Avaya Solution & Interoperability Test Lab

Application Notes for Configuring TELUS SIP Trunking Release 2 using SIP Registration with Avaya Aura® Communication Manager 7.1, Avaya Aura® Session Manager 7.1 and Avaya Session Border Controller for Enterprise 7.2 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between TELUS and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 7.1, Avaya Aura® Communication Manager 7.1, Avaya Session Border Controller for Enterprise 7.2 and various Avaya endpoints.

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

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

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between TELUS and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 7.1, Avaya Aura® Communication Manager 7.1, Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.2 and various Avaya endpoints.

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to TELUS SIP Trunk via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and the Avaya SBCE with various types of Avaya phones.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the TELUS SIP Trunk Service did not include use of any specific encryption features as requested by TELUS.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various Avaya deskphone types including H.323, SIP, digital, and analog at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider
- Outgoing PSTN calls from various Avaya deskphone types including H.323, SIP, digital, and analog at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider
- Inbound and outbound PSTN calls to/from softphones. Two Avaya soft phones were used in testing: Avaya one-X® Communicator (1XC) and Avaya Equinox™ for Windows. 1XC supports two work modes (Computer and Other Phone). Each supported mode was tested. 1XC also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Both protocols were tested. Avaya Equinox™ for Windows was used in testing as a simple SIP endpoint for basic inbound and outbound calls
- SIP transport using UDP, port 5060, between the Avaya enterprise and TELUS
- Direct IP-to-IP Media (also known as "Shuffling") over a SIP Trunk. Direct IP-to-IP Media allows Communication Manager to reconfigure the RTP path after call establishment directly between the Avaya phones and the Avaya SBCE releasing media processing resources on the Avaya Media Gateway or Avaya Media Server.
- Various call types including: local call, international, outbound toll-free.
- Codec G.711MU, G.729A
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call transfer, conference, off-net call forwarding, forwarding to Avaya Aura® Messaging and EC500 mobility (extension to cellular)
- SIP re-Invite/Refer in off-net call transfer
- SIP Diversion/PAI header in off-net call forward
- Call Center scenarios
- Fax using G.711 pass through and T.38 modes
- DTMF - RFC2833
- Registration and Authentication
- Remote Worker

The following was not supported and not tested:

- TELUS does not support TLS/SRTP SIP Transport
- TELUS supports inbound toll-free service, however there was no inbound toll-free numbers built in their production lab during the compliance testing

- TELUS supports outbound call to international number, however this call was not available in TELUS production lab during the compliance testing
- TELUS supports outbound call to Local Directory Assistance service 411, however this call was not available in TELUS production lab during the compliance testing
- TELUS supports outbound call to Emergency 911, however this call was not available in TELUS production lab during the compliance testing

2.2. Test Results

Interoperability testing of TELUS SIP Trunk was completed successfully with the below observation:

- Multiple “481 Call Leg/Transaction Does Not Exist” SIP messages are generated for transfer/conference scenarios. This is essentially a race condition. For example, after the REFER for a transfer is sent, both parties send a BYE for the call leg going away. When Avaya receives another BYE from TELUS, it responds with a "481 Call Leg/Transaction Does Not Exist" (since each party has already sent its own BYE for that call leg). The transfer/conference calls were not impacted and still worked well

2.3. Support

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

For technical support on TELUS SIP Trunking, contact TELUS at http://www.TELUS.com/business/voice-networks/ip-trunking/

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to TELUS SIP Trunk. This is the configuration used for compliance testing.

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. The 10.10.98.X network has been subdivided and the inside of the SBCE is connected to the 10.10.98.0/25 network while the outside of the SBCE is connected to the 10.10.98.96/27 network.

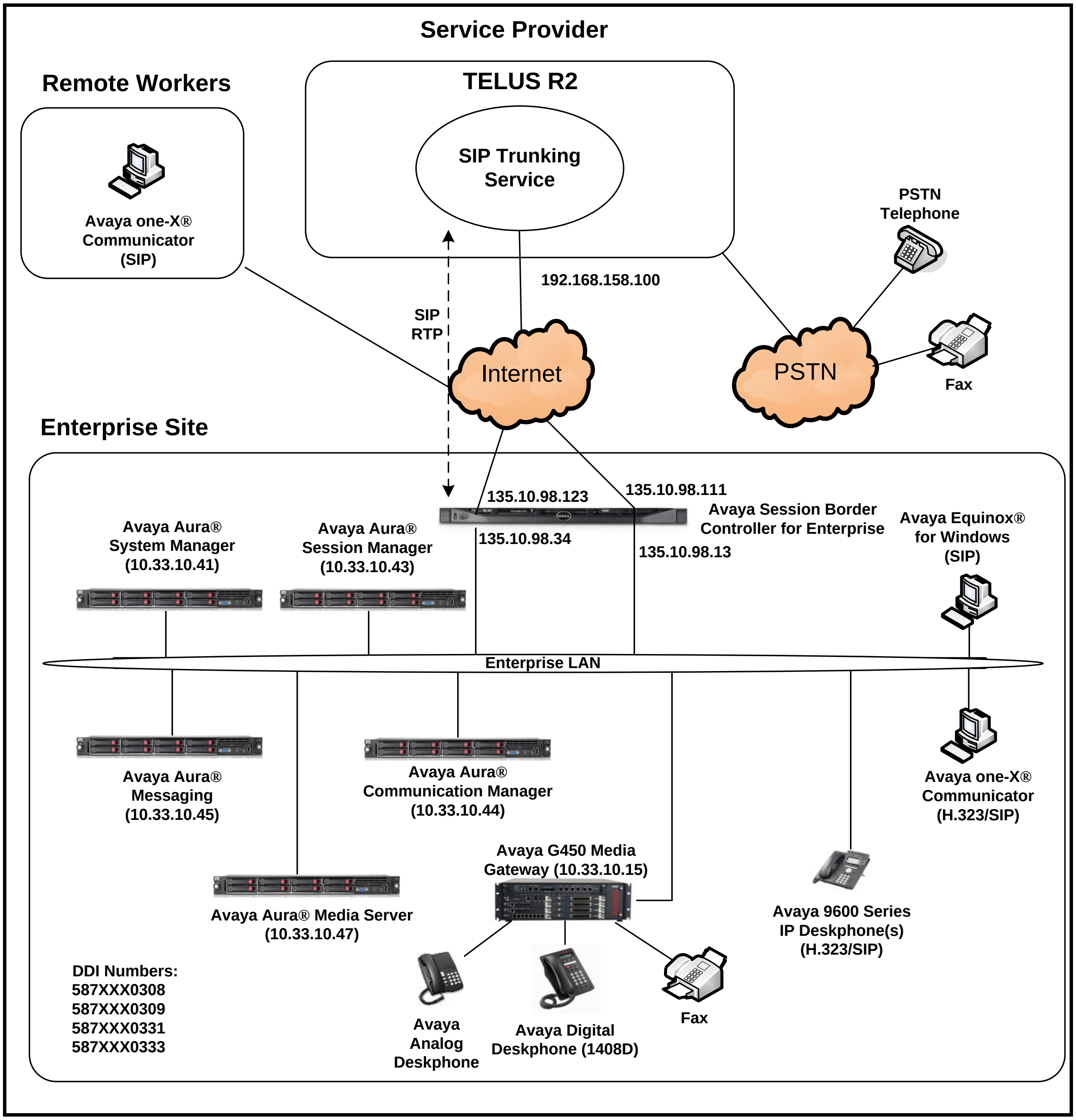

Figure 1: Avaya IP Telephony Network and TELUS SIP Trunk

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	**Release/Version**
Avaya Aura® Communication Manager running on VMware®-based Avaya appliance	7.1 (R017x.01.0.532.0-24598)
Avaya G450 Media Gateway – MM711AP Analog – MM712AP Digital – MM710AP	HW2 FW38.21 HW46 FW096 HW10 FW014 HW5 FW020
Avaya Aura® Session Manager running on VMware®-based Avaya appliance	7.1.3.0.713014
Avaya Aura® System Manager running on VMware®-based Avaya appliance	7.1.3.0 Build No. – 7.1.0.0.1125193 Software Update Revision No: 7.1.3.0.037763 Feature Pack 3
Avaya Aura® Messaging running on VMware®-based Avaya appliance	7.0.0.0.441.0.117.4 - SP0 (Patch 3 - N7.0-52.0-017Caa+Aac+----mae+-)
Avaya Aura® Media Server running on VMware®-based Avaya appliance	8.0.0.8
Avaya Session Border Controller for Enterprise running on Dell R210 V2 Server	7.2.1.0-05-14222
Avaya 9621G IP Deskphone (SIP)	Avaya® Deskphone SIP 7.1.2.0.14
Avaya 9621G IP Deskphone (H.323)	Avaya® IP Deskphone 6.6.5
Avaya 9641 IP Deskphone (H.323)	Avaya® IP Deskphone 6.6.5
Avaya Digital Deskphone (1408D)	R48
Avaya Equinox™ for Windows	3.4.0.152.46
Avaya one-X® Communicator (H.323 & SIP)	6.2.12.22-SP12-P12
Avaya Analog Deskphone	N/A
HP Officejet 4500 Fax	N/A
TELUS SIP Trunk Components	
Equipment/Software	**Release/Version**
Ribbon	C20 R19
Oracle SBC	7.4m1p5

Table 1: Equipment and Software Tested

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

Note: From Release 7.0, Avaya uses the VMware®- based Avaya Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya appliance offer. Avaya-appliance offer includes:

- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, HP ProLiant DL360 G7 (It was used for the compliance testing), and HP ProLiant DL360p G8.
- S8300D and S8300E.

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. With Appliance Virtualization Platform, customers can run any combination of supported applications such as Avaya Aura® Communication Manager, Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Messaging, and Avaya Aura® Media Server on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements. Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.

It is assumed the general installation of VMware®- based Avaya Appliance Virtualization Platform, Avaya Aura® Communication Manager, Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Messaging, Avaya Aura® Media Server and Avaya Media Gateway has been previously completed and is not discussed in this document.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for TELUS SIP Trunk.

The Communication Manager configuration 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 the service provider. The example shows that 4000 SIP trunks are available and 100 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 4000  0
           Maximum Concurrently Registered IP Stations: 2400  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  5
                       Maximum Administered SIP Trunks: 4000  100
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

Figure 2: System-Parameters Customer-Options Form – Page 2

On **Page 4**, verify that **ARS** is set to **y**.

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
  A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                      DCS (Basic)? y
          ASAI Link Core Capabilities? y                DCS Call Coverage? y
          ASAI Link Plus Capabilities? y               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n     Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? Y
```

Figure 3: System-Parameters Customer-Options Form – Page 4

On **Page 6**, verify that **Private Networking** and **Processor Ethernet** are set to **y**.

```
display system-parameters customer-options                      Page   6 of  11
                                OPTIONAL FEATURES

                Multinational Locations? n             Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n      Station as Virtual Extension? y
                    Multiple Locations? n
                                           System Management Data Transfer? n
           Personal Station Access (PSA)? y               Tenant Partitioning? y
                       PNC Duplication? n       Terminal Trans. Init. (TTI)? y
                  Port Network Support? n               Time of Day Routing? y
                       Posted Messages? y       TN2501 VAL Maximum Capacity? y
                                                        Uniform Dialing Plan? y
                    Private Networking? y     Usage Allocation Enhancements? y
              Processor and System MSP? y
                    Processor Ethernet? y                 Wideband Switching? y
                                                                    Wireless? n
                         Remote Office? y
          Restrict Call Forward Off Net? y
                 Secondary Data Module? y
```

Figure 4: System-Parameters Customer-Options Form – Page 6

5.2. System Features

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

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

Figure 5: System-Parameters Features Form – Page 1

On **Page 9**, verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **anonymous** for both. The value of **anonymous** is replaced for restricted numbers and unavailable numbers (refer to **Section 5.8**).

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

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

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

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

SCCAN PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

Figure 6: System-Parameters Features Form – Page 9

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 as below:

- Messaging: **Name**: **AAMVM**, **IP Address**: **10.33.10.45**
- Media Server: **Name**: **AMS**, **IP Address**: **10.33.10.47**
- Session Manager: **Name**: **bvwasm2**, **IP Address**: **10.33.10.43**
- Communication Manager: **Name**: **procr**, **IP Address**: **10.33.10.44**

These node names will be needed for defining the service provider signaling group in **Section 5.7**.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name               IP Address
AAMVM                10.33.10.45
AMS                  10.33.10.47
bvwasm2              10.33.10.43
default              0.0.0.0
procr                10.33.10.44
procr6               ::
```

Figure 7: Node-Names IP Form

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. In the compliance test, **ip-codec-set 1** was used for this purpose. TELUS supports the **G.711MU**, and **G.729A** codecs. Default values can be used for all other fields.

```
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.729A        n            2        20


Media Encryption                          Encryption SRCTP: enfore-unenc-srtcp
1: 1-srtp-aescm128-hmac80
2: none
```

Figure 8: IP-Codec-Set Form – Page 1

On **Page 2**, set the **FAX Mode** to **t.38-standard** or **pass-through**. TELUS supports Fax using either T.38 or pass-through modes.

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

                          IP CODEC SET

                              Allow Direct-IP Multimedia? n



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

Figure 9: IP-Codec-Set Form – Page 2

5.5. IP Network Region for Media Gateway, Media Server

Network region provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, both Avaya G450 Media Gateway and Avaya Media Server were tested and used region 1. For the compliance test, IP network region **1** was chosen for the service provider trunk.

Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **bvwdev.com**. This name appears in the From header of SIP messages originating from this IP region
- Enter a descriptive name in the **Name** field
- Enable IP-IP Direct Audio (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya Media Server. Set both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes**. Shuffling can be further restricted at the trunk level on the Signaling Group form in **Section 5.7**
- 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: bvwdev.com
    Name: procr                 Stub Network Region: n
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
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Figure 10: IP-Network-Region Form

The following display command shows that **media-gateway 1** is an Avaya G450 Media Gateway configured for **Network Region 1**. It can also be observed that the **Controller IP Address** is the Avaya Processor Ethernet (**10.33.10.44**), and that the gateway **MGP IPv4 Address** is **10.33.10.15**. These fields are not configured in this screen, but just display the current information for the Media Gateway.

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

                    Type: g450
                    Name: g450
               Serial No: 12TGXXX00244
    Link Encryption Type: any-ptls/tls       Enable CF? n
          Network Region: 1                   Location: 1
                                             Site Data:
           Recovery Rule: none

             Registered?  y
   FW Version/HW Vintage: 38 .21 .0 /1
        MGP IPV4 Address: 10.33.10.15
        MGP IPV6 Address:
   Controller IP Address: 10.33.10.44
             MAC Address: 3c:3a:73:6b:c5:a8

   Mutual Authentication? optional
```

Figure 11: Media Gateway – Page 1

The following screen shows Page 2 for Media Gateway 1. The gateway has an **MM712** media module supporting Avaya digital phones in slot **V1**, an **MM711** supporting analog phones on slot **V2**, and the capability to provide announcements and music on hold via "**gateway-announcements**" in logical slot **V9**.

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

                                 Type: g450

Slot   Module Type             Name                     DSP Type  FW/HW version
 V1:   MM712                   DCP MM                   MP80      162   7
 V2:   MM711                   ANA MM
 V3:
 V4:
 V5:
 V6:
 V7:
 V8:                                                  Max Survivable IP Ext: 8
 V9:   gateway-announcements   ANN VMM
```

Figure 12: Media Gateway – Page 2

The following display command shows that **media-server 1** is an Avaya Media Server configured for **Network Region 1**. It can also be observed that the **Node Name: AMS** (Defined in **Section 5.3**) and the **Signaling Group: 11** (Defined in **Section 5.7**) have been used. These fields are not configured in this screen, but just display the current information for the Media Server.

```
display media-server 1
                                  MEDIA SERVER

                    Media Server ID: 1

                    Signaling Group: 11
         Voip Channel License Limit: 10
    Dedicated Voip Channel Licenses: 10

                          Node Name: AMS
                     Network Region: 1
                           Location: 1
          Announcement Storage Area:
```

Figure 13: Media Server

5.6. Configure IP Interface for procr

Use the **change ip-interface procr** command to change the Processor Ethernet (procr) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the procr for SIP Trunk signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones. Ensure **Enable Interface** is **y** and **Network Region** is **1**.

```
change ip-interface procr
                                  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

                                 IPV4 PARAMETERS
             Node Name: procr                   IP Address: 10.33.10.44
           Subnet Mask: /24
```

Figure 14: IP-Interface Form

5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups between Communication Manager and Session Manager. For the compliance test, signaling group **20** was used for both outbound and inbound calls between the service provider and the enterprise. It was configured using the parameters highlighted below. Note: The signaling group between Communication Manager and Session Manager used for SIP phones is not mentioned in these Application Notes.

