Avaya Solution & Interoperability Test Lab

Application Notes for MTS Allstream SIP Trunking Service with Avaya Aura® Communication Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 – Issue 1.0

Abstract

These Application Notes describe the steps to configure a Session Initiation Protocol (SIP) trunk between the MTS Allstream SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 6.3, Avaya Session Border Controller for Enterprise 6.2 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Session Border Controller for Enterprise.

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

1. Introduction

These Application Notes describe the steps to configure a SIP trunk between MTS Allstream SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.3 configured as an Evolution Server, Avaya Session Border Controller for Enterprise 6.2(Avaya SBCE) and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with MTS Allstream are able to place and receive PSTN calls via a broadband Internet connection. This converged network solution is an alternative to a traditional PSTN trunk such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

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

MTS Allstream is a member of the Avaya DevConnect Service Provider Program. The general test approach is to connect a simulated enterprise to MTS Allstream via the Internet and exercise the features and functionalities listed in **Section 2.1**.

2.1. Interoperability Compliance Testing

To verify MTS Allstream SIP Trunking Service interoperability, the following features and functionalities are covered in the compliance testing:

- Inbound PSTN calls to various phone types including H.323, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types including H.323, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phone. Both the1XC Computer Mode (where 1XC is used for call control as well as audio path) and the 1XC Telecommuter Mode (where 1XC is used for call control and a separate telephone is used for audio path) are tested.
- Dialing plans including local, long distance, international, outbound toll-free, operator assisted, local directory assistance (411) calls etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Codec G.711MU and G.729.
- Media and Early Media transmissions.
- Incoming and outgoing fax using G.711MU and T.38.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.

- User features such as hold and resume, transfer, forward and conference.
- Off-net call forward with Diversion method.
- EC500 mobility (extension to cellular) with Diversion method.
- Routing inbound vector call to call center agent queues.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.
- Emergency calls (911).

Items that are supported and not tested including the following:

- Inbound toll-free.
- MTS Allstream SIP Trunking was not configured to send SIP OPTIONS messages during the compliance test but will respond to the OPTIONS messages sent by the Avaya SBCE.
- Local outbound calling using 7 digit dialing is not supported. These calls require dialing 10 digits. Inbound local calls can be configured for 7 digits but this was not tested.
- Incoming call redirection on VDN before answer using “302 Moved Temporarily” method is not supported.
- Incoming call redirection after answer of incoming VDN calls using SIP REFER method is not supported.

2.2. Test Results

Interoperability testing of MTS Allstream SIP Trunking Service with the Avaya SIP-enabled enterprise solution is completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Call Display on PSTN Phone** – Call display was not properly updated on PSTN phone involved in a call transfer. After the call transfer was completed, the PSTN phone did not display the actual connected party but instead showed the party that initiated the transfer. However, it does not affect the end user.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com.

For technical support on the MTS Allstream SIP Trunking Service, contact MTS Allstream Customer Care by calling 866-282-0111 or by sending email to ABC3@mtsallstream.com.

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to the MTS Allstream SIP Trunking Service (Vendor Validation circuit) through a public Internet connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

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

- Avaya S8800 Servers running Avaya Aura® Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Avaya Aura® Messaging
- Avaya Session Border Controller for Enterprise
- Avaya 9600 Series IP Deskphones (H.323)
- Avaya one-X® Communicator (H.323)
- Avaya digital and analog telephones

Located at the edge of the enterprise network is the Avaya SBCE. It has a public side that connects to MTS Allstream via Internet and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flows through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and MTS Allstream across the public network is UDP. The transport protocol between the Avaya SBCE and Communication Manager is TCP.

In the compliance testing, the Avaya Customer-Premises Equipment (CPE) environment was configured with SIP domain “bvwlab.com” for the enterprise. The Avaya SBCE is used to adapt the enterprise SIP domain to the IP address based URI-Host known to MTS Allstream. **Figure 1** below illustrates the network diagram for the enterprise. All voice application elements are connected to internal trusted LAN.

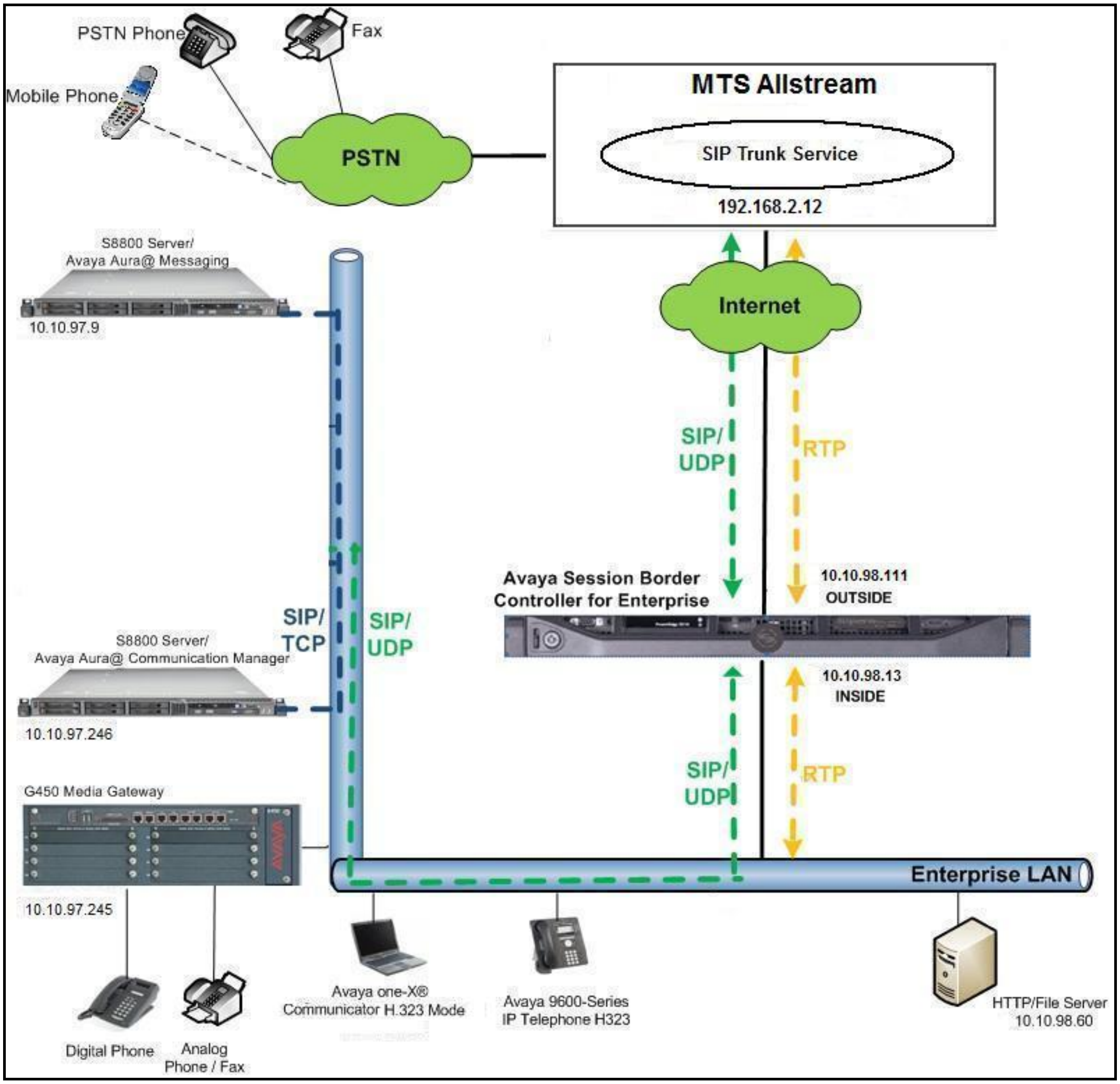


Figure 1: Avaya IP Telephony Network connecting to MTS Allstream SIP Trunking Service

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on an Avaya S8800 Server	6.3 (Avaya Communication Manager/ R016x.03.0.124.0 with Service Pack (03.0.124.0-21591)
Avaya G450 Media Gateway	33.13.0
Avaya Aura® Messaging running on an Avaya S8800 Server	6.1-11.0
Avaya Session Border Controller for Enterprise	6.2.1 Q16
Avaya 9611G IP Deskphone (H.323)	Avaya one-X® Deskphone Edition S6.0.0
Avaya 9630G IP Deskphone (H.323)	Avaya one-X® Deskphone Edition 3.1 SP5
Avaya one-X® Communicator (H.323)	6.1.7.04-SP7-39506
Avaya 1408 Digital Telephone	1400R10
Avaya 6210 Analog Telephone	n/a
MTS Allstream SIP Trunking Service Components	
Component	Release
Genband S3 SBC	Software Release: 7.1.14.5
Genband CS2K telephony switch	Release: CVM 17

Table 1: Equipment and Software Tested

Note: This solution will be compatible with other Avaya Server and Media Gateway platforms running similar version of Communication Manager.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for MTS Allstream SIP Trunking. It is assumed the general installation of Communication Manager and Avaya G450 Media Gateway has been previously completed and is not discussed here.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

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 and from the service provider. 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 sale representative to add the additional capacity or feature.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 4000   50
           Maximum Concurrently Registered IP Stations: 2400   1
             Maximum Administered Remote Office Trunks: 4000   0
Maximum Concurrently Registered Remote Office Stations: 2400   0
              Maximum Concurrently Registered IP eCons: 68     0
  Max Concur Registered Unauthenticated H.323 Stations: 100    0
                       Maximum Video Capable Stations: 2400    0
                  Maximum Video Capable IP Softphones: 2400    3
                       Maximum Administered SIP Trunks: 24000 289
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000   0
   Maximum Number of DS1 Boards with Echo Cancellation: 80     0
                          Maximum TN2501 VAL Boards: 10        0
                  Maximum Media Gateway VAL Sources: 50        1
           Maximum TN2602 Boards with 80 VoIP Channels: 128    0
          Maximum TN2602 Boards with 320 VoIP Channels: 128    0
   Maximum Number of Expanded Meet-me Conference Ports: 300    0

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

5.2. System Features

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

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

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. The compliance test used the value of ***anonymous*** for restricted calls and unavailable calls.

```
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: 1
          International Access Code: 001

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager **(procr**) and Avaya Session Border Controller for Enterprise (**ASBCE62**). These node names will be needed for defining the service provider signaling groups in **Section 5.6**.

```
change node-names ip                                        Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
ASBCE62             10.10.98.13
DevAAM              10.33.10.9
default             0.0.0.0
procr               10.10.97.246
procr6              ::
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to be used for calls between the enterprise and the service provider. This compliance test used ip-codec-set 1. MTS Allstream supports G.711MU and G729. To use this codec, enter ***G.711MU*** and ***G.729*** in the **Audio Codec** column of the table in the order of preference.

The following screen shows the configuration for ip-codec-set 1. During testing, the codec set specifications are varied to test for individual codec support as well as codec negotiation between the enterprise and the network at call setup time.

