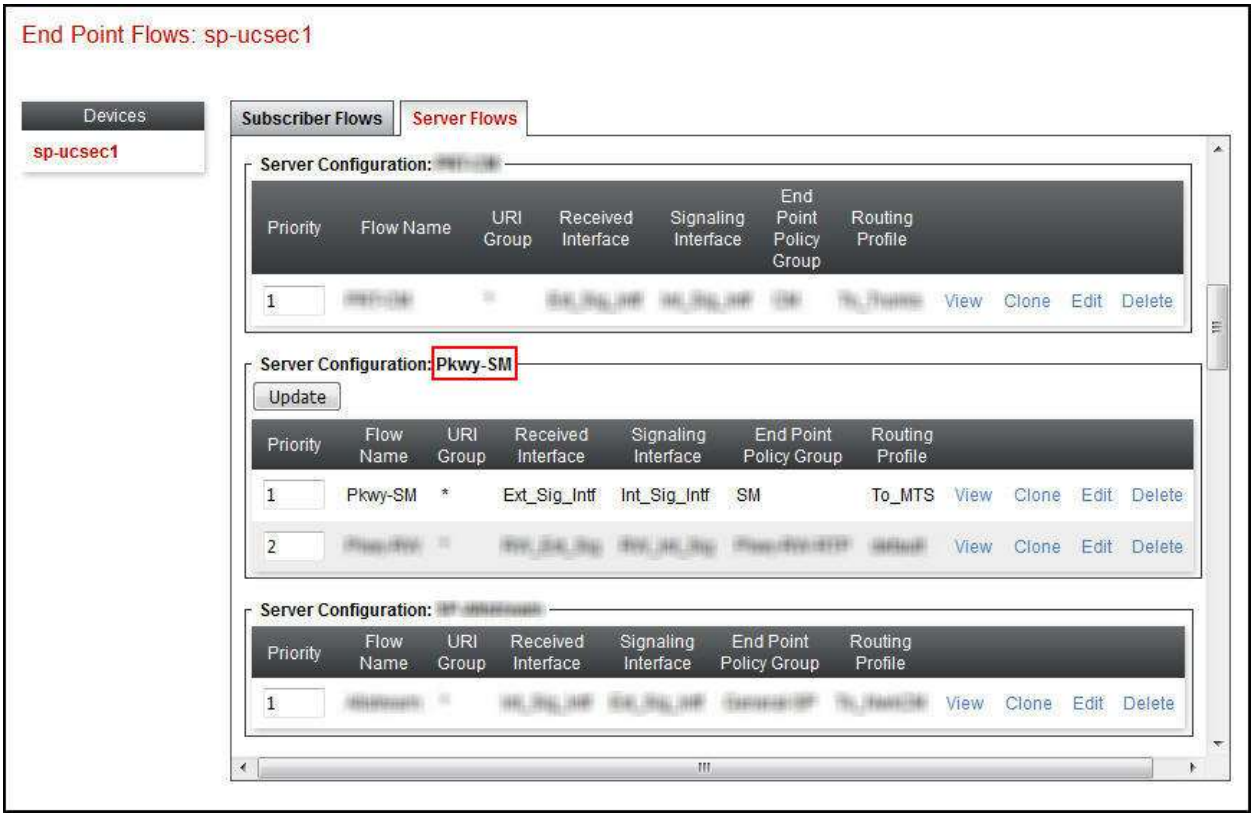
For the compliance test, the endpoint flow **Pkwy-SM** was created for Session Manager. All traffic from Session Manager will match this flow as the source flow and use the specified **Routing Profile** to determine the destination server and corresponding destination flow. The **End Point Policy Group** and **Topology Hiding** profiles will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Session Manager server created in **Section 7.7.1**.
- To match all traffic, set **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set **Received Interface** to the external signaling interface.
- Set **Signaling Interface** to the internal signaling interface.
- Set **Media Interface** to the internal media interface.
- Set **End Point Policy Group** to the endpoint policy group defined for Session Manager in **Section 7.11.1**.
- Set **Routing Profile** to the routing profile defined in **Section 7.12.2** for MTS.
- Set **Topology Hiding Profile** to the topology hiding profile defined for Session Manager in **Section 7.13.1**.