- Set the **Group Type** field to **sip**
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager
- Set the **Transport Method** to the value of **tls** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**
- Set the **Far-end Node Name** to **bvwasm2**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port for TLS, such as **5061**

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**
- Set the **Far-end Domain** to **bvwdev.com**, the enterprise domain
- Set **Direct IP-IP Audio Connections** to **y**. This setting will enable media shuffling on the SIP trunk so that Communication Manager will re-route media traffic directly between the SIP trunk and the enterprise endpoint. Note that the Avaya G450 Media Gateway or Avaya Media Server will not remain in the media path of all calls between the SIP trunk and the endpoint
- Set the **Alternate Route Timer (sec)** to **6**. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval
- Default values may be used for all other fields

```
add signaling-group 20                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 20              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 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: bvwasm2
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1
                                   Far-end Secondary Node Name:
Far-end Domain: bvwdev.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

Figure 15: Signaling-Group 20

For the compliance test, signaling group **11** was used for the signaling group between Communication Manager and Media Server. It was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**
- Set the **Transport Method** to the value of **tls** (Transport Layer Protocol). The transport method specified here is used between Communication Manager and Media Server
- Set the **Peer Detection Enabled** field to **n** and **Peer Server** to **AMS**
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**

- Set the **Far-end Node Name** to **AMS**. This node name maps to the IP address of Media Server as defined in **Section 5.3**
- Set the **Near-end Listen Port** to **9061** and **Far-end Listen Port** to a valid unused port for TLS, such as **5071**
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**
- Set the **Far-end Domain** to **10.33.10.47**

```
change signaling-group 11                                       Page   1 of   2
                                SIGNALING GROUP

 Group Number: 11             Group Type: sip
                        Transport Method: tls


  Peer Detection Enabled? n  Peer Server: AMS



   Near-end Node Name: procr                 Far-end Node Name: AMS
 Near-end Listen Port: 9061                Far-end Listen Port: 5071
                                        Far-end Network Region: 1

Far-end Domain: 10.33.10.47
```

Figure 16: Signaling-Group 11

5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.7**.
For the compliance test, trunk group **20** was used for both outbound and inbound calls to the service provider. It 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. (i.e. ***020**). Note: Refer to **Section 5.10** for adding * in dialing plan
- Set Class of Restriction (**COR**) to **1**
- Set **Direction** to **two-way** for trunk group **20**
- Set the **Service Type** field to **public-ntwrk**
- Set **Member Assignment Method** to **auto**
- Set the **Signaling Group** to the signaling group configured in **Section 5.7**. Trunk group **20** was associated to signaling group **20**
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk
- Default values were used for all other fields

```
add trunk-group 20                                             Page   1 of  21
                                TRUNK GROUP

Group Number: 20                    Group Type: sip          CDR Reports: y
  Group Name: SIP Trunks                   COR: 1        TN: 1        TAC: *020
   Direction: two-way         Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 20
                                                     Number of Members: 50
```

Figure 17: Trunk-Group – Page 1

On **Page 2**, set the **Redirect On OPTIM Failure** timer to the same amount of time as the **Alternate Route Timer** on the signaling group form in **Section 5.7**. Note that the **Redirect On OPTIM Failure** timer is defined in milliseconds. Verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to the service provider. This value defines the interval that UPDATEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

```
add trunk-group 20                                              Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 6000

            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
```

Figure 18: Trunk-Group – Page 2

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end (refer to **Section 5.9** for the public-unknown-numbering format). The compliance test used 10 digit numbering format. Thus, **Numbering Format** was set to **public** and the **Numbering Format** field in the route pattern was set to **pub-unk** (see **Section 5.10**).

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

```
add trunk-group 20                                                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

                                         Hold/Unhold Notifications? y
                                 Modify Tandem Calling Number: no


 Show ANSWERED BY on Display? y
```

Figure 19: Trunk-Group – Page 3

On **Page 4**, the **Network Call Redirection** field should be set to **y** (default setting is n). This option is set to **y** so that CM will send SIP Refer in redirected calls. Note: In the compliance test, TELUS worked to use either SIP Refer or SIP re-Invite successfully in redirected calls.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **y**. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been redirected. Note: For voice mail purposes, Communication Manager sends SIP Invite with History Info to Avaya Aura Messaging. The **Diversion Header** is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. TELUS used PAI header in off-net call redirection instead.

```
add trunk-group 20                                                 Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? Y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? y
                                   Support Request History? y
                              Telephone Event Payload Type: 101

                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
```

Figure 20: Trunk-Group – Page 4

5.9. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "P-Asserted-Identity" headers. Since public numbering was selected to define the format of this number (**Section 5.8**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs), and it is used to authenticate the caller.

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single public-unknown-numbering entry can be applied for all extensions. In the compliance test, all stations with a 4-digit extension beginning with **03** will send the calling party number as the **CPN Prefix** plus the extension number.

Note: The entry applies to SIP connection to Session Manager, therefore the resulting number must be a complete E.164 number. Communication Manager automatically inserts a '+' in front of user number in From, P-Asserted-Identity, Contact, and Diversion headers. This plus sign will be removed by using the SIP manipulation on SBCE (See **Session 7.2.3**)

```
change public-unknown-numbering 0                                 Page   1 of   2
                           NUMBERING - PUBLIC/UNKNOWN FORMAT

Ext Ext              Trk        CPN             Total
Len Code             Grp(s)     Prefix         CPN Len

 4  03                20        587XXX           10         Total Administered: 2
                                                             Maximum Entries: 240
```

Figure 21: Public-Unknown-Numbering Form

5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit **6** is used as the ARS access code. Enterprise callers will dial **6** to reach an "outside line". This configuration is illustrated below. Use the **change dialplan analysis** command to define the **Dialed String** as following:

- **Dialed String** beginning with **03** for extension (**ext**)
- **Dialed String** beginning with **6** for feature access code (**fac**)
- **Dialed String** beginning with ***** for dial access code (**dac**). It is used for Trunk Access Code (TAC) defined on Trunk group 20 in **Section 5.8**

```
change dialplan analysis                                         Page   1 of  12
                               DIAL PLAN ANALYSIS TABLE
                                     Location: all          Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
    03       4    ext
    181      4    ext
    189      4    ext
    3        4    ext
    6        1    fac
    800      4    ext
    *        4    dac
```

Figure 22: Dialplan–Analysis Form

Use the **change feature-access-codes** command to configure **6** as the **Auto Route Selection (ARS) – Access Code 1**.

```
change feature-access-codes                                     Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialin3g List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *111
                       Answer Back Access Code:
                         Attendant Access code:
      Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) - Access Code 1: 6     Access Code 2:
                 Automatic Callback Activation:     Deactivation:
Call Forwarding Activation Busy/DA:        All:     Deactivation:
   Call Forwarding Enhanced Status:        Act:     Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:        Close Code:
```

Figure 23: Feature–Access-Codes Form

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **6**. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to **Route Pattern 20** which contains the SIP trunk group to the service provider (as defined next).

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

    Dialed            Total      Route       Call   Node  ANI
    String           Min  Max  Pattern      Type   Num   Reqd
      0               1    15     20         pubu
      1416           11    11     20         pubu          n
      1613           11    11     20         pubu          n
      1800           11    11     20         pubu          n
```

Figure 24: ARS–Analysis Form

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used in route pattern **20** for the compliance test.

- **Pattern Name**: Enter a descriptive name
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **20** 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**: Set this field to **pub-unk** since public-unknown-numbering format should be used for this route (see **Section 5.8**)

```
change route-pattern 20                                          Page   1 of   3
                    Pattern Number: 5   Pattern Name: SP
                             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: 20    0                                                               n   user
 2:                                                                       n   user
 3:                                                                       n   user
 4:                                                                       n   user
 5:                                                                       n   user
 6:                                                                       n   user

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

Figure 25: Route–Pattern Form

Use the **change cor 1** command to change the Class of Restriction (COR) for the outbound call over SIP trunk. Set **Calling Party Restriction**: **none**. This setting allows the outbound call using feature access code (fac) 6 over SIP trunks.

```
change cor 1                                                     Page   1 of  23
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description:

                      FRL: 0                                 APLT? y
   Can Be Service Observed? n           Calling Party Restriction: none
Can Be A Service Observer? n             Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                 Direct Agent Calling? n
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                  Can Change Coverage? n

            Access to MCT? y             Fully Restricted Service? n
Group II Category For MFC: 7             Hear VDN of Origin Annc.? n
         Send ANI for MFE? n              Add/Remove Agent Skills? n
            MF ANI Prefix:               Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                        Can Be Picked Up By Directed Call Pickup? n
                                      Can Use Directed Call Pickup? n
                                      Group Controlled Restriction: inactive
```

Figure 26: Class of Restriction Form

5.11. Incoming Call Handling Treatment

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. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by the service provider is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group **20**. Use the **change inc-call-handling-trmt trunk-group 20** to convert incoming DID numbers as followings:

- The incoming DID number **587XXX0333** to **8000** by deleting **10** of the incoming digits for voicemail testing purpose
- The incoming DID number **587XXX** to 4 digit extension by deleting **6** of the incoming digits for inbound call testing purpose

```
change inc-call-handling-trmt trunk-group 20                    Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/           Number     Number           Del Insert
 Feature            Len        Digits
 public-ntwrk       10         587XXX0333        10  8000
 public-ntwrk       10         587XXX            6
```

Figure 27: Inc-Call-Handling-Trmt Form

5.12. Contact Center Configuration

This section describes the basic commands used to configure Announcements, Hunt-Groups, Vector Directory Numbers (VDNs) and corresponding vectors. These vectors contain steps that invoke Communication Manager to perform various call-related functions.

5.12.1. Announcements

Various announcements will be used within the vectors. In the sample configuration, these announcements were sourced by the Avaya G450 Media Gateway. The following abridged list command summarizes the announcements used in conjunction with the vectors in this section. To add an announcement extension, use the command "add announcement <extension>". The extension is an unused extension number.

```
list announcement

                           ANNOUNCEMENTS/AUDIO SOURCES
Announcement                                                              Num of
Extension            Type       Name                         Source       Files
1898                 integrated SP2                           001V9       1
1899                 integrated SP1                           001V9       1
```

Figure 28: Announcement Configuration

5.12.2. ACD Configuration for Call Queued for Handling by Agent

This section provides a simple example configuration for VDN, vector, hunt-group, and agent-loginID used to queue inbound calls for handling by an agent.

The following screens show an example ACD hunt group. On page 1, note the bolded values.

```
display hunt-group 13                                              Page   1 of   3
                                    HUNT GROUP

      GROUP NUMBER: 13                                     ACD? y
                 Group Name: SP                          Queue? y
            GROUP EXTENSION: 3211                       Vector? y
                 GROUP TYPE: UCD-MIA
                         TN: 1
                        COR: 1                     MM Early Answer? n
      SECURITY CODE: 1234             Local Agent Preference? n
ISDN/SIP Caller Display:

                   Queue Limit: unlimited
            Calls Warning Threshold:      Port:
            Time Warning Threshold:      Port:
```

Figure 29: Hunt Group Configuration – Page 1

The following screens show an example ACD hunt group. On the abbreviated page 2 shown below, note that **Skill** is set to **y**.

```
display hunt-group 13                                           Page   2 of   3
                                  HUNT GROUP

       Skill? y              Expected Call Handling Time (sec): 180
         AAS? n              Service Level Target (% in sec): 80 in 20
```

Figure 30: Hunt Group Configuration – Page 2

VDN 0331, shown below, is associated with vector 3

```
display vdn 0331                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             EXTENSION: 0331
                                Name*: Contact Center
                           DESTINATION: VECTOR NUMBER        3
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none
```

Figure 31: VDN Configuration

In this simple example, vector 3 briefly plays ring back, then plays announcement 1899 (Step 02). This is an announcement heard when the call is first answered before the call is queued to the skill 13 (Step 03). If an agent is available to handle the call, the call will be delivered to the agent, if agent is not available, the call will be re-queued and the caller will hear announcement 1898 (Step 05). Once agent becomes available, the call will be delivered to the agent.

```
display vector 3                                               Page   1 of   6
                                 CALL VECTOR

      Number: 3              Name: Contact Center
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
Variables? y   3.0 Enhanced? y

01 wait-time    2   secs hearing ringback
02 announcement 1899
03 queue-to     skill 13   pri m
04 wait-time    2   secs hearing silence
05 announcement 1898
06 goto step    3            if unconditionally
```

Figure 32: Vector 3 Configuration

The following screen illustrates an example agent-loginID 3311. In the sample configuration, an Avaya IP Deskphone logged in using agent-loginID 3311 and the configured password to staff and take a call for skill 13.

```
add agent-loginID 3311                                      Page   1 of   2
                                 AGENT LOGINID

                Login ID: 3311                                  AAS? n
                    Name: SP                                  AUDIX? n
                      TN: 1                           LWC Reception: spe
                     COR: 1                  LWC Log External Calls? n
           Coverage Path:                  AUDIX Name for Messaging:
           Security Code: 1234
                                        LoginID for ISDN/SIP Display? n
                                                            Password: 1234
                                              Password (enter again): 1234
                                                         Auto Answer: station
                                                   MIA Across Skills: system
                                           ACW Agent Considered Idle: system
                                           Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                            Forced Agent Logout Time:   :
```

Figure 33: Agent-loginID Configuration – Page 1

The following abridged screen shows Page 2 for agent-loginID 3311. Note that the Skill Number (**SN**) has been set to **13**.

```
Display agent-loginID 3311                                         Page   2 of   2
                          AGENT LOGINID
      Direct Agent Skill:                                   Service Objective? n
Call Handling Preference: skill-level                  Local Call Preference? n

         SN   RL SL          SN   RL SL
      1: 13      1       16:
      2:                 17:
```

Figure 34: Agent LoginID Configuration – Page 2

To enable a telephone or one-X® Agent client to log in with the agent-loginID shown above, ensure that **Expert Agent Selection (EAS) Enabled** is set to **y** as shown in the screen below.

