Avaya Solution & Interoperability Test Lab

Application Notes for Bell Canada SIP Trunking Service with Avaya Aura® Communication Manager Release 6.3, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.3 – Issue 1.0

Abstract

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

Bell Canada 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.

Table of Contents

1. Introduction

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

Customers using this Avaya SIP-enabled enterprise solution with Bell 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.

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

2.1. Interoperability Compliance Testing

To verify Bell interoperability, the following features and functionalities are covered in the compliance testing:

- Inbound PSTN calls to various phone types including H.323, SIP, 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, SIP, 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, 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.
- 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.

Item that is supported but not tested includes the following:

- Inbound toll-free.

Items that are not supported include the following:

- Incoming call redirection after answer of incoming VDN calls using REFER method is not supported.
- Call redirection (consultative/blind transfer) using REFER is not supported.
- Fax T.38 is not supported.

2.2. Test Results

Interoperability testing of Bell with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the exception of the observations and limitations described below:.

- **SIP Options** - Bell was configured to send SIP OPTIONS messages with Max-Forwards header with value equal to 0. This was by design from Bell. Avaya SBCE responded correctly with 483 Too Many Hops. However, Bell would accept this and keep the trunk up.
- **Outbound Calls with "+" -** Bell does not accept "+" in front of 10 digit in the From, To, Contact and P-Asserted-Identity headers. Signaling Manipulation script was used to remove the "+" sign.
- **Route header –** This header was proprietary from Bell in all SIP signaling messages. Signaling Manipulation script was used to remove this header.
- **Outbound Calls Required Leading "1" –** Bell system was configured incorrectly to require enterprise system to add "1" in front of 10 digits in the To header. Communication Manager was configured to accommodate this issue. Bell production system will not see this issue.
- **Network Call Redirection (Blind/Consultative Transfer) with "REFER" -** Communication Manager sent a "REFER" SIP message to redirect the call to off net PSTN transfer target, Bell Canada responded with a 202 Accepted. There is no NOTIFY message. From Avaya Enterprise system perspective, the call is completed and the transfer is successful. But the call between the 2 PSTN phones (Transferee and Transfer target) is failed, call dropped. Bell does not have a solution for this interoperability issue. Therefore the blind and consultative transfers using REFER method are not supported on Bell SIP trunking services.
- **Calling Party Name Display Blocked –** Bell specification required for **user=phone** be presented in **From** header for every call scenarios. Using Communication Server trunk

group to set up “Mark Users as Phone” parameter to “y” would satisfy this condition. However, there were other headers, that included **user=phone**, such as; **Contact** and **To**. These were violating Bell specification. Therefore, using signaling manipulated script to remove **user=phone** instances from **Contact** and **To** headers was required.

2.3. Support

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

For technical support on Bell Canada SIP Trunking, contact Bell Canada at http://www.bell.ca/enterprise/EntPrd_SIP_Trunking.page.

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to the Bell (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 Server running Avaya Aura® Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Avaya Aura® System Manager
- Avaya S8800 Server running Avaya Aura® Session Manager
- Avaya S8800 Server running Avaya Aura® Messaging
- Avaya Session Border Controller for Enterprise
- Avaya 9600Series IP Deskphones (H.323, SIP)
- Avaya one-X® Communicator soft phones (H.323, SIP)
- 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 Bell 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 Bell across the public network is UDP. The transport protocol between the Avaya SBCE, Session Manager and Communication Manager is TCP.

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

In this configuration, Avaya SBCE on enterprise side is configured to periodically perform OPTIONs ping to Bell system. Also outbound calls from enterprise Communication Manager to PSTN will be required authentication with Bell system.

Additionally, external interface of Avaya SBCE is connecting to Bell’s load balancer over the internet for outbound call from the enterprise to PSTN via single IP address. For inbound from PSTN to enterprise, calls will coming in to enterprise via two IP addresses as shown in **Figure 1**.

For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

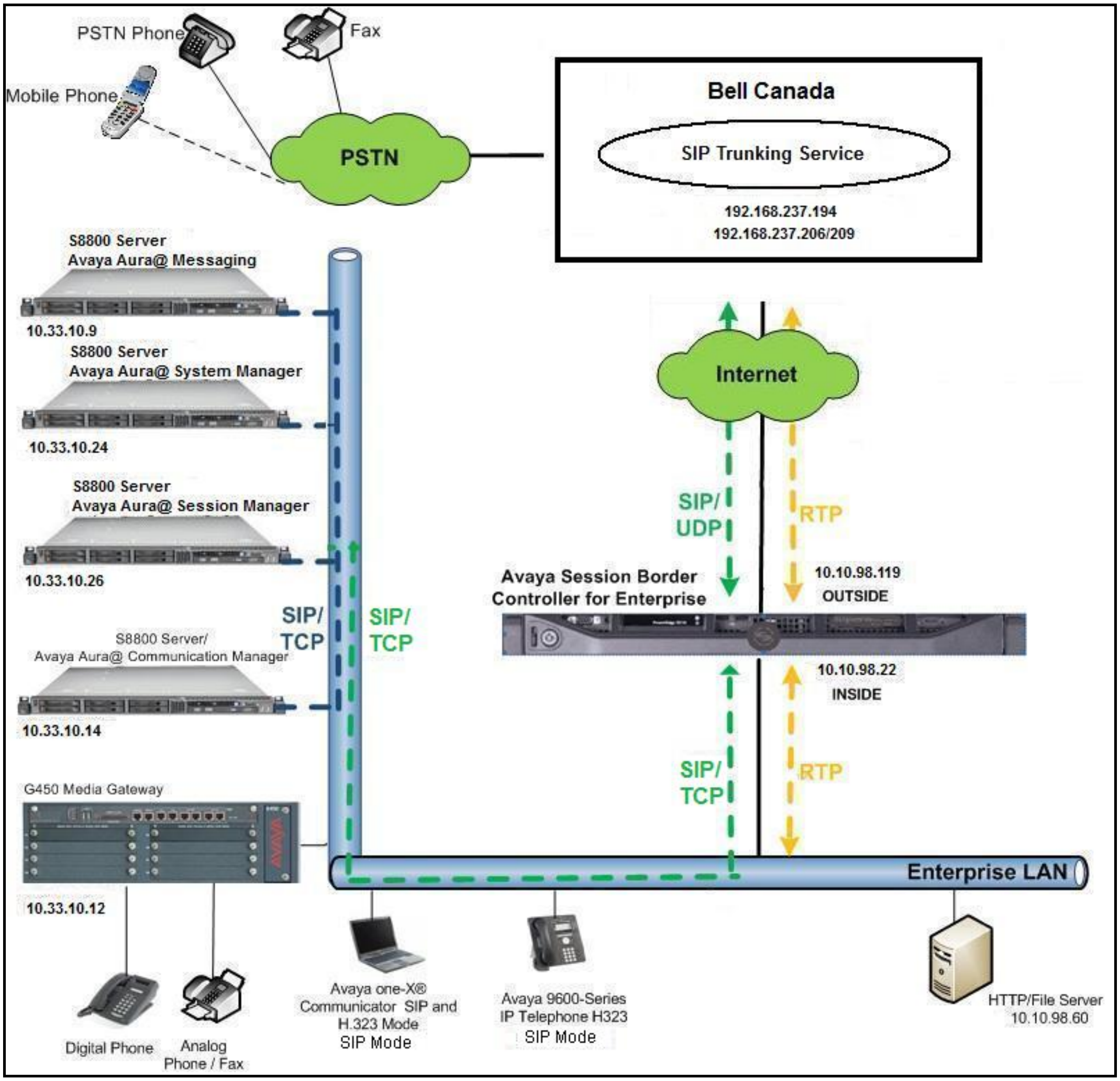


Figure 1: Avaya IP Telephony Network connecting to Bell Networks

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 (CM: R016x.03.0.124 Patch 21460)
Avaya G450 Media Gateway	35.8.0
Avaya Aura® System Manager running on an Avaya S8800 Server	6.3.9 (Build No 6.3.9.1.2.538)
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.3.7 (6.3.7.0.637008)
Avaya Aura® Messaging running on an Avaya S8800 Server	6.2 SP2
Avaya Session Border Controller for Enterprise	6.3
Avaya 9650C IP Deskphone (H.323)	Avaya one-X® Deskphone Edition S3.220A
Avaya 9630G IP Deskphone (SIP)	Avaya one-X® Deskphone Edition 6.4.0.33
Avaya one-X Communicator (H.323/SIP)	6.2.3.05-FP3
Avaya 1408 Digital Telephone	1400R10
Avaya 6210 Analog Telephone	n/a
Bell SIP Trunking Service Components	
Component	Release
F5 Load Balancer	11
Oracle ACME Packet Net-Net 4500	6.3.7 MR-3 Patch 1
BroadSoft Broadworks	18
Legacy Nortel CS2K Media Gateway	SN10 PVG/IW-SPM

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.

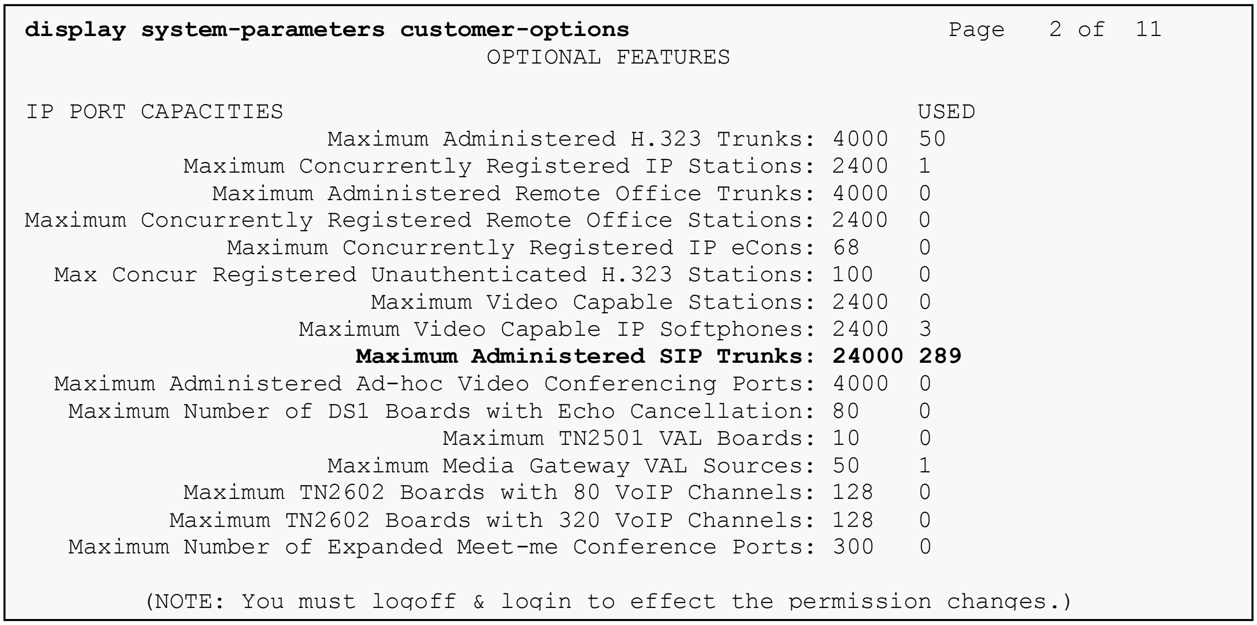
5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for Bell. 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 Session Manager (**SM**). 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
SM                  10.33.10.26
default             0.0.0.0
procr               10.33.10.14
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. One Source 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 ***T.38-G711-fallback*** faxing which Bell supported G.711 fax.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

                 Mode                Redundancy
    FAX          t.38-G711-fallback  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 ***avayalab.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: avayalab.com
    Name: ToSM
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/SIP phones, Session Manager 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                                                                   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.

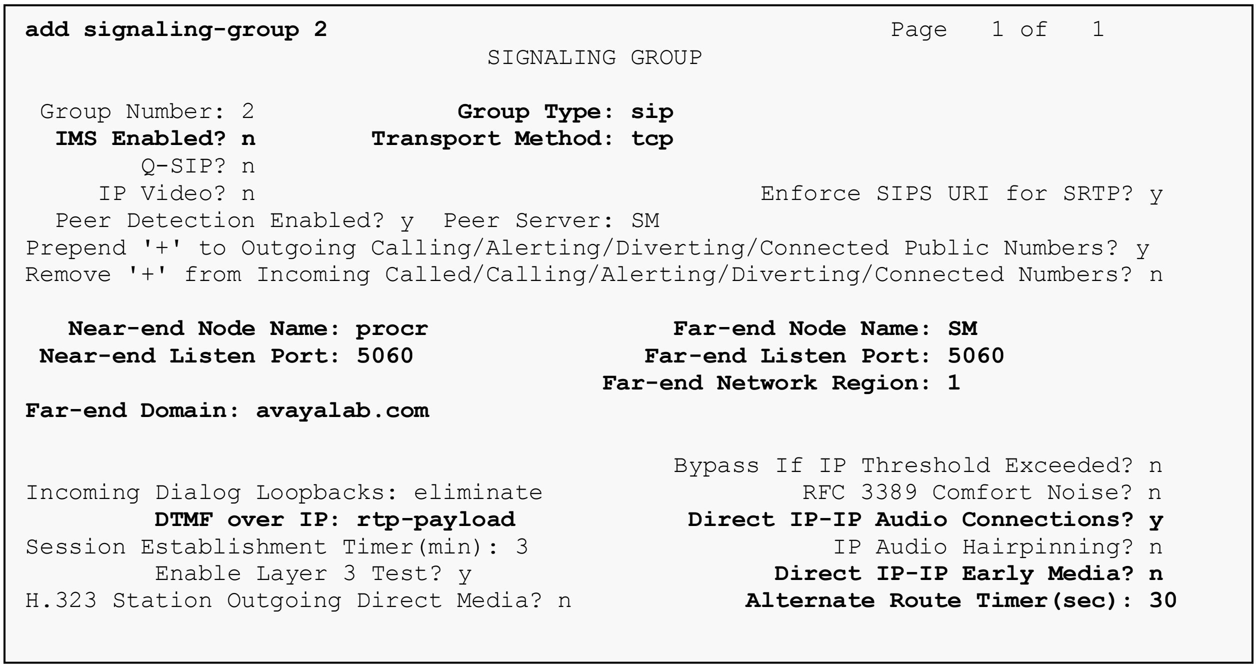
```
change media-gateway 1                                          Page   1 of   2
                             MEDIA GATEWAY 1

                    Type: g450
                    Name: SPMGC
               Serial No: 12N517873797
            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 Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group ***2*** was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***.
- Set the **Transport Method** to ***tcp.*** The transport method specified here is used between Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to ***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 ***SM***. 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 ***avayalab.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 Session Manager 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 2                                       Page   1 of   1
                                SIGNALING GROUP

 Group Number: 2              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: SM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1
Far-end Domain: avayalab.com

                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     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 ***2*** was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available Trunk Access Code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **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 2                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 2                    Group Type: sip           CDR Reports: y
  Group Name: SP Trunk                    COR: 1        TN: 1        TAC: #02
   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: 2
                                                     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 2                                          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 ***public***. 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” headers. The addition of the + sign impacted interoperability with the service provider. Thus, the **Numbering Format** is set to ***public*** and the **Numbering Format** in the route pattern is set to ***pub-unk*** (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 2                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y

                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

                    Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```

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

- Set **Mark Users as Phone** to ***y*** as Bell specification requires ***user=phone*** including in From, PAI and Diversion headers**.**
- 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 INVITE from the enterprise.
- Set the **Telephone Event Payload Type** to ***101***.

```
add trunk-group 2                                            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 public numbering is selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the service provider. They are used to authenticate the caller.

The screen below shows a subset of the 10 digits DID numbers assigned for testing. These 3 numbers were mapped to the 3 enterprise extensions 60396, 60397 and 60398. 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 public-unknown-numbering 0                               Page   1 of   2
                           NUMBERING - PUBLIC/UNKNOWN FORMAT

Ext Ext                Trk        CPN               Total
Len Code               Grp(s)     Prefix            Len
 5  60396              2         613XXX6506       10       Total Administered: 3
 5  60397              2         613XXX6507       10          Maximum Entries: 540
 5  60398              2         613XXX6508       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 Bell 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  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 613XXX6506       10  60396
 public-ntwrk    10 613XXX6507       10  60397
 public-ntwrk    10 613XXX6508       10  60398
……
```

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**.

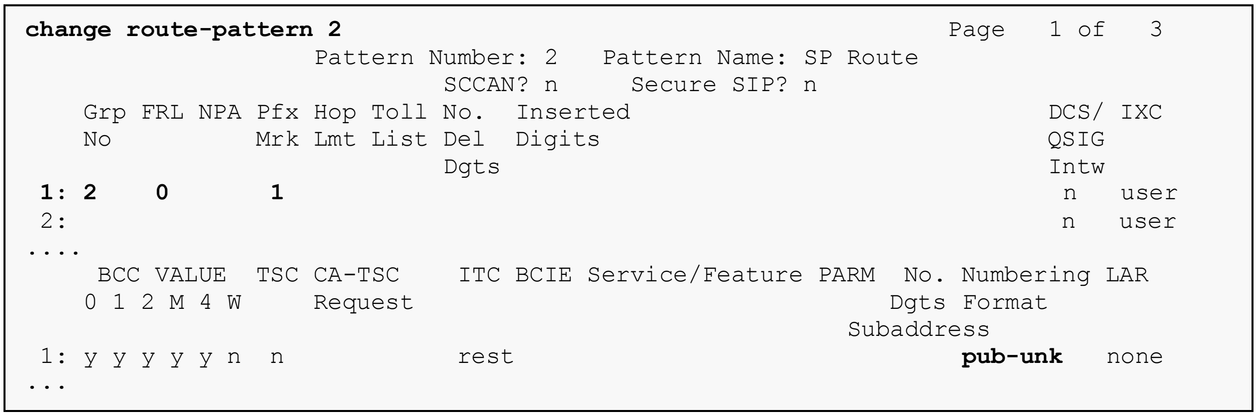
```
change feature-access-codes                                   Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *05
                       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 ***2*** 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    2        op           n
    011                   10   18    2        intl         n
    1                     11   11    2        pubu         n
    300                   10   10    2        pubu         n
    411                   3    3     2        svcl         n
    613                   10   10    2        pubu         n
    866                   10   10    2        pubu         n
    911                   3    3     2        svcl         n
    512                   10   10    2        pubu         n
```

As 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 ***2*** 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 ***2*** was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.
- **Numbering Format**: **pub-unk** All calls using this route pattern will use the public numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.8**.