©2015 Avaya Inc. All Rights Reserved.

The screen below shows the saved **Pkwy-SM** configuration as a Server Flow. Note the server name by the **Server Configuration** heading.

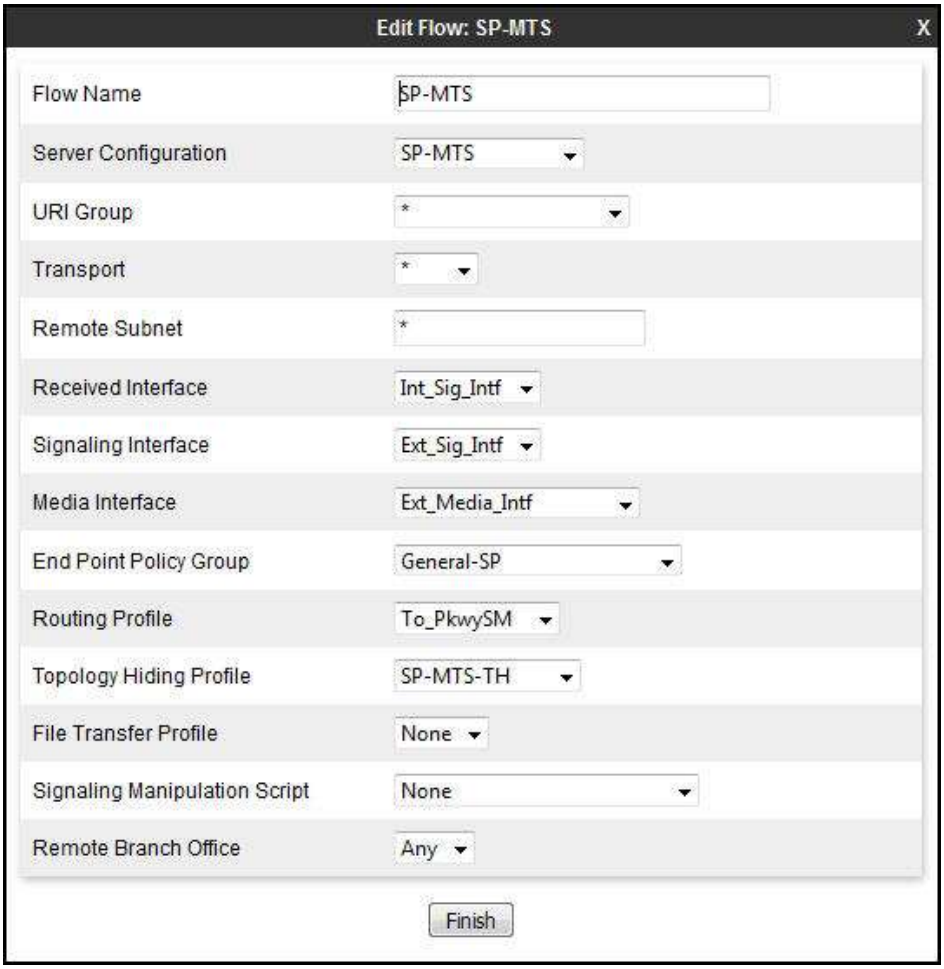


©2015 Avaya Inc. All Rights Reserved.