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

                          IP Codec Set
    Codec Set: 1

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

On **Page 2**, set the **Fax Mode** to ***pass-through*** faxing which is supported by MTS Allstream.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

                    Mode                Redundancy
    FAX             pass-through          1
    Modem           off                   0
    TDD/TTY         US                    3
    Clear-channel   n                     0
```

5.5. IP Network Region

A separate IP network region for the service provider trunk group is created. This allows separate codec or quality of service setting to be used (if necessary) for a call between the enterprise and the service provider versus a call within the enterprise or elsewhere. For the compliance testing, ip-network-region 1 was created by the **change ip-network-region *1*** command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance testing, the domain name is ***bvwlab.com***. This domain name appears in the "From" header of SIP message 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 Media Gateway. By default, both **Intra-region** and **Inter-region IP-IP Direct Audio** are set to ***yes***. Shuffling can be further restricted at the trunk level under the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: bvwlab.com
    Name: ToDevASM
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
...
```

On **Page 4**, define the IP codec set to be used for traffic between region 1 and other regions. In the compliance testing, Communication Manager, the Avaya G450 Media Gateway, IP phones and the Avaya SBCE were assigned to the same region 1. To configure the IP codec set between regions, enter the desired IP codec set in the **codec set** column of the table with appropriate destination region (**dst rgn**). Default values may be used for all other fields. The example below shows codec set 1 will be used for a call between region 1 and other regions.

```
change ip-network-region 1                                      Page   4 of  20

 Source Region: 1     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    1                                                                all
 2    1      y    NoLimit                                            n       t
 3                                                                   n       t
```

Non-IP telephones (e.g., analog, digital) derive network region from IP interface of the Avaya G450 Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping.

To define network region 1 for IP interface **procr**, use **change ip-interface procr** command as shown in the following screen.

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


                  Type: PROCR
                                                       Target socket load: 4800

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

To define network region 1 for the Avaya G450 Media Gateway, use **change media-gateway** command as shown in the following screen.

```
change media-gateway 1                                          Page   1 of   2
                            MEDIA GATEWAY 1

                    Type: g450
                    Name: G450
               Serial No: 12TG18000244
            Encrypt Link? y                    Enable CF? n
          Network Region: 1                     Location: 1
                                               Site Data:
           Recovery Rule: none
...
```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Avaya Session Border Controller (Avaya SBCE) 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 ***50*** was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***y***.
- Set the **Transport Method** to ***tcp.*** The transport method specified here is used between Communication Manager and Avaya SBCE.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to ***5060***.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP interface of **procr** defined in **Section 5.3**.

- Set the **Far-end Node Name** to ***ASBCE62***. This node name maps to the IP address of Avaya SBCE as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region ***1*** defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to ***bvwlab.com***.
- Set the **DTMF over IP** to ***rtp-payload***. This setting enables Communication Manager to send or receive the DTMF transmissions using RFC2833.
- Set **Enable Layer 3 Test?** to ***y***. This setting allows Communication Manager to send OPTIONS heartbeat to Avaya SBCE on the SIP trunk.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to ***n***, then the Avaya G450 Media Gateway will remain in the media path between the SIP trunk and the endpoint for the duration of the call. Depending on the number of media resources available in the Avaya G450 Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **Direct IP-IP Early Media** is set to ***n***.
- Set the **Alternate Route Timer** to ***30***. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before canceling the call.
- Default values may be used for all other fields.

```
add signaling-group 50                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 50             Group Type: sip
  IMS Enabled? y        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y

   Near-end Node Name: procr                  Far-end Node Name: ASBCE62
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1
Far-end Domain: bvwlab.com

                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 30
```

5.7. Trunk Group

Use the **add trunk-group** command to create trunk group for the signaling group created in **Section 5.6**. For the compliance testing, trunk group ***50*** 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 **Outgoing Display** to ***y*** to enable name display on the trunk.
- Set the **Service Type** field to ***public-ntwrk***.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**.
- Set the **Number of Members** field to ***32***. It is the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk group.
- Default values are used for all other fields.

```
add trunk-group 50                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 50                   Group Type: sip          CDR Reports: y
  Group Name: SP Trunk                    COR: 1        TN: 1        TAC: *003
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 50
                                                     Number of Members: 32
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to service provider. This value defines the interval a re-INVITEs must be sent to refresh the Session Timer. For the compliance testing, a default value of ***600*** seconds was used.

```
add trunk-group 50                                         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
```

On **Page 3**, set the **Numbering Format** field to ***private***. This field specifies the format of the CPN sent to the far-end. The public numbers are automatically preceded with a + sign when passed in the "From", "Contact" and "P-Asserted Identity" SIP headers. The addition of the + sign impacted interoperability with the service provider. Thus, the **Numbering Format** is set to ***private*** and the **Numbering Format** in the route pattern is set to ***lev0-pvt*** (see **Section 5.98**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on the local endpoint to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. Default values are used for all other fields.

```
add trunk-group 50                                                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
```

On **Page 4**, the **Network Call Redirection** field should be set to ***n***. The setting of **Network Call Redirection** flag to ***y*** enables use of the SIP REFER message to transfer an inbound call back to the PSTN.

- Set **Mark Users as Phone** to ***y.***
- Set the **Send Diversion Header** field to ***y***. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound call back to PSTN and Extension to Cellular (EC500) call scenarios.
- Set the **Support Request History** field to ***n***. This parameter determines if History-Info header will be excluded in the call-redirection SIP INVITE from the enterprise.
- Set the **Telephone Event Payload Type** to ***101***, the value is preferred by MTS Allstream.

```
add trunk-group 50                                                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
...
```

5.8. Calling Party Information

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

The screen below shows a subset of the DID numbers assigned for testing. These 4 numbers were mapped to the 4 enterprise extensions 1130, 1131, 1132 and 1133. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

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

Ext Ext              Trk         Private            Total
Len Code             Grp(s)      Prefix             Len
 4  1130             50          6477761251         10       Total Administered: 11
 4  1131             50          6477761252         10          Maximum Entries: 540
 4  1132             50          6477761253         10
 4  1133             50          6477761238         10
```

5.9. Inbound Routing

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. DID number sent by MTS Allstream can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group. Use the **change inc-call-handling-trmt trunk-group** command to create an entry for each DID.

```
change inc-call-handling-trmt trunk-group 50                    Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 6477761251       10  1130
 public-ntwrk    10 6477761252       10  1131
 public-ntwrk    10 6477761253       10  1132
 public-ntwrk    10 6477761238       10  1133
```

5.10. Outbound Routing

In these Application Notes, the **Automatic Route Selection** (ARS) feature is used to route an outbound call via the SIP trunk to the service provider. In the compliance testing, a single digit 9 was used as the ARS access code. An enterprise caller will dial 9 to reach an outside line. To define feature access code (**fac**) 9, use the **change dialplan analysis** command as shown below.

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

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   11          4   ext
   3           4   udp
   4           4   ext
   6           1   fac
   6           4   ext
   7           4   ext
   9           1   fac
```

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

```
change feature-access-codes                                        Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *007
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: *008
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
```

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 testing. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern ***50*** for an outbound call 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: 0

          Dialed           Total     Route    Call   Node   ANI
          String          Min  Max  Pattern   Type   Num    Reqd
    0                     1    11    50       op            n
    011                   13   13    50       intl          n
    1                     11   11    50       pubu          n
    300                   10   10    50       pubu          n
    411                   3    3     50       svcl          n
    613                   10   10    50       pubu          n
    866                   10   10    50       pubu          n
    911                   3    3     50       svcl          n
    647                   10   10    50       pubu          n
```

As being mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for route pattern ***50*** in the following manner.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group ***50*** 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**: **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 5.8**.

```
change route-pattern 50                                             Page   1 of   3
                    Pattern Number: 50   Pattern Name: SP Route
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                                DCS/ IXC
    No          Mrk Lmt List Del  Digits                                  QSIG
                             Dgts                                         Intw
 1: 50   0       1                                                         n   user
 2:                                                                        n   user
....
     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                unk-unk   none
...
```

5.11. Saving Communication Manager Configuration Changes

The command **save translation all** can be used to save the configuration changes made on Communication Manager.

6. Configure Avaya Session Border Controller for Enterprise

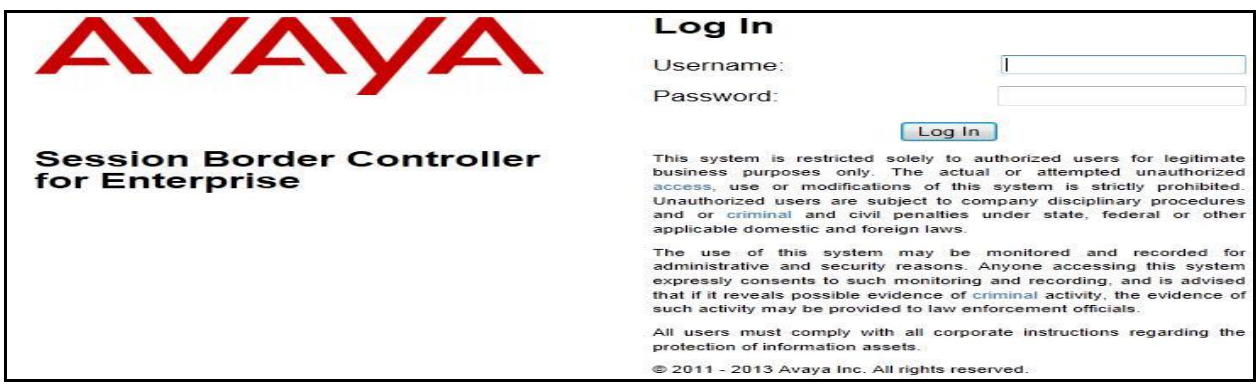
In the sample configuration, an Avaya SBCE is used as the edge device between the Avaya CPE and MTS Allstream SIP Trunking service.

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

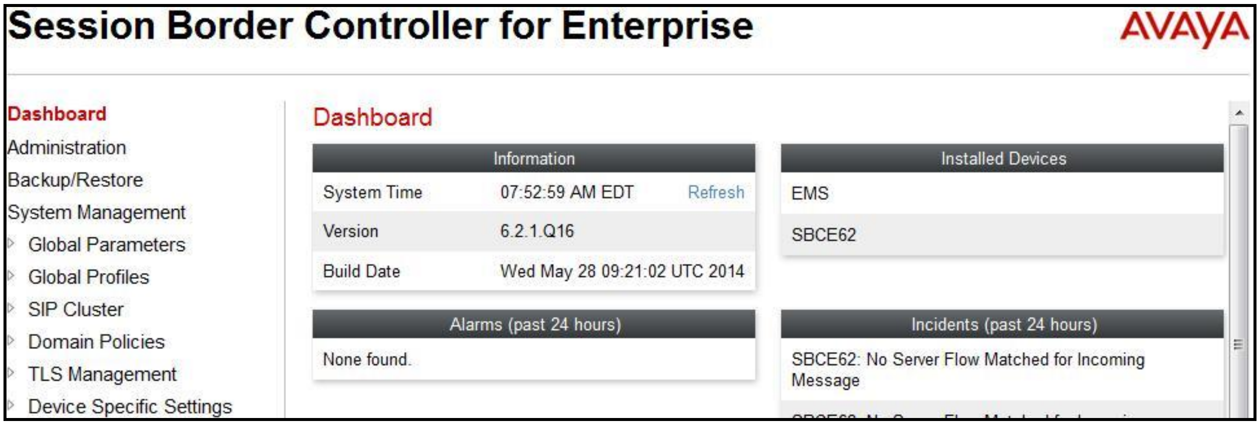
6.1. Avaya Session Border Controller for Enterprise Login

Use a Web browser to access the Avaya SBCE web interface, enter https://<ip-addr>/ucsec in the address field of the web browser (not shown), where <ip-addr> is the management LAN IP address of Avaya SBCE.