```
change route-pattern 2                                          Page   1 of   3
                    Pattern Number: 2   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: 2    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                               pub-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 Aura® Session Manager

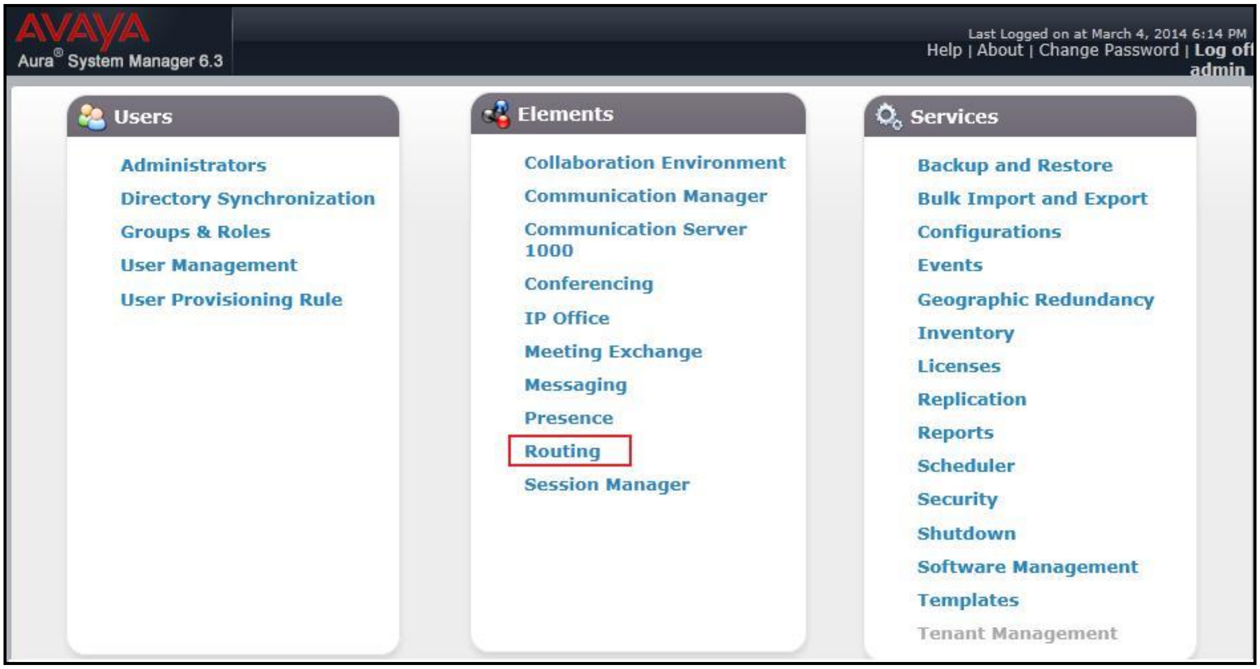
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be used by SIP Entities
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Session Manager server to be managed by System Manager

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

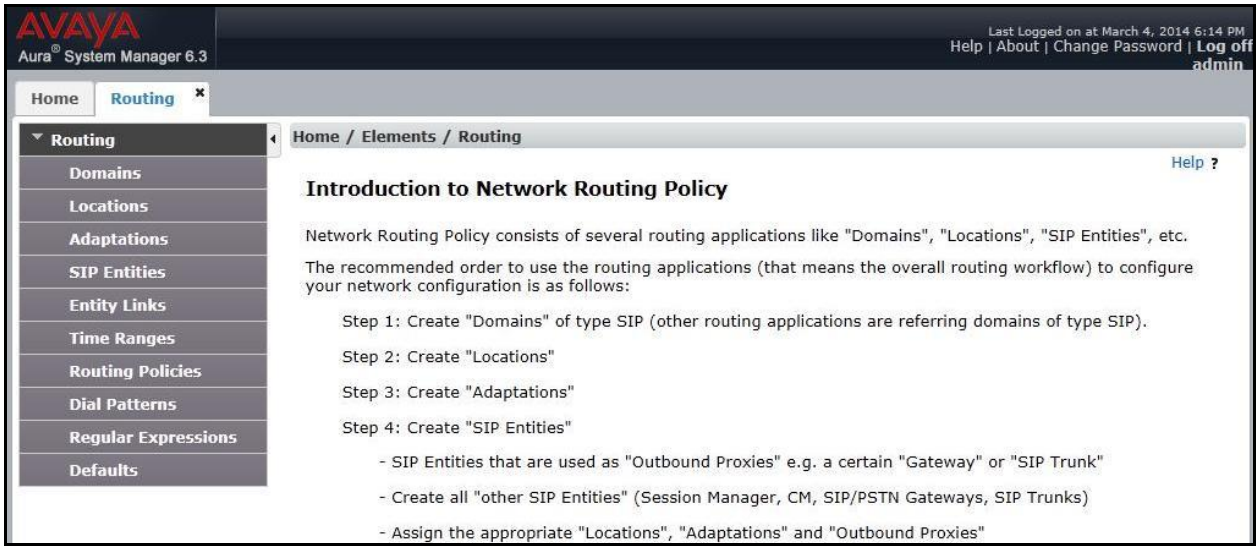
6.1. System Manager Login and Navigation

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



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

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



Introduction to Network Routing Policy

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

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

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

Step 2: Create "Locations"

Step 3: Create "Adaptations"

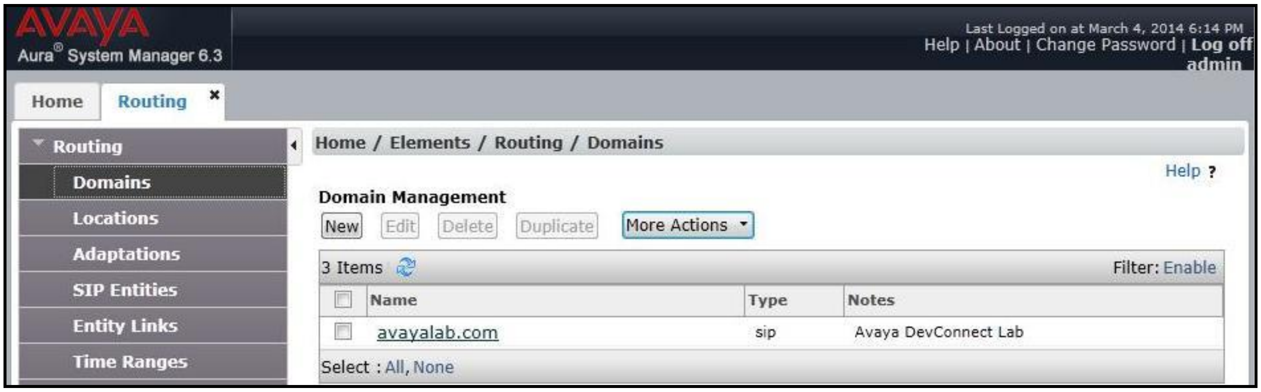
Step 4: Create "SIP Entities"

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

6.2. Specify SIP Domain

To view or change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button (not shown) after changes are completed.

The following screen shows the list of configured SIP domains. The domain “avayalab.com” was already created for communication between Session Manager and Communication Manager. The domain “avayalab.com” is not known to Bell. It will be adapted by the Avaya SBCE to IP address based URI-Host to meet the SIP specification of Bell system.



Domain Management

3 Items

□	Name	Type	Notes
□	avayalab.com	sip	Avaya DevConnect Lab

6.3. Add Location

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

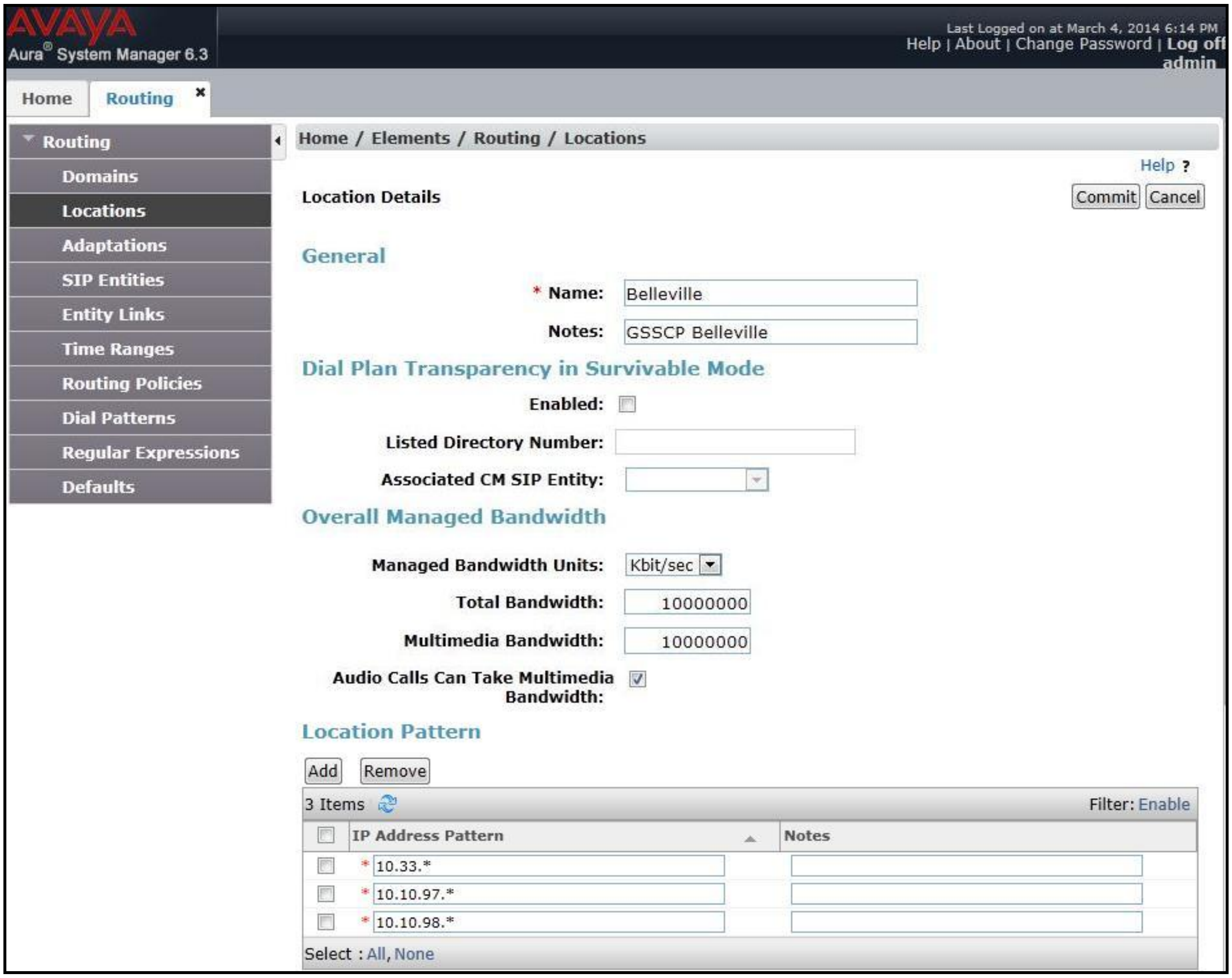
In **General** section, enter the following values:

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

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

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

Displayed below are the screenshots for location ***Belleville***, which includes all equipment on the ***10.33.x, 10.10.98.x*** and ***10.10.97.x*** subnet including Communication Manager, Session Manager and Avaya SBCE. Click **Commit** to save.



Home / Elements / Routing / Locations

Location Details

General

* Name: Belleville

Notes: GSSCP Belleville

Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 10000000

Multimedia Bandwidth: 10000000

Audio Calls Can Take Multimedia Bandwidth: ☑

Location Pattern

3 Items

□	IP Address Pattern	Notes
□	* 10.33.*	
□	* 10.10.97.*	
□	* 10.10.98.*	

6.4. Add SIP Entities

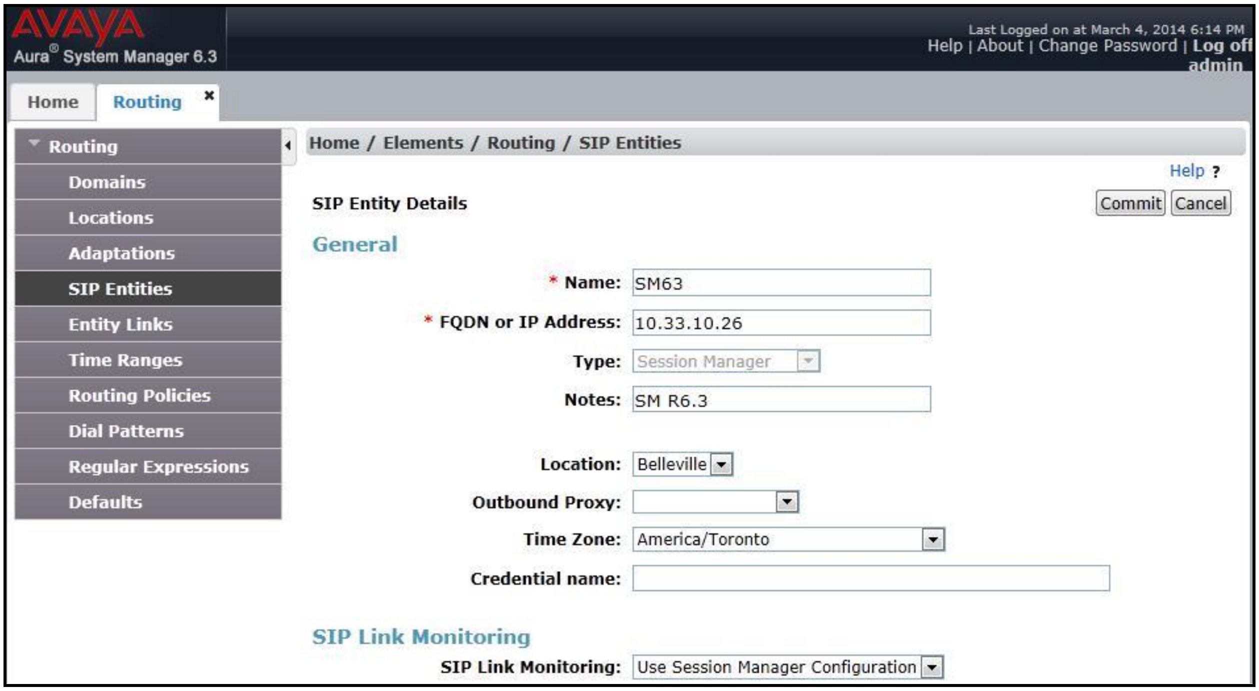
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes Communication Manager and Avaya SBCE.

To add a new SIP Entity, navigate to **Routing → SIP Entities** in the left navigation pane and click **New** button in the right pane (not shown).

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

- **Name**: Enter a descriptive name.
- **FQDN or IP Address**: Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select ***Session Manager*** for Session Manager, ***CM*** for Communication Manager and ***Other*** for the Avaya SBCE.
- **Location:** Select one of the locations defined in **Section** Error! Reference source not found..
- **Time Zone**: Select the time zone for the location above.

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



SIP Entity Details

General

* Name:	SM63
* FQDN or IP Address:	10.33.10.26
Type:	Session Manager
Notes:	SM R6.3
Location:	Belleville
Outbound Proxy:	
Time Zone:	America/Toronto
Credential name:	

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

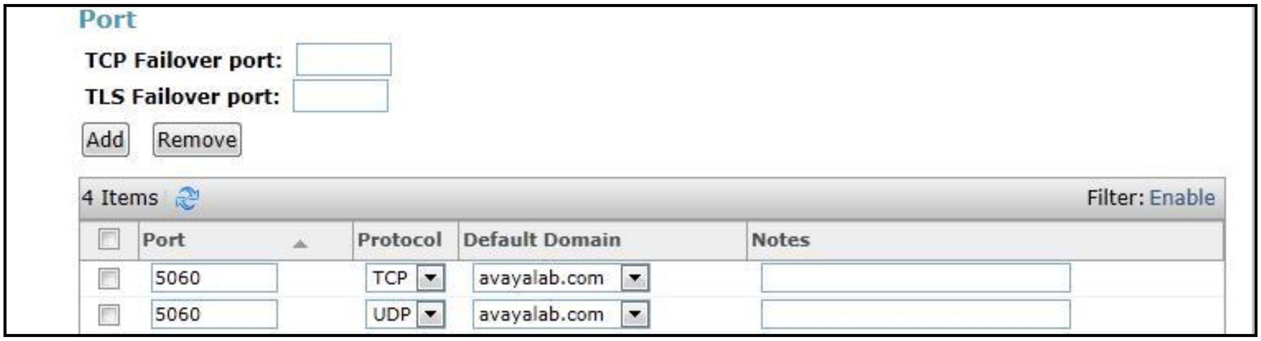
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

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

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

Defaults can be used for the remaining fields. Click **Commit** to save (not shown).

The compliance test used **Port** entry **5060** with **TCP** for connecting to Communication Manager and **Port** entry **5060** with **TCP** for connecting to the Avaya SBCE.



Port

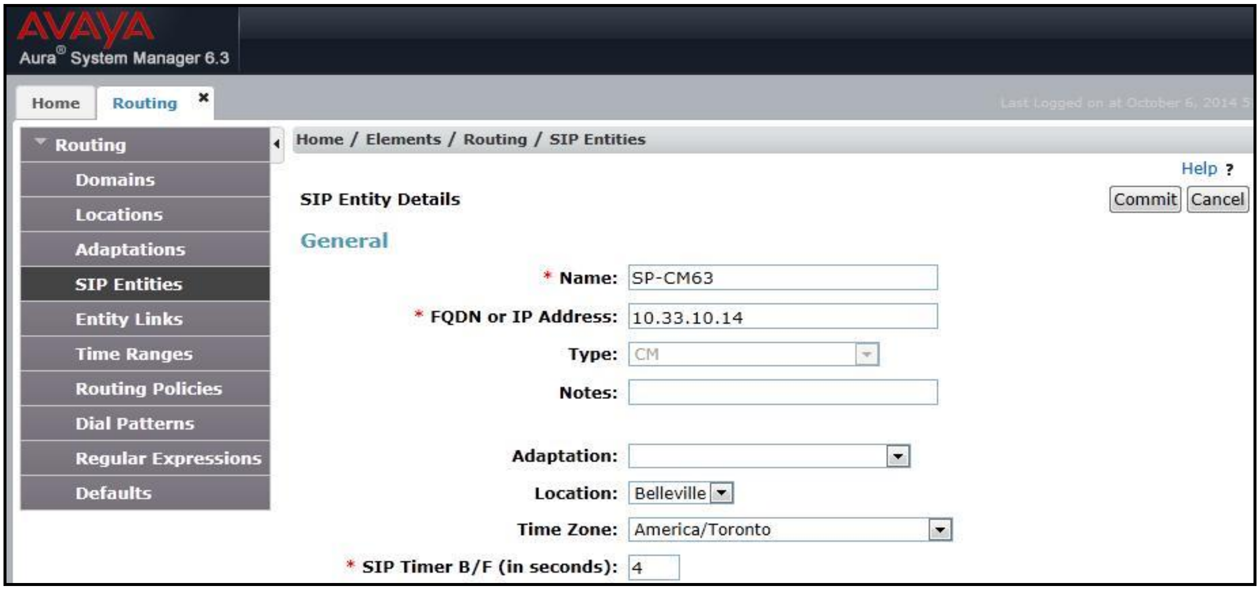
TCP Failover port:

TLS Failover port:

4 Items

□	Port	Protocol	Default Domain	Notes
□	5060	TCP	avayalab.com	
□	5060	UDP	avayalab.com	

The following screen shows the addition of Communication Manager SIP Entities. In order for Session Manager to send SIP traffic on an entity link to Communication Manager, it is necessary to create a SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to IP address of Communication Manager and **Type** to ***CM***. Then set Location and Time Zone parameters as shown in capture bellow.