```
change system-parameters features                                    Page 11 of 19
             FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
EAS

Expert Agent Selection (EAS) Enabled? y
Minimum Agent-LoginID Password Length: 4
```

Figure 35: Enable Expert Agent Selection

5.13. Avaya Aura® Communication Manager Stations

In the sample configuration, four-digit station extensions were used with the format 03XX. Use the **add station 0308** command to add an Avaya H.323 IP Deskphone.

- Enter **Type**: **9641**, **Name**: **H323-0308**, **Security Code**: **1234**, **Coverage Path 1**: **1**, **IP SoftPhone**: **y** (if using this extension as a Softphone such as Avaya one-X® Communicator)
- Leave other values as default

```
add station 0308                                             Page   1 of   5
                                     STATION

Extension: 0308                          Lock Messages? n               BCC: 0
     Type: 9641                            Security Code: *            TN: 1
     Port: S000027                       Coverage Path 1: 1             COR: 1
     Name: H323-0308                          Coverage Path 2:          COS: 1
                                       Hunt-to Station:                Tests? y
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 0308
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: English                Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal             Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? y

                                                IP Video softphone? n
                                   Short/Prefixed Registration Allowed: default


                                            Customizable Labels? y
```

Figure 36: Add-Station Form

5.14. Save Avaya Aura® Communication Manager Configuration Changes

Use the **save translation** command to save the configuration.

6. Configure Avaya Aura® Session Manager

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

- SIP Domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which define route destinations and control call routing between the SIP Entities
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call

It may not be necessary to create all the items above when configuring 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. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL as **https://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. At the **System Manager Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button (not shown). The initial screen shown below is then displayed.

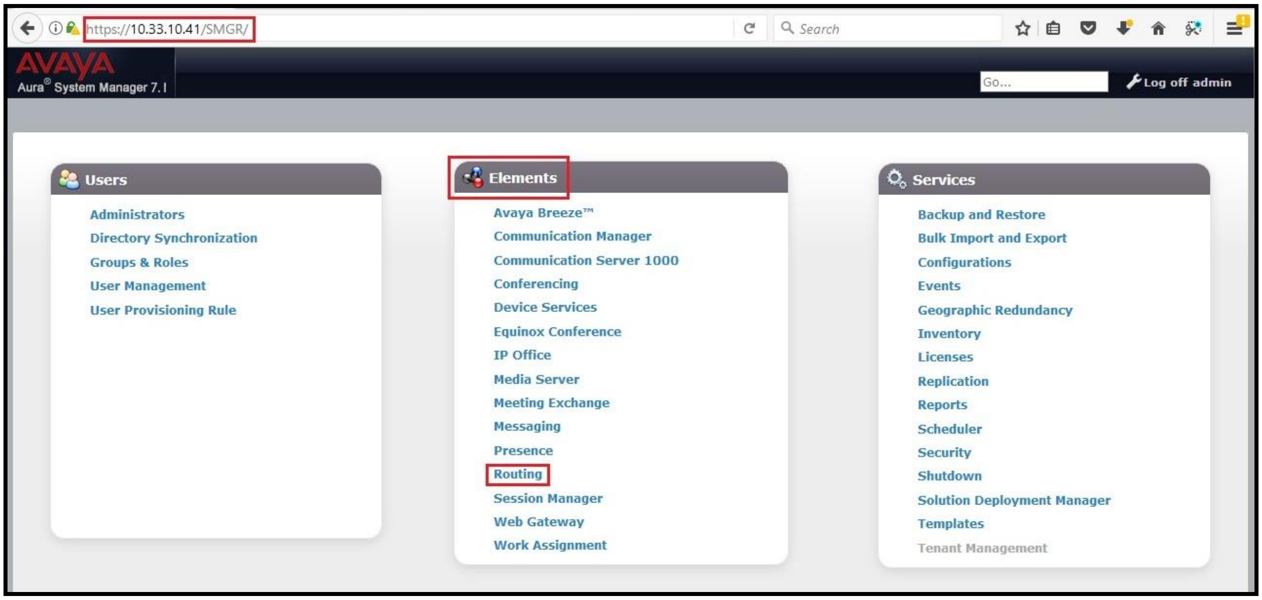

Figure 37: System Manager Home Screen

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.

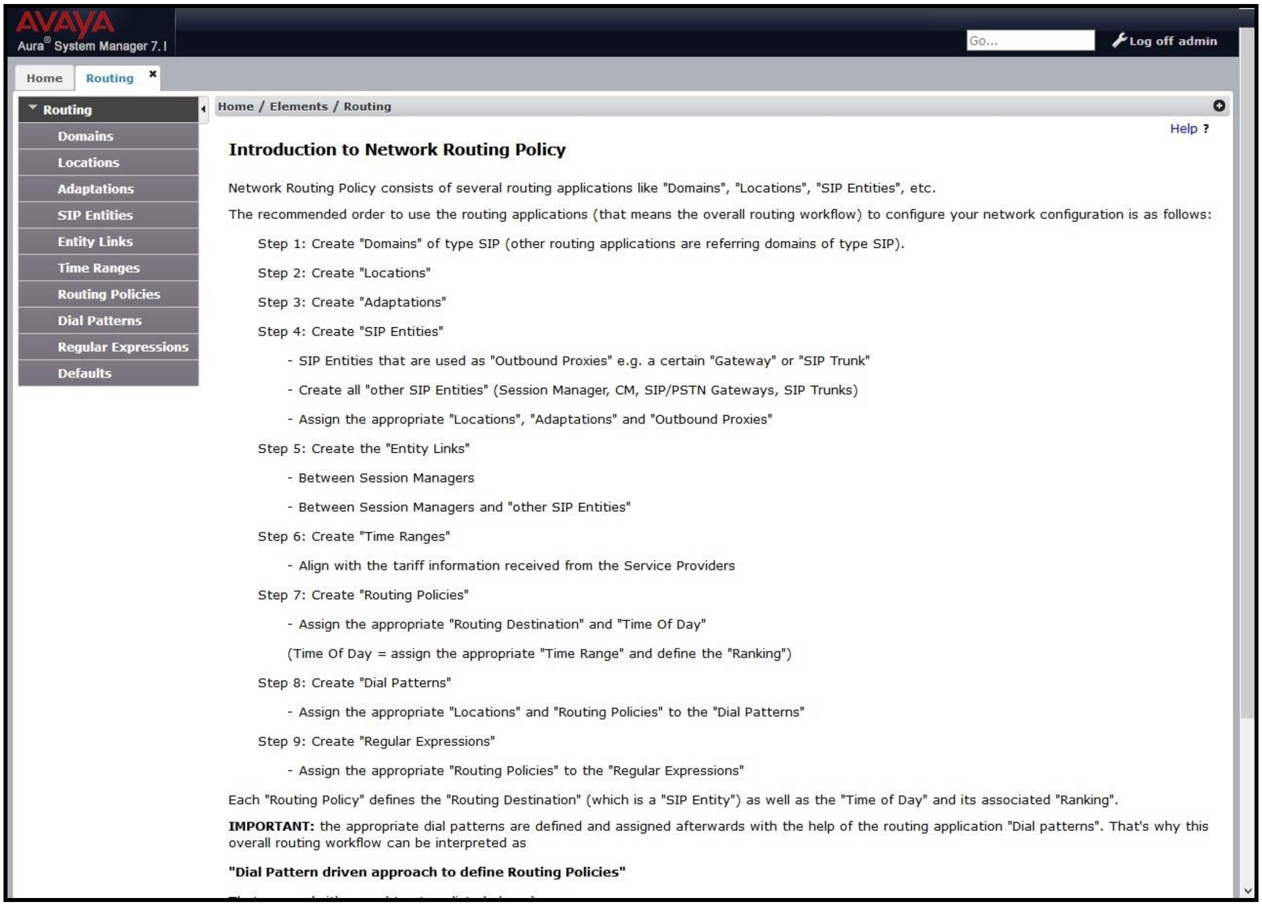

Figure 38: Network Routing Policy

6.2. Specify SIP Domain

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

Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane. In the new right pane that appears (not shown), fill in the following:

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

Click **Commit** (not shown) to save.

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

Figure 39: Domain Management

6.3. Add Location

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

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

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

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

Click **Commit** to save

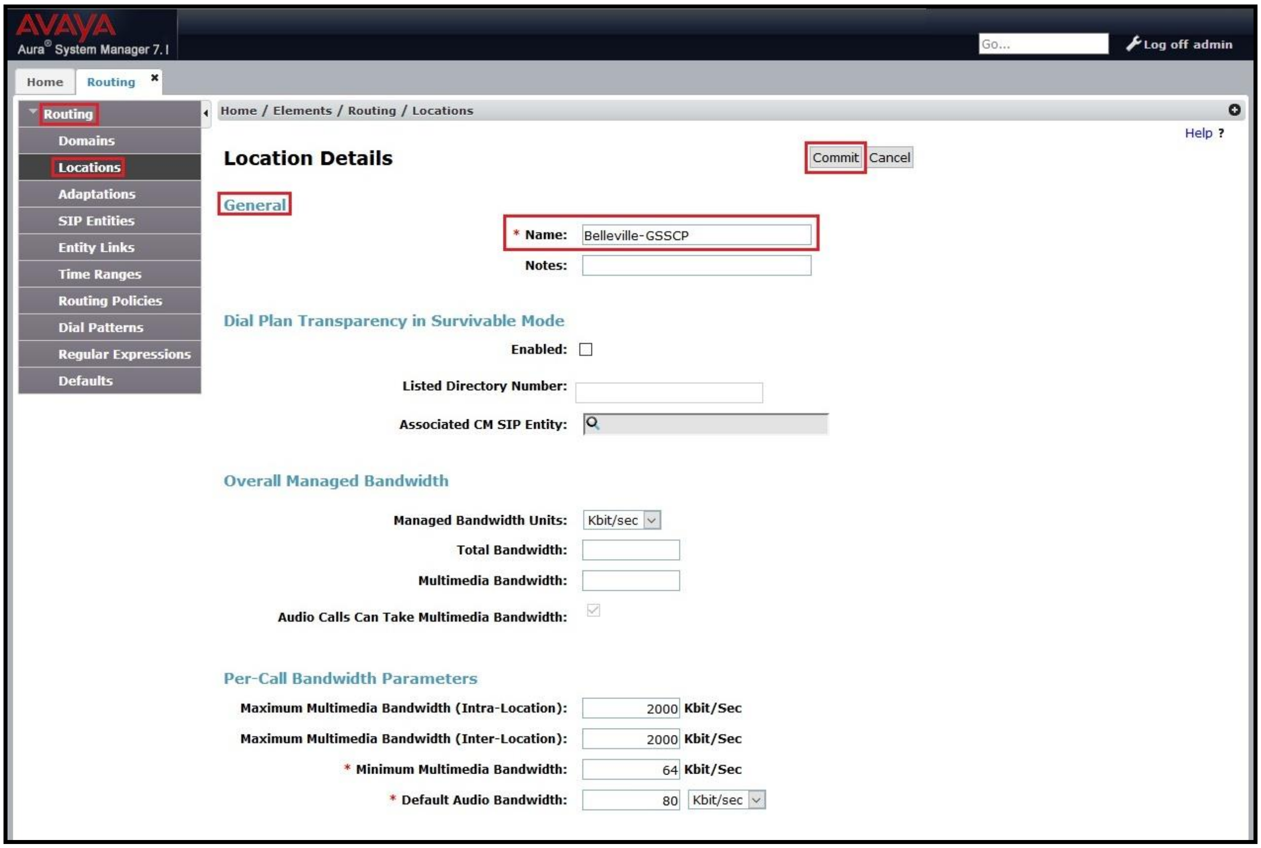

Figure 40: Location Configuration

In the **Location Pattern** section, click **Add** to enter **IP Address Pattern**. The following patterns were used in testing:

- **IP Address Pattern**: **10.33.10.***, **10.33.5.***, **10.10.98.***
- Click **Commit** to save

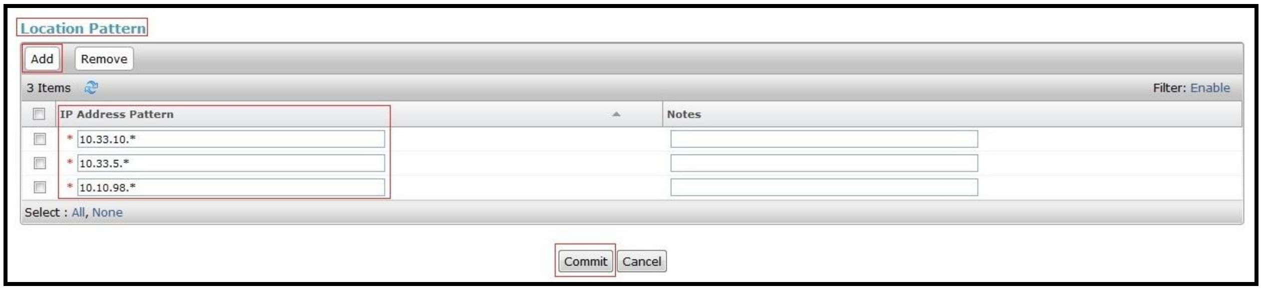

Figure 41: IP Ranges Configuration

Note: Call bandwidth management parameters should be set per customer requirement.

6.4. Add SIP Entities

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

Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

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

- **Name**: Enter a descriptive name
- **FQDN or IP Address**: Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling
- **Type**: Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for Avaya SBCE
- **Adaptation**: This field is only present if **Type** is not set to **Session Manager**. Adaptation modules were not used in this configuration
- **Location**: Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location **Belleville-GSSCP**
- **Time Zone**: Select the time zone for the Location above

In this configuration, there are three SIP Entities:

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Avaya Session Border Controller for Enterprise SIP Entity

6.4.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **bvwasm2**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.10.43**. The user will need to select the specific values for the **Location** and **Time Zone**.

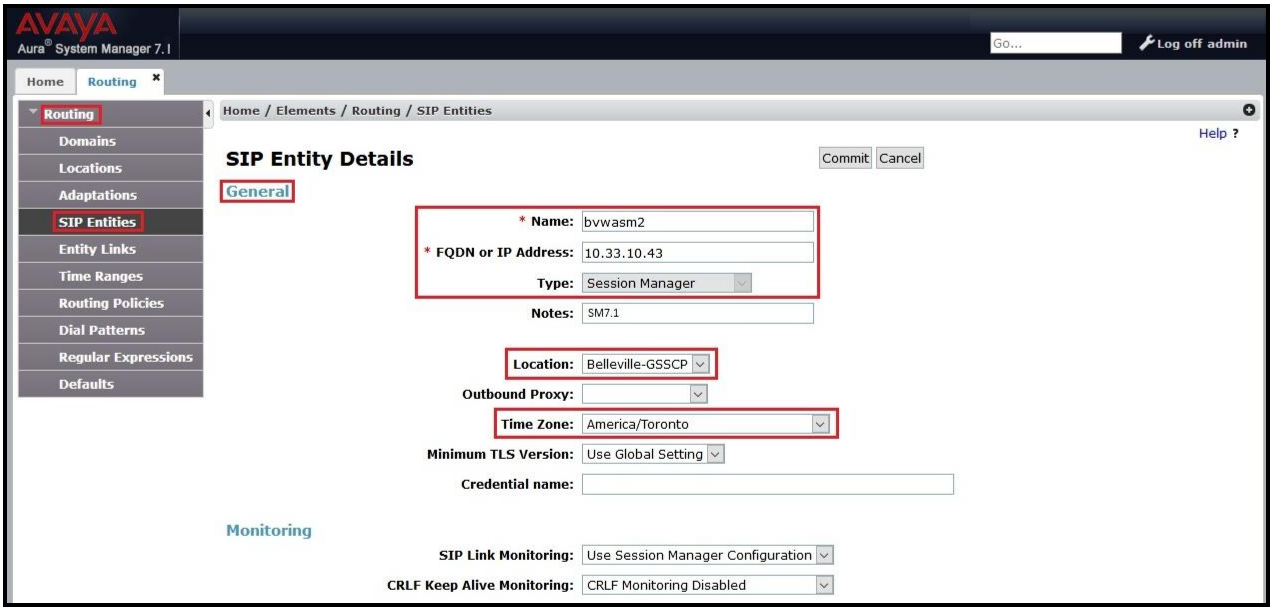

Figure 42: Session Manager SIP Entity

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

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

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

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

The compliance test used port **5061** with **TLS** for connecting to Communication Manager and Avaya SBCE

Figure 43: Session Manager SIP Entity Port

6.4.2. Configure Communication Manager SIP Entity

The following screen shows the addition of the Communication Manager SIP Entity named **CM71**. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created during Session Manager installation. The original SIP entity is used with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of Communication Manager **10.33.10.44**. Note that **CM** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

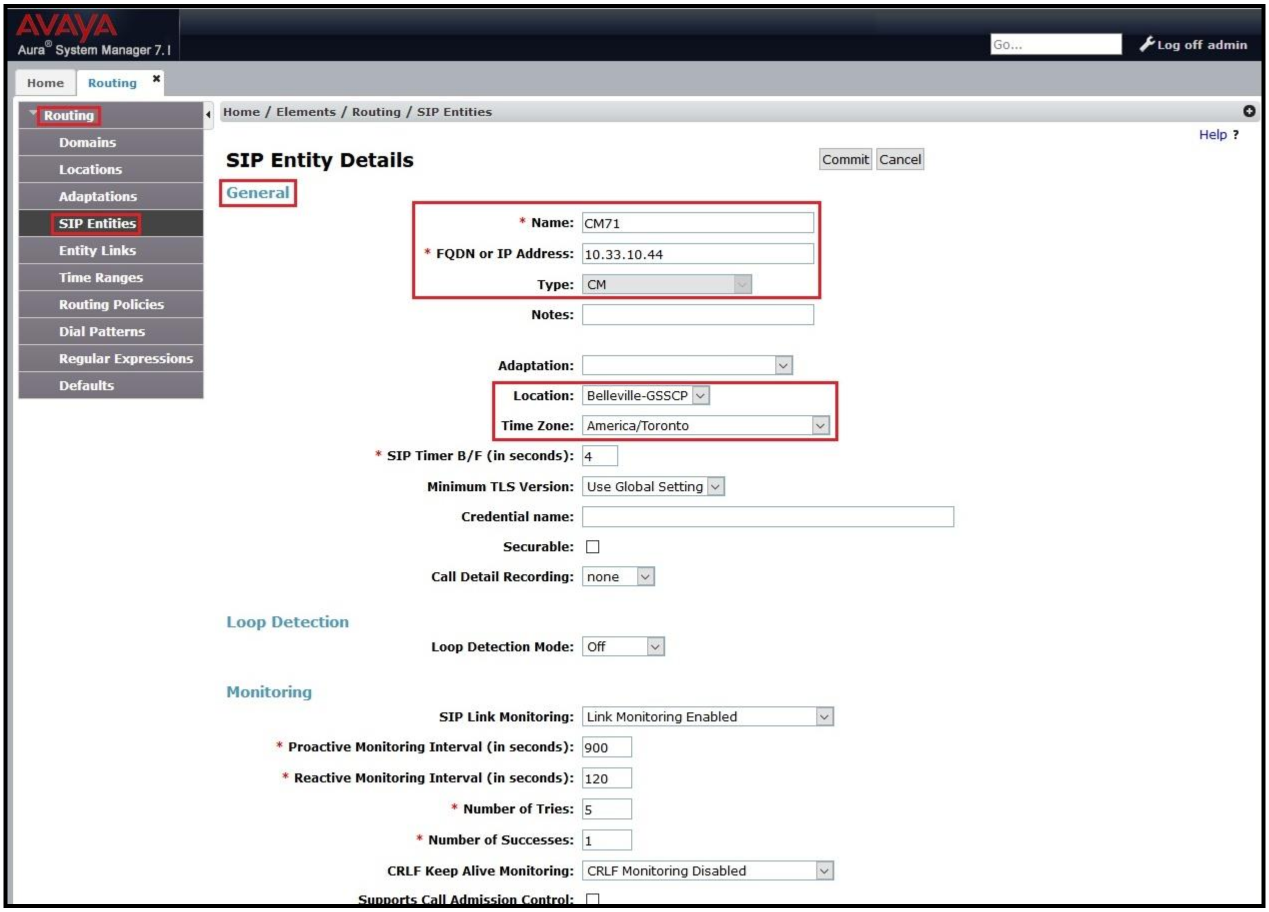

Figure 44: Communication Manager SIP Entity

6.4.3. Configure Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the addition of Avaya SBCE SIP entity named **SBCE**. The **FQDN or IP Address** field is set to the IP address of the SBCE's private network interface **10.10.98.13**. Note that **SIP Trunk** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

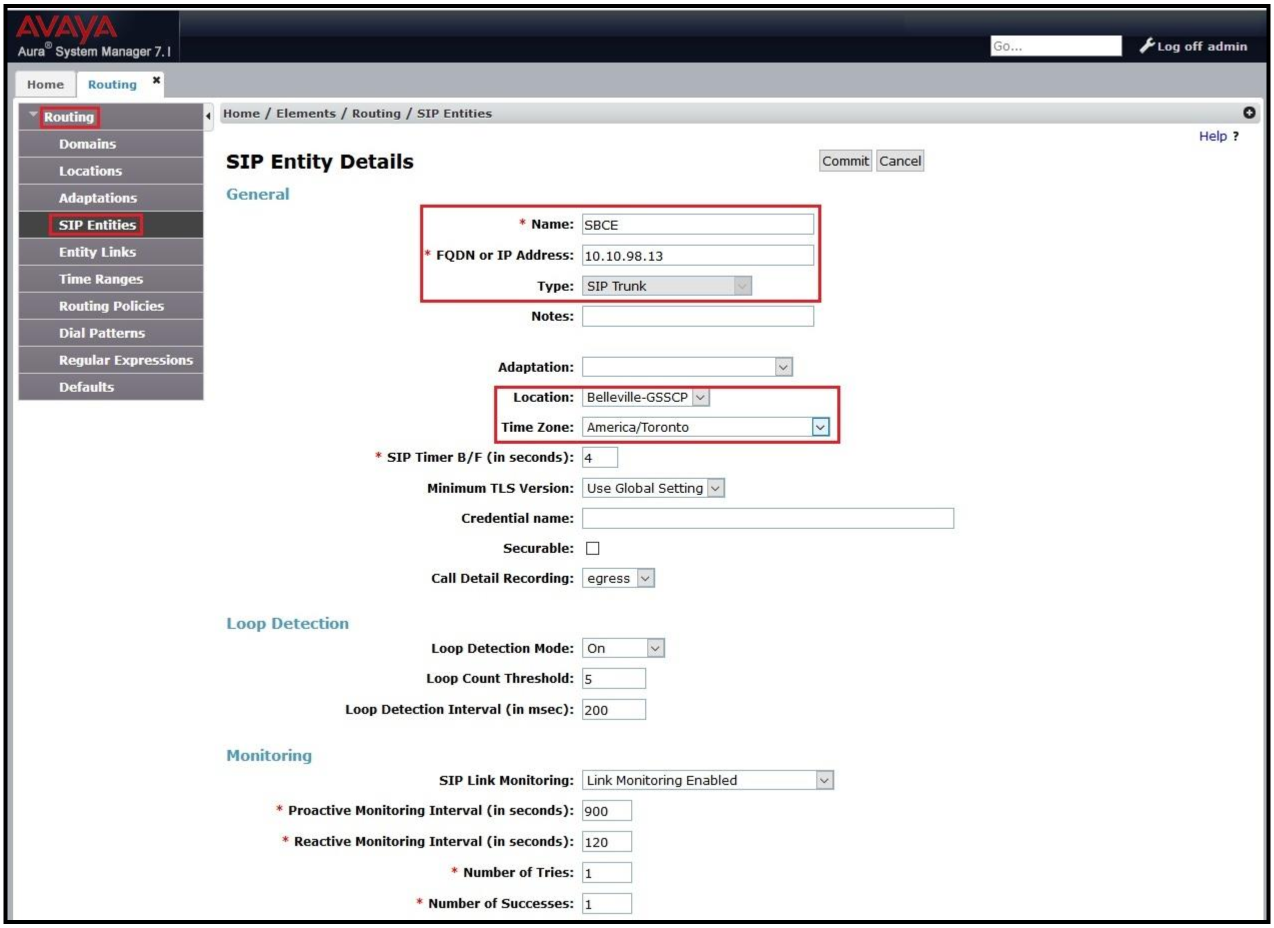

Figure 45: Avaya SBCE SIP Entity

6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by the service provider traffic and one to the Avaya SBCE.

To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

- **Name**: Enter a descriptive name
- **SIP Entity 1**: Select the Session Manager being used
- **Protocol**: Select the transport protocol used for this link
- **Port**: Port number on which Session Manager will receive SIP requests from the far-end
- **SIP Entity 2**: Select the name of the other system as defined in **Section 6.4**
- **Port**: Port number on which the other system receives SIP requests from the Session Manager
- **Connection Policy**: Select **trusted**. **Note**: If **trusted** is not selected, calls from the associated SIP Entity specified in **Section 6.4** will be denied

Click **Commit** to save

The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.7**.

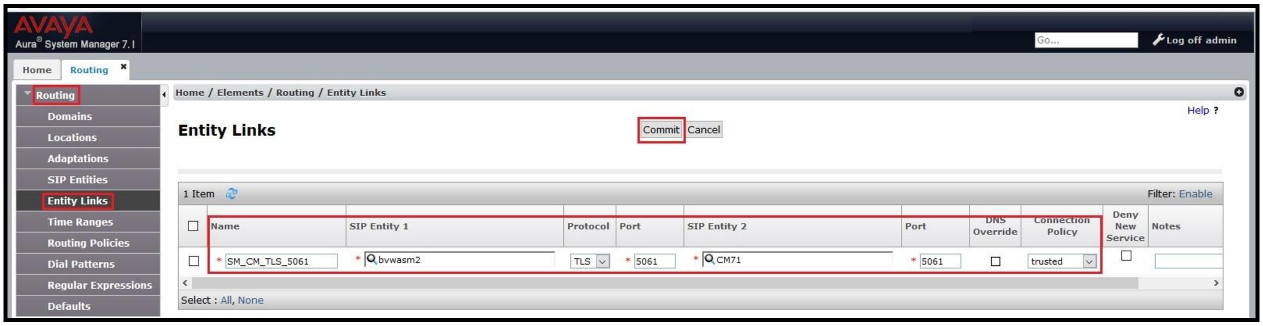

Figure 46: Communication Manager Entity Link