Enter appropriate credentials and click ***Log In***.



The main page of the Avaya SBCE will appear as shown below.



6.2. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

6.2.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, "*" is used for all incoming and outgoing traffic.

6.2.2. Routing Profiles

Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

To create a Routing Profile, select **Global Profiles → Routing**. Click on the **Add** button.

In the compliance testing, a Routing Profile **EN-to-SP** was created to use in conjunction with the server flow defined for Communication Manager. This entry is to route the outbound call from the enterprise to MTS Allstream.

In the opposite direction, a Routing Profile named **SP-to-EN** was created to be used in conjunction with the server flow defined for MTS Allstream. This entry is to route the inbound call from MTS Allstream to the enterprise.

6.2.2.1 Routing Profile for MTS Allstream

The screenshot below illustrate the routing profile from Avaya SBCE to the MTS Allstream network, **Global Profiles → Routing**: **EN-to-SP**. As shown in **Figure 1**, the MTS Allstream SIP trunk is connected with transportation protocol UDP (not shown). If there is a match in the "To" or "Request URI" headers with the URI Group **SP** defined in **Section 6.2.1**, the call will be routed to the **Next Hop Server 1** which is the IP address of MTS Allstream SIP trunk on port 5060.

6.2.2.2 Routing Profile for Communication Manager

The Routing Profile for MTS Allstream to Communication Manager, **SP-to-EN**, was defined to route call where the "To" header matches the URI Group **SP** defined in **Section 6.2.1** to **Next Hop Server 1** which is the IP address of Communication Manager, on port 5060 as a destination. As shown in **Figure 1**, the SIP trunk between Communication Manager and the Avaya SBCE is connected with transportation protocol TCP.

6.2.3. Topology Hiding

Topology Hiding is an Avaya SBCE security feature which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user.

To create a Topology Hiding profile, select **Global Profiles → Topology Hiding**. Click on the **Add** button.

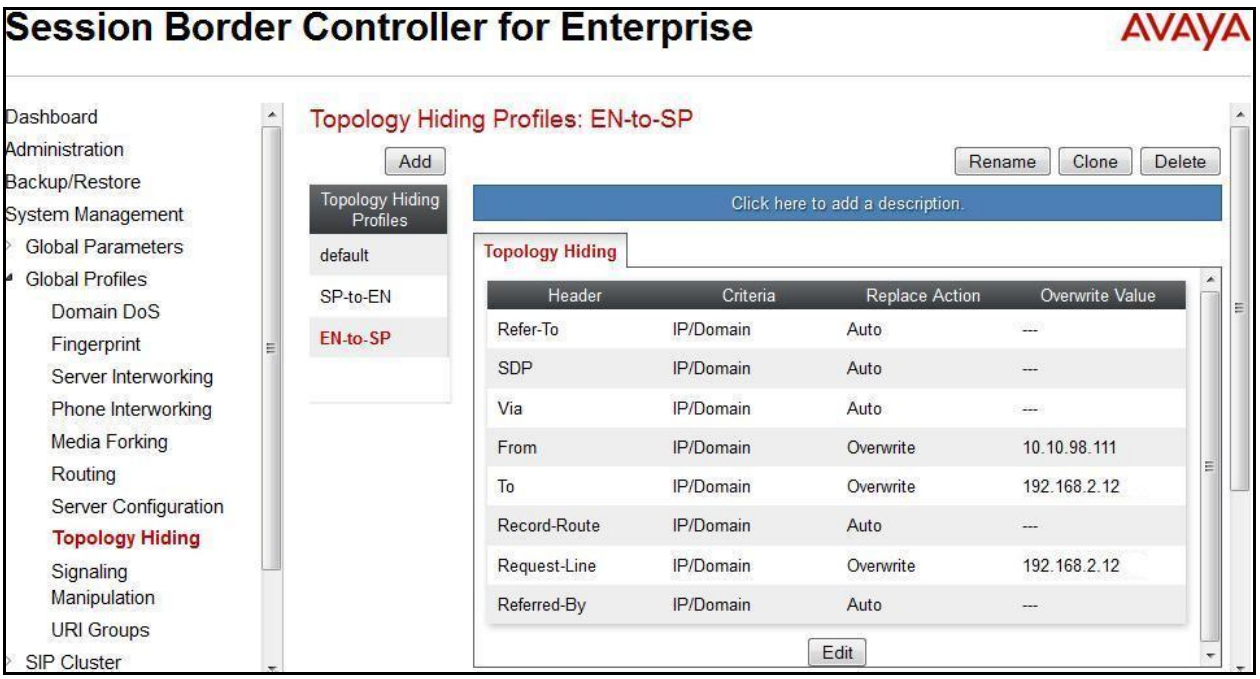
In the compliance testing, two Topology Hiding profiles **EN-to-SP** and **SP-to-EN** were created.

6.2.3.1 Topology Hiding Profile for MTS Allstream

Profile **EN-to-SP** was defined to mask the enterprise SIP domain bvwlab.com in "Request-URI" and "To" headers to MTS Allstream IP address and "From" header to the Avaya SBC external interface IP address; mask the enterprise SIP domain bvwlab.com in the "From" and "PAI" headers to IP ***10.10.98.111*** (the Avaya SBCE public IP address). It is to secure the enterprise network topology and to meet the SIP requirement of the service provider.

- The **Criteria** should be selected as **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on "From" header also applies to "Referred-By" and "P-Asserted-Identity" headers.
- The masking applied on "To" header also applies to "Refer-To" header.

The screenshots below illustrate the Topology Hiding profile **EN-to-SP**.

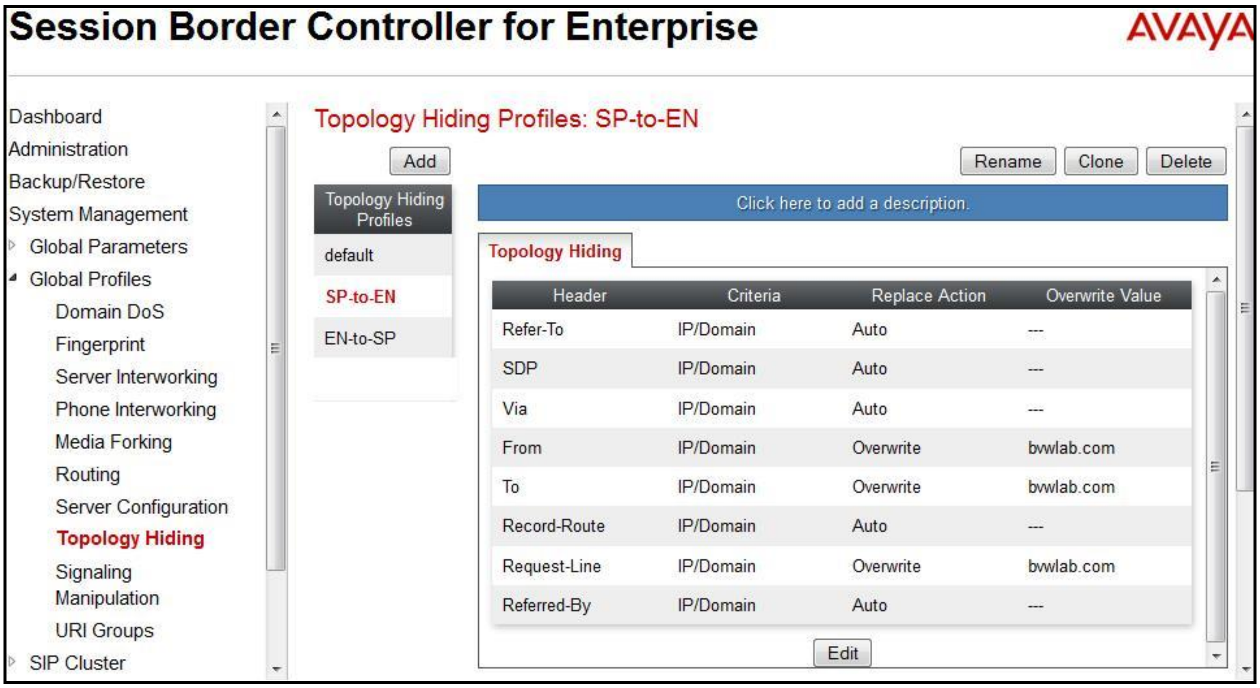


6.2.3.2 Topology Hiding Profile for Communication Manager

Profile **SP-to-EN** was also created to mask MTS Allstream URI-Host in "Request-URI", "From", "To" headers to the enterprise domain ***bvwlab.com***, replace Record-Route, via headers and SDP added by MTS Allstream to internal IP address known to Communication Manager.

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on "From" header also applies to "Referred-By" and "P-Asserted-Identity" headers.
- The masking applied on "To" header also applies to "Refer-To" header.

The screenshots below illustrate the Topology Hiding profile **SP-to-EN**.



6.2.4. Server Interworking

Interworking Profile features are configured differently for Call Server and Trunk Server.

To create a Server Interworking profile, select **Global Profiles → Server Interworking**. Click on the **Add** button.

In the compliance testing, two Server Interworking profiles were created for MTS Allstream and Communication Manager respectively.

6.2.4.1 Server Interworking profile for MTS Allstream

Profile **SP=SI** was defined to match the specification of MTS Allstream. The **General** and **Advanced** settings are configured with the following parameters while the other settings for **Timers**, **URI Manipulation** and **Header Manipulation** are kept as default.