SIP Entity Details

General

* Name: SP-CM63

* FQDN or IP Address: 10.33.10.14

Type: CM

Notes:

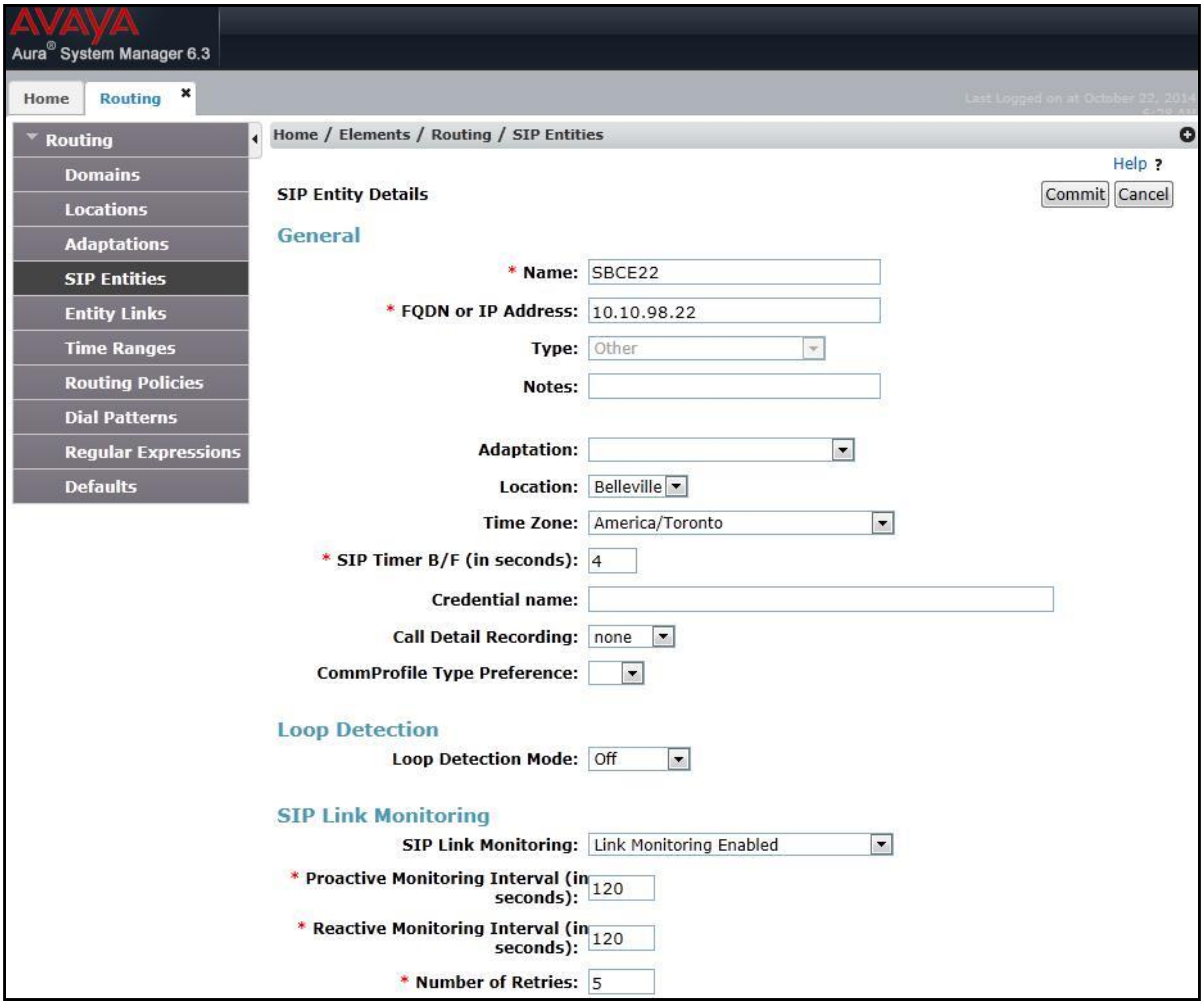
Adaptation:

Location: Belleville

Time Zone: America/Toronto

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

The following screen shows the addition of the SIP Entity for Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Select **Type** as ***Other***. Select **SIP Link Monitoring** as **Link Monitoring Enabled** with the interval of ***120*** seconds. This setting allows Session Manager to send outbound OPTIONS heartbeat in every ***120*** seconds to service provider (which is forwarded by the Avaya SBCE) to query for the status of the SIP trunk connecting to service provider.



SIP Entity Details

General

* Name: SBCE22

* FQDN or IP Address: 10.10.98.22

Type: Other

Notes:

Adaptation:

Location: Belleville

Time Zone: America/Toronto

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 120

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 5

6.5. Add Entity Links

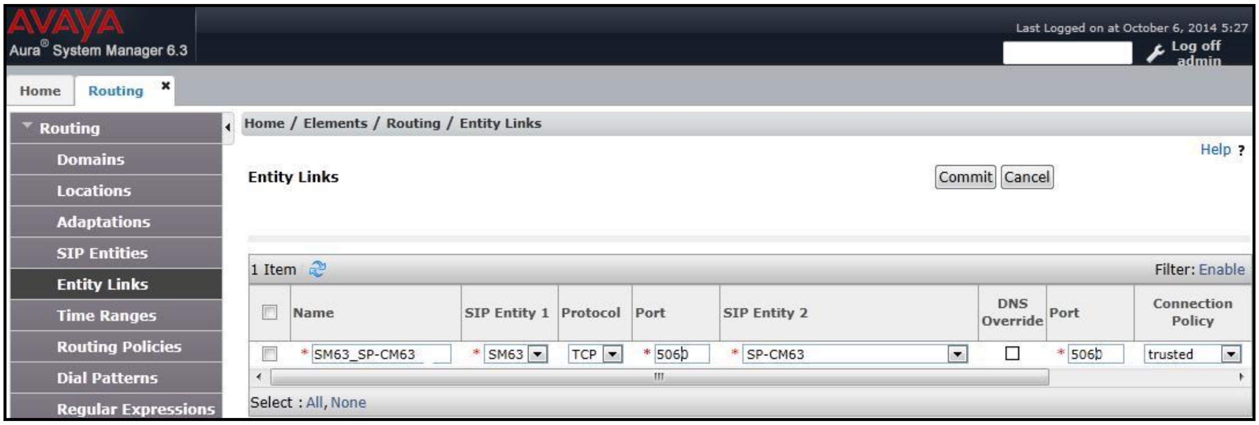
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. During compliance testing, two Entity Links were created, one for Communication Manager and other for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager defined in **Section 6.4**.

- **Protocol:** Select the transport protocol used for this link, ***TCP*** for the Entity Link to Communication Manager and ***TCP*** for the Entity Link to the Avaya SBCE.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other systems. For Communication Manager, select the Communication Manager SIP Entity defined in **Section** Error! Reference source not found.. For Avaya SBCE, select Avaya SBCE SIP Entity defined in **Section** Error! Reference source not found..
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager in **Section 5.6**.
- **Connection Policy:** Select **Trusted**. **Note**: If this is not selected, calls from the associated SIP Entity specified in **Section** Error! Reference source not found. will be denied.
- Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and to Avaya SBCE.

Entity Link to Communication Manager



Entity Links

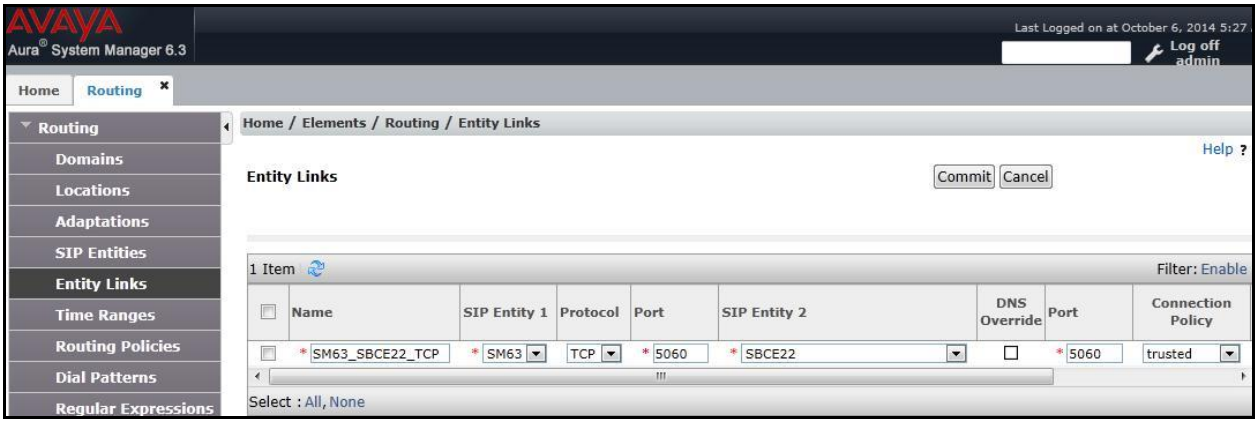
1 Item

Filter: Enable

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
☐	* SM63_SP-CM63	* SM63	TCP	* 5060	* SP-CM63	☐	* 5060	trusted

Select : All, None

Entity Link to Avaya SBCE



Entity Links

1 Item

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
☐	* SM63_SBCE22_TCP	* SM63	TCP	* 5060	* SBCE22	☐	* 5060	trusted

6.6. Add Routing Policies

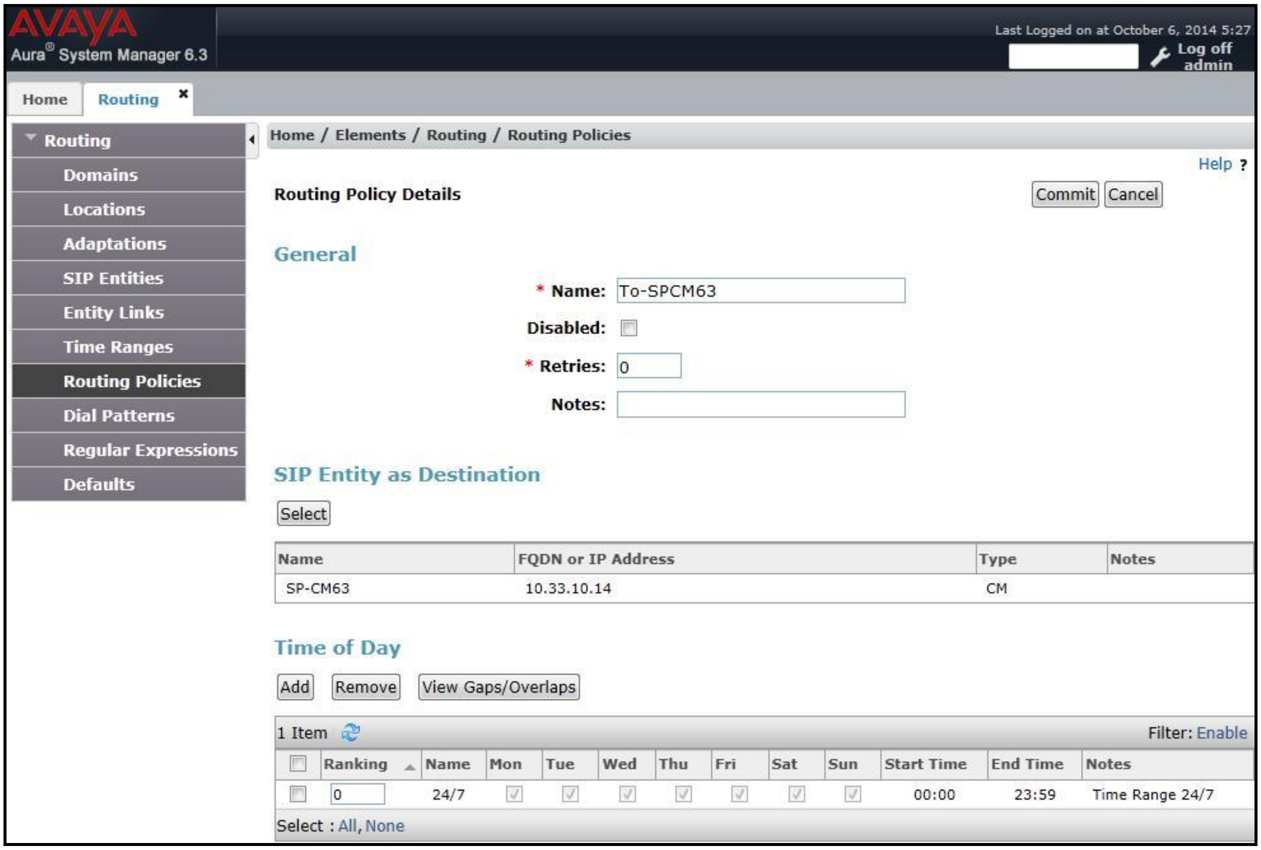
Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section** Error! Reference source not found.. Two routing policies were added, one for Communication Manager and other for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click **New** button in the right pane (not shown). The following screen is displayed.

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

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

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

The following screens show the Routing Policies for Communication Manager.



Routing Policy Details

General

* Name: To-SPCM63

Disabled: □

* Retries: 0

Notes:

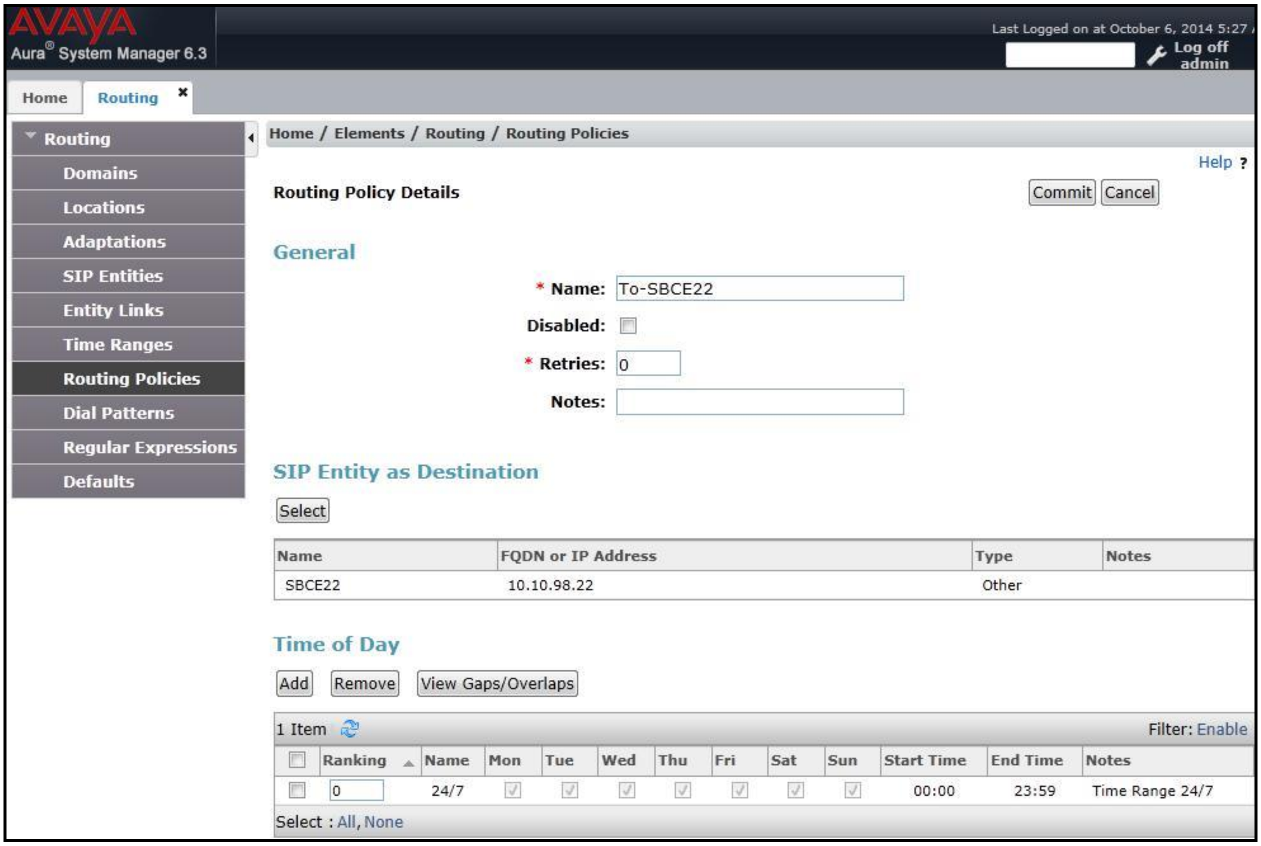
SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SP-CM63	10.33.10.14	CM	

Time of Day

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

The following screens show the Routing Policies for the Avaya SBCE.



Routing Policy Details

General

* Name: To-SBCE22

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SBCE22	10.10.98.22	Other	

Time of Day

1 Item   Filter: Enable

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

Select : All, None

6.7. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to Bell and vice versa. Dial Patterns define which routing 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 navigation pane and click **New** button in the right pane (not shown).