The following screen illustrates the Entity Links to Avaya SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.2.4**, **7.2.6** and **7.4.3**.

Figure 47: Avaya SBCE Entity Link

6.6. Configure Time Ranges

Time Ranges are configured for time-based-routing. In order to add a Time Range, select **Routing → Time Ranges** and then click **New** button. The Routing Policies shown subsequently will use the 24/7 range since time-based routing was not the focus of these Application Notes.

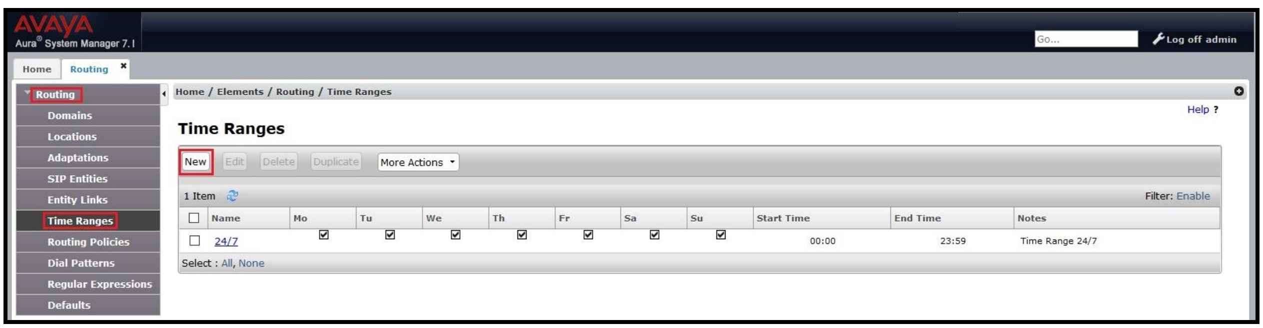

Figure 48: Time Ranges

6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two Routing Policies must be added; one for Communication Manager and one for Avaya SBCE.

To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

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

- **Name**: Enter a descriptive name

- **Notes**: Add a brief description (optional)

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

Click **Commit** to save

The following screen shows the **Routing Policy Details** for the policy named **TELUS_Inbound_Call** associated with incoming PSTN calls from TELUS to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **CM71**.

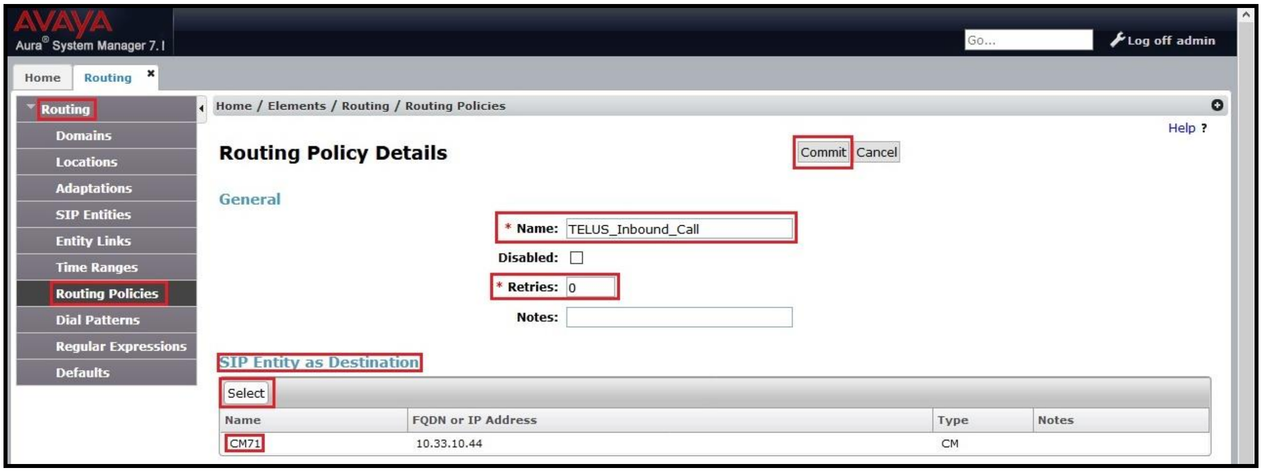

Figure 49: Routing to Communication Manager

The following screen shows the **Routing Policy Details** for the policy named **TELUS_Outbound_Call** associated with outgoing calls from Communication Manager to the PSTN via TELUS SIP Trunk through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.

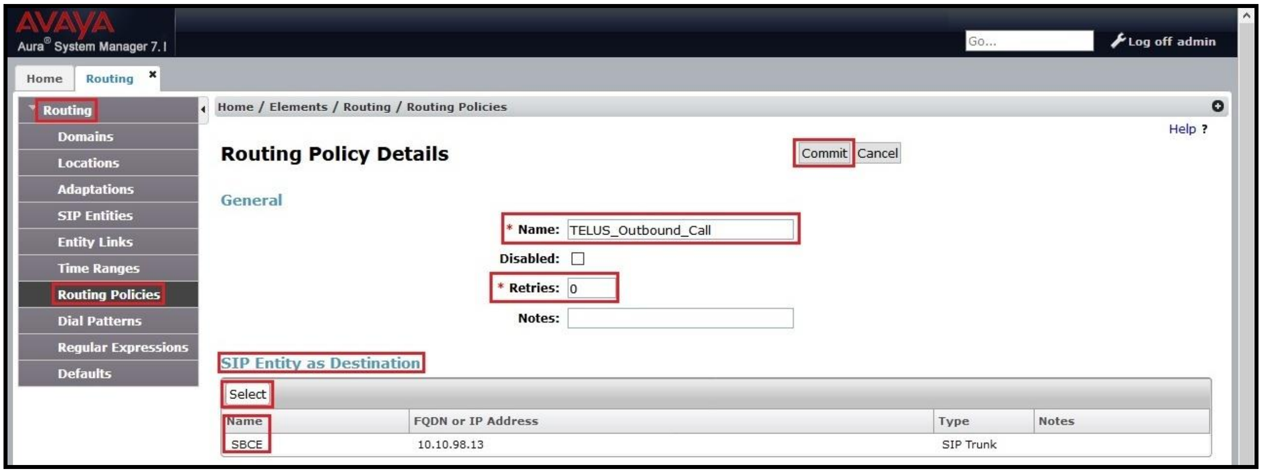

Figure 50: Routing to TELUS SIP Trunk

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from Communication Manager to TELUS SIP Trunk through the Avaya SBCE and vice versa. Dial Patterns define which Route Policy will be selected as route destination for a particular call based on the dialed digits, destination Domain and originating Location.

To add a Dial Pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

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

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

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

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

Two examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other Dial Patterns were similarly defined.

The first example shows that outbound 11-digit dialed numbers that begin with **1613** and have a destination **SIP Domain** of **bvwdev.com** uses **Routing Policy Name** as **TELUS_Outbound_Call** which is defined in **Section 6.7**.

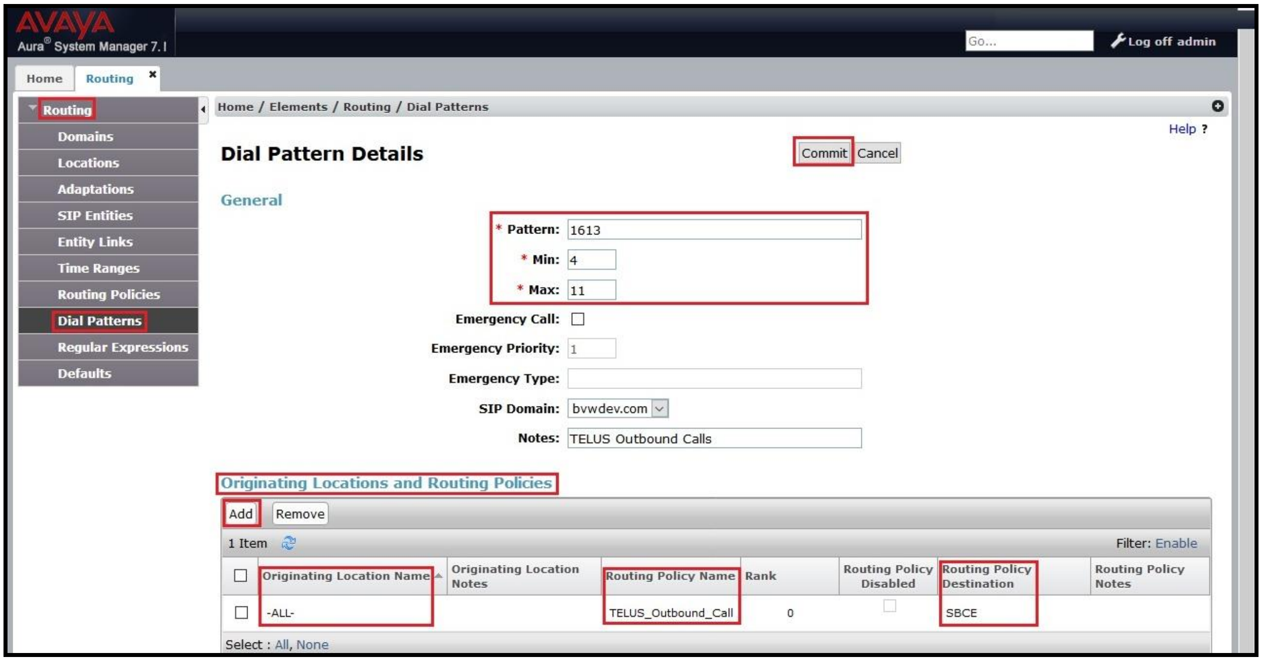

Figure 51: Dial Pattern_1613

Note that with the above Dial Pattern, TELUS did not restrict outbound calls to specific US/Canada area codes. In real deployments, appropriate restriction can be exercised per customer business policies.

Also note that **-ALL-** was selected for **Originating Location Name**. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed back to the PSTN.

The second example shows that inbound 10-digit numbers that start with **587** use **Routing Policy Name** as **TELUS_Inbound_Call** which is defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by TELUS.

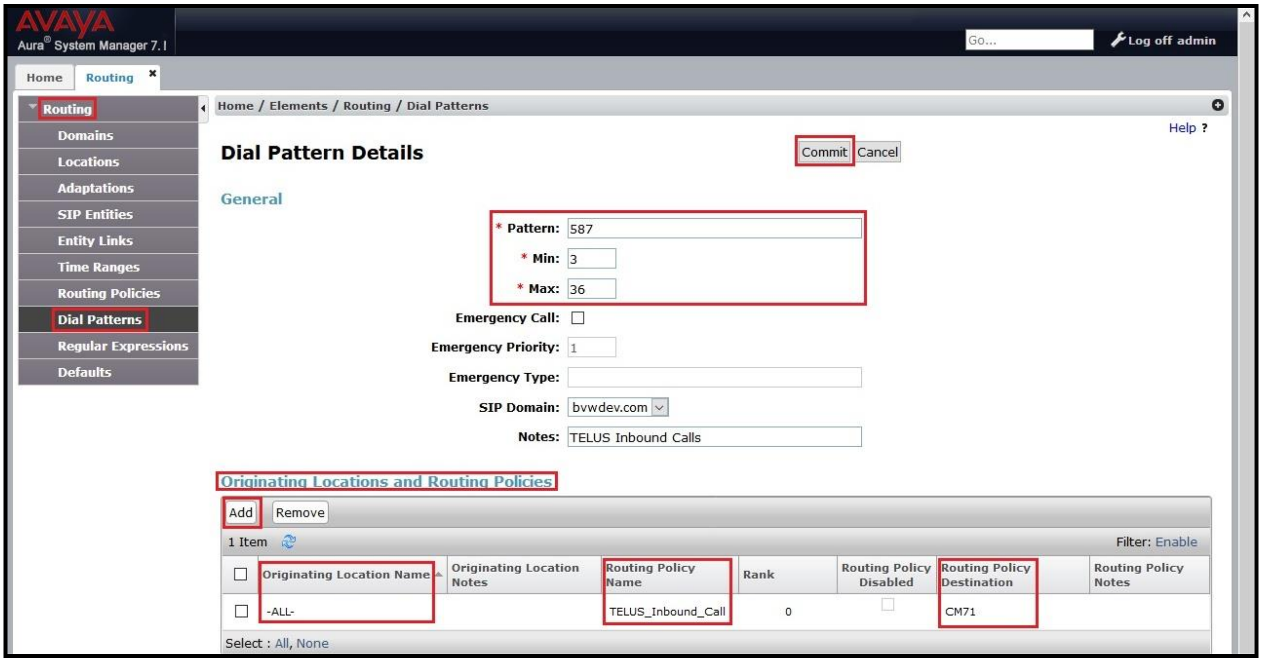

Figure 52: Dial Pattern_587

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.

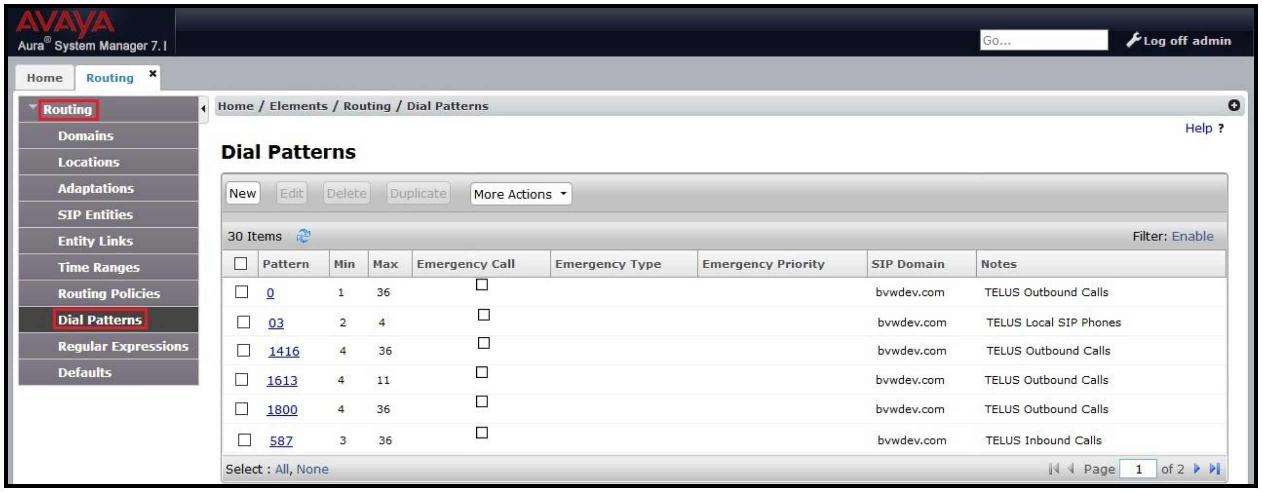

Figure 53: Dial Pattern List

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and the TELUS system.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the TELUS system resides on the Public side of the network.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, refer to the documentation listed in **Section 11** of these Application Notes.

7.1. Log in to Avaya Session Border Controller for Enterprise