7.14.2. End Point Flow – MTS

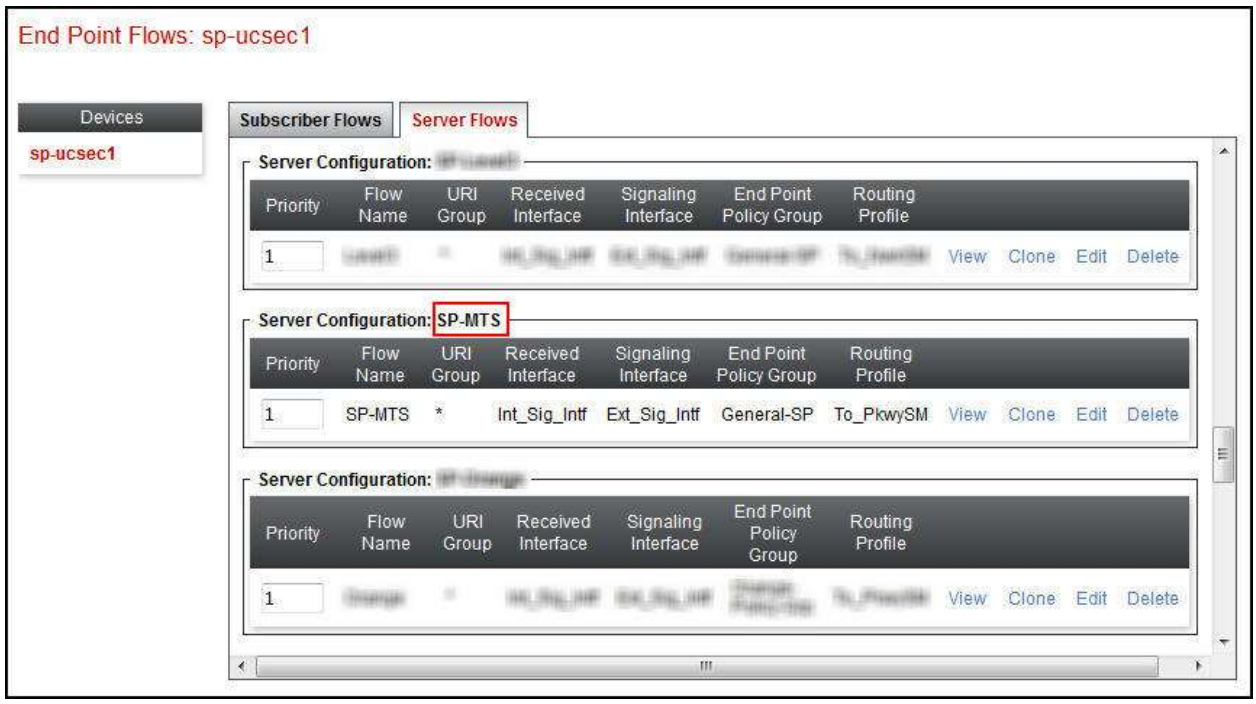
For the compliance test, the endpoint flow **SP-MTS** was created for the MTS SIP server. All traffic from MTS will match this flow as the source flow and use the specified **Routing Profile** to determine the destination server and corresponding destination flow. The **End Point Policy** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the MTS SIP server created in **Section 7.7.2**.
- To match all traffic, set **URI Group**, **Transport**, and **Remote Subnet** to *****.
- Set **Received Interface** to the internal signaling interface.
- Set **Signaling Interface** to the external signaling interface.
- Set **Media Interface** to the external media interface.
- Set **End Point Policy Group** to the endpoint policy group defined for MTS in **Section 7.11.2**.
- Set **Routing Profile** to the routing profile defined in **Section 7.12.1** for Session Manager.
- Set **Topology Hiding Profile** to the profile defined for MTS in **Section 7.13.2**.



©2015 Avaya Inc. All Rights Reserved.

The screen below shows the saved **SP-MTS** configuration as a Server Flow. Note the server name by the **Server Configuration** heading.



©2015 Avaya Inc. All Rights Reserved.

8. MTS SIP Trunking Service Configuration

MTS is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the access interface IP address used to reach the enterprise (i.e., the IP address of the public interface on the Avaya SBCE). MTS will provide the necessary information to complete the configurations for Communication Manager, Session Manager and the Avaya SBCE discussed in the previous sections, including:

- Access interface IP addresses and domain name of the MTS SIP Trunking Service.
- SIP credentials for trunk registration and Digest Authentication for outbound calls.
- Transport and port for the MTS SIP connection to the Avaya SBCE at the enterprise.
- DID numbers to assign to users at the enterprise.
- Supported codecs and their preference order.