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

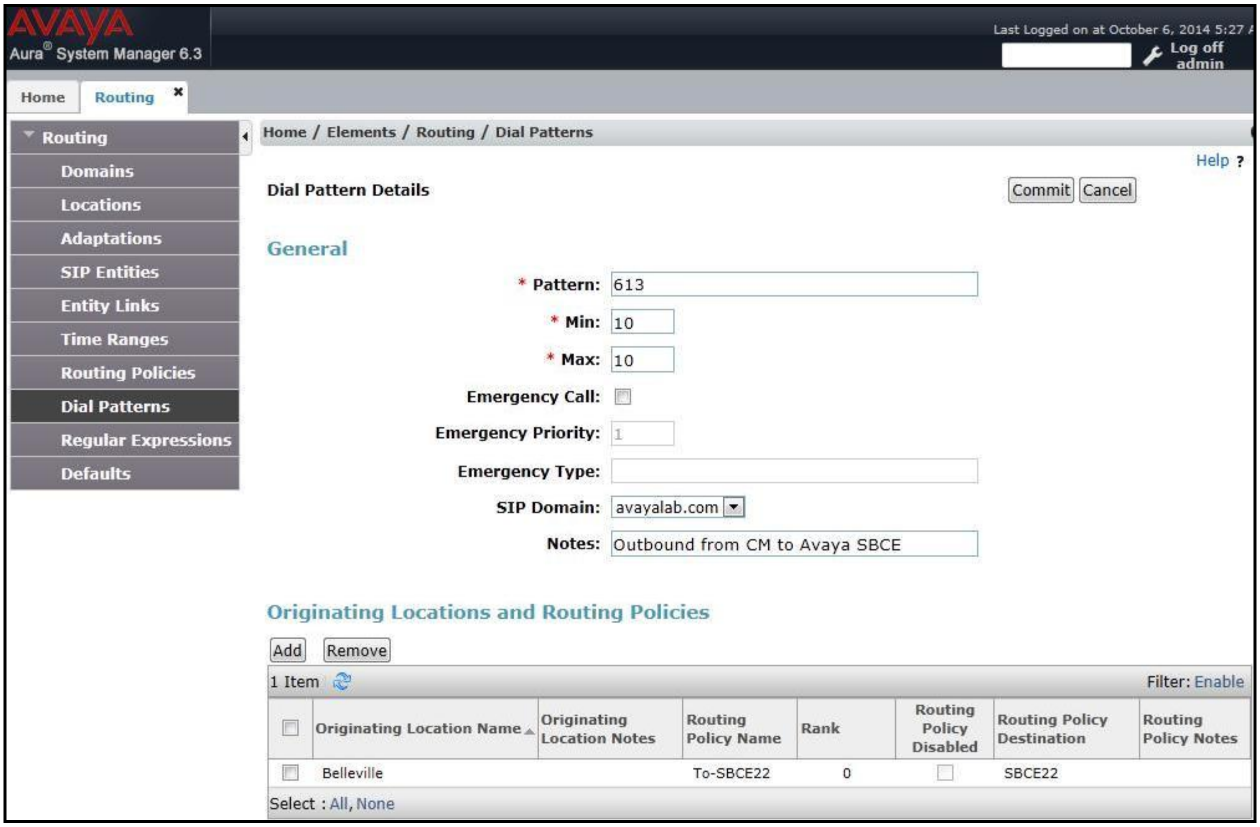
- **Pattern:** Enter a dial string that will be matched against the “Request-URI” of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:**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

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

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

Two examples of the dial patterns used for the compliance testing were shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise.

The first example shows that 10-digit dialed numbers that has a destination domain of "avayalab.com" uses route policy to Avaya SBCE as defined in **Section** Error! Reference source not found..



Dial Pattern Details

General

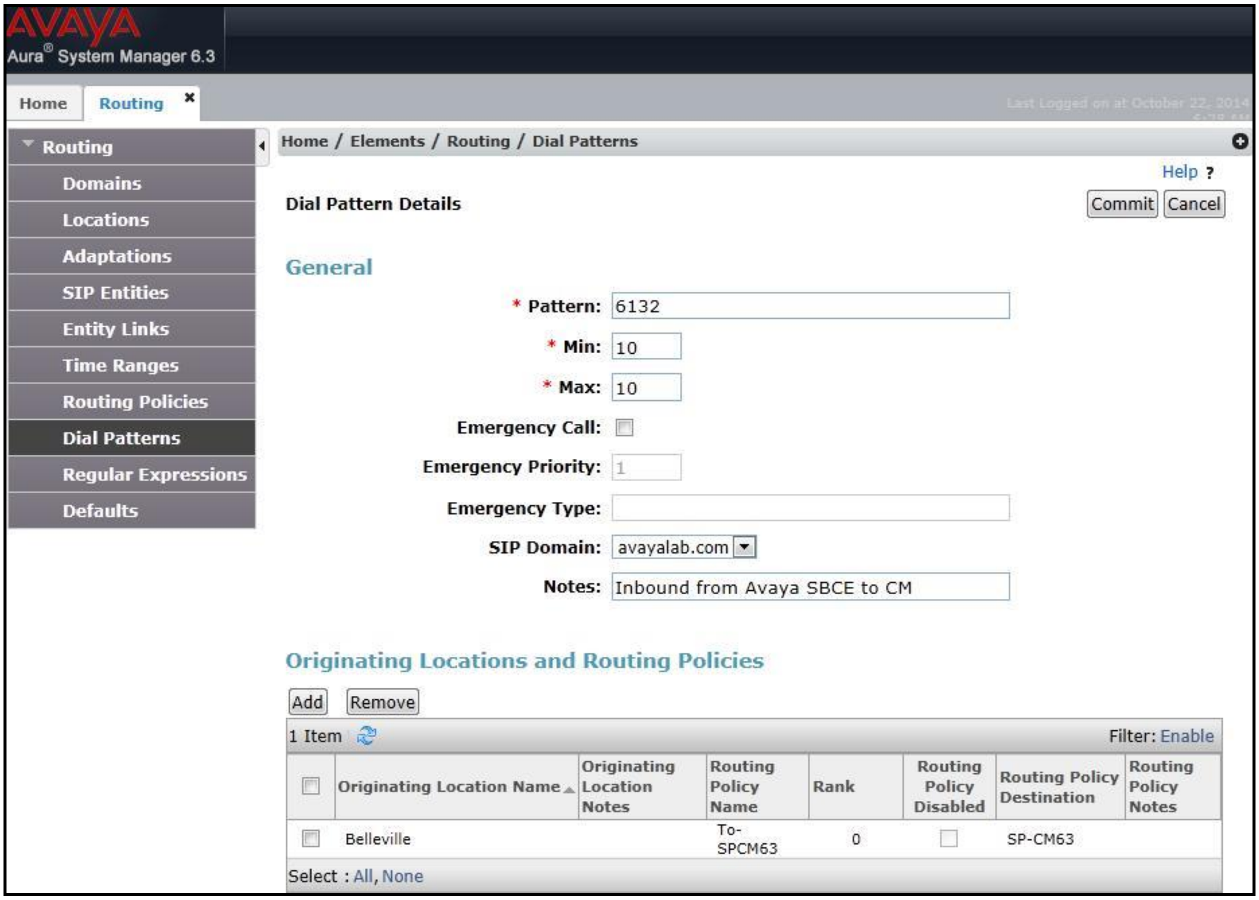
* Pattern:	613
* Min:	10
* Max:	10
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	avayalab.com
Notes:	Outbound from CM to Avaya SBCE

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Belleville		To-SBCE22	0	□	SBCE22	

The second example shows that inbound 10-digit numbers that start with 6132 to domain "avayalab.com" uses route policy to Communication Manager as defined in **Section** Error! Reference source not found.. These are the DID numbers assigned to the enterprise by Bell.



Dial Pattern Details

General

* Pattern: 6132

* Min: 10

* Max: 10

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: avayalab.com

Notes: Inbound from Avaya SBCE to CM

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Belleville		To-SPCM63	0	□	SP-CM63	

Select : All, None

6.8. Add/View Session Manager

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

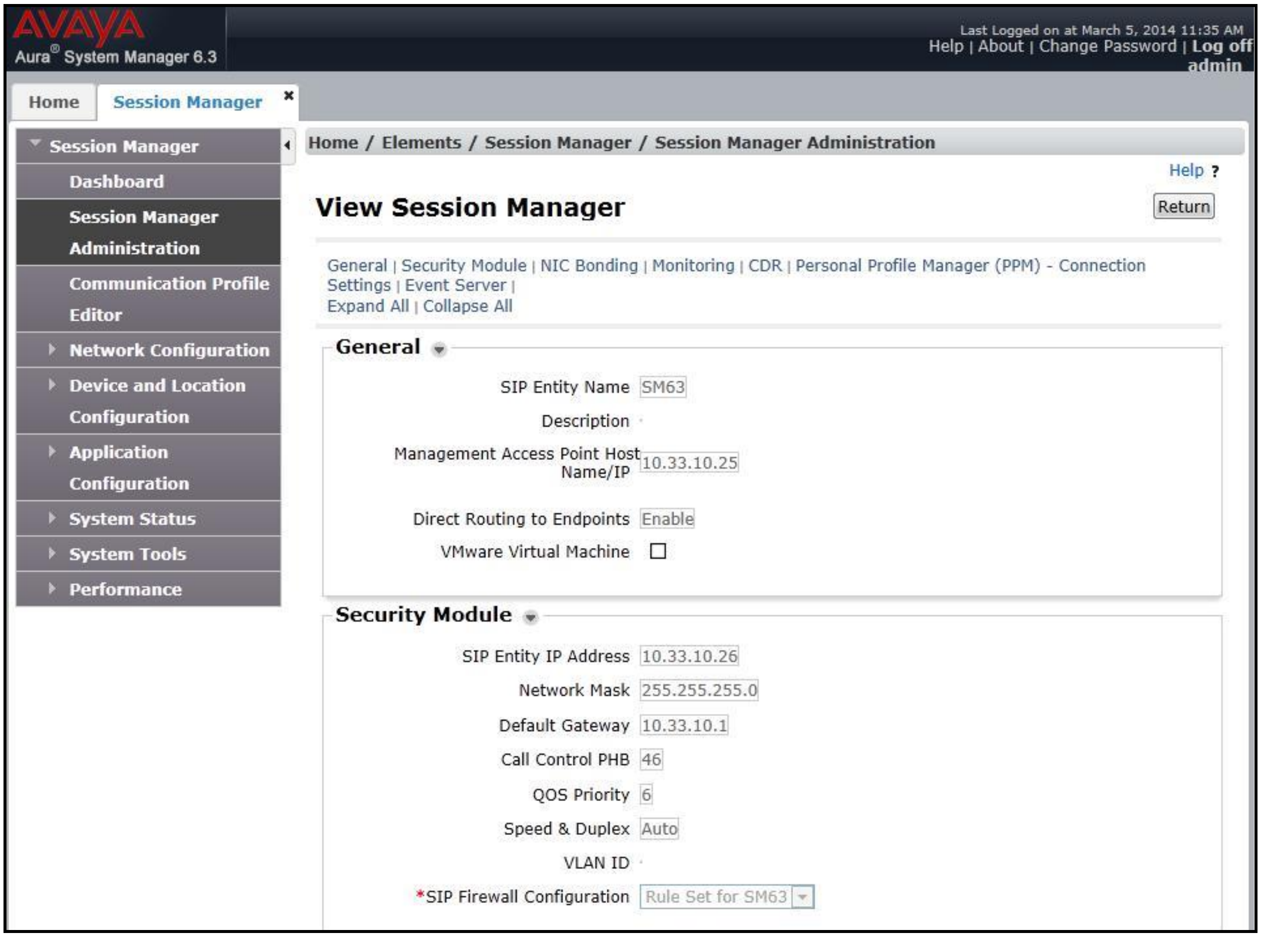
In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.
- **Directs Routing to Endpoints**: Enabled, to enable call routing on the Session Manager.

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name.
- **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 **Commit** to save (not shown).

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


AVAYA
Aura® System Manager 6.3
Last Logged on at March 5, 2014 11:35 AM
Help | About | Change Password | Log off admin
Home
Session Manager
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager / Session Manager Administration
Help ?
Return
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

View Session Manager

General

SIP Entity Name SM63

Description

Management Access Point Host Name/IP 10.33.10.25

Direct Routing to Endpoints Enable

VMware Virtual Machine □

Security Module

SIP Entity IP Address 10.33.10.26

Network Mask 255.255.255.0

Default Gateway 10.33.10.1

Call Control PHB 46

QOS Priority 6

Speed & Duplex Auto

VLAN ID

*SIP Firewall Configuration Rule Set for SM63

7. 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 Bell SIP Trunking Service.

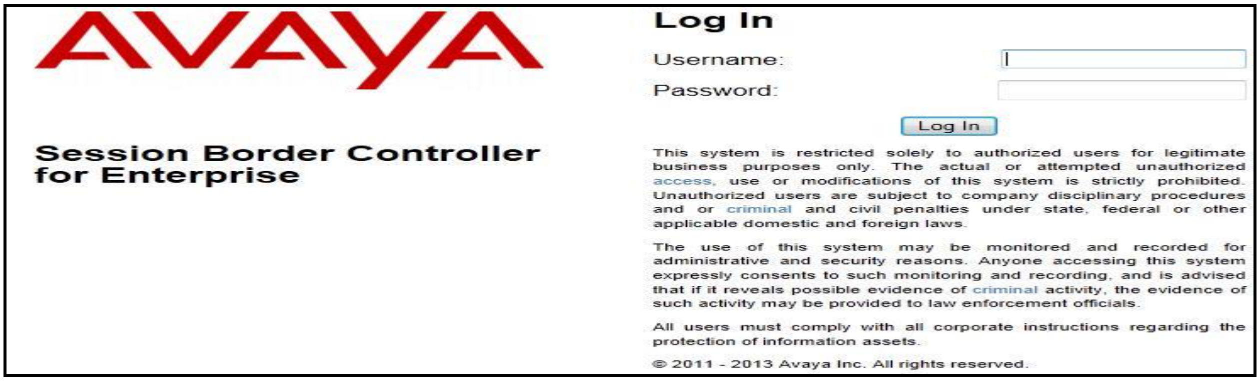
These Application Notes assume that the installation of the Avaya SBCE and the assignment of a management IP Address have already been completed.

In this session, the naming convention for Bell is Service Provider (SP) which is connecting to external interface of Avaya SBCE. And for Avaya side is Enterprise (EN) which is connected to internal interface of Avaya SBCE.

7.1. 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***.



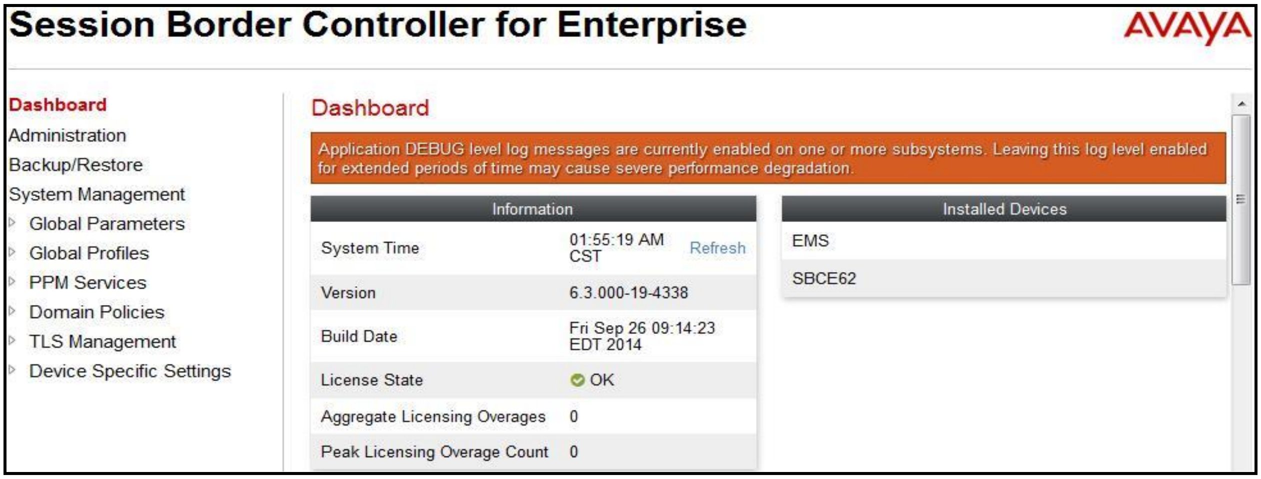
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

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



Application DEBUG level log messages are currently enabled on one or more subsystems. Leaving this log level enabled for extended periods of time may cause severe performance degradation.

Information		
System Time	01:55:19 AM CST	Refresh
Version	6.3.000-19-4338	
Build Date	Fri Sep 26 09:14:23 EDT 2014	
License State	✓ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	

Installed Devices
EMS
SBCE62

7.2. Global Profiles

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

7.2.1. 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.

7.2.2. 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.

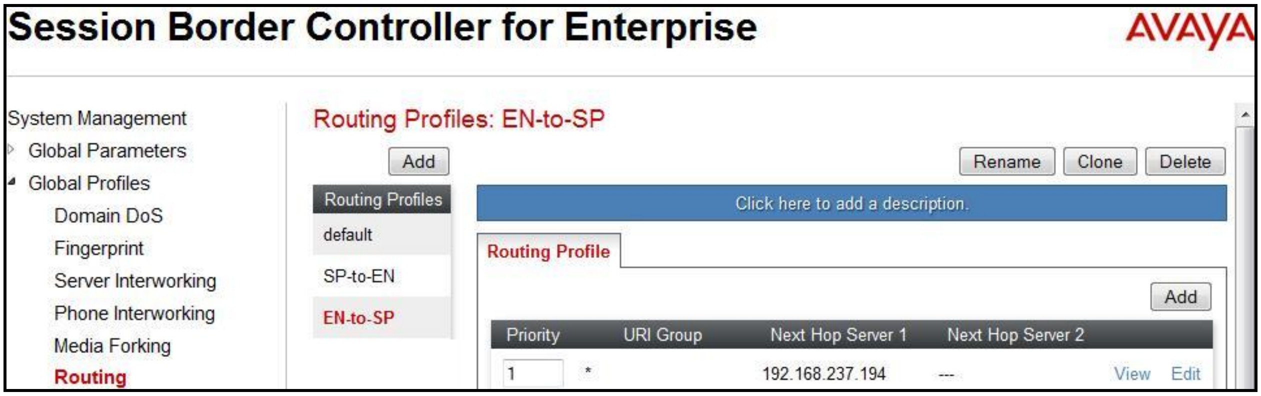
To create a Routing Profile, select **Global Profiles → Routing**. Click on the **Add** button.

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

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

Routing Profile for SP

The screenshot below illustrate the routing profile from Avaya SBCE to the SP network, **Global Profiles → Routing**: **EN-to-SP**. As shown in **Figure 1**, the SP 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 7.2.1**, the call will be routed to the **Next Hop Server 1** which is the IP address of SP SIP trunk on port 5060.