Access the web interface by typing "**https://x.x.x.x/sbc/**" (where x.x.x.x is the management IP of the Avaya SBCE).

Enter the **Username** and **Password** and click on **Log In** button.

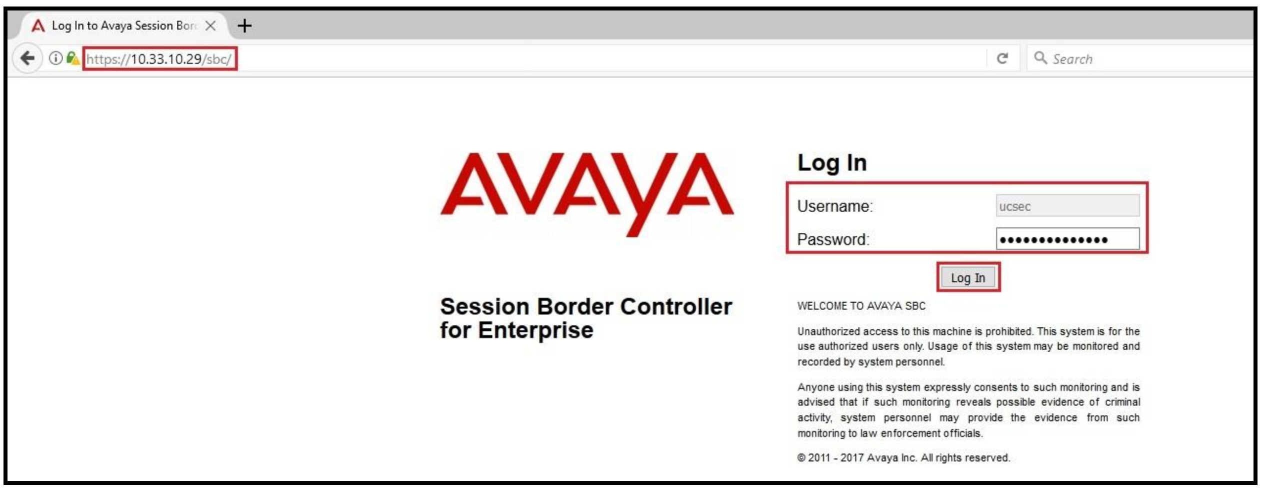

Figure 54: Avaya SBCE Login

The **Dashboard** main page will appear as shown below.

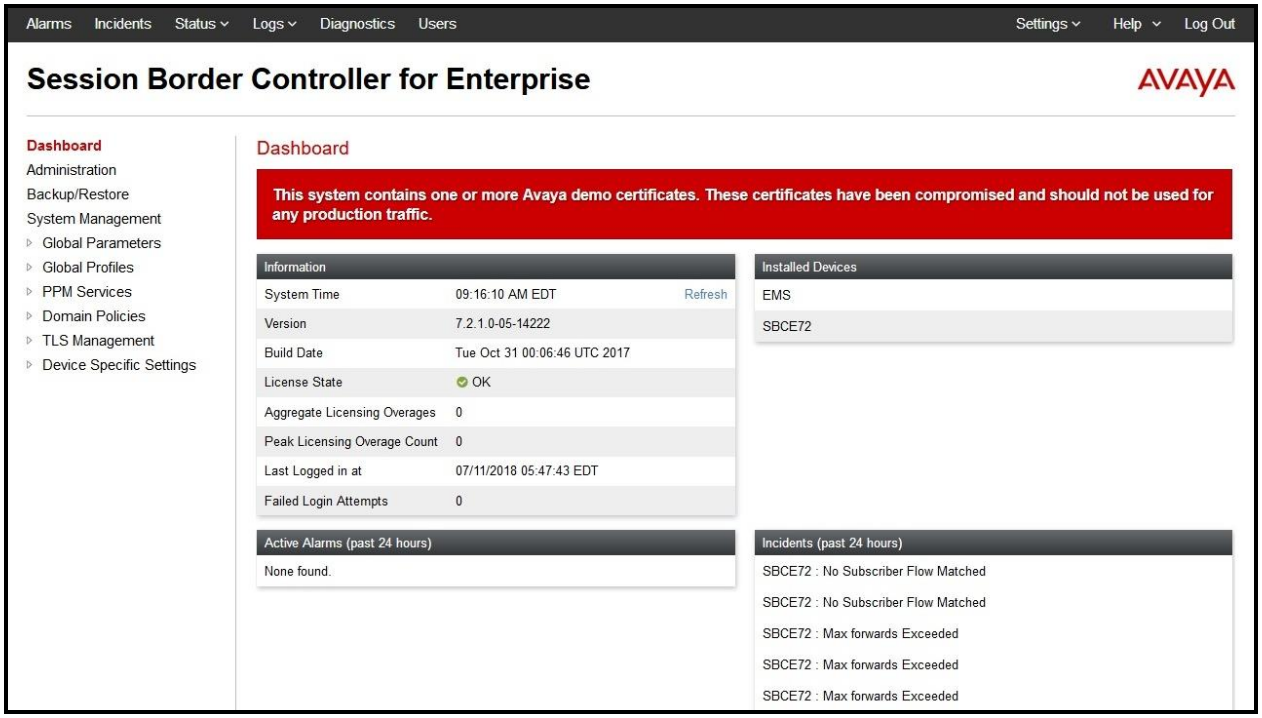

Figure 55: Avaya SBCE Dashboard

To view system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **SBCE72** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.

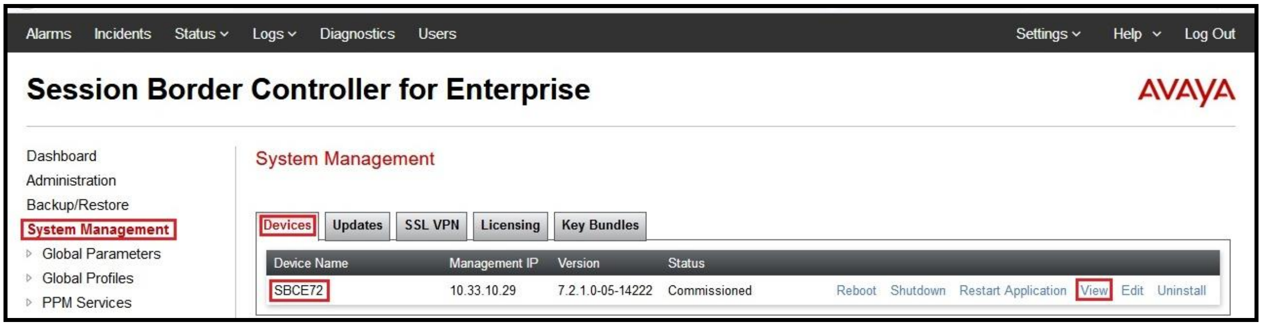

Figure 56: Avaya SBCE System Management

The **System Information** screen shows **General Configuration**, **Device Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**.

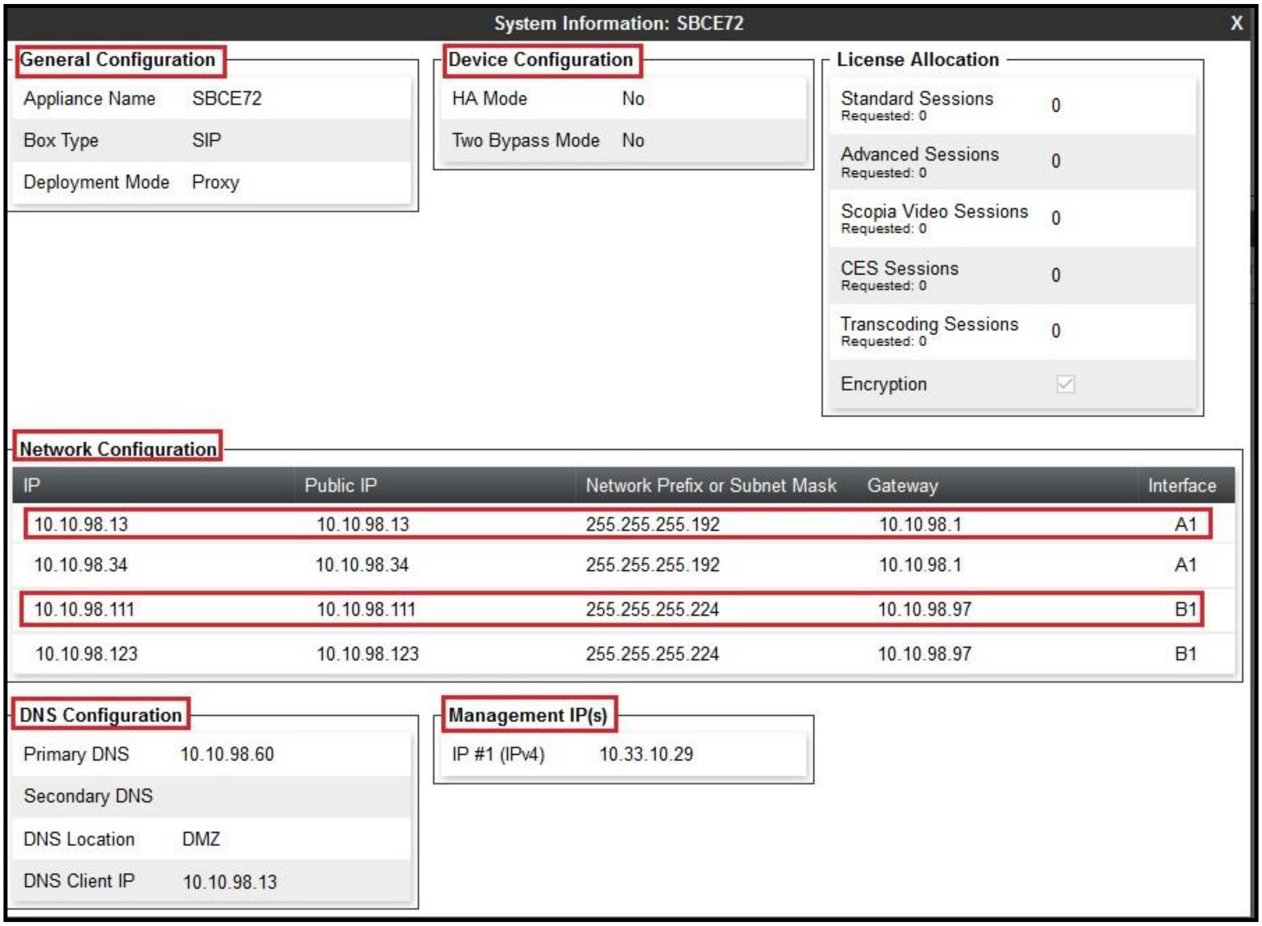

Figure 57: Avaya SBCE System Information

7.2. Global Profiles

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

7.2.1. Configure Server Interworking Profile - Avaya Site

Server Interworking profile allows administrator to configure and manage various SIP call server specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select **Global Profiles → Server Interworking**

- Select **avaya-ru** in **Interworking Profiles**
- Click **Clone**
- Enter **Clone Name**: **SMVM** and click **Finish** (not shown)
- Select **SMVM** in **Interworking Profiles**
- Click **Edit** button
- Check **T.38 Support** option and click **Finish** (not shown).

The following screen shows that Session Manager server interworking profile (named: **SMVM**) was added.

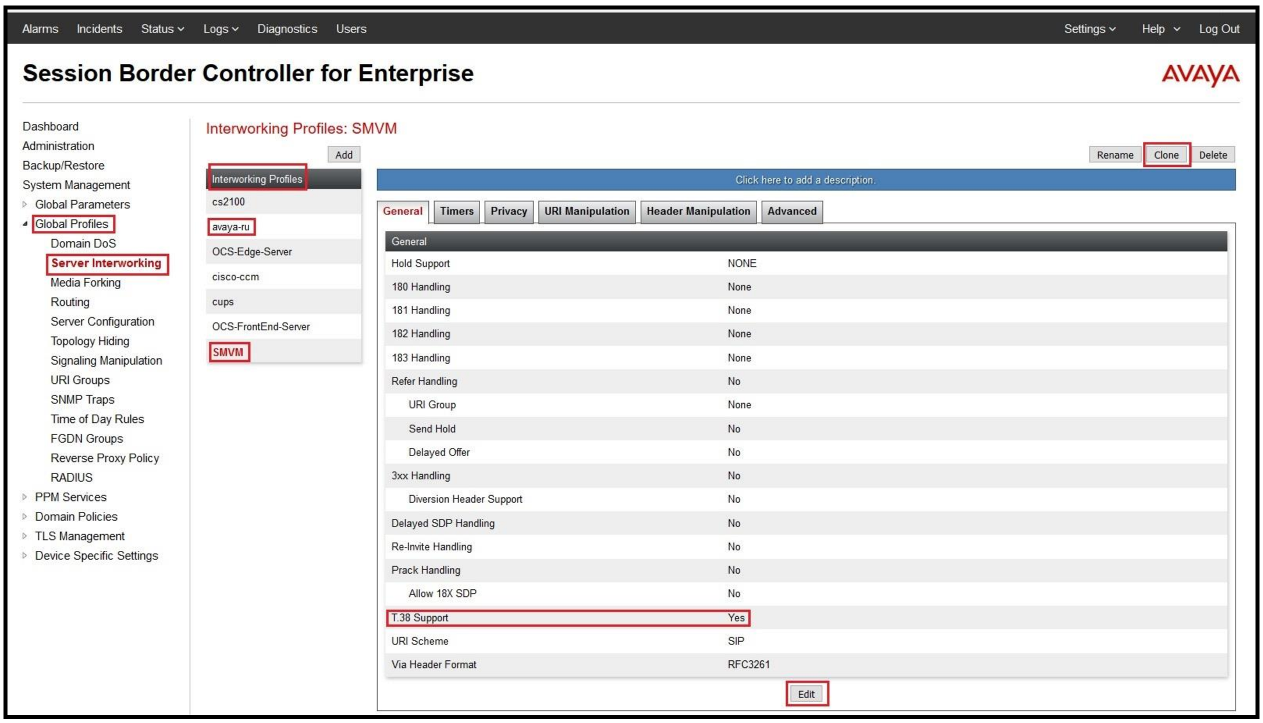

Figure 58: Server Interworking – Avaya site

7.2.2. Configure Server Interworking Profile – TELUS SIP Trunk Site

From the menu on the left-hand side, select **Global Profiles → Server Interworking → Add**

- Enter **Profile Name**: **SP4** (not shown)
- Click **Next** button to leave all options at default
- Click **Finish** (not shown)
- Select **SP4** in **Interworking Profiles**
- Click **Edit** button
- Check **T.38 Support** option and click **Finish** (not shown)

The following screen shows that TELUS server interworking profile (named: **SP4**) was added.

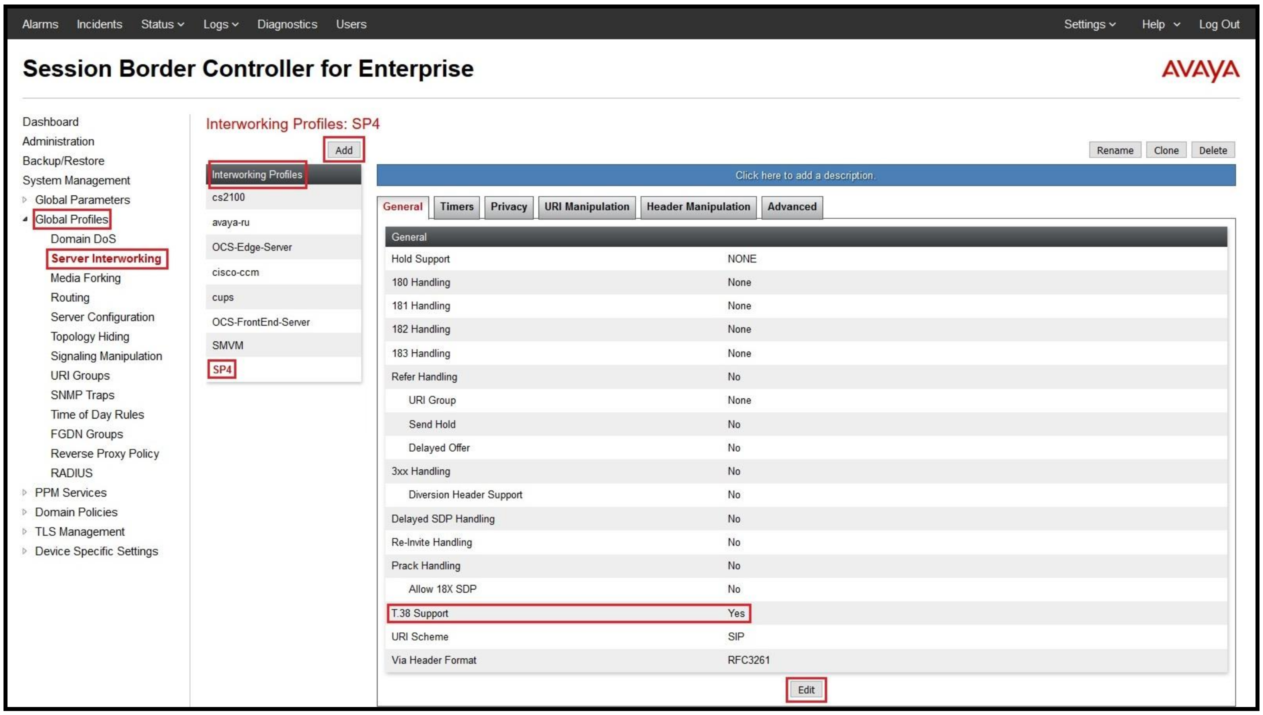

Figure 59: Server Interworking – TELUS SIP Trunk site

7.2.3. Configure Signaling Manipulation

The SIP signaling header manipulation feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

From the menu on the left-hand side, select **Global Profiles → Signaling Manipulation → Add**

- Enter script **Title**: **SP4-TELUS**. In the script editing window, enter the text exactly as shown in the below screenshot to perform the following:
  - Replace user of SIP URI in Request-Line header of the SIP OPTIONS coming from TELUS
  - Set Max-forward = 0 on the outbound SIP OPTION. This is optional testing only as TELUS requests.
  - Remove plus sign in From, PAI, Contact, Diversion headers for outbound calls
  - Modify user of SIP URI in PAI header in off-net call forward
  - Remove un-wanted headers
  - Click **Save** (not shown)

Note: See **Appendix A** in **Section 13** for the reference of this signaling manipulation (SigMa) script.

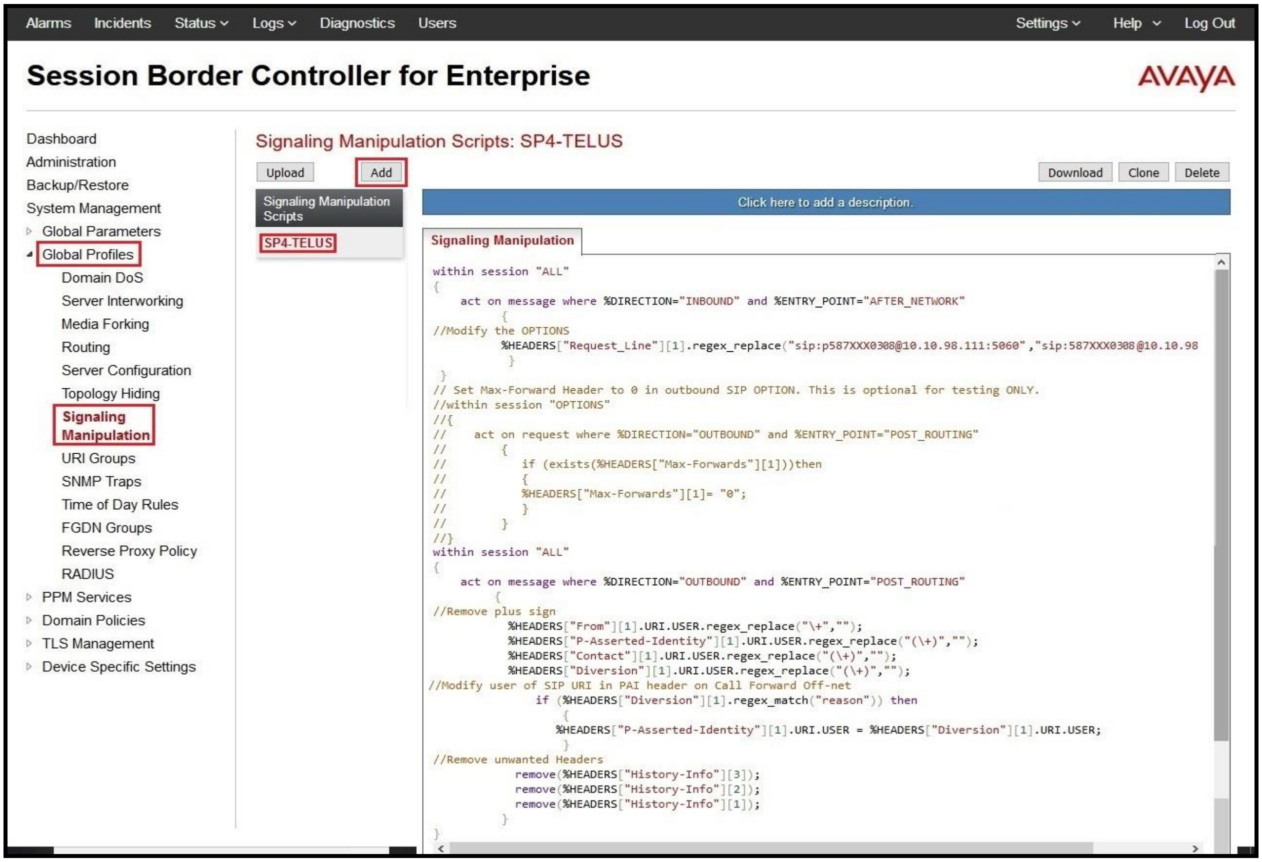

Figure 60: Signaling Manipulation

7.2.4. Configure Server – Avaya Site

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server specific parameters such as port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**

Enter **Profile Name**: **SMVM**

On **General** tab, enter the following:

- **Server Type**: Select **Call Server**
- **TLS Client Profile**: Select **AvayaSBCClient71**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
- **IP Address/FQDN**: **10.33.10.43** (Session Manager IP Address)