9. Verification Steps

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

Verification Steps:

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Troubleshooting:

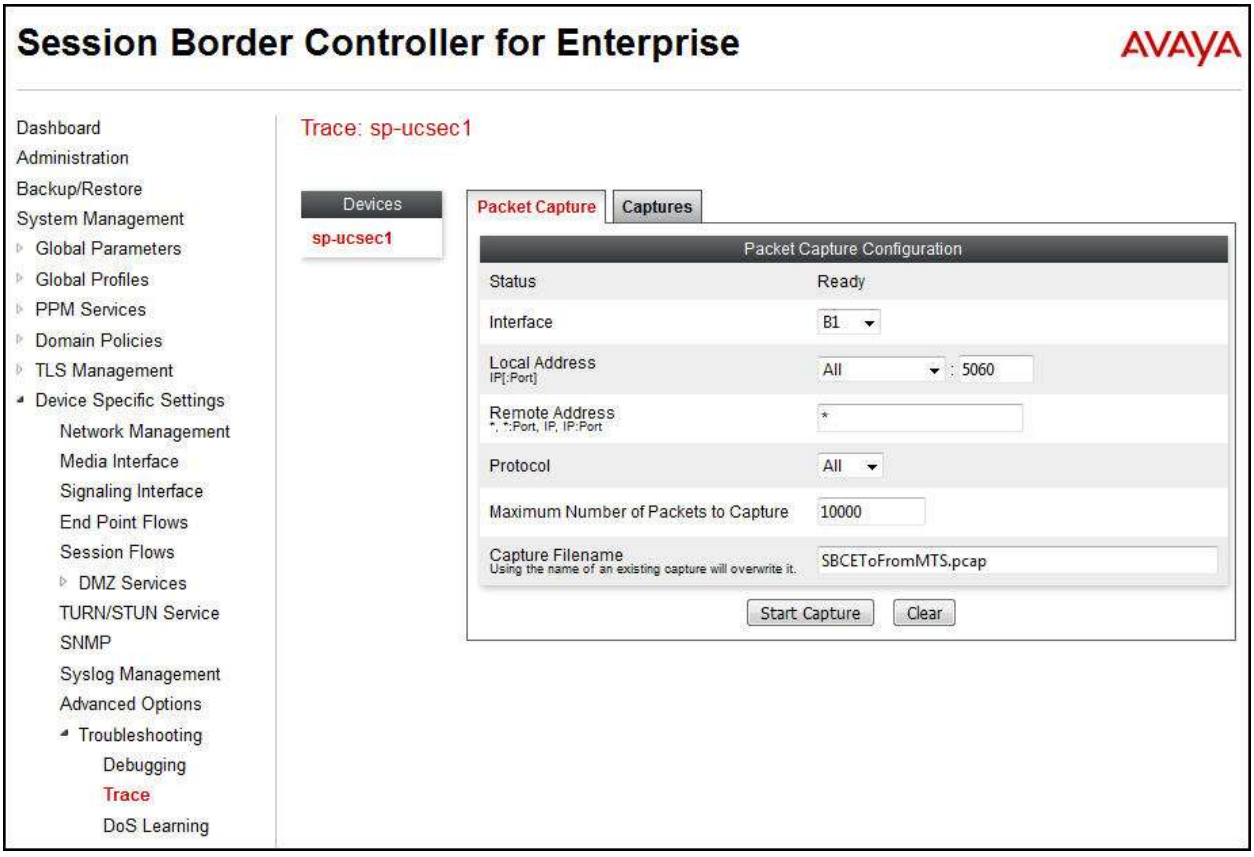
1. Communication Manager:
    - **list trace station** <extension number> - Traces calls to and from a specific station.
    - **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
    - **status station** <extension number> - Displays signaling and media information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

©2015 Avaya Inc. All Rights Reserved.