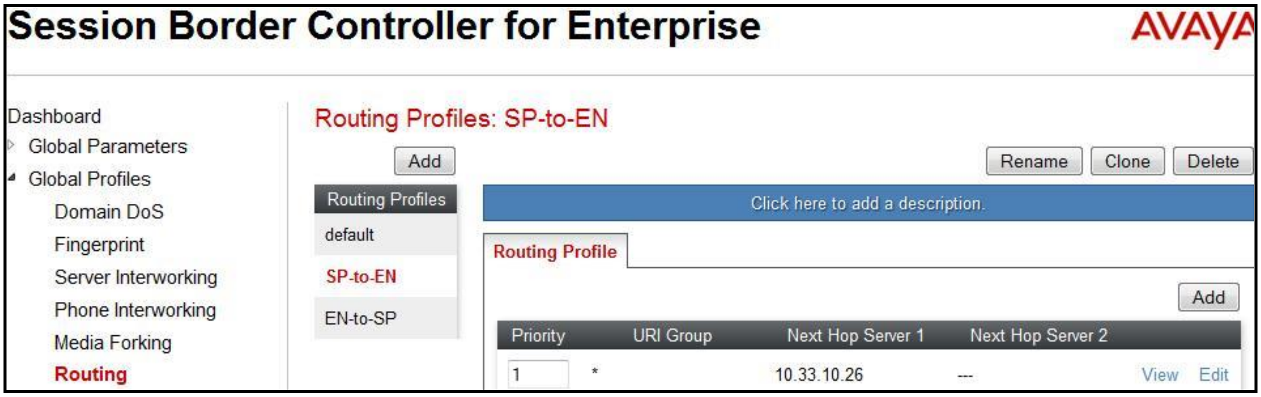


Routing Profiles: EN-to-SP

Priority	URI Group	Next Hop Server 1	Next Hop Server 2		
1	*	192.168.237.194	---	View	Edit

Routing Profile for EN

The Routing Profile for SP to EN, **SP-to-EN**, was defined to route call where the "To" header matches the URI Group **SP** defined in **Section 7.2.1** to **Next Hop Server 1** which is the IP address of Session Manager, on port 5060 as a destination. As shown in **Figure 1**, the SIP trunk between EN and the Avaya SBCE is connected with transportation protocol TCP.



Routing Profiles: SP-to-EN

Priority	URI Group	Next Hop Server 1	Next Hop Server 2		
1	*	10.33.10.26	---	View	Edit

7.2.3. 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.

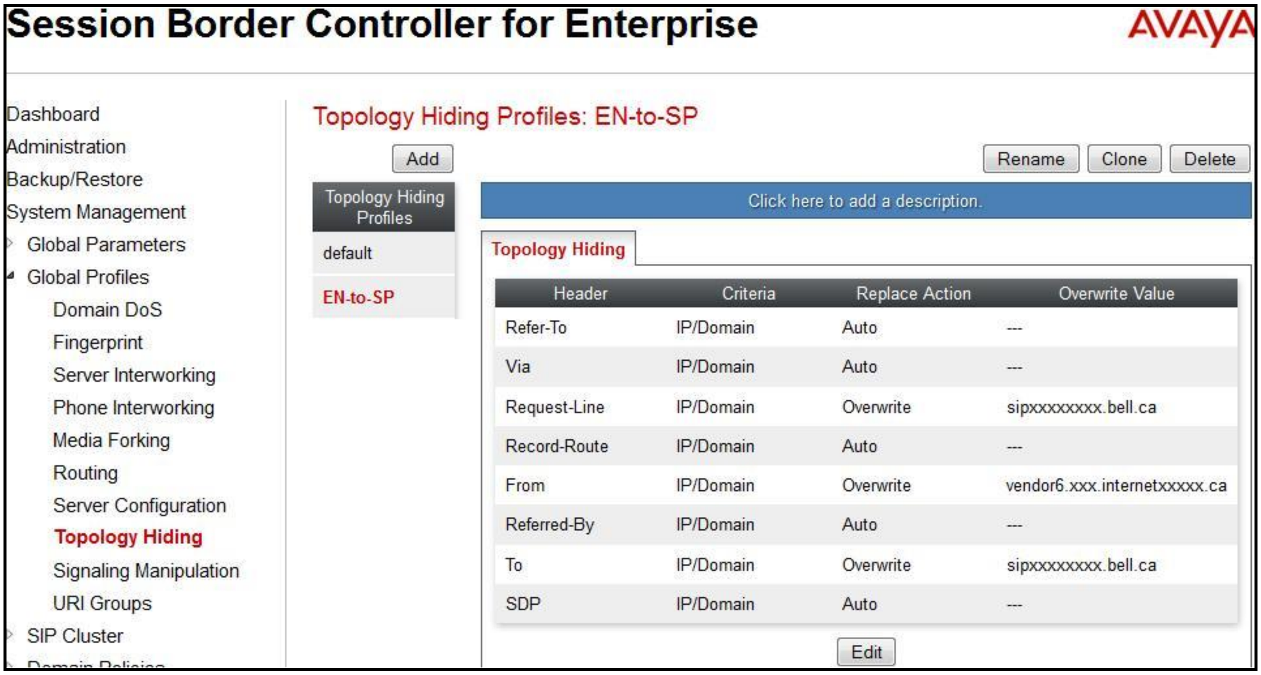
Topology Hiding Profile for SP

Profile **EN-to-SP** was defined to mask the enterprise SIP domain avayalab.com in “Request-URI” and “To” headers to SP provided domain “***sipxxxxxxxx.bell.ca***” and “From” header to the provided domain “***vendor6.xxx.internetxxxxx.ca***. It is to secure the enterprise network topology and to meet the SIP requirement of the service provider.

Notes:

- 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**.



Topology Hiding Profiles: EN-to-SP

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	sipxxxxxxxx.bell.ca
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	vendor6.xxx.internetxxxxx.ca
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Overwrite	sipxxxxxxxx.bell.ca
SDP	IP/Domain	Auto	---

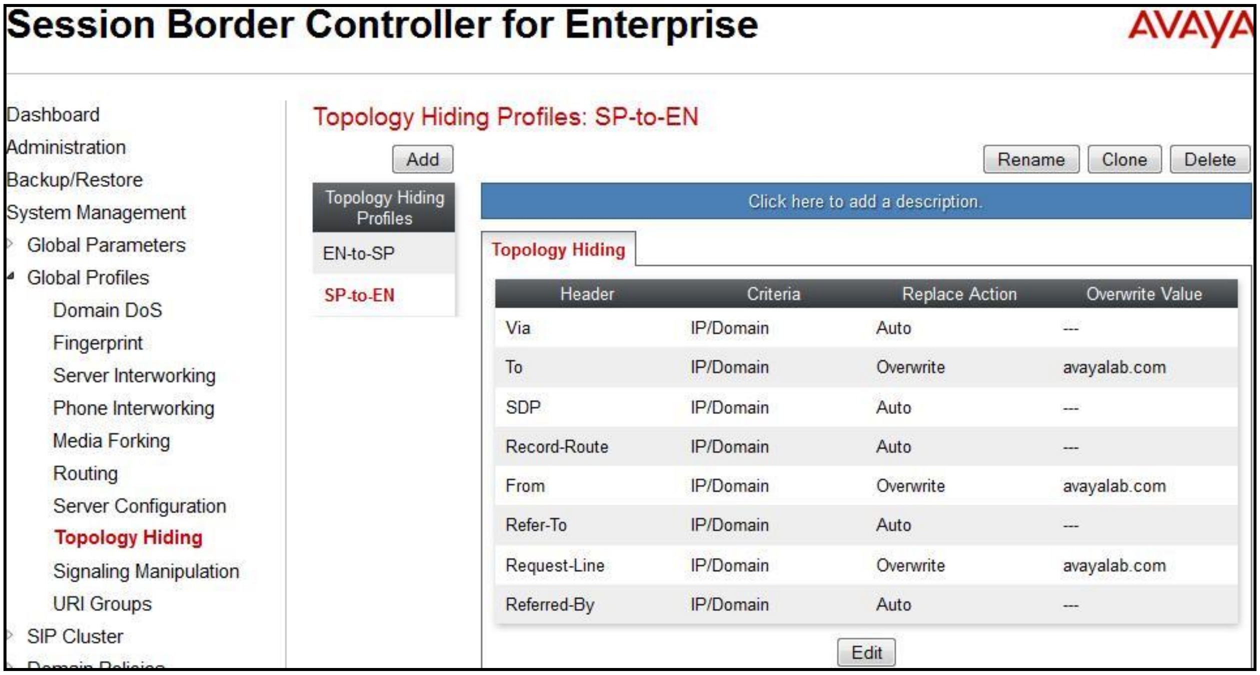
Topology Hiding Profile for EN

Profile **SP-to-EN** was also created to mask SP URI-Host in “Request-URI”, “From”, “To” headers to the enterprise domain ***avayalab.com***, replace Record-Route, Via headers and SDP added by SP to internal IP address known to EN.

Notes:

- 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**.



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

7.2.4. 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 SP and EN respectively.

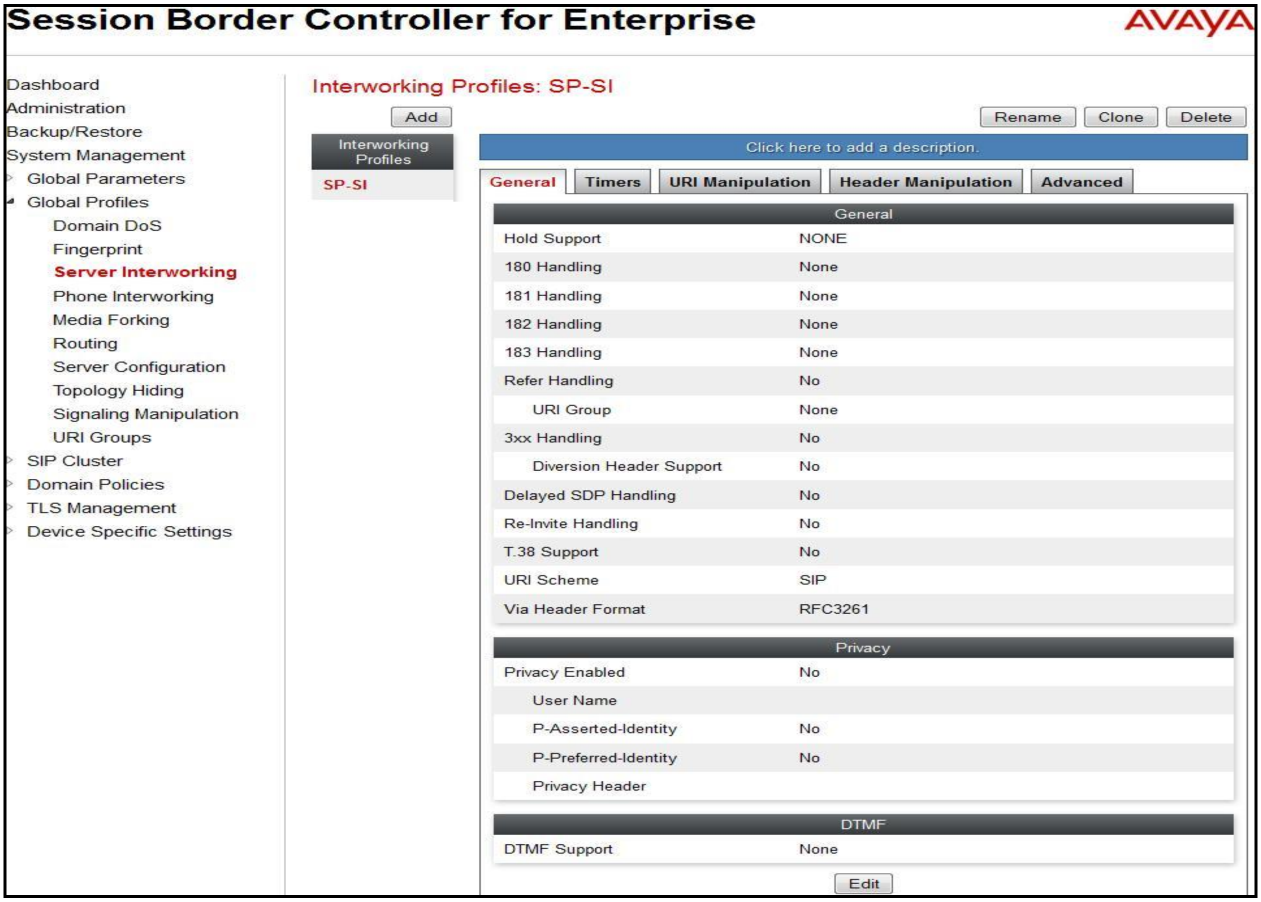
Server Interworking profile for SP

Profile **SP-SI** was defined to match the specification of SP. 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 EN to SP.
- **18X Handling** = *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from EN to SP.
- **Refer Handling** = ***No.*** The Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from EN to SP.
- **T.38 Support** = ***No***. SP does not 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 SP.
- **DTMF Support** = ***None***. The Avaya SBCE will send original DTMF method from EN to SP.

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



Interworking Profiles: SP-SI

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

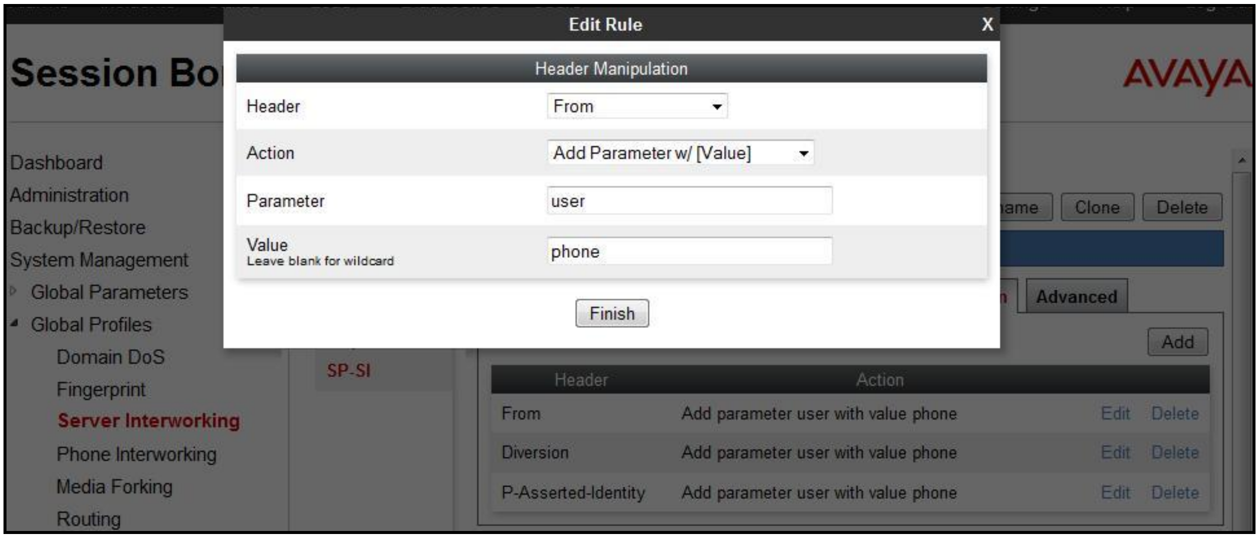
Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

Header Manipulation:
Header rules are added to include the parameter ***user=phone*** to the **From**, **Diversion** and **P-Asserted-Identify** headers as Bell required.

- **Header**: This field is where ***From***, ***Diversion*** and ***P-Asserted-Identity*** is selected.
- **Action**: ***Add Parameter w/[Value]*** is selected.
- **Parameter** = ***user***.
- **Value** = ***phone***.

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



Header Manipulation

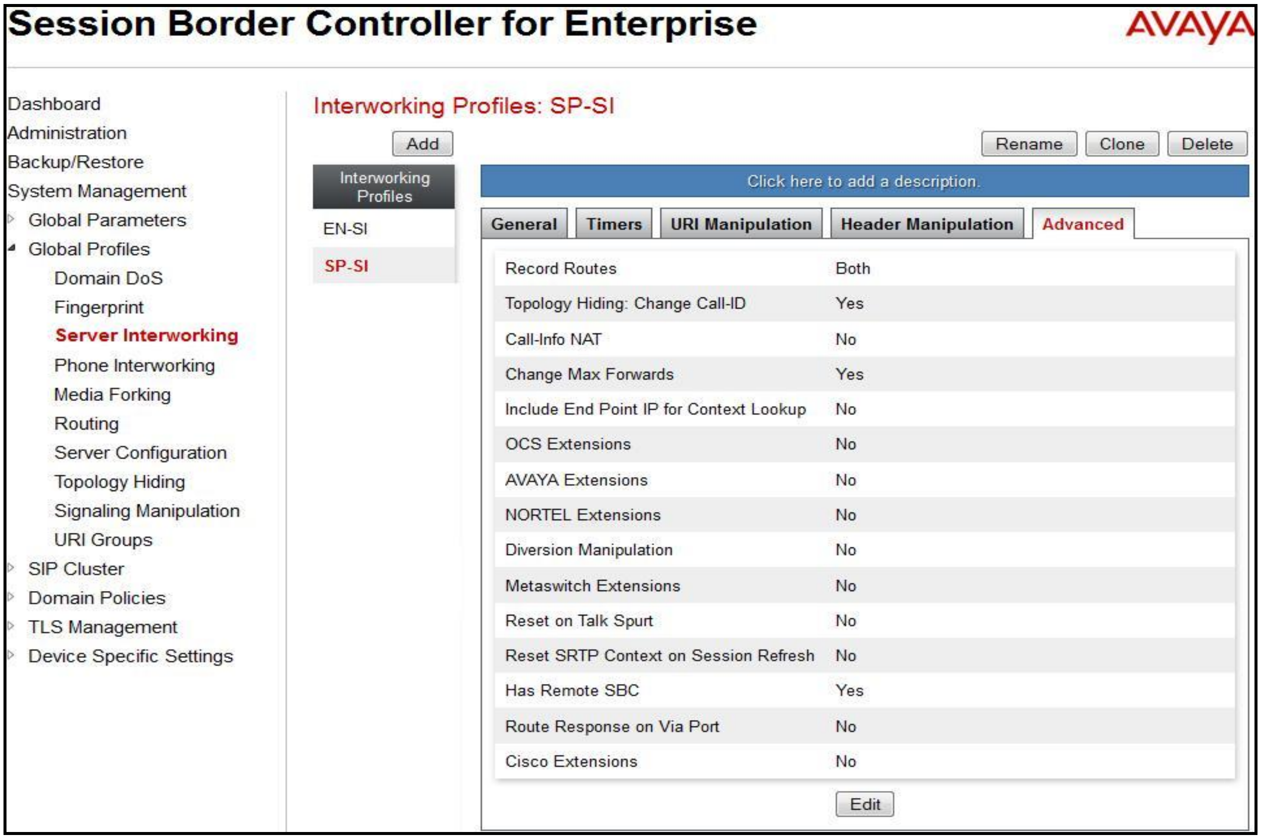
Header	From
Action	Add Parameter w/ [Value]
Parameter	user
Value Leave blank for wildcard	phone

Header	Action		
From	Add parameter user with value phone	Edit	Delete
Diversion	Add parameter user with value phone	Edit	Delete
P-Asserted-Identity	Add parameter user with value phone	Edit	Delete

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 SP.
- **Change Max Forwards** = ***Yes***. The Avaya SBCE will adjust the original Max-Forwards value from EN to SP by reducing the intermediate hops involving in the call flow.
- **Has Remote SBC** = ***Yes***. SP 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 SP for the media.