- **Port**: **5061**
- **Transport**: **TLS**
- Click **Finish** (not shown)

Figure 61: Server Configuration – General - Avaya site

On the **Advanced** tab:

- **Enable Grooming** box is checked
- Select **SMVM** for **Interworking Profile** (see **Section 7.2.1**)
- Click **Finish** (not shown)

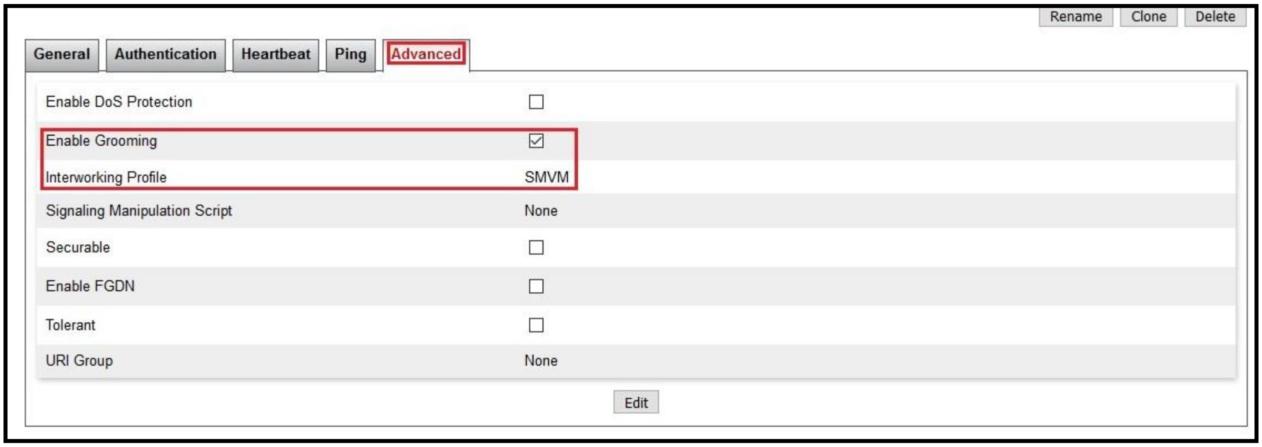

Figure 62: Server Configuration – Advanced - Avaya site

7.2.5. Configure Server – TELUS SIP Trunk

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**

Enter **Profile Name**: **SP4**

On **General** tab, enter the following:

- **Server Type**: Select **Trunk Server**
- **IP Address/FQDN**: **192.168.158.100** (TELUS SIP Signaling Server IP Address)
- **Port**: **5060**
- **Transport**: **UDP**
- Click **Finish** (not shown)

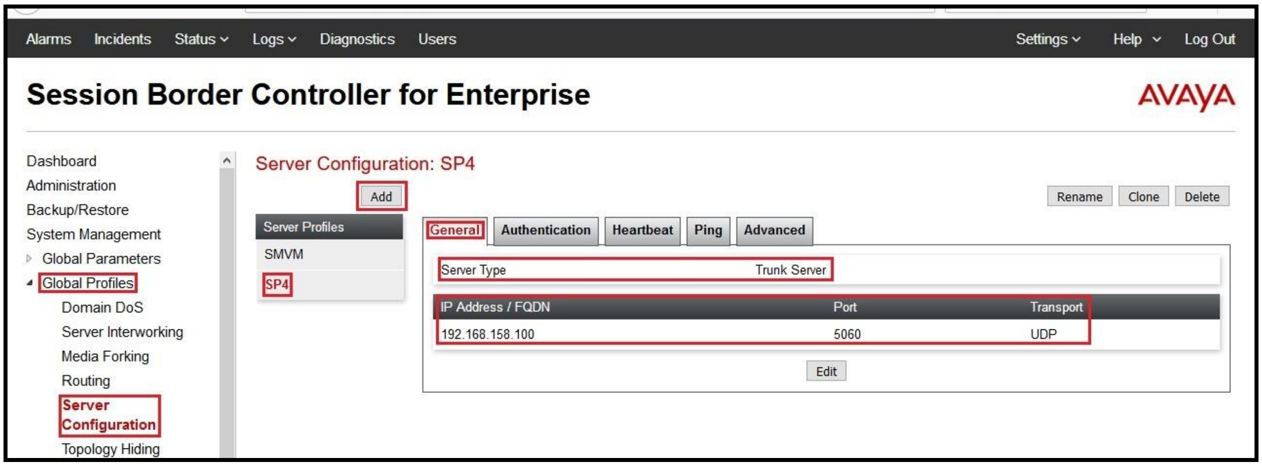

Figure 63: Server Configuration – General - TELUS site

On **Authentication** tab, click **Edit** button to enter the following:

- Check **Enable Authentication o**ption
- Input **User Name**: **p587XXX0308** (TELUS provides the user name)
- **Realm**: leave it blank as default
- **Password: ********** (TELUS provides the password)
- **Confirm Password: ********** (TELUS provides the password)

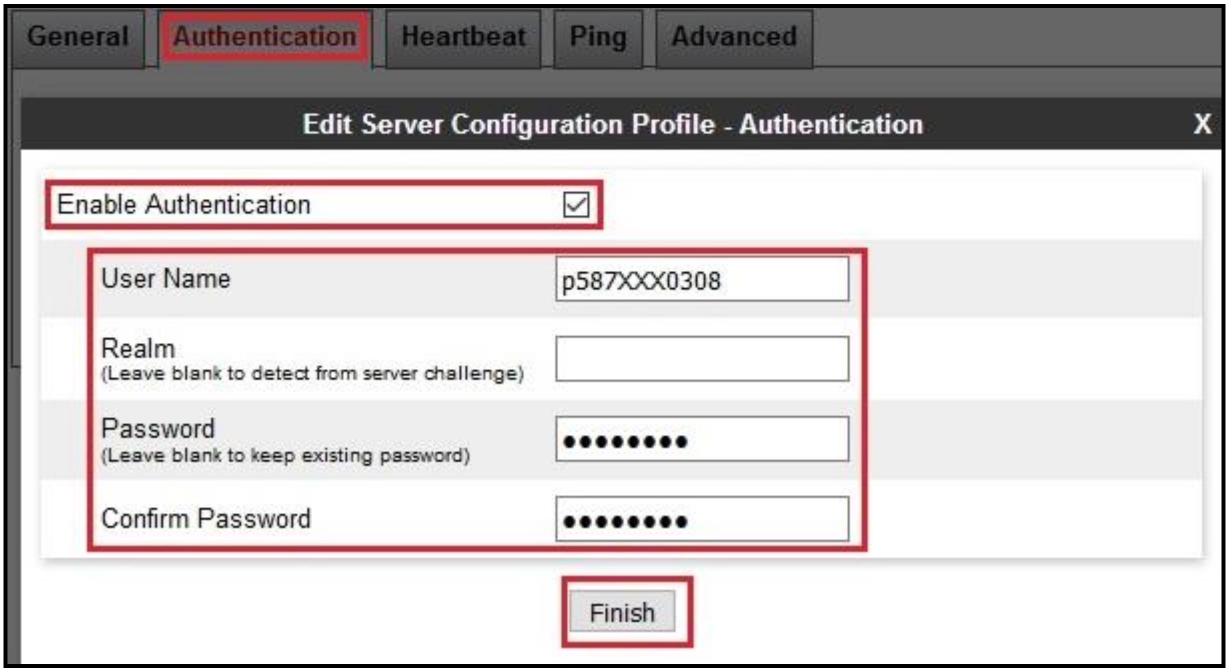

Figure 64: Server Configuration – Authentication - TELUS site

On **Heartbeat** tab, click **Edit** button to enter the following:

- Check **Enable Heartbeat**
- Select **Method**: **REGISTER**
- **Frequency**: **60 seconds**
- **From URI**: **p587XXX0308@IPINET5.com**
- **To URI**: **p587XXX0308@IPINET5.com**

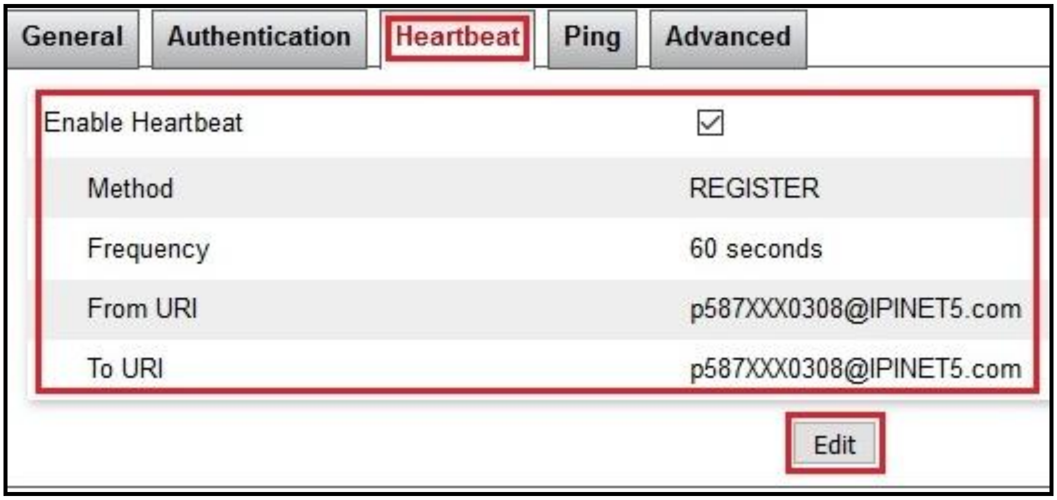

Figure 65: Server Configuration – Heartbeat - TELUS site

On the **Advanced** tab, enter the following:

- **Interworking Profile**: **SP4** (see **Section 7.2.2**)
- **Signaling Manipulation Script**: **SP4-TELUS** (see **Section 7.2.3**)
- Click **Finish** (not shown)

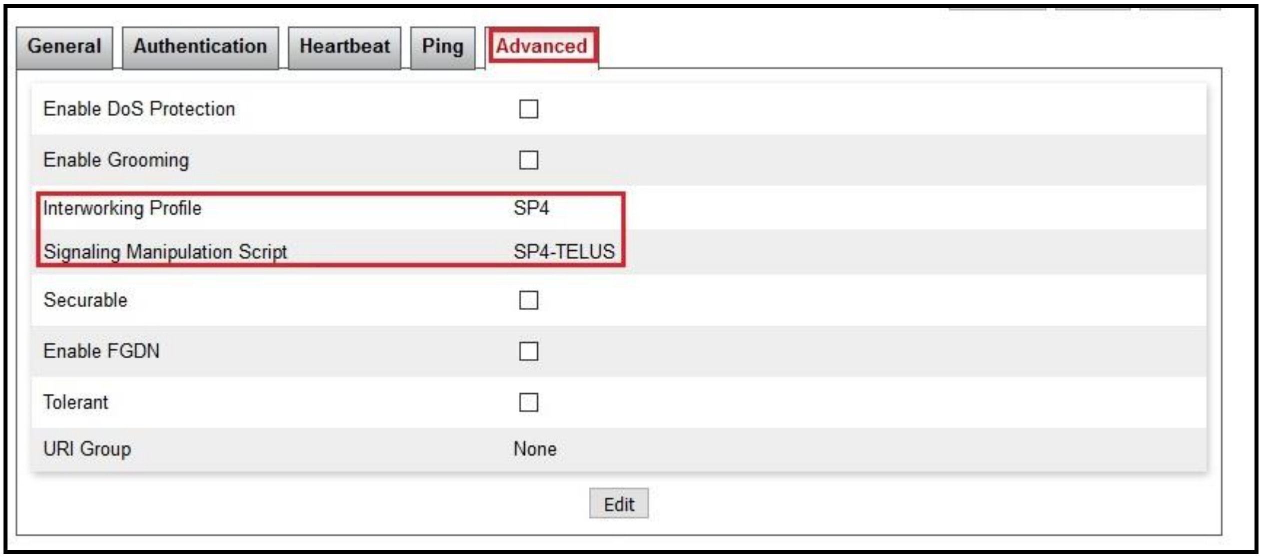

Figure 66: Server Configuration – Advanced - TELUS site

7.2.6. Configure Routing – Avaya Site

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.

From the menu on the left-hand side, select **Global Profiles → Routing** and click **Add** as highlighted below.

Enter **Profile Name**: **SP4_To_SMVM** and click **Next** button (Not Shown)

- Select **Load Balancing**: **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight**: **1**
- **Server Configuration**: **SMVM** (see **Section 7.2.4**)
- **Next Hop Address**: **10.33.10.43:5061 (TLS)** (Session Manager IP Address)
- Click **Finish**

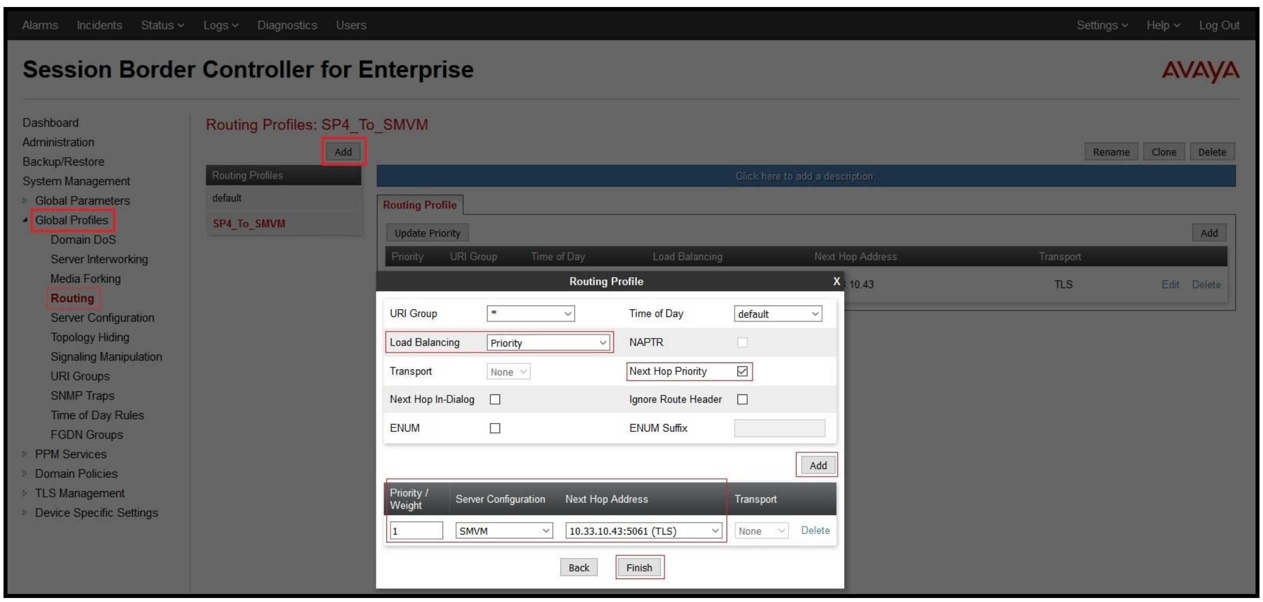

Figure 67: Routing to Session Manager

7.2.7. Configure Routing – TELUS SIP Trunk Site

The Routing Profile allows one to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select **Global Profiles → Routing** and click **Add** as highlighted below.

Enter **Profile Name**: **SMVM_To_SP4** and click **Next** button (not shown)

- **Load Balancing**: **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight**: **1**
- **Server Configuration**: **SP4** (see **Section 7.2.5**)
- **Next Hop Address**: **192.168.158.100:5060 (UDP)** (TELUS Signaling Server IP Address)
- Click **Finish**

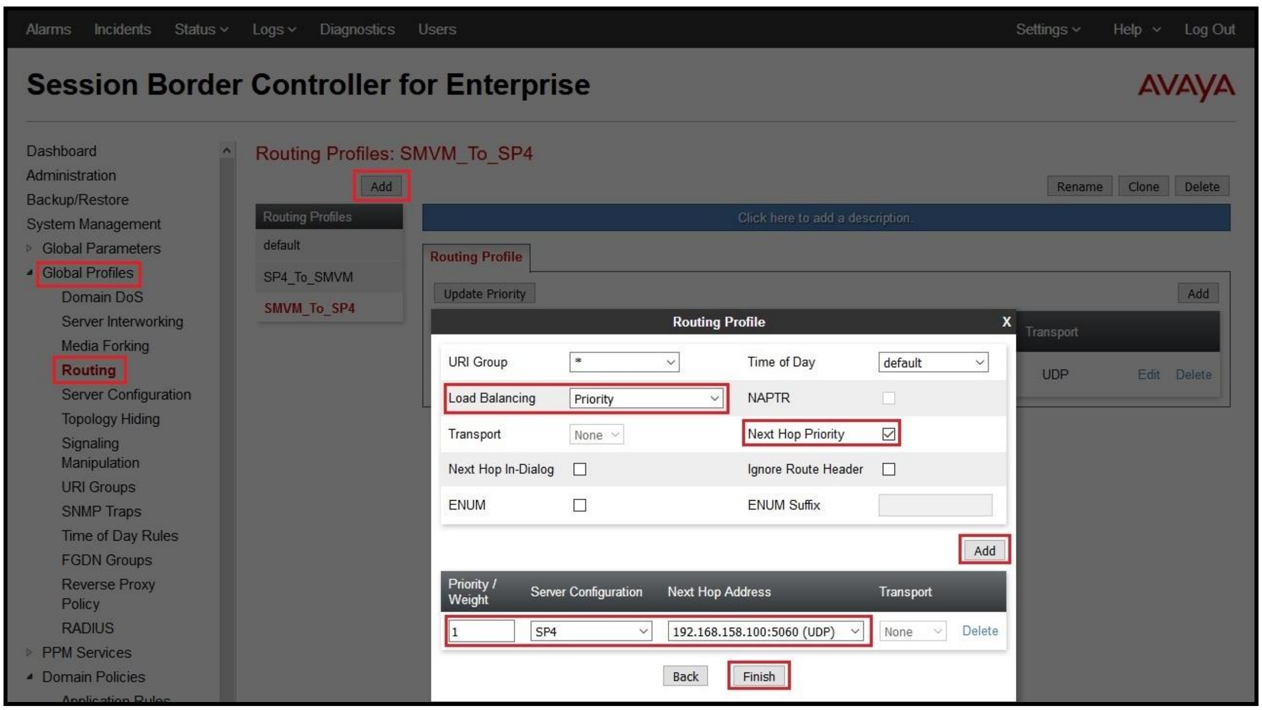

Figure 68: Routing to TELUS SIP Trunk

7.2.8. Configure Topology Hiding

The **Topology Hiding** screen allows an administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name**: **SP4_To_SMVM** and click **Finish** (not shown)
- Select **SP4_To_SMVM** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- For the Header **Request-Line**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev.com**
- For the Header **To**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev.com**