2. Session Manager:
   - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

3. Avaya SBCE:
   The Avaya SBCE can take internal traces on specified interfaces. SIP signaling crossing both interfaces A1 and B1 can be captured for troubleshooting. In the Avaya SBCE management web interface, navigate to **Device Specific Settings → Troubleshooting → Trace** to invoke this facility. In the **Packet Capture** tab, select or supply the relevant information (e.g., A1 or B1 or any interfaces, IP/port, protocol, number of packets to capture, capture file name, etc.), then press the **Start Capture** button to start the trace. The captured trace file, after the capture has been stopped, can then be downloaded from the **Captures** tab for examination using a protocol sniffer application such as Wireshark.

   The screen below shows the setup for capturing packets to and from the public interface of the Avaya SBCE (B1). The captured traffic will be capped at 10000 packets and be saved to a file named "SBCEToFromMTS.pcap".



©2015 Avaya Inc. All Rights Reserved.

10. Conclusion

The MTS SIP Trunking Service passed compliance testing with the Avaya SIP-enabled enterprise solution composed of Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.3. These Application Notes describe the configuration necessary to connect the Avaya solution to the MTS SIP Trunking Service as shown in **Figure 1**. Test results and observations are noted in **Section 2.2**.

11. References

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

Avaya Aura® System Platform

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3, Issue 5, June 2015.
[2] *Administering Avaya Aura® System Platform*, Release 6.3, Issue 5, June 2015.

Avaya Aura® Session Manager/System Manager

[3] *Deploying Avaya Aura® Session Manager*, Release 6.3, Issue 6, November 2014.
[4] *Administering Avaya Aura® Session Manager,* Release 6.3, Issue 7, September 2014.
[5] *Deploying Avaya Aura® System Manager on System Platform,* Release 6.3, Issue 4, June 2014.
[6] *Upgrading Avaya Aura® System Manager to 6.3.13 on System Platform,* Release 6.3, Issue 5, April 2015.
[7] *Administering Avaya Aura® System Manager for Release 6.3.13*, Release 6.3, Issue 8, July 2015.

Avaya Aura® Communication Manager

[8] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 6.3, Issue 12, June 2015, *D*ocument Number 555-245-205.
[9] *Administering Avaya Aura® Communication Manager*, Release 6.3, Issue 10, August 2015, Document Number 03-300509.
[10] *Programming Call Vectoring Features in Avaya Aura® Call Center Elite*, Release 6.3.6, June 2014.

©2015 Avaya Inc. All Rights Reserved.

Avaya Endpoints

[11] *Avaya 1600 Series IP Deskphones Administrator Guide*, Release 1.3.6, Issue 6, August 2014, Document Number 16-601438.

[12] *Administering Avaya 9608/9608G/9611G/9621G/9641G IP Deskphones H.323*, Release 6.4, Issue 19, June 2014, Document Number 16-300698.

[13] *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G IP Deskphones SIP*, Release 6.4, Issue 5, August 2014, Document Number 16-601944.

[14] *SIP Software for Avaya 1100 Series IP Deskphone - Administration*, Release 4.4, Issue 06.05 Standard, July 2015, Document Number NN43170-600.

[15] *Administering Avaya one-X® Communicator*, Release 6.2 Feature Pack 6, April 2015.

[16] *Administering Avaya Communicator for Android, iPad, iPhone, and Windows, Release 2.1, Issue 4, June 2015*.

Avaya Session Border Controller for Enterprise

[17] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.

[18] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 6.3, Issue 3, October 2014.

[19] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communication Manager Rel. 6.3 and Avaya Aura® Session Managers Rel. 6.3*, Issue 1.0, October 2014.

Internet Engineering Task Force (IETF®) SIP RFC

[20] RFC 3261 *SIP: Session Initiation Protocol*, http://www.ietf.org/

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

Product documentation for the MTS SIP Trunking Service is available from MTS Inc..

©2015 Avaya Inc. All Rights Reserved.

©2015 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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