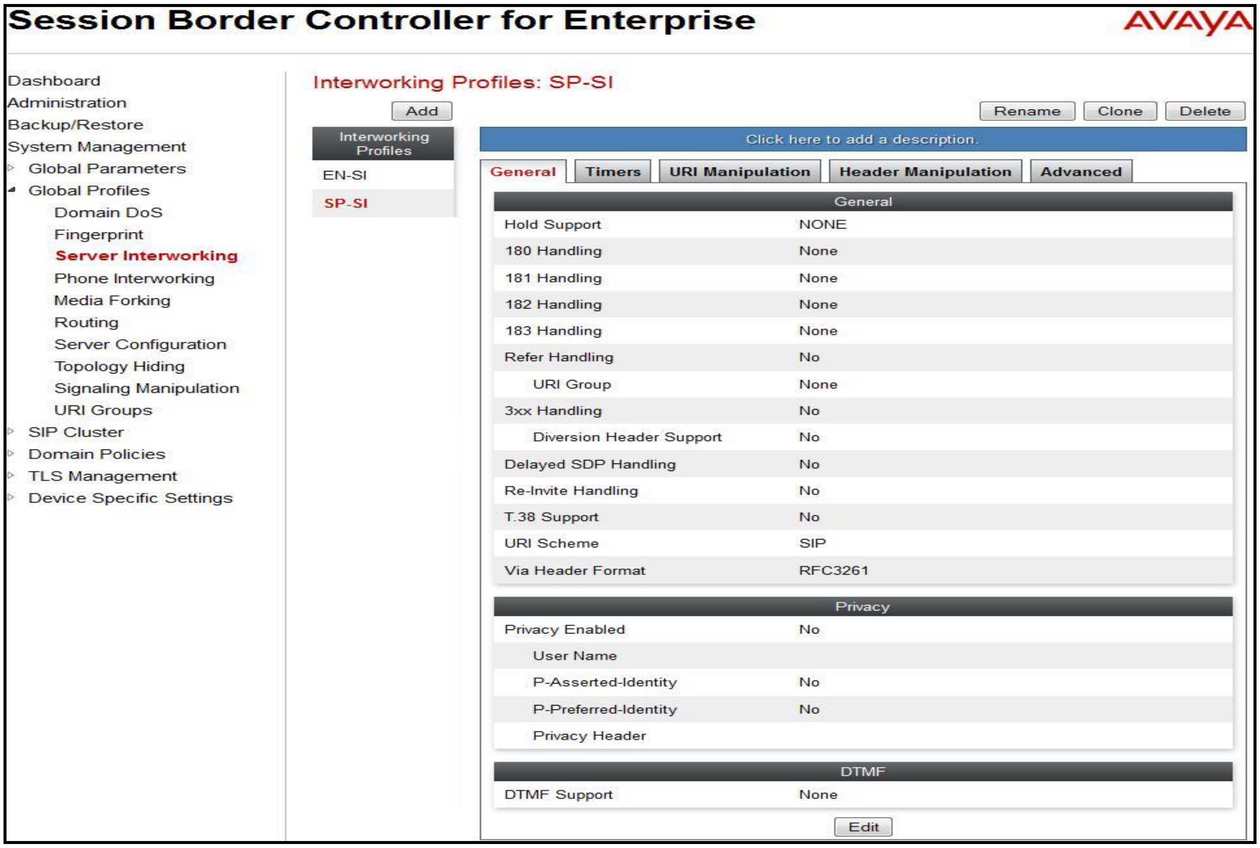
General settings:

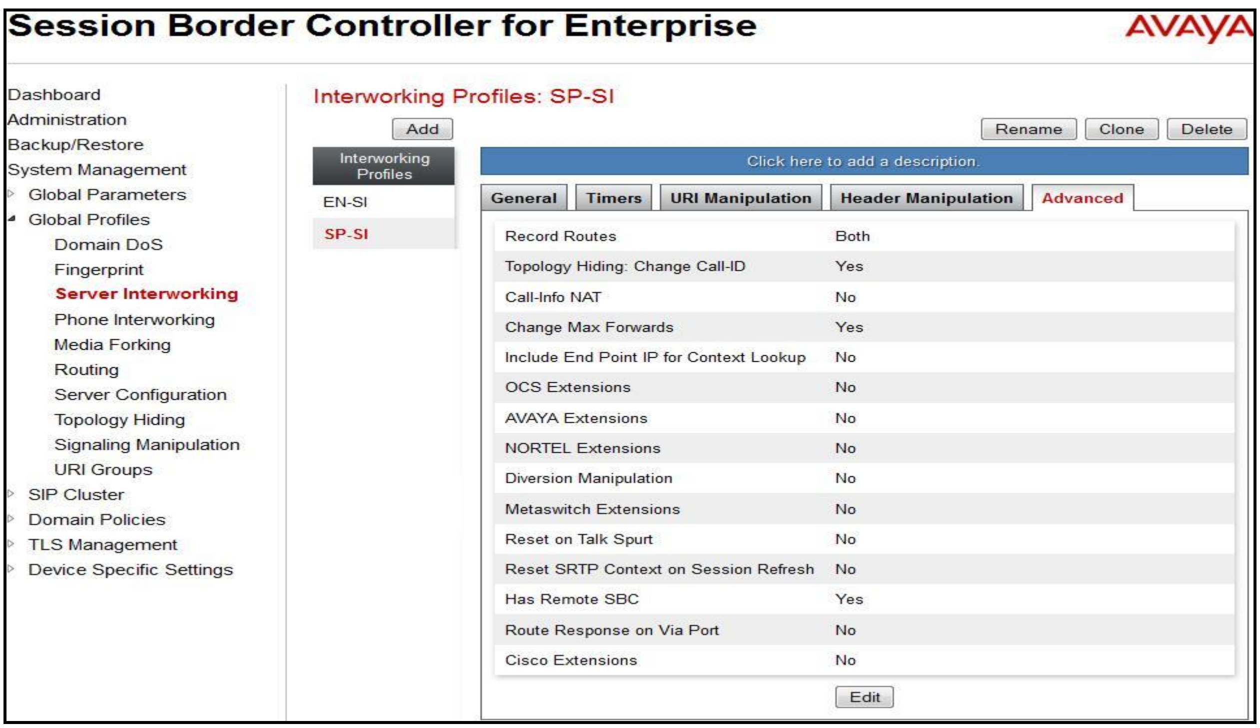
- **Hold Support** = ***NONE***. The Avaya SBCE will not modify the hold/ resume signaling from Communication Manager to MTS Allstream.
- **18X Handling** = ***None***. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from Communication Manager to MTS Allstream.
- **Refer Handling** = ***No*** The Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from Communication Manager to MTS Allstream.
- **T.38 Support** = ***Yes***. MTS Allstream does support T.38 fax in the compliance testing.
- **Privacy Enabled** = ***No***. The Avaya SBCE will not mask the “From” header with anonymous for the outbound call to MTS Allstream. It depends on Communication Manager to enable/ disable privacy on an individual call basis.
- **DTMF Support** = ***None***. The Avaya SBCE will send original DTMF method from Communication Manager to MTS Allstream.

Advanced settings:

- **Record Routes** = ***Both Sides***. The Avaya SBCE will send “Record-Route” header to both call and trunk servers.
- **Topology Hiding**: **Change Call-ID** = ***Yes***. The Avaya SBCE will modify “Call-ID” header for the call toward MTS Allstream.
- **Change Max Forwards** = ***Yes***. The Avaya SBCE will adjust the original Max-Forwards value from Communication Manager to MTS Allstream by reducing the intermediate hops involving in the call flow.
- **Has Remote SBC** = ***Yes***. MTS Allstream has a SBC which interfaces its Central Office (CO) to the enterprise SIP trunk. This setting allows the Avaya SBCE to always use the SDP received from MTS Allstream for the media.

The screenshots below illustrate the Server Interworking profile **SP-SI**.





6.2.4.2 Server Interworking profile for Communication Manager

Profile **CM63** was defined to match the specification of Communication Manager. The **General** and **Advanced** settings are configured with the following parameters while the other settings for **Timers**, **URI Manipulation** and **Header Manipulation** are kept as default.

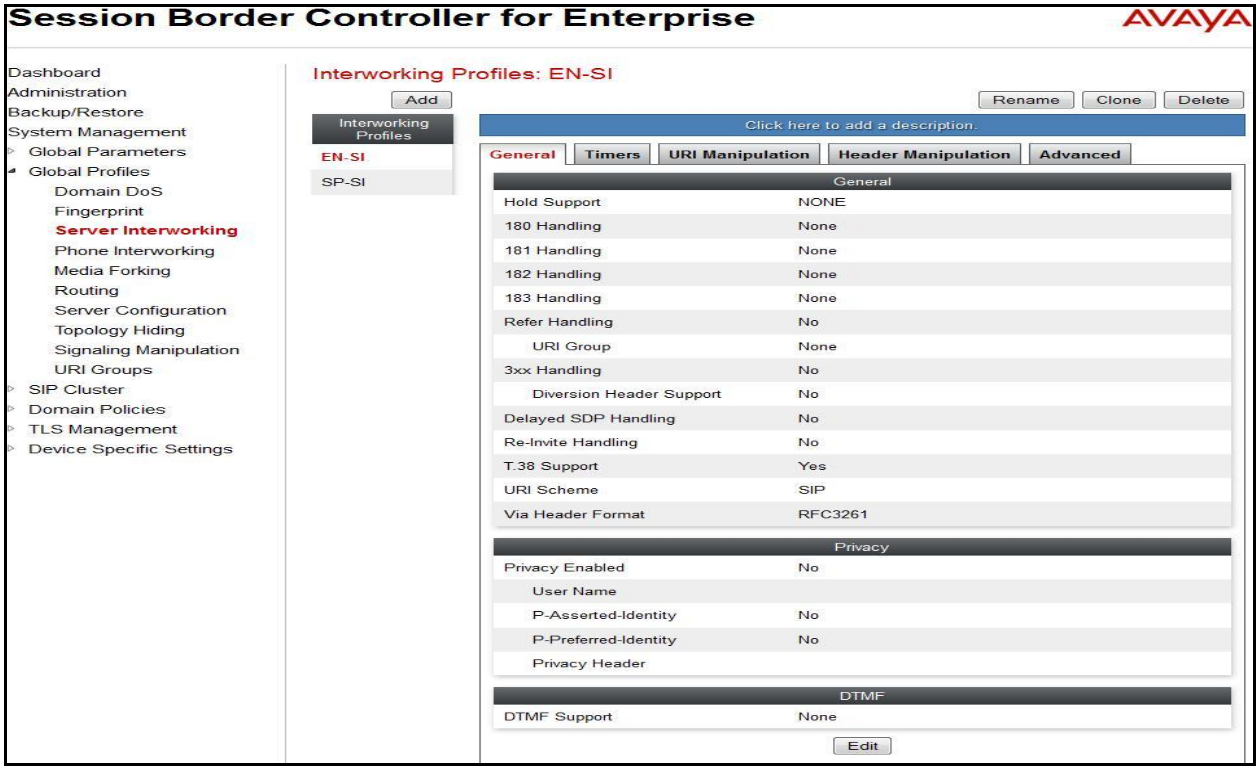
General settings:

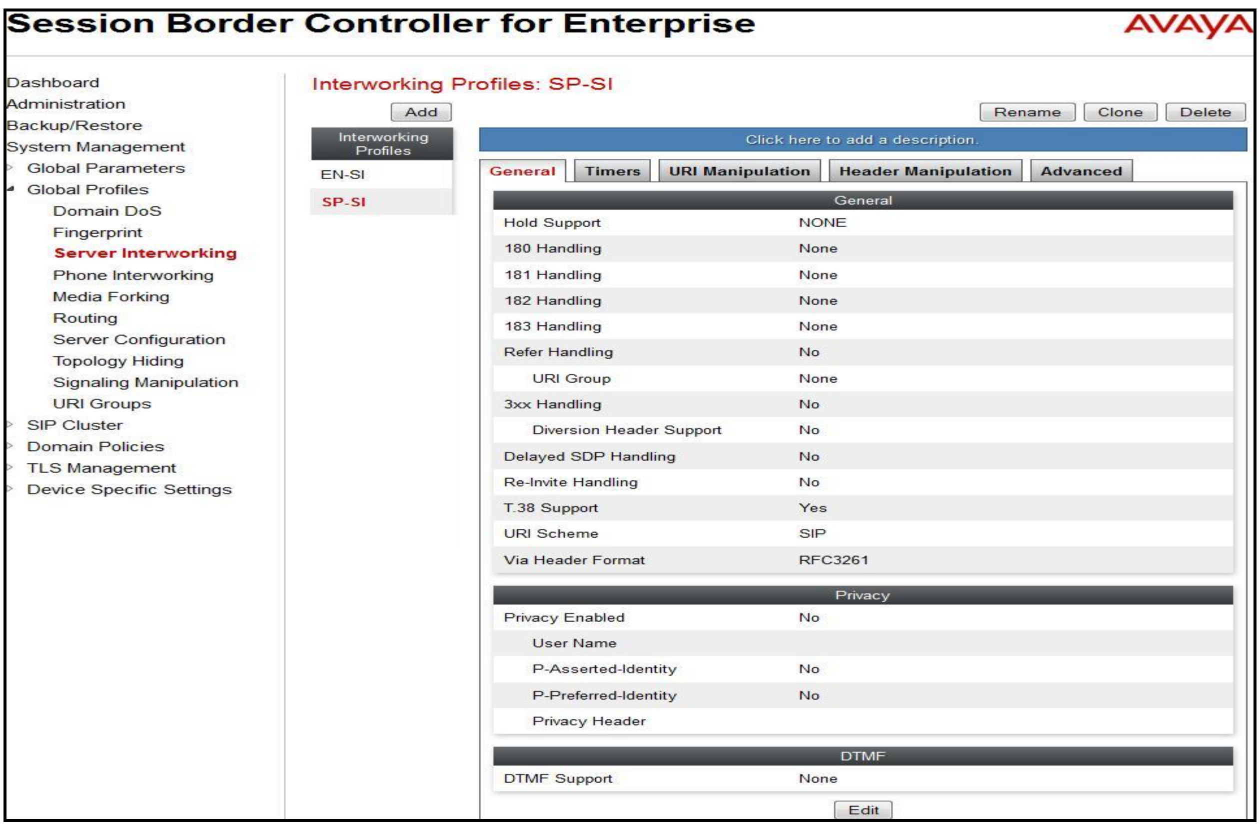
- **Hold Support** = ***None***.
- **18X Handling** = ***None***. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from MTS Allstream to Communication Manager.
- **Refer Handling** = ***No***. The Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from MTS Allstream to Communication Manager.
- **T.38 Support** = ***Yes***. MTS Allstream does support T.38 fax in the compliance testing.
- **Privacy Enabled** = ***No***. The Avaya SBCE will not mask the "From" header with anonymous for an inbound call from MTS Allstream. It depends on MTS Allstream to enable/ disable privacy on an individual call basis.
- **DTMF Support** = ***None***. The Avaya SBCE will send original DTMF method from MTS Allstream to Communication Manager.

Advanced settings:

- **Record Routes** = ***Both Sides***. The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Topology Hiding**: **Change Call-ID** = ***No***. The Avaya SBCE will modify "Call-ID" header for the call toward Communication Manager.
- **Change Max Forwards** = ***Yes***. The Avaya SBCE will adjust the original Max-Forwards value from MTS Allstream to Communication Manager by reducing the intermediate hops involving in the call flow.
- **Has Remote SBC** = ***Yes***. This setting allows the Avaya SBCE to always use the SDP received from Communication Manager for the media.

The screenshots below illustrate the Server Interworking profile **EN-SI**.





6.2.5. Server Configuration

Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat** and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

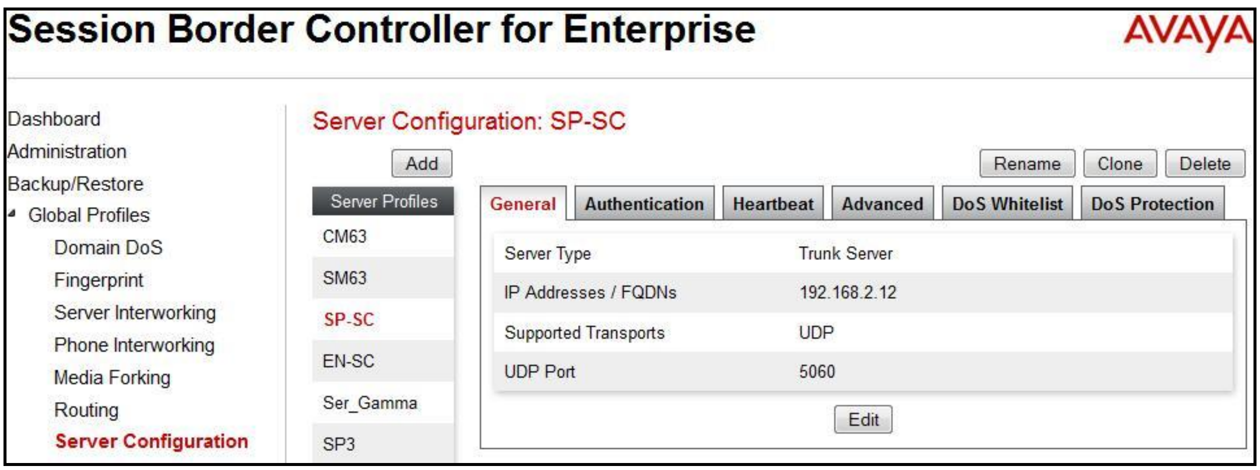
To create a Server Configuration entry, select **Global Profiles →Server Configuration**. Click on the **Add** button.

In the compliance testing, two separate Server Configurations were created, server entry **SP-SC** for MTS Allstream and server entry **EN-SC** for Communication Manager.

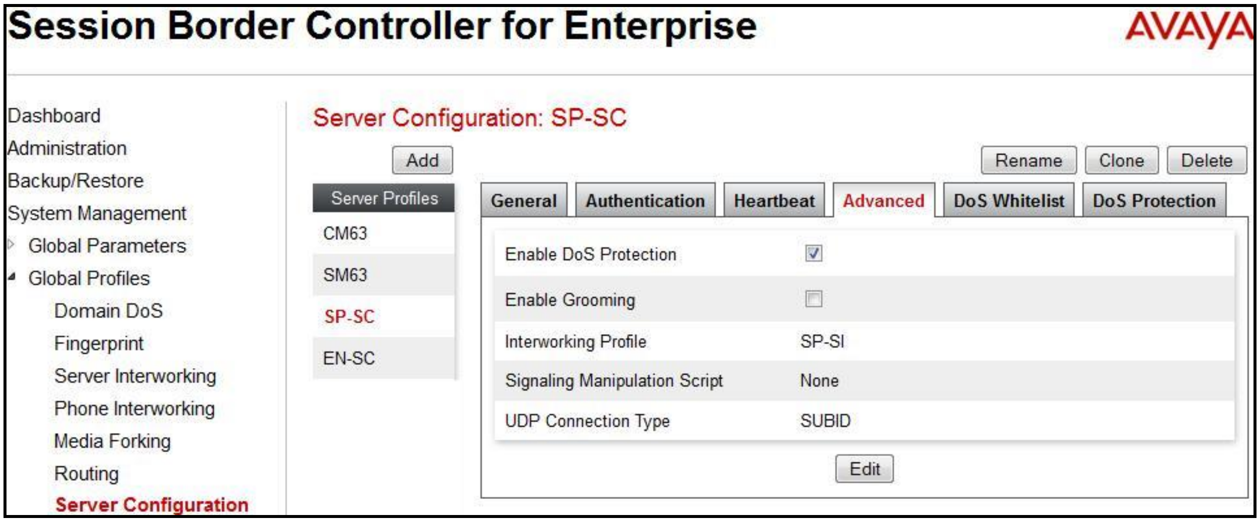
6.2.5.1 Server Configuration for MTS Allstream

Server Configuration named **SP-SC** was created for MTS Allstream. It will be discussed in detail below. **General, Authentication** and **Advanced** tabs are provisioned for MTS Allstream as they require implementation of authentication on the SIP trunk for every outbound call from enterprise to PSTN. The **Heartbeat** tab is enabled to allow the Avaya SBCE to forward the OPTIONS heartbeat from Communication Manager to MTS Allstream to query the status of the SIP trunk. The additional **DoS Whitelist** and **DoS Protection** tabs are displayed after **DoS Protection** is enabled under **Advanced** tab, the settings for these tabs are kept as default.

In the **General** tab, click on the **Edit** button then set **Server Type** for MTS Allstream as ***Trunk Server***. In the compliance testing, MTS Allstream supported ***UDP*** and listened on port ***5060***.



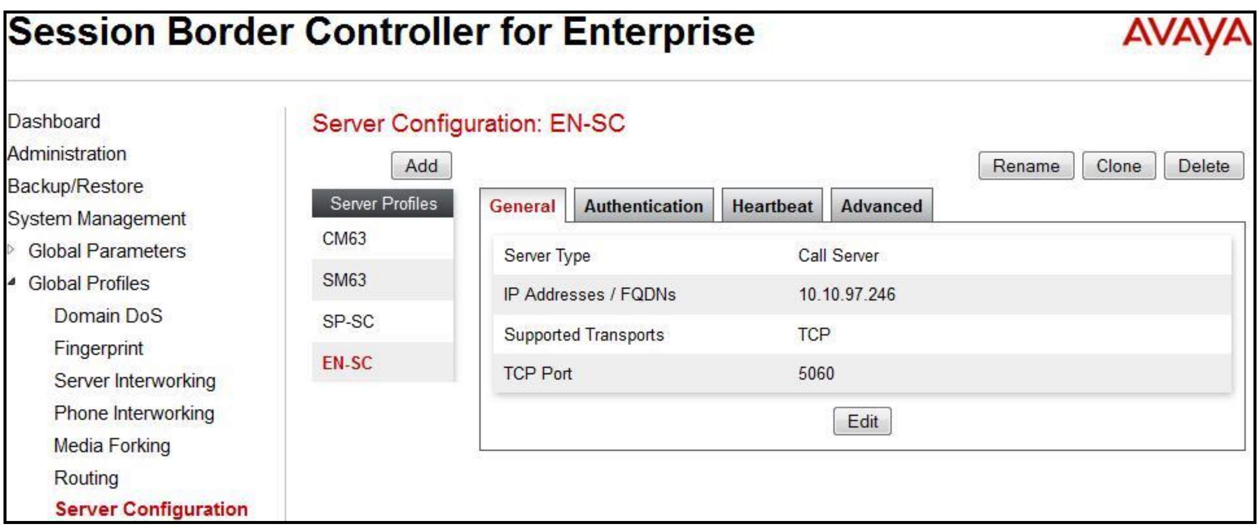
Under **Advanced** tab, check on **Enable DoS Protection**. From the **Interworking Profile** drop down list, select ***SP-SC*** as defined in **Section 6.2.4**. For **Signaling Manipulation Script**, select ***None***. This configuration applies the specific SIP profile to the MTS Allstream traffic. The other settings are kept as default.