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



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

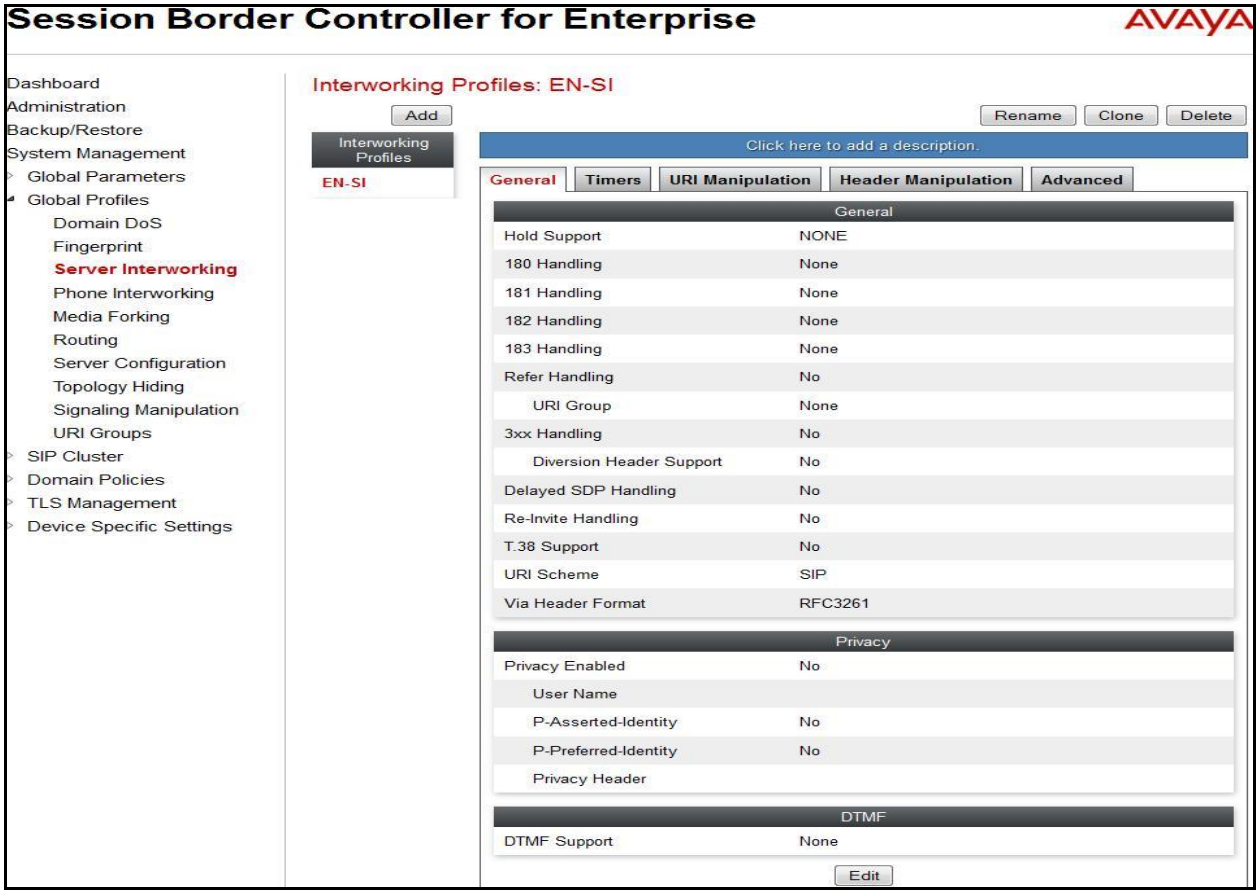
Server Interworking profile for EN

Profile **EN-SI** was defined to match the specification of EN. 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 SP to EN.
- **Refer Handling** = *No*. The Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from SP to EN.
- **T.38 Support** = *No*. EN does support T.38 fax, but SP doesn't in the compliance testing.
- **Privacy Enabled** = *No*. The Avaya SBCE will not mask the "From" header with anonymous for an inbound call from SP. It depends on SP to enable/ disable privacy on an individual call basis.
- **DTMF Support** = *None*. The Avaya SBCE will send original DTMF method from SP to EN.

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



Interworking Profiles: EN-SI

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

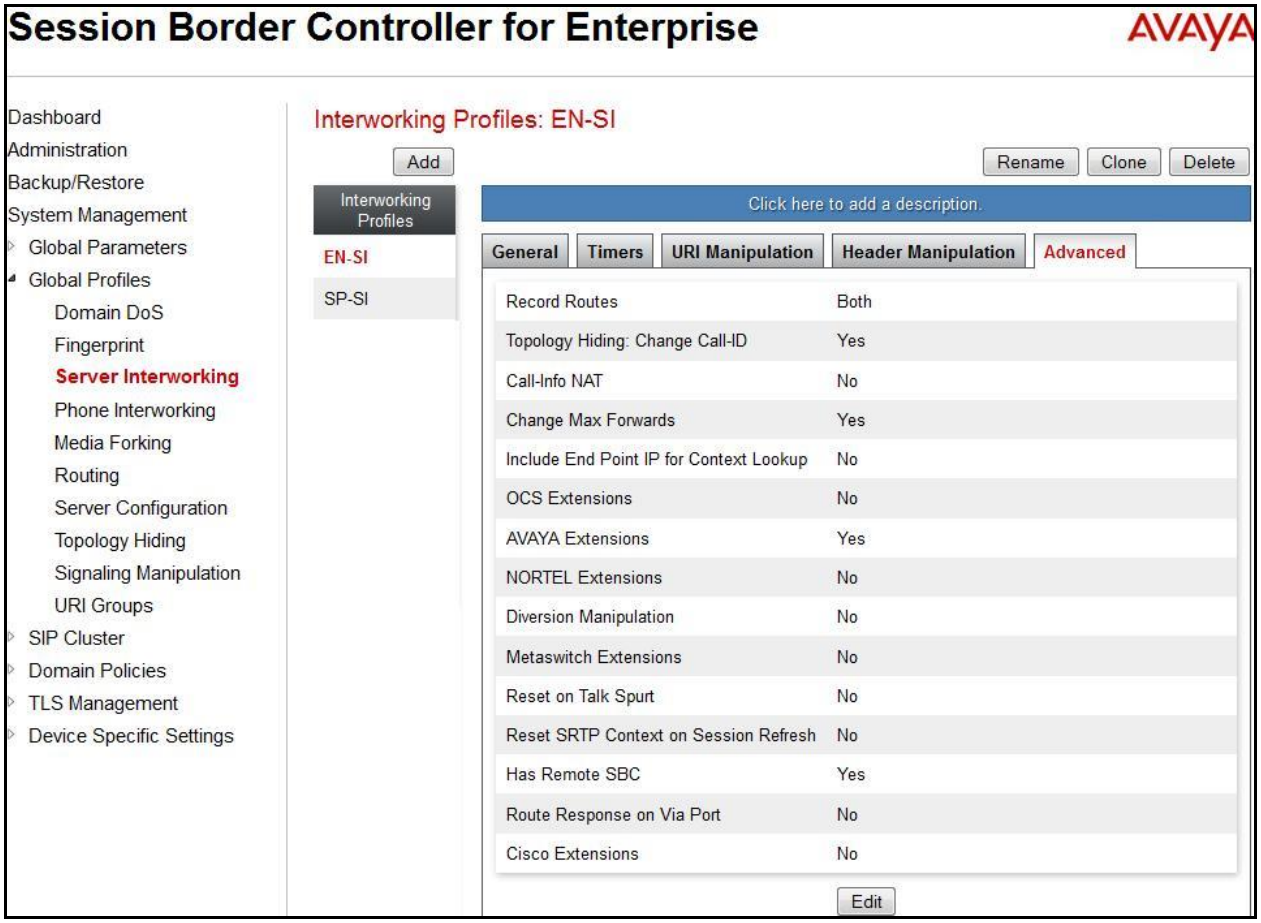
Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

Advanced settings:

- **Record Routes** = ***Both***. 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 EN.
- **Change Max Forwards** = ***Yes***. The Avaya SBCE will adjust the original Max-Forwards value from SP to EN 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 EN for the media.

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



Interworking Profiles: EN-SI

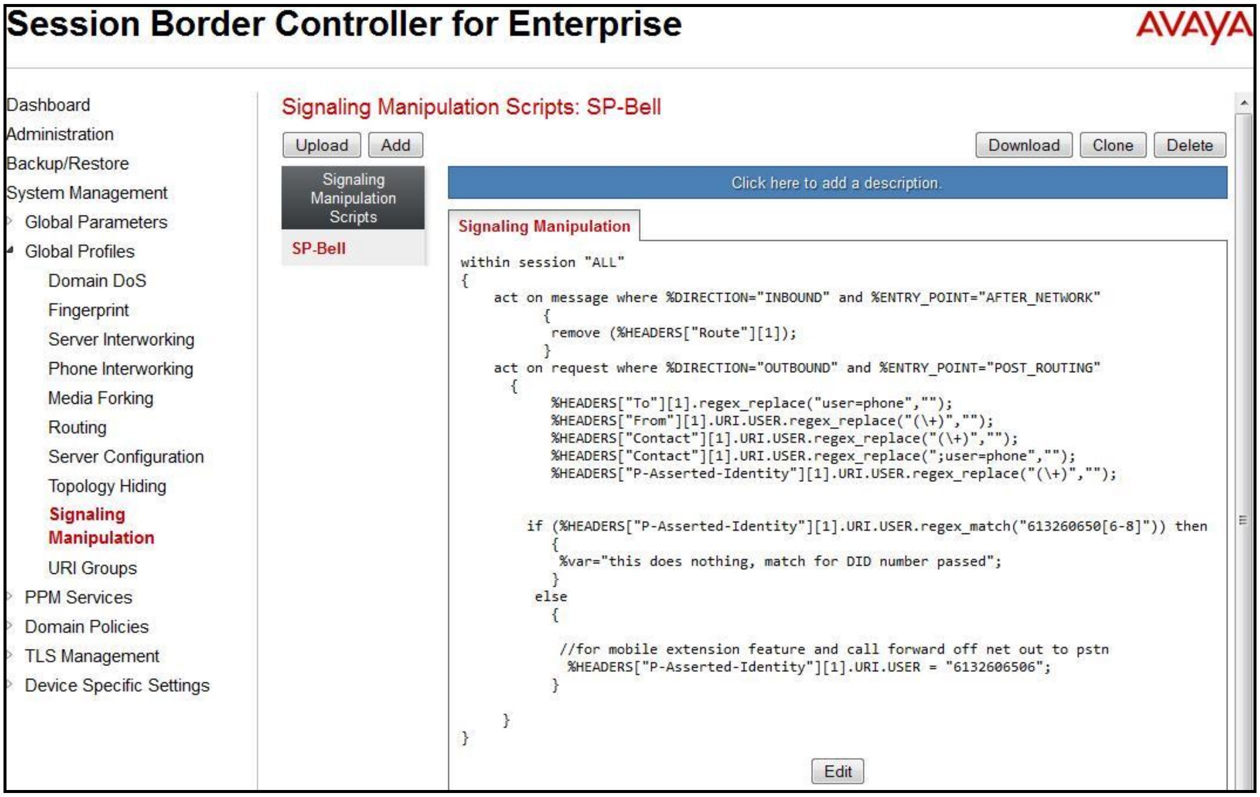
Record Routes	Both
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session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

7.2.5. Configure Signaling Manipulation

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

To create a Signaling Manipulation script, select **Global Profiles → Signaling Manipulation**. Click **Add Script** (not shown).

In the compliance testing, a SigMa SP-Bell script is created for Server Configuration for SP and its details are captured below.



```
within session "ALL"
{
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
          {
           remove (%HEADERS["Route"][1]);
          }
    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
      {
           %HEADERS["To"][1].regex_replace("user=phone","");
           %HEADERS["From"][1].URI.USER.regex_replace("(\+)","");
           %HEADERS["Contact"][1].URI.USER.regex_replace("(\+)","");
           %HEADERS["Contact"][1].URI.USER.regex_replace(";user=phone","");
           %HEADERS["P-Asserted-Identity"][1].URI.USER.regex_replace("(\+)","");


        if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("613260650[6-8]")) then
           {
            %var="this does nothing, match for DID number passed";
           }
         else
           {

            //for mobile extension feature and call forward off net out to pstn
             %HEADERS["P-Asserted-Identity"][1].URI.USER = "6132606506";
           }

      }
}
```

7.2.6. 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.

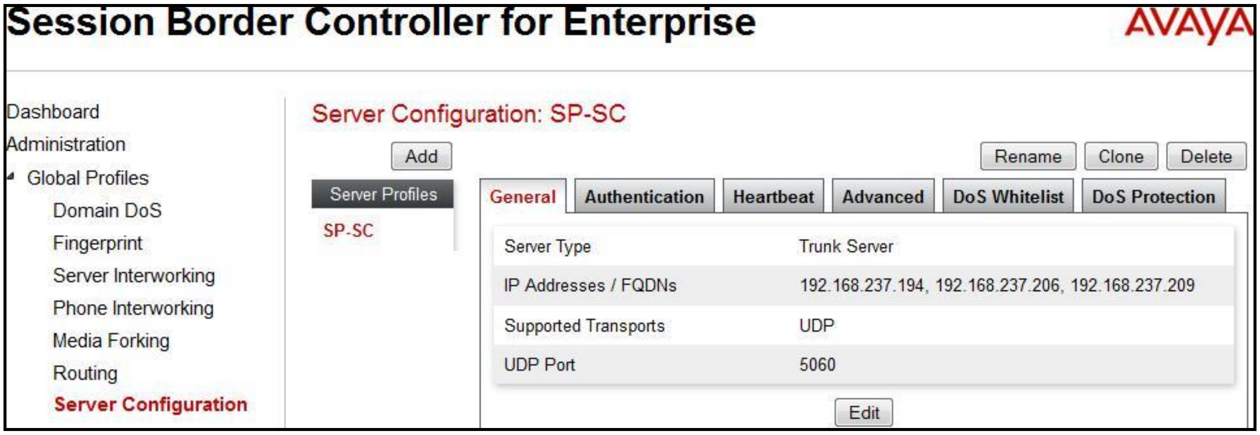
To create a Server Configuration entry, select **Global Profiles →Server Configuration**. Click on the **Add** button.

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

Server Configuration for SP

Server Configuration named **SP-SC** was created for SP. It will be discussed in detail below. **General** and **Advanced** tabs are provisioned for SP on the SIP trunk for every outbound call from enterprise to PSTN. 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. The **Heartbeat** tab is kept as ***disabled*** as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from EN to SP to query the status of the SIP trunk.

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

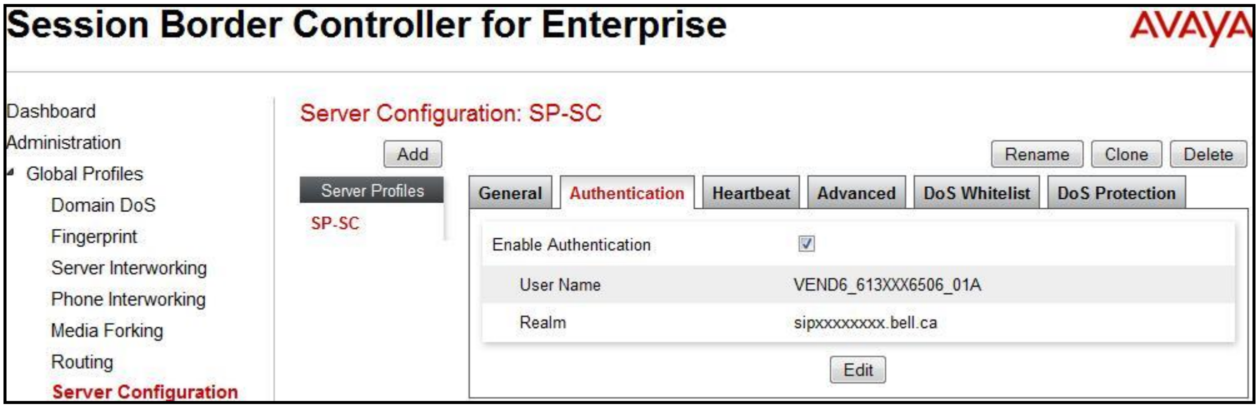


Server Configuration: SP-SC

Server Type	Trunk Server
IP Addresses / FQDNs	192.168.237.194, 192.168.237.206, 192.168.237.209
Supported Transports	UDP
UDP Port	5060

In the **Authentication** tab, click on the **Edit** button and enter following information.

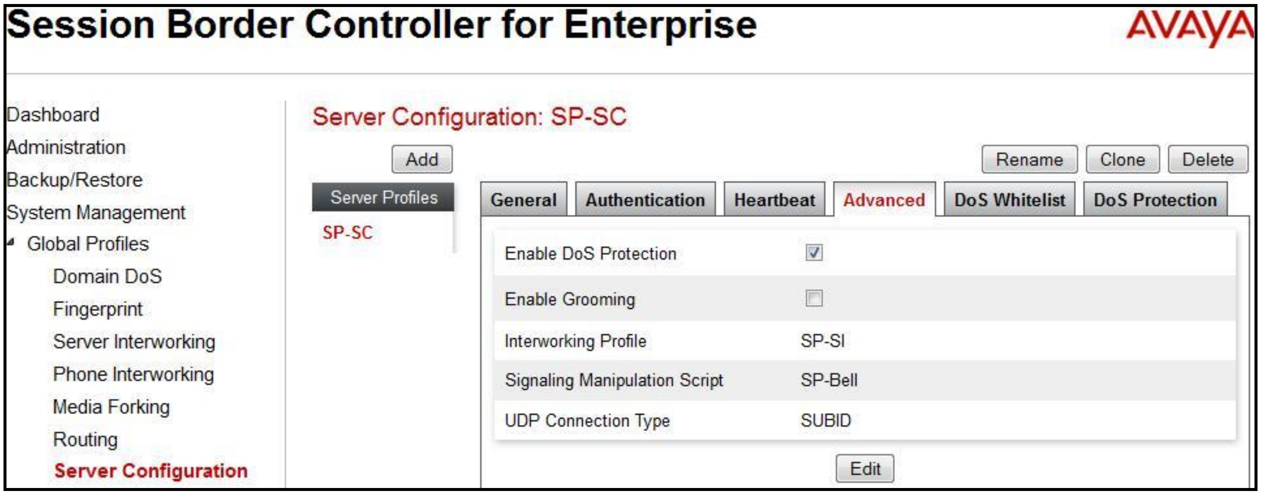
- Check **Enable Authentication** check box.
- Enter **User Name** (provided by SP).
- Enter **Realm** (provided by SP).
- Enter **Password** and **Confirm Password** (provided by SP) (not shown).
- Click **Finish**.