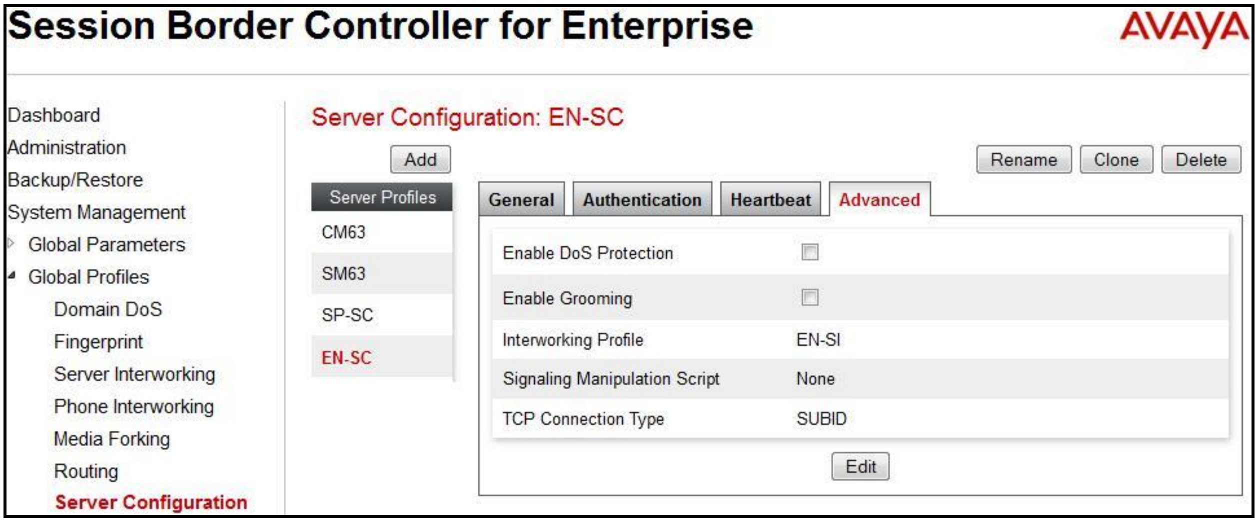
Server Configuration for Communication Manager

Server Configuration named **EN-SC** created for Communication Manager is discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from MTS Allstream to Communication Manager to query the status of the SIP trunk.

In the **General** tab, click on the **Edit** button then specify **Server Type** for Communication Manager as ***Call Server***. In the compliance testing, the link between the Avaya SBCE and Communication Manager was ***TCP*** and listened on port ***5060***.



Under **Advanced** tab, click on the **Edit** button, from the **Interworking Profile** drop down list select ***EN-SI*** as defined in **Section 6.2.4** and from the **Signaling Manipulation Script** drop down list select ***None***. The other settings are kept as default.



6.3. Domain Policies

Domain Policies configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

6.3.1. Signaling Rules

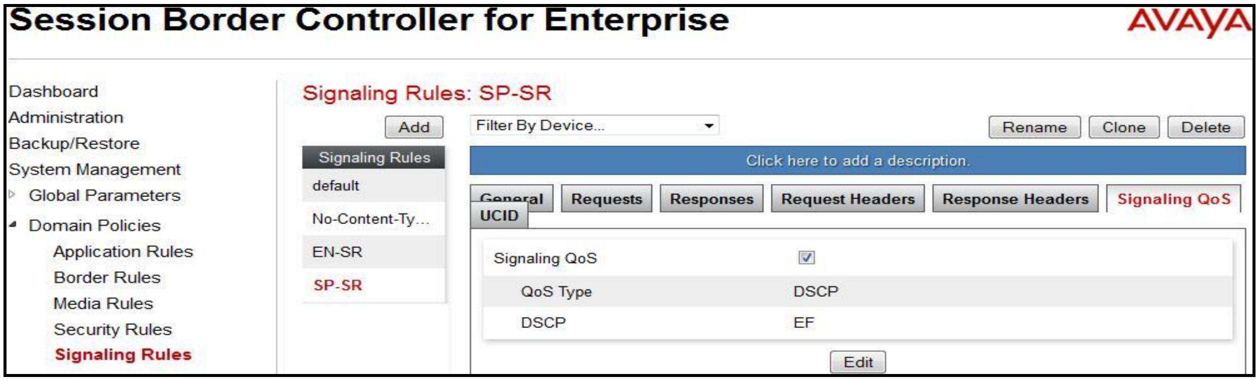
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined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

To clone a Signaling Rule, navigate to **Domain Policies → Signaling Rules**. With the **default** rule chosen, click on the **Clone** button.

6.3.1.1 Signaling Rules for MTS Allstream

In the compliance testing, signaling rule **SP-SR** is created for MTS Allstream. All the tabs are kept as default values except **Signaling QoS** tab.

In **Signaling QoS** tab, click on **Edit** button then check on **Enable** box. Then select ***EF*** value for **DSCP** option.



6.3.1.2 Signaling Rules for Communication Manager

In the compliance testing, signaling rule **EN-SR** is created for Communication Manager. All the tabs are kept as default values except **Signaling QoS** tab.

In **Signaling QoS** tab, click on **Edit** button then check on **Enable** box. Then select ***EF*** value for **DSCP** option.

6.3.2. Endpoint Policy Groups

The rules created within the **Domain Policy** section are assigned to an **Endpoint Policy Group**. The **Endpoint Policy Group** is then applied to a **Server Flow** defined in the next section.

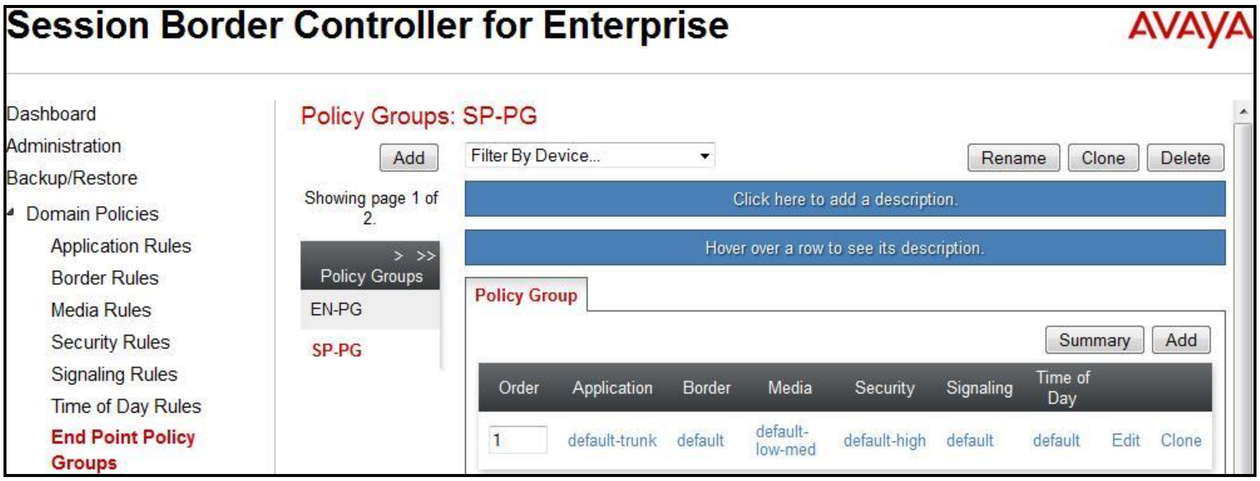
Endpoint Policy Groups were created for MTS Allstream and Communication Manager.

To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add**.

6.3.2.1 Endpoint Policy Group for MTS Allstream

The following screen shows **SP-PG** created for MTS Allstream:

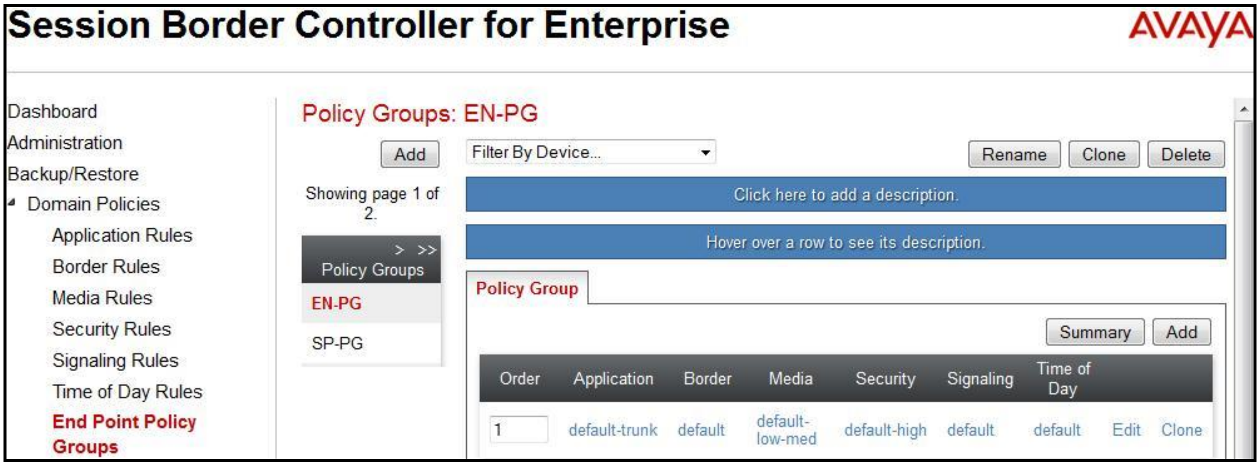
- Set Application Rule to ***default-trunk***.
- Set Border Rule to ***default***.
- Set Media Rule to ***default-low-med***.
- Set Security Rule to ***default-high***
- Set Signaling Rule to ***SP-SR*** as created in **Section 6.3.1**.
- Set Time of Day Rule to ***default***.



6.3.2.2 Endpoint Policy Group for Communication Manager

The following screen shows **EN-PG** created for Communication Manager:

- Set Application Rule to ***default-trunk***.
- Set Border Rule to ***default***.
- Set Media Rule to ***default-low-med***.
- Set Security Rule to ***default-low*.**
- Set Signaling Rule to ***EN-SR*** as created in **Section 6.3.1**.
- Set Time of Day Rule to ***default***.