Server Configuration: SP-SC

Enable Authentication	☑
User Name	VEND6_613XXX6506_01A
Realm	sipxxxxxxxxx.bell.ca

- Under **Advanced** tab, check on **Enable DoS Protection**. From the **Interworking Profile** drop down list, select ***SP-SI*** as defined in **Section 7.2.4**. For **Signaling Manipulation Script**, select ***SP-Bell*** as defined in **Section 7.2.5**. This configuration applies the specific SIP profile to the SP traffic. The other settings are kept as default.



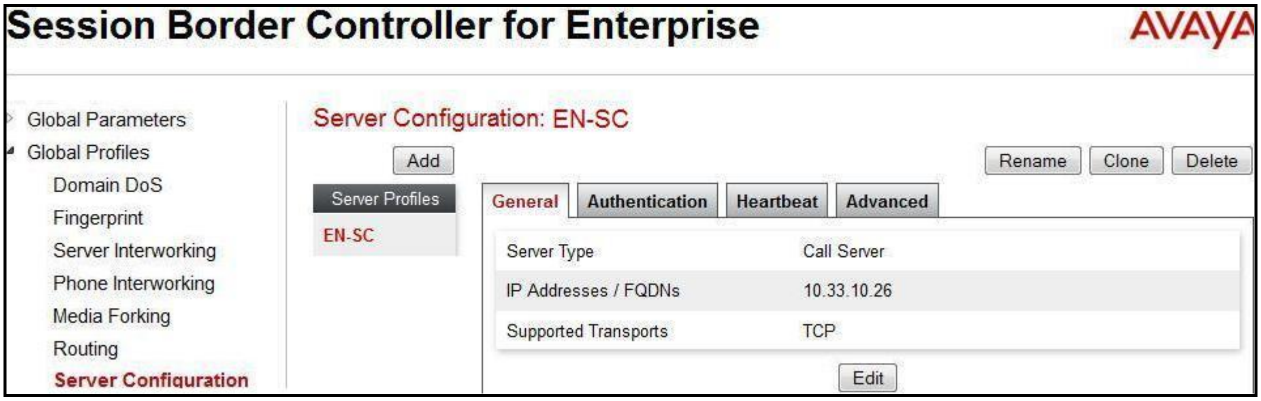
Server Configuration: SP-SC

Enable DoS Protection	☑
Enable Grooming	□
Interworking Profile	SP-SI
Signaling Manipulation Script	SP-Bell
UDP Connection Type	SUBID

Server Configuration for EN

Server Configuration named **EN-SC** created for EN 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 SP to EN to query the status of the SIP trunk.

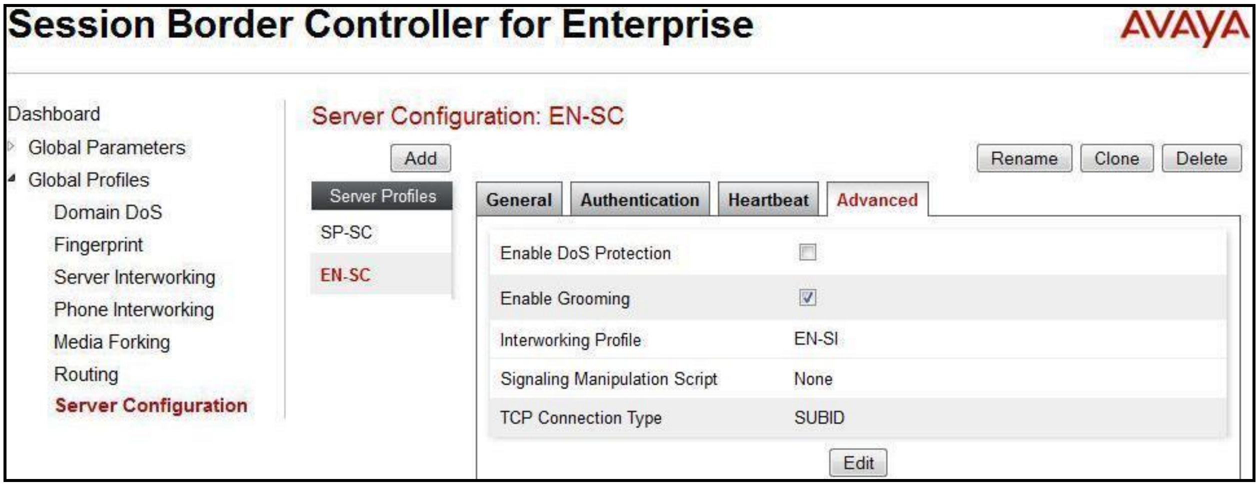
In the **General** tab, click on the **Edit** button then specify **Server Type** for EN as ***Call Server***. In the compliance testing, the link between the Avaya SBCE and EN was ***TCP*** and listened on port ***5060***.



Server Configuration: EN-SC

Server Type	Call Server
IP Addresses / FQDNs	10.33.10.26
Supported Transports	TCP

Under **Advanced** tab, click on the **Edit** button, from the **Interworking Profile** drop down list select ***EN-SI*** as defined in **Section 7.2.4** and from the **Signaling Manipulation Script** drop down list select ***None***. The other settings are kept as default.



Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	EN-SI
Signaling Manipulation Script	None
TCP Connection Type	SUBID

7.3. 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.

7.3.1. Signaling Rules

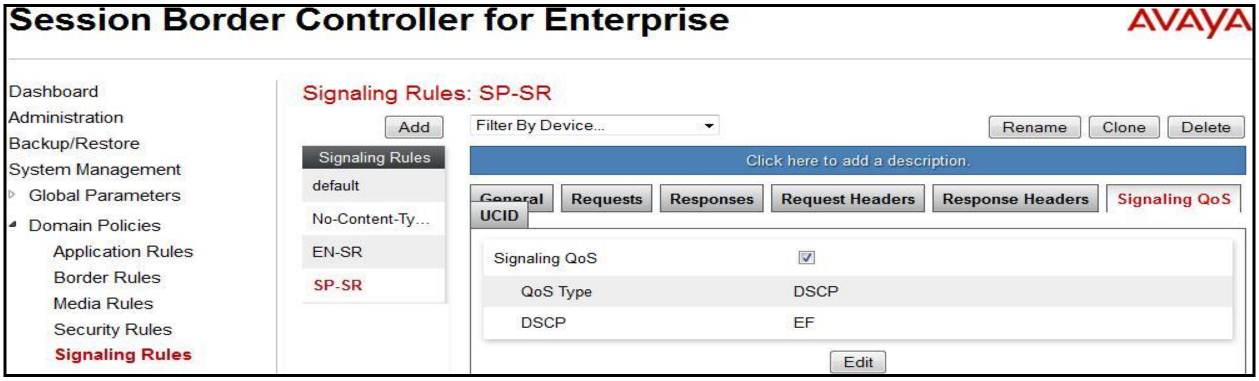
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined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

Signaling Rules for SP

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

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

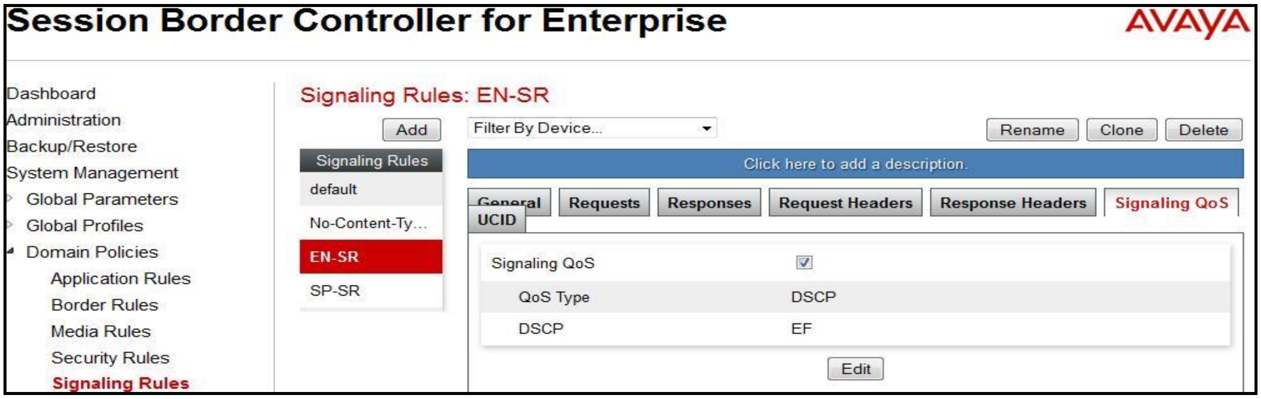


Signaling QoS	☑
QoS Type	DSCP
DSCP	EF

Signaling Rules for EN

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

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



Signaling QoS	☑
QoS Type	DSCP
DSCP	EF

7.3.2. Endpoint Policy Groups

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

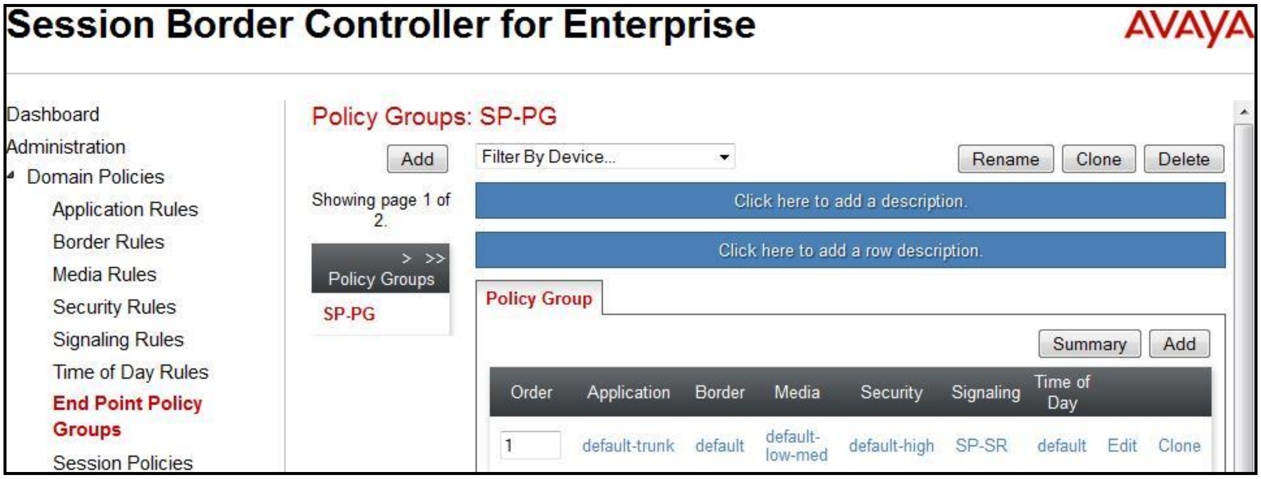
Endpoint Policy Groups were created for SP and EN.

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

Endpoint Policy Group for SP

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

- 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 7.3.1**.
- Set Time of Day Rule to ***default***.



Policy Groups: SP-PG

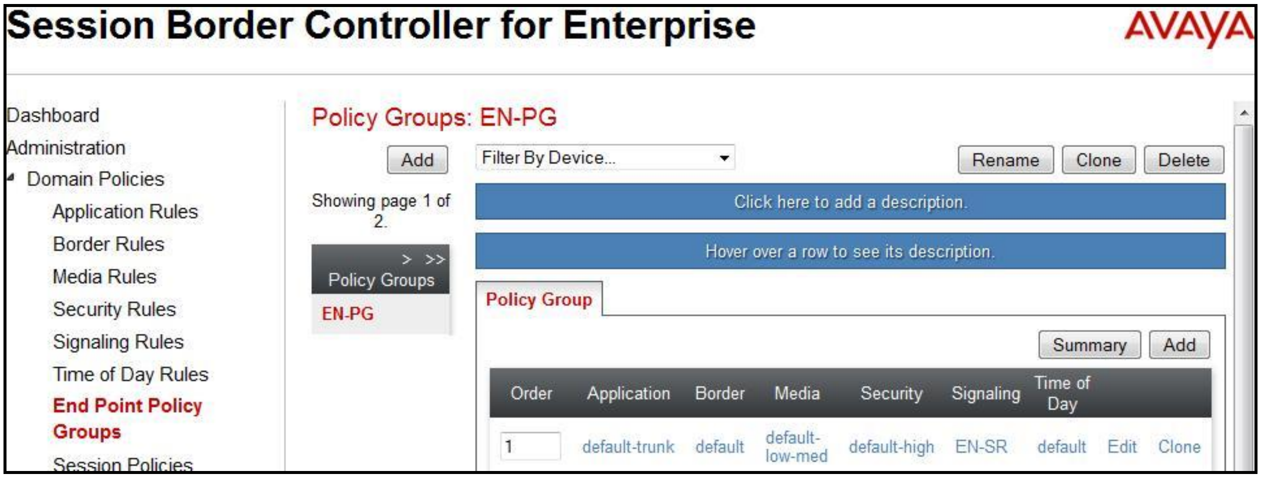
Policy Group

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default-trunk	default	default-low-med	default-high	SP-SR	default	Edit	Clone

Endpoint Policy Group for EN

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

- 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 7.3.1**.
- Set Time of Day Rule to ***default***.



Policy Groups: EN-PG

Policy Group

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default-trunk	default	default-low-med	default-high	EN-SR	default	Edit	Clone

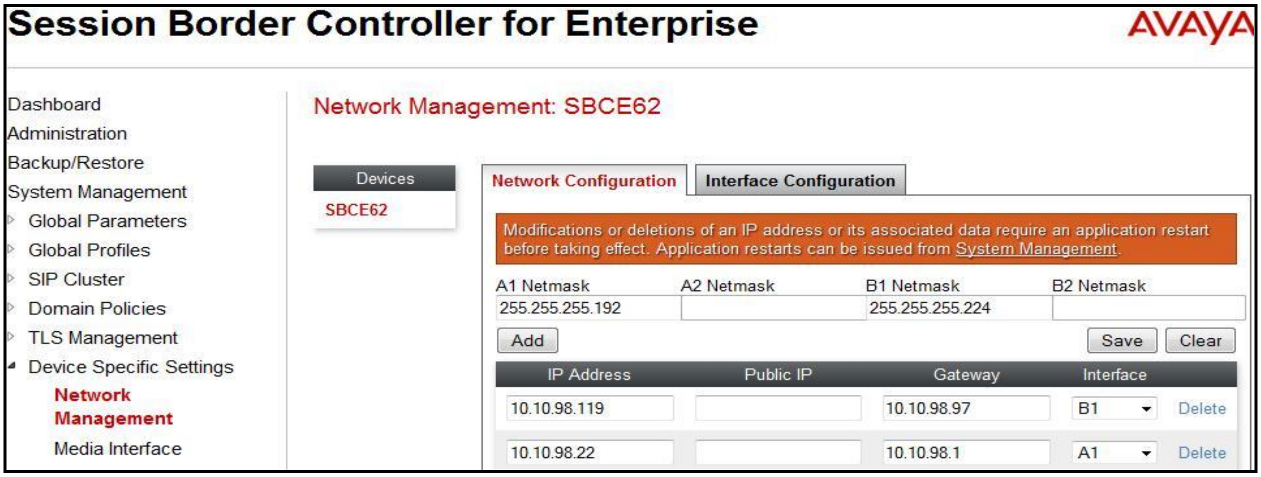
7.4. Device Specific Settings

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.

7.4.1. 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**.



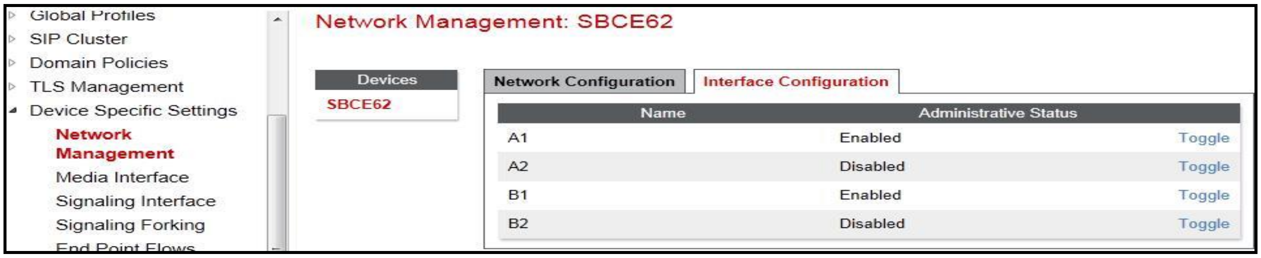
Network Management: SBCE62

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

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.192		255.255.255.224	

IP Address	Public IP	Gateway	Interface	
10.10.98.119		10.10.98.97	B1	Delete
10.10.98.22		10.10.98.1	A1	Delete

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.



Network Management: SBCE62

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

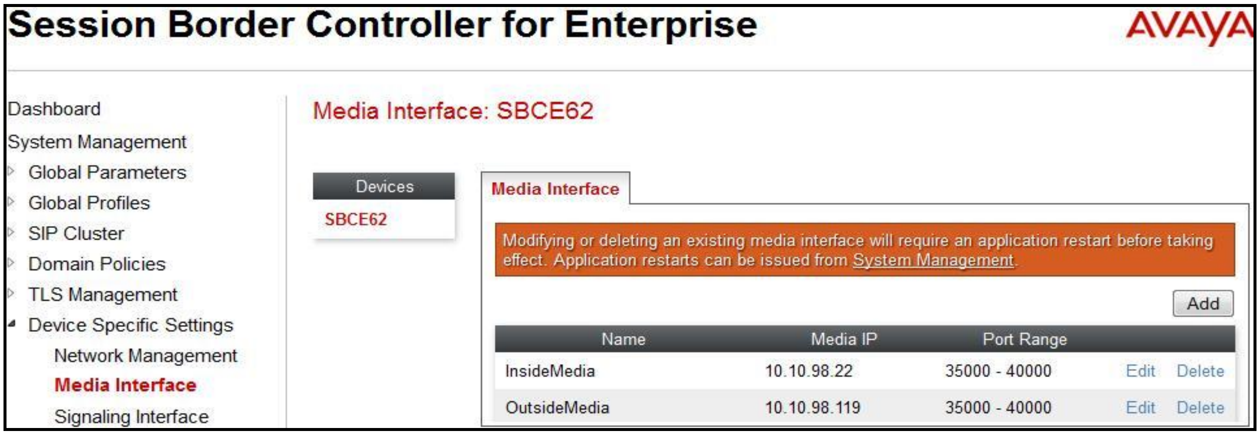
7.4.2. Media Interface

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.