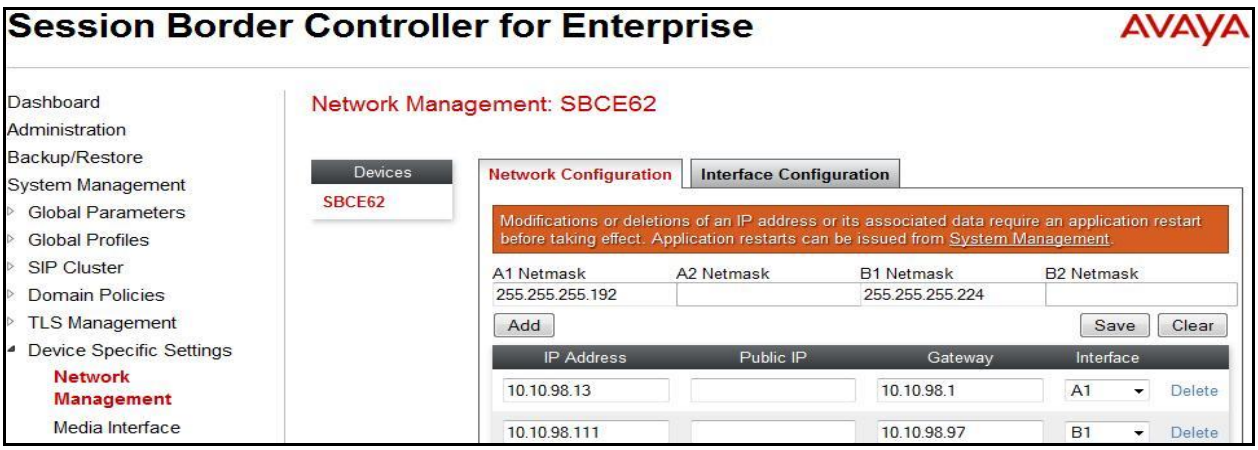
6.4. Device Specific Settings

Device Specific Settings allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

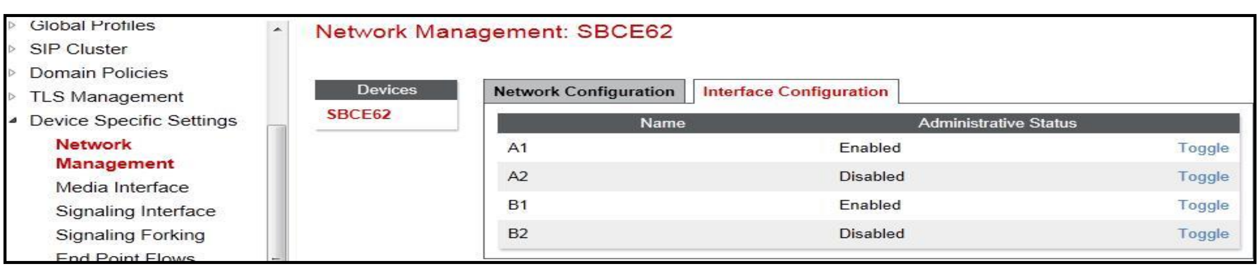
6.4.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information was defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. This information populates the **Network Management** tab, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings → Network Management** and under the **Network Configuration** tab verify the IP addresses assigned to the interfaces. The following screen shows the private interface is assigned to **A1** and the public interface is assigned to **B1**.



Enable the interfaces used to connect to the inside and outside networks on the **Interface Configuration** tab. The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface, click its **Toggle** button.

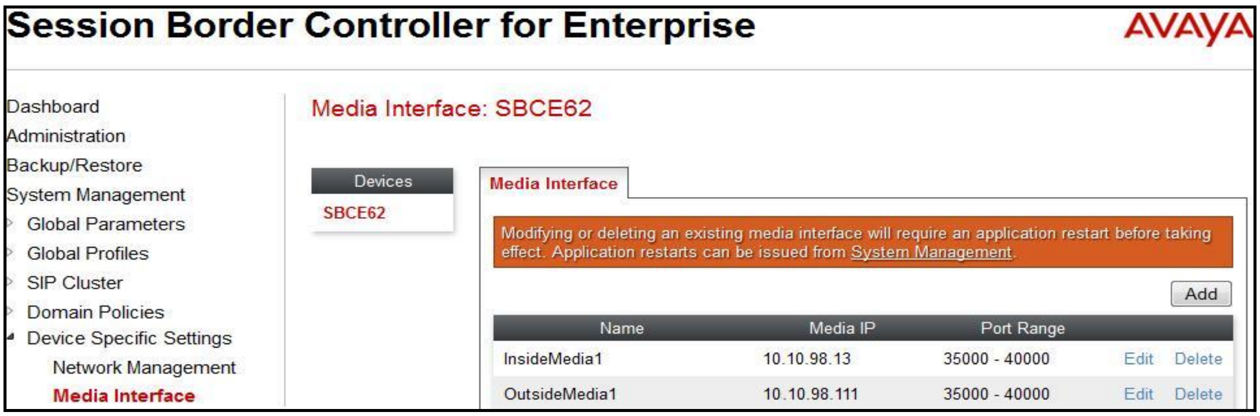


6.4.2. Media Interface

The Media Interface screen is where the media ports are defined. The Avaya SBCE will open a connection for RTP on the defined ports.

To create a new Media Interface, navigate to **Device Specific Settings → Media Interface** and click **Add**.
Separate Media Interfaces were created for both inside and outside interfaces. The following screen shows the Media Interfaces created in the compliance testing.

Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.

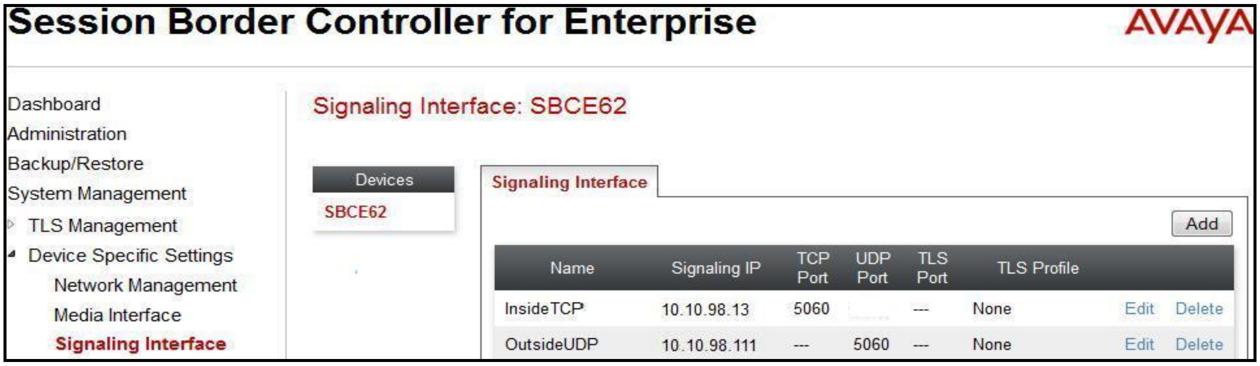


6.4.3. Signaling Interface

The Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP requests on the defined port.

To create a new Signaling Interface, navigate to **Device Specific → Settings → Signaling Interface** and click **Add**.

Separate Signaling Interfaces were created for both inside and outside interfaces. The following screen shows the Signaling Interfaces were created in the compliance testing with UDP/5060 for the outside interface to MTS Allstream and TCP/5060 for the inside interface to Communication Manager.



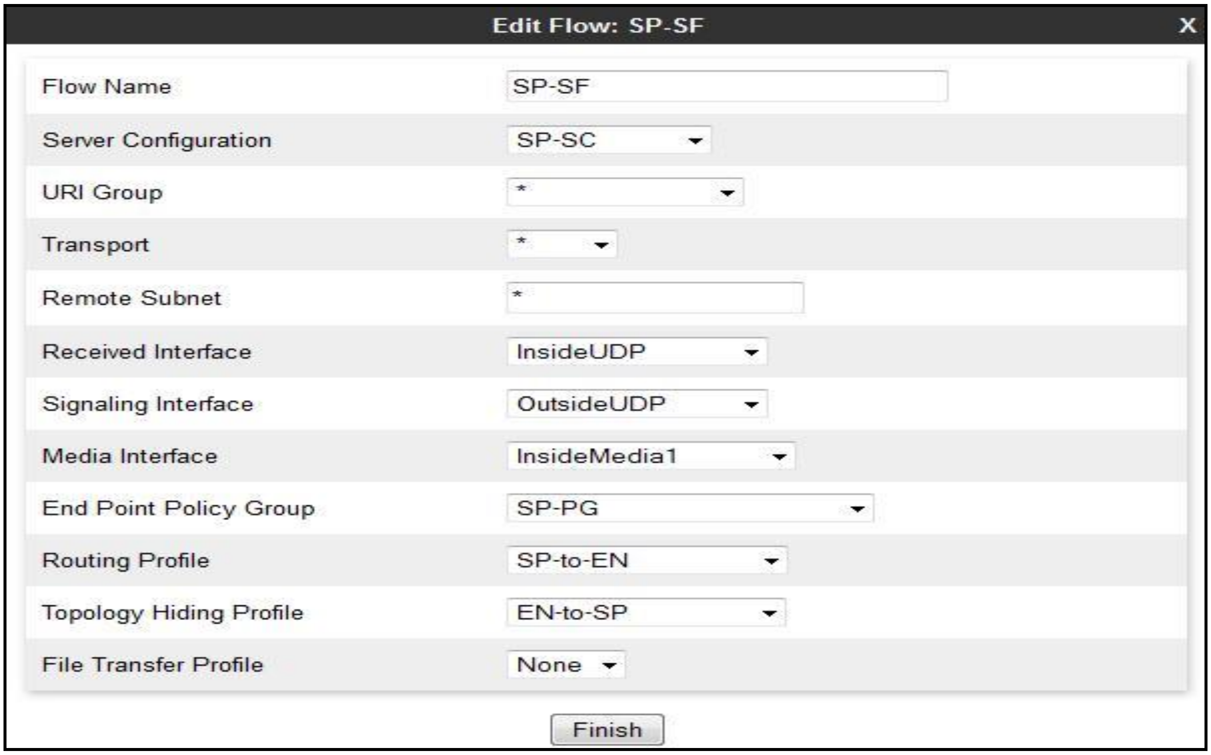
6.4.4. End Point Flows - Server Flow

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

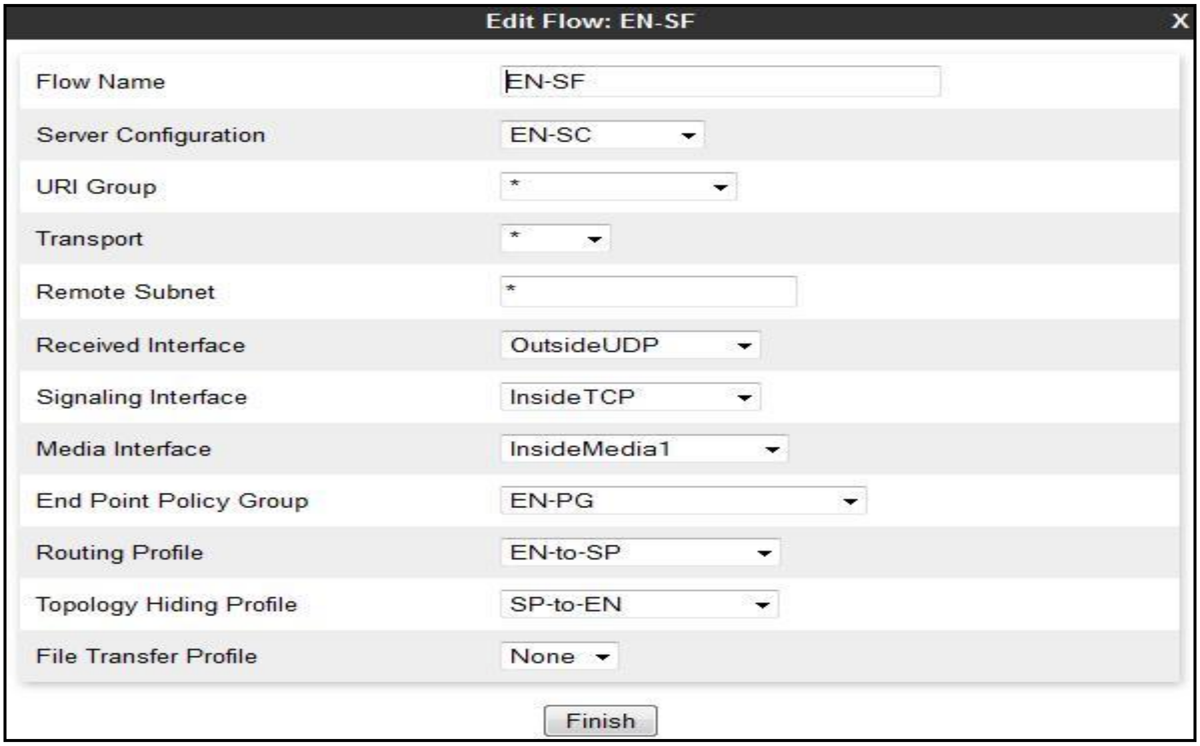
In the compliance testing, separate Server Flows were created for MTS Allstream and Communication Manager. To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown). In the new window that appears, enter the following values. The other fields are kept default.