Media Interface: SBCE62

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

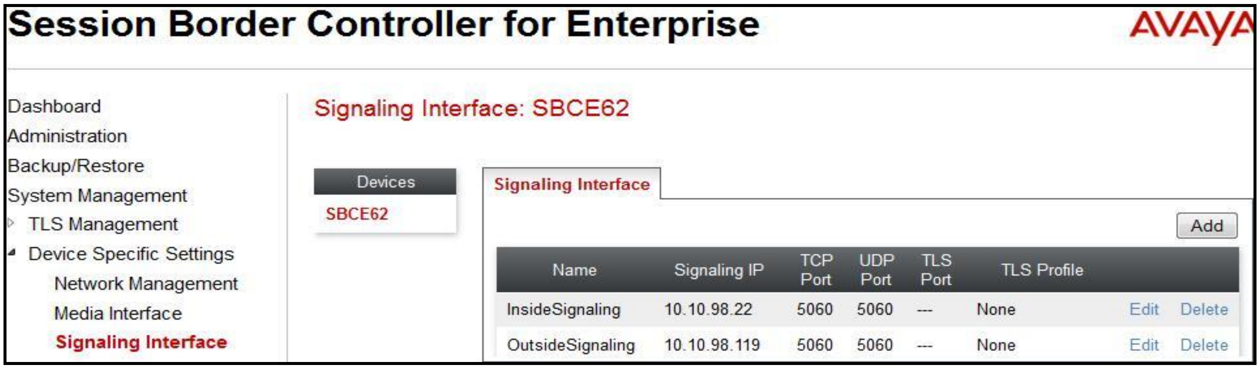
Name	Media IP	Port Range		
InsideMedia	10.10.98.22	35000 - 40000	Edit	Delete
OutsideMedia	10.10.98.119	35000 - 40000	Edit	Delete

7.4.3. 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 SP and TCP/5060 for the inside interface to EN.



Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
InsideSignaling	10.10.98.22	5060	5060	---	None	Edit	Delete
OutsideSignaling	10.10.98.119	5060	5060	---	None	Edit	Delete

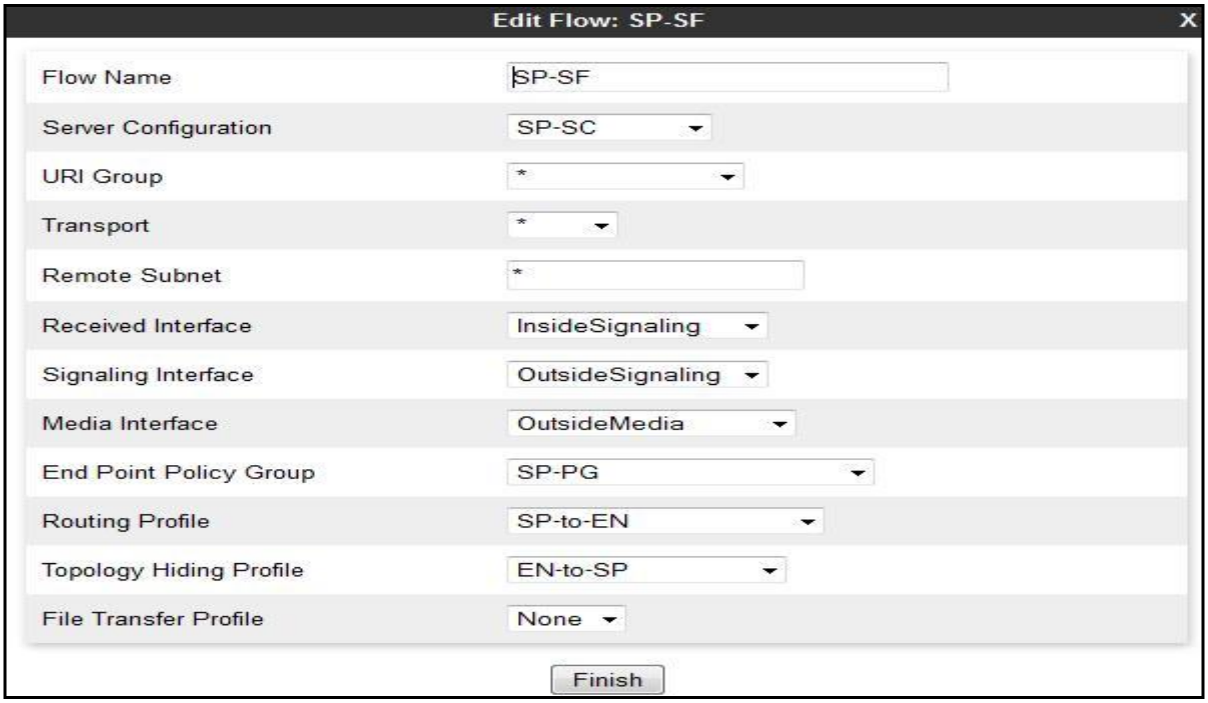
7.4.4. End Point Flows - Server Flow

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 screens illustrate the flow through the Avaya SBCE to secure a SIP Trunk call.

In the compliance testing, separate Server Flows were created for SP and EN. 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 7.2.6** to assign to the Flow.
- **URI Group**: Select the URI Group created in **Section 7.2.1** 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 7.4.3** that the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface**: Select the Signaling Interface created in **Section 7.4.3** used to communicate with the Server Configuration.
- **Media Interface**: Select the Media Interface created in **Section 7.4.2** used to communicate with the Server Configuration.
- **End Point Policy Group**: Select the End Point Policy Group created in **Section 7.3.2** to assign to the Server Configuration.
- **Routing Profile**: Select the Routing Profile created in **Section 7.2.2** that the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile**: Select the Topology-Hiding profile created in **Section 7.2.3** to apply to the Server Configuration.
- Click **Finish**.

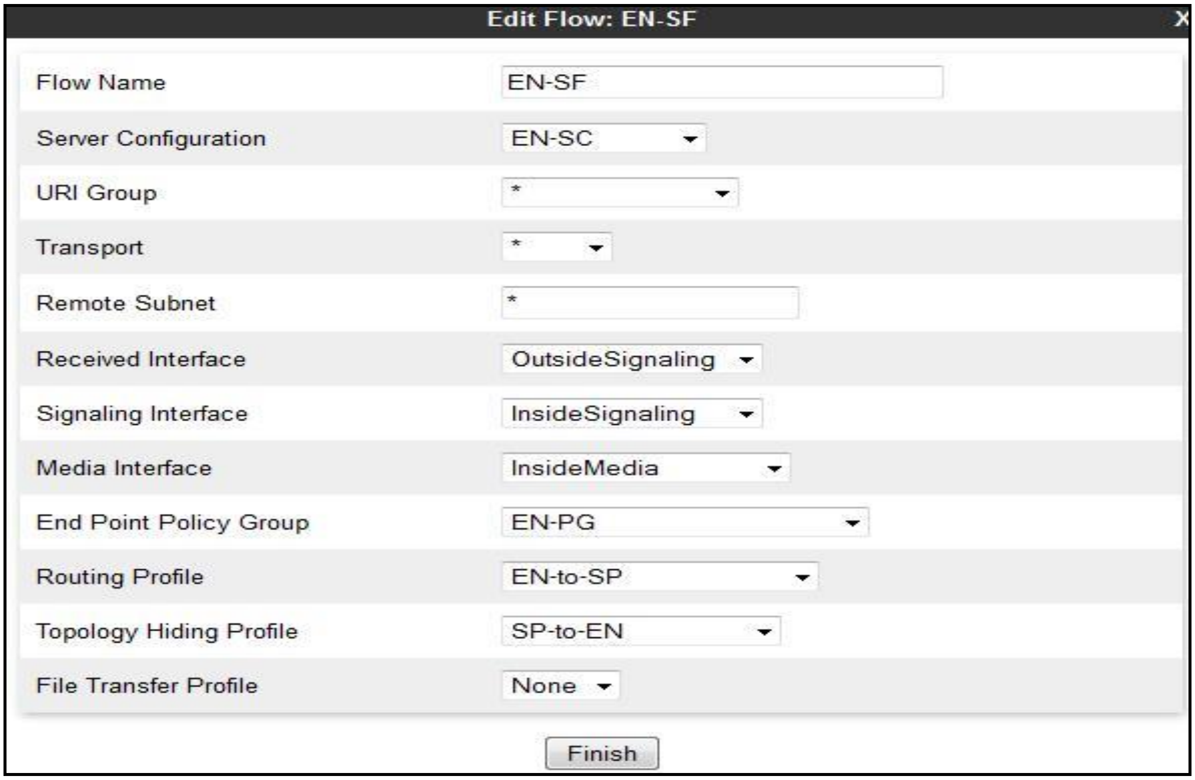
The following screen shows the Server Flow **SP-SF** configured for SP.



Edit Flow: SP-SF

Flow Name	SP-SF
Server Configuration	SP-SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	InsideSignaling
Signaling Interface	OutsideSignaling
Media Interface	OutsideMedia
End Point Policy Group	SP-PG
Routing Profile	SP-to-EN
Topology Hiding Profile	EN-to-SP
File Transfer Profile	None

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



Edit Flow: EN-SF

Flow Name	EN-SF
Server Configuration	EN-SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	OutsideSignaling
Signaling Interface	InsideSignaling
Media Interface	InsideMedia
End Point Policy Group	EN-PG
Routing Profile	EN-to-SP
Topology Hiding Profile	SP-to-EN
File Transfer Profile	None

8. Bell Canada Service Configuration

Bell 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. Bell will provide the customer with the necessary information to configure the SIP connection from the enterprise to Bell. The information provided by Bell 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).
- Bell SIP domain. In the compliance testing, Bell preferred to use IP address as an URI-Host.
- CPE SIP domain. In the compliance testing, Bell preferred to use IP address of the Avaya SBCE as an URI-Host.
- Supported codecs.
- DID numbers.

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

9. Verification and Troubleshooting

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

9.1. 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.

9.2. 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.

9.3. Troubleshooting:

9.3.1. The Avaya SBCE

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

Following is an example inbound call from Bell to the enterprise.

- Inbound INVITE request from Bell:

```
INVITE sip:613XXX6507@vendor6.xxx.internetxxxxx.ca;transport=udp SIP/2.0
Via: SIP/2.0/UDP 192.168.237.209:5060;branch=z9hG4bKbmob192030k19hv5s0q0.1
From: <sip:+01116139675258@sipxxxxxxxx.bell.ca;user=phone>;tag=SDqc8te01-744430387-
1414076590590-
To: "User 613XXX6507"<sip:613XXX6507@vendor6.xxx.internetxxxxx.ca>
Call-ID: SDqc8te01-067607d846d568de1c845a75d00338bf-a80e7b0
CSeq: 516175104 INVITE
Contact: <sip:+01116139675258@192.168.237.209:5060;transport=udp>
Supported: 100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp,multipart/mixed
Max-Forwards: 19
Content-Type: application/sdp
Content-Length: 250
Route: <sip:613XXX6507@vendor6.xxx.internetxxxxx.ca:5060;lr>

v=0
o=- 1640366883 1 IN IP4 192.168.237.209
s=-
c=IN IP4 192.168.237.209
t=0 0
m=audio 49158 RTP/AVP 96 18 0 101
a=rtpmap:96 G729/8000
a=fmtp:96 annexb=no
a=rtpmap:18 G729/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

- 200OK/SDP response by the enterprise:

```
SIP/2.0 200 OK
From: <sip:01116139675258@sipxxxxxxxx.bell.ca;user=phone>;tag=SDqc8te01-744430387-
1414076590590-
To: "User 613XXX6507"
<sip:613XXX6507@vendor6.xxx.internetxxxxx.ca>;tag=0a0d1d22460e411352545620a100
CSeq: 516175104 INVITE
Call-ID: SDqc8te01-067607d846d568de1c845a75d00338bf-a80e7b0
Contact: "SIP, 60397" <sip:+613XXX6507@10.10.98.119:5060;user=phone;gsid=a841c550-
5ac4-11e4-a084-
e41f13b32ca8;epv=%3csip:60397%40avayalab.com%3bgr%3d1ad4a284d2508bbb094c3fa81cf792a5%
3e>
Record-Route: <sip:10.10.98.119:5060;ipcs-line=236624;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 one-X Deskphone 6.4.0.33 (33)
Via: SIP/2.0/UDP 192.168.237.209:5060;branch=z9hG4bKbmob192030k19hv5s0q0.1
Accept-Language: en
Server: Avaya CM/R016x.03.0.124.0 AVAYA-SM-6.3.7.0.637008
P-Asserted-Identity: "SIP, 60397"
<sip:+613XXX6507@vendor6.xxx.internetxxxxx.ca;user=phone>
Session-Expires: 1200;refresher=uas
Content-Type: application/sdp
Endpoint-View: <sip:60397@avayalab.com;gr=1ad4a284d2508bbb094c3fa81cf792a5>;local-
tag=544924fc-4b6d991f201a6u203xck5i3z16123r536g2w6c2b5w_T6039710.33.5.71;call-
id=0a0d1d22460e411752545620a100;remote-tag=0a0d1d22460e411652545620a100
P-Location:
SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Belleville"
;termlocname="Belleville";termsiglocname="Belleville";termmedialocname="Belleville";s
maccounting="true"
Av-Global-Session-ID: a841c550-5ac4-11e4-a084-e41f13b32ca8
P-AV-Message-Id: 1_3
Content-Length: 192

v=0
o=- 1414076802 2 IN IP4 10.10.98.119
s=-
c=IN IP4 10.10.98.119
b=TIAS:64000
t=0 0
m=audio 35762 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=ptime:20
```

Following is an example outbound call from the enterprise to Bell.

- Outbound INVITE request from the enterprise:

```
INVITE sip:6139675203@sipxxxxxxxx.bell.ca;user=phone SIP/2.0
From: "SIP, 60397"
<sip:613XXX6507@vendor6.xxx.internetxxxxx.ca;user=phone>;tag=06658c02660e414952545620
a100
To: <sip:6139675203@sipxxxxxxxx.bell.ca>
CSeq: 2 INVITE
Call-ID: cb59a35669d7a708beb06252b274bb5b
Contact: "SIP, 60397" <sip:613XXX6507@10.10.98.119:5060;gsid=92c620c0-5ac6-11e4-a084-
e41f13b32ca8;epv=%3csip:60397%40avayalab.com%3bgr%3d1ad4a284d2508bbb094c3fa81cf792a5%
3e>
Record-Route: <sip:10.10.98.119:5060;ipcs-line=236867;lr;transport=udp>
Allow: INVITE, ACK, BYE, CANCEL, SUBSCRIBE, NOTIFY, REFER, INFO, PRACK, PUBLISH,
UPDATE
Supported: 100rel, join, replaces, sdp-anat, timer
User-Agent: Avaya one-X Deskphone 6.4.0.33 (33) AVAYA-SM-6.3.7.0.637008 Avaya
CM/R016x.03.0.124.0 AVAYA-SM-6.3.7.0.637008
Max-Forwards: 60
Via: SIP/2.0/UDP 10.10.98.119:5060;branch=z9hG4bK-s1632-001348934609-1--s1632-
Accept-Language: en
Alert-Info: <cid:internal@avayalab.com>;avaya-cm-alert-type=internal
Authorization: Digest username="VEND6_613XXX6506_01A", realm="sipxxxxxxxx.bell.ca",
nonce="BroadWorksXi1m96nccTgjzj6jBW", uri="sip:avayalab.com",
response="df43da00454800d38b14d203941fa193", algorithm=MD5, cnonce="0a4f113b",
qop=auth, nc=00000001
P-Asserted-Identity: "SIP, 60397"
<sip:613XXX6507@vendor6.xxx.internetxxxxx.ca;user=phone>
Session-Expires: 1200;refresher=uac
Min-SE: 1200
Content-Type: application/sdp
Endpoint-View: <sip:60397@avayalab.com;gr=1ad4a284d2508bbb094c3fa81cf792a5>;local-
tag=54492833-74d8b18c5d165hc1k46452l3m3ax66494y27u15u_F6039710.33.5.71;call-
id=55_54492833-1690d37a2v401y3ar5b325w1pnp2f4d351t5oj2p_I6039710.33.5.71
P-AV-Message-Id: 1_2
P-Charging-Vector: icid-value="92c620c0-5ac6-11e4-a084-e41f13b32ca8"
Av-Global-Session-ID: 92c620c0-5ac6-11e4-a084-e41f13b32ca8
P-Location:
SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Belleville"
;termlocname="Belleville";termsiglocname="Belleville";smaccounting="true"
Content-Length: 274

v=0
o=- 1414077630 1 IN IP4 10.10.98.119
s=-
c=IN IP4 10.10.98.119
b=TIAS:64000
t=0 0
a=avf:avc=n prio=n
a=csup:avf-v0
m=audio 35766 RTP/AVP 0 18 120
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:120 telephone-event/8000
a=ptime:20
```

- 200OK/SDP response by Bell:

```
SIP/2.0 200 OK
From: "SIP, 60397"
<sip:613XXX6507@vendor6.xxx.internetxxxxx.ca;user=phone>;tag=06658c02660e414952545620a100
To: <sip:6139675203@sipxxxxxxxx.bell.ca>;tag=SDe3l4099-348405768-1414077419427
CSeq: 2 INVITE
Call-ID: cb59a35669d7a708beb06252b274bb5b
Via: SIP/2.0/UDP 10.10.98.119:5060;branch=z9hG4bK-s1632-001348934609-1--s1632-
Record-Route: <sip:10.10.98.119:5060;ipcs-line=236867;lr;transport=udp>
Supported:
Contact: <sip:6139675203@192.168.237.206:5060;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 177

v=0
o=- 1638271014 1 IN IP4 192.168.237.206
s=-
c=IN IP4 192.168.237.206
t=0 0
m=audio 49182 RTP/AVP 0 120
a=rtpmap:120 telephone-event/8000
a=fmtp:120 0-15
a=ptime:20
```

9.3.2. 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.

10. Conclusion

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

All of the test cases were 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 Bell Canada SIP Trunking Service is considered **compliant** with Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.3.

11.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 6.3.4, July 2014.

[2] *Administering Avaya Aura® System Platform*, Release 6.3.4, July 2014.

[3] *Administering Avaya Aura® Session Manager,* Release 6.3, September 2014.

[4] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* Release 3.2, January 2013.

[5] *Administering Avaya one-X®Deskphone SIP for9620/9620C/9620L/9630/9630G/9640/9640G/9650/9650C IP deskphones,Release 2.6.10, May* 2013.

[6] *Administering Avaya one-X® Communicator*, July 2013.

[7] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, June 2013.

[8] *Administering Avaya Session Border Controller for Enterprise,* Release 6.2, June 2014.

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

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

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

Product documentation for Bell Networks' SIP Trunking Solution is available from Bell.

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.