- **Flow Name**: Enter a descriptive name.
- **Server Configuration**: Select a Server Configuration created in **Section 6.2.5** to assign to the Flow.
- **URI Group**: Select the URI Group created in **Section 6.2.1** to assign to the Flow. **Note**: URI Group can be set to “*” to match all calls.
- **Received Interface**: Select the Signaling Interface created in **Section 6.4.3** that the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface**: Select the Signaling Interface created in **Section 6.4.3** used to communicate with the Server Configuration.
- **Media Interface**: Select the Media Interface created in **Section 6.4.2** used to communicate with the Server Configuration.
- **End Point Policy Group**: Select the End Point Policy Group created in **Section 6.3.2** to assign to the Server Configuration.
- **Routing Profile**: Select the Routing Profile created in **Section 6.2.2** that the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile**: Select the Topology-Hiding profile created in **Section 6.2.3** to apply to the Server Configuration.
- Click **Finish**.

The following screen shows the Server Flow **SP-SF** configured for MTS Allstream.



Similarly, the following screen shows the Server Flow **EN-SF** configured for Communication Manager.



7. MTS Allstream SIP Trunking Service Configuration

MTS Allstream is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise side. MTS Allstream will provide the customer with the necessary information to configure the SIP connection from the enterprise to MTS Allstream. The information provided by MTS Allstream includes:

- IP address and port number used for signaling through security devices (if any).
- IP address and port number used for media through security devices (if any).
- MTS Allstream SIP domain. In the compliance testing, MTS Allstream preferred to use IP address as an URI-Host.
- CPE SIP domain. In the compliance testing, MTS Allstream preferred to use IP address of the Avaya SBCE as an URI-Host.
- Supported codecs.
- DID numbers.

The sample configuration between MTS Allstream and the enterprise for the compliance testing is a static configuration. There is no registration on the SIP trunk implemented on either MTS Allstream or enterprise side.

8. Verification and Troubleshooting

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

8.1. Verification Steps

- Verify that endpoints at the enterprise site can place call to PSTN and that the call remains active for more than 35 seconds. This time period is included to satisfy SIP protocol timers.
- Verify that endpoints at the enterprise site can receive call from PSTN and that the call can remain active for more than 35 seconds. This time period is included satisfy SIP protocol timers.
- Verify that the user on PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

8.2. Protocol Traces

The following SIP headers are inspected using Wireshark trace analysis:

- Request-URI: verify the called party number and SIP domain.
- From: verify the calling party name and number.
- To: verify the called party name and number.
- P-Asserted-Identity: verify the calling party name and number.
- Privacy: verify the value "user" and/or "id" presents the private call scenario.

The following attributes in SIP message body are inspected using Wireshark trace analysis:

- Connection Information (c line): verify IP address of near end and far end endpoints.
- Time Description (t line): verify session timeout value of near end and far end endpoints.
- Media Description (m line): verify audio port, codec, DTMF event description.
- Media Attribute (a line): verify specific audio port, codec, ptime, send/ receive ability, DTMF event and fax attributes.

8.3. Troubleshooting:

8.3.1. The Avaya SBCE

Use a network sniffing tool (e.g., Wireshark) to monitor the SIP signaling messages between MTS Allstream and the Avaya SBCE.

Following is an example inbound call from MTS Allstream to the enterprise.

- Inbound INVITE request from MTS Allstream:

```
INVITE sip:6477761252@10.10.98.111;user=phone SIP/2.0
Max-Forwards: 69
Session-Expires: 3600;refresher=uac
Min-SE: 600
Supported: timer, 100rel
To: <sip:6477761252@10.10.98.111;user=phone>
From: <sip:01116139675203@192.168.2.12>;tag=3617979799-442929
Call-ID: 196907-3617979799-442919@nextone-msw-lab-3.mtsallstream.com
CSeq: 1 INVITE
Allow: CANCEL, ACK, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE,
PRACK, UPDATE, MESSAGE, PUBLISH
Via: SIP/2.0/UDP 192.168.2.12:5060;branch=z9hG4bK48795716c366b51f8e5df87c6e69df95
Contact: <sip:01116139675203@192.168.2.12:5060;tgrp=TOROONSBCIOT1>
Content-Type: application/sdp
```

```
Accept: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 517947116 517947116 IN IP4 192.168.2.12
s=sip call
c=IN IP4 192.168.2.13
t=0 0
m=audio 20252 RTP/AVP 18 0 8 101
a=ptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

- 200OK/SDP response by the enterprise:

```
SIP/2.0 200 OK
From: <sip:01116139675203@192.168.2.12>;tag=3617979799-442929
To: <sip:6477761252@10.10.98.111;user=phone>;tag=80d493e5582de41287b53d958fc00
CSeq: 1 INVITE
Call-ID: 196907-3617979799-442919@nextone-msw-lab-3.mtsallstream.com
Contact: "H323 1131" <sip:6477761252@10.10.98.111:5060;transport=udp>
Record-Route: <sip:10.10.98.111:5060;ipcs-line=34034;lr;transport=udp>
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH,UPDATE
Supported: 100rel,join,replaces,sdp-anat,timer
Via: SIP/2.0/UDP 192.168.2.12:5060;branch=z9hG4bK48795716c366b51f8e5df87c6e69df95
Accept-Language: en
Require: timer
Server: Avaya CM/R016x.03.0.124.0
P-Asserted-Identity: "H323 1131" <sip:6477761252@10.10.98.111>
Session-Expires: 3600;refresher=uac
Content-Type: application/sdp
Content-Length: 173

v=0
o=- 1409010059 2 IN IP4 10.10.98.13
s=-
c=IN IP4 10.10.98.13
b=AS:64
t=0 0
m=audio 35786 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

Following is an example outbound call from the enterprise to MTS Allstream.

- Outbound INVITE request from the enterprise:

```
INVITE sip:6139675203@192.168.2.12 SIP/2.0
From: "H323 1131" <sip:6477761252@10.10.98.111>;tag=052f325592de412e7b53d958fc00
To: <sip:6139675203@192.168.2.12>
CSeq: 1 INVITE
Call-ID: 636cf24c613eed6decf5ef2814de5f0a
Contact: "H323 1131" <sip:6477761252@10.10.98.111:5060>
Record-Route: <sip:10.10.98.111:5060;ipcs-line=34046;lr;transport=udp>
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH,UPDATE
Supported: 100rel,join,replaces,sdp-anat,timer
User-Agent: Avaya CM/R016x.03.0.124.0
Max-Forwards: 70
Via: SIP/2.0/UDP 10.10.98.111:5060;branch=z9hG4bK-s1632-000875357799-1--s1632-
Accept-Language: en
Alert-Info: <cid:internal@bvwlab.com>;avaya-cm-alert-type=internal
P-Asserted-Identity: "H323 1131" <sip:6477761252@10.10.98.111>
Session-Expires: 1200;refresher=uac
Min-SE: 1200
Content-Type: application/sdp
Content-Length: 255

v=0
o=- 1409010166 1 IN IP4 10.10.98.13
s=-
c=IN IP4 10.10.98.13
b=AS:64
t=0 0
a=avf:avc=n prio=n
a=csup:avf-v0
m=audio 35788 RTP/AVP 0 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
```

- 200OK/SDP response by MTS Allstream:

```
SIP/2.0 200 OK
Session-Expires: 1200;refresher=uac
Require: timer
Via: SIP/2.0/UDP 10.10.98.111:5060;branch=z9hG4bK-s1632-000875357799-1--s1632-
Record-Route: <sip:10.10.98.111:5060;ipcs-line=34046;lr;transport=udp>
To: <sip:6139675203@192.168.2.12>;tag=3617979909-38479
From: "H323 1131" <sip:6477761252@10.10.98.111>;tag=052f325592de412e7b53d958fc00
Call-ID: 636cf24c613eed6decf5ef2814de5f0a
CSeq: 1 INVITE
Allow: CANCEL, ACK, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE,
PRACK, UPDATE, MESSAGE, PUBLISH
Contact: <sip:6139675203@192.168.2.12:5060>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 208

v=0
o=nextone-msw-lab-3 241838807 241838807 IN IP4 192.168.2.12
s=sip call
c=IN IP4 192.168.2.13
t=0 0
m=audio 20354 RTP/AVP 0 18 101
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=ptime:20
```

8.3.2. Communication Manager

- **list trace station** <extension number>. Traces call to and from a specific station.
- **list trace tac** <trunk access code number>. Trace call 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.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2 to MTS Allstream SIP Trunking Service. MTS Allstream SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large the enterprises. MTS Allstream SIP Trunking Service provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The MTS Allstream SIP Trunking Service is considered **compliant** with Avaya Aura® Communication Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2.

10. References

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

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.2.2, December 2012.

[2] *Administering Avaya Aura® System Platform*, Release 6.2.2, December 2012.

[3] *Administering Avaya Aura® Communication Manager, Document ID 03-300509,* Release 6.3, Issue 8, May 2013.

[4] *Programming Call Vectoring Features in Avaya Aura® Call Center Elite*, Release 6.3, Issue 1, May 2013.

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

[6] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide* , Document Number 16-601944 Release 2.*6*, June 2010.

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

[8] *Using Avaya one-X® Communicator*, April 2011.

[9] *Avaya SBCE Install Guide (*102-5224-400v1.01*)*

[10] *Avaya SBCE Administration Guide (*010-5423-400v106*)*

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

[12] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, http://www.ietf.org/

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

[14] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013

[15] *Avaya Session Border Controller for Enterprise Overview and Specification*, Issue 2, March 2013

Product documentation for MTS Allstream SIP Trunking Service is available from MTS Allstream.

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.