- For the Header **From**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**

    In the **Overwrite Value** column: **bvwdev.com**

Click **Finish** (not shown)

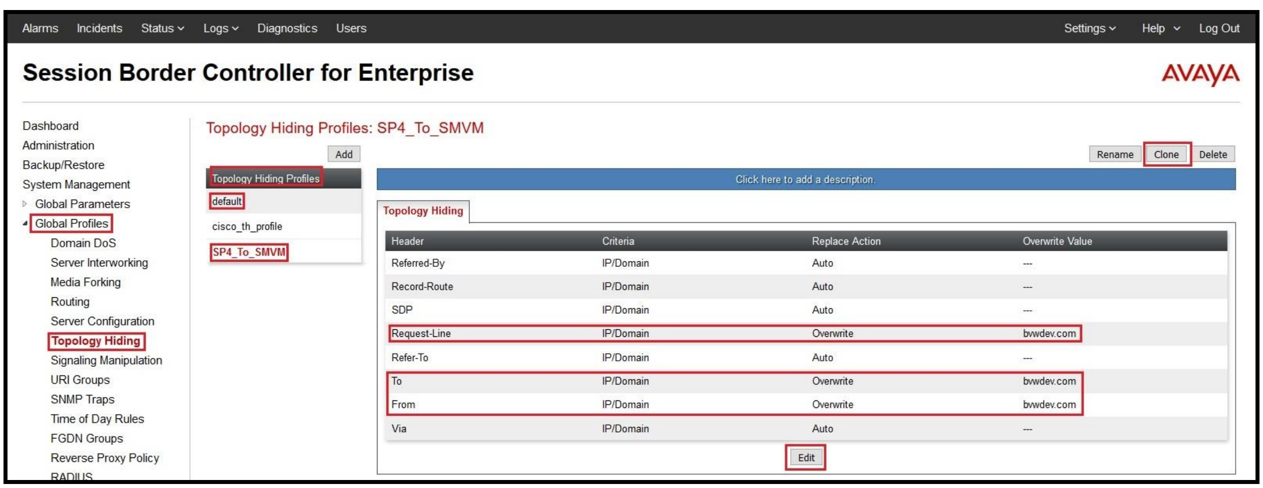

Figure 69: Topology Hiding To Session Manager

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name**: **SMVM_To_SP4** and click **Finish** (not shown)
- Select **SMVM_To_SP4** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- For the Header **Request-Line**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **IPINET5.com**
- For the Header **From**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
    In the **Overwrite Value** column: **IPINET5.com**
- For the Header **To**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **IPINET5.com**
- Click **Finish** (not shown)

Click **Finish** (not shown)

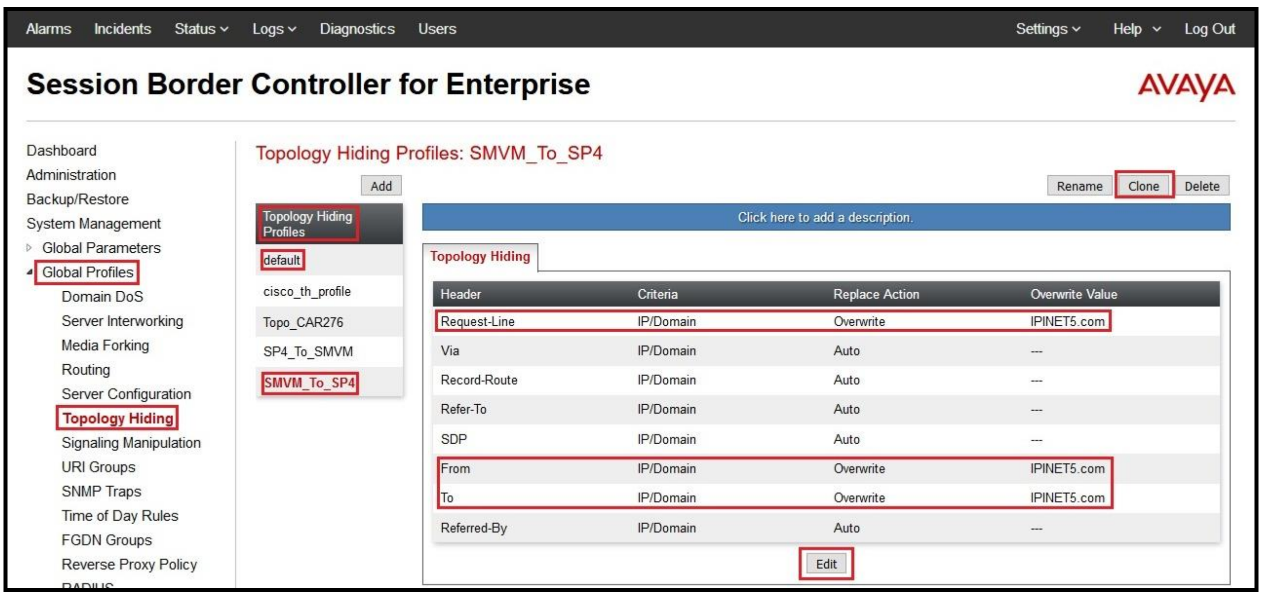

Figure 70: Topology Hiding To TELUS

7.3. Domain Policies

The Domain Policies feature allows administrator to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or an administrator can create a custom domain policy.

7.3.1. Create Media Rules

Media Rules allow one to define media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, the predefined **default-low-med-enc** media rule (shown below) was used to clone and edit.

From the menu on the left-hand side, select **Domain Policies** → **Media Rules**

- Select the **default-low-med-enc** rule, click **Clone**. Enter **Clone Name**: **SMVM_SP4** Click **Finish** (not shown)
- Select **SMVM_SP4** under **Media Rules** to **Edit**

The **Encryption** tab indicates that **RTP** and **SRTP_AES_CM_128_HMAC_SHA1_80** encryption was used as **Preferred Formats** for Audio Encryption.

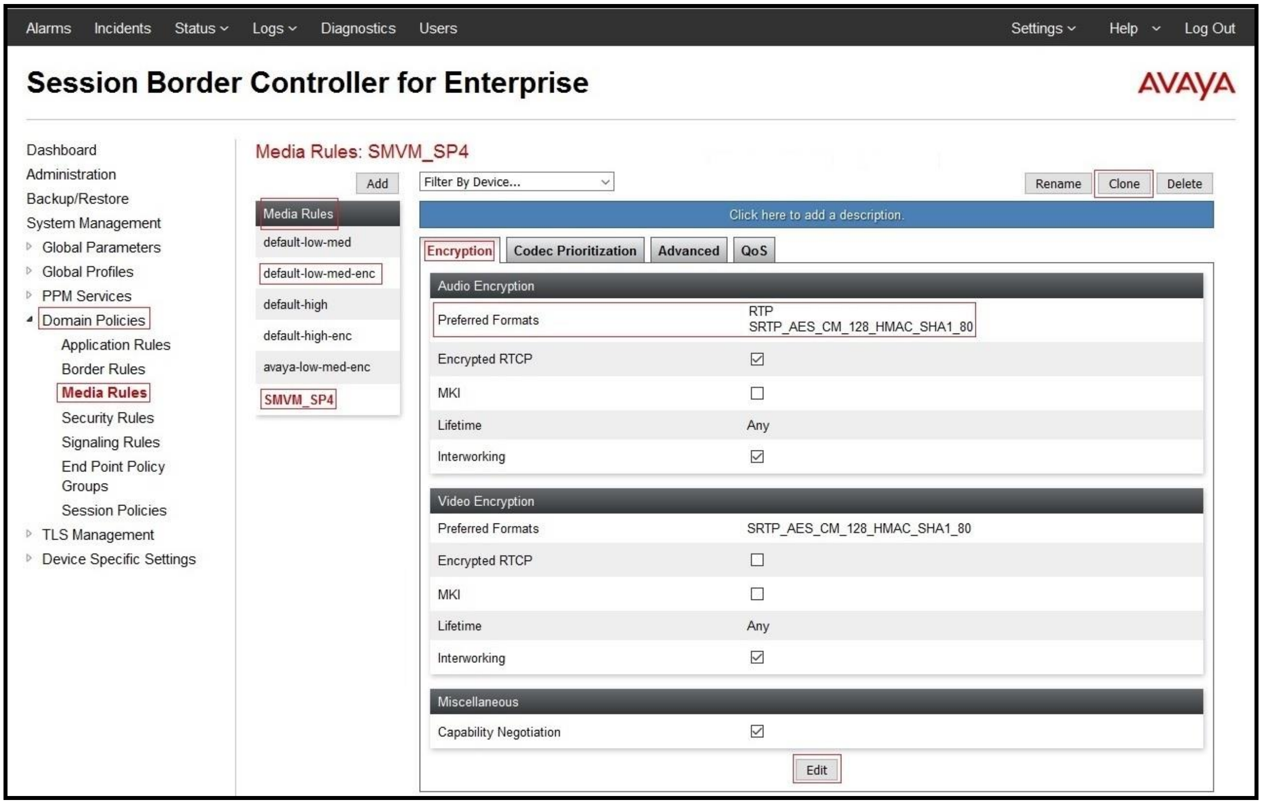

Figure 71: Media Rule

7.3.2. Create Endpoint Policy Groups

The End Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, each of which was created using the procedures contained in the previous sections.) A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**

- Select **Add**.
- Enter **Group Name**: **SMVM_SP4**
  - **Application Rule**: **default**
  - **Border Rule**: **default**
  - **Media Rule**: **SMVM_SP4** (See in **Section 7.3.1**)
  - **Security Rule**: **default-low**
  - **Signaling Rule**: **default**
- Select **Finish** (not shown)

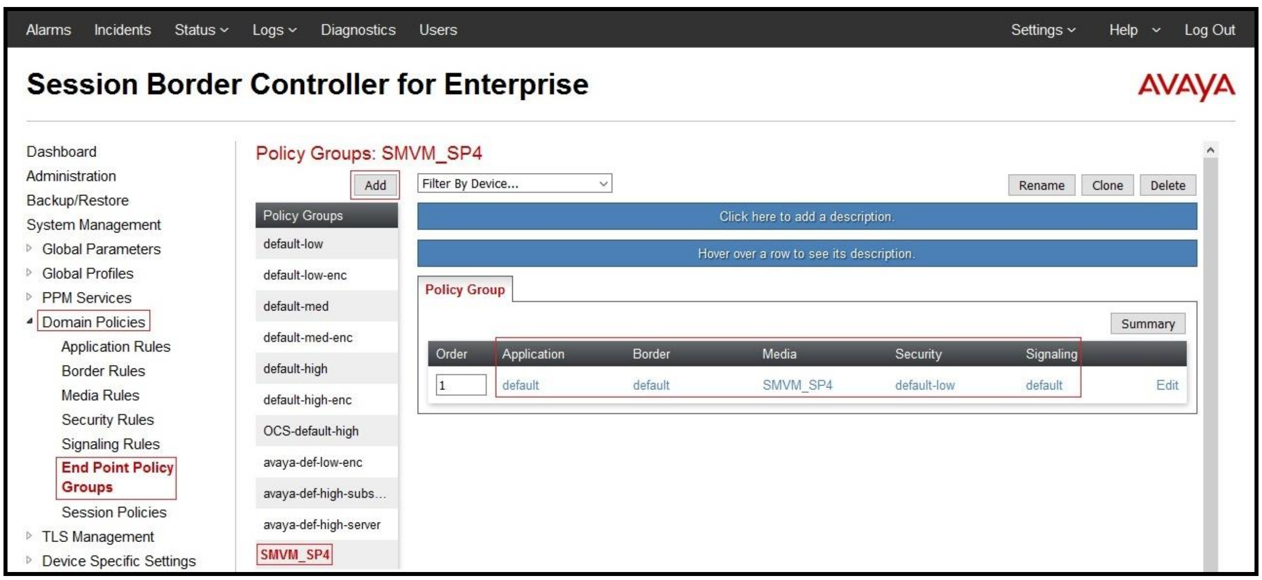

Figure 72: Endpoint Policy

7.4. Device Specific Settings

The Device Specific Settings feature for SIP allows one to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, one has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

7.4.1. Manage Network Settings

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select **Networks** tab and click the **Add** button to add a network for the inside interface as follows:
  - **Name**: **Network_A1**
  - **Default Gateway**: **10.10.98.1**
  - **Subnet Mask**: **255.255.255.192**
  - **Interface**: **A1** (This is the Avaya SBCE inside interface)
  - Click the **Add** button to add the **IP Address** for inside interface: **10.10.98.13**
  - Click the **Finish** button to save the changes

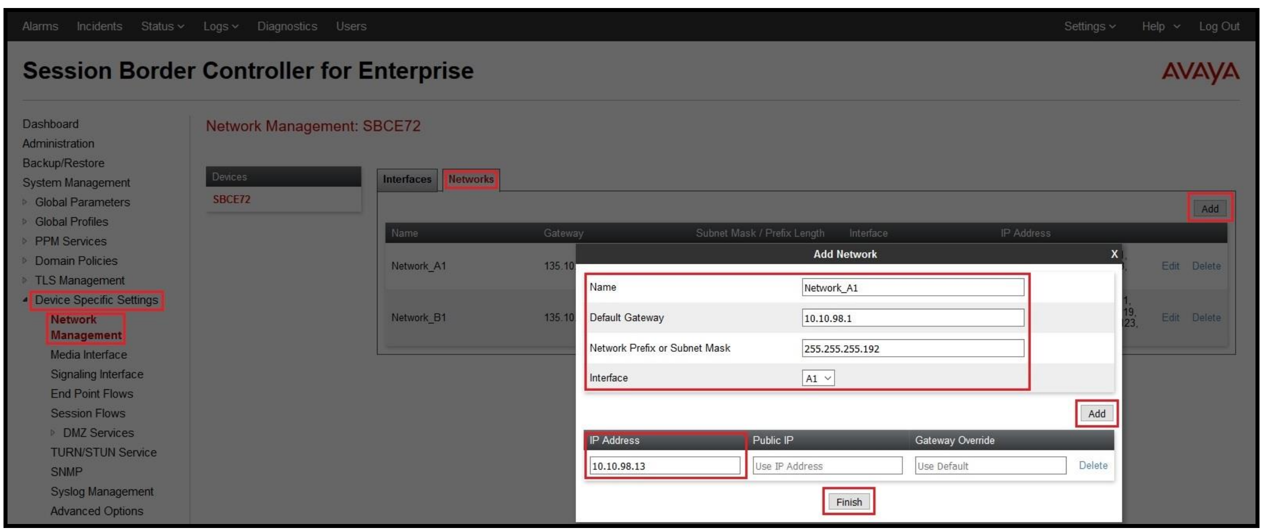

Figure 73: Network Management – Inside Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select **Networks** tab and click **Add** button to add a network for the outside interface as follows:
  - **Name**: **Network_B1**
  - **Default Gateway**: **10.10.98.97**
  - **Subnet Mask**: **255.255.255.224**
  - **Interface**: **B1** (This is the Avaya SBCE outside interface)
  - Click the **Add** button to add the **IP Address** for outside interface: **10.10.98.111**
  - Click the **Finish** button to save the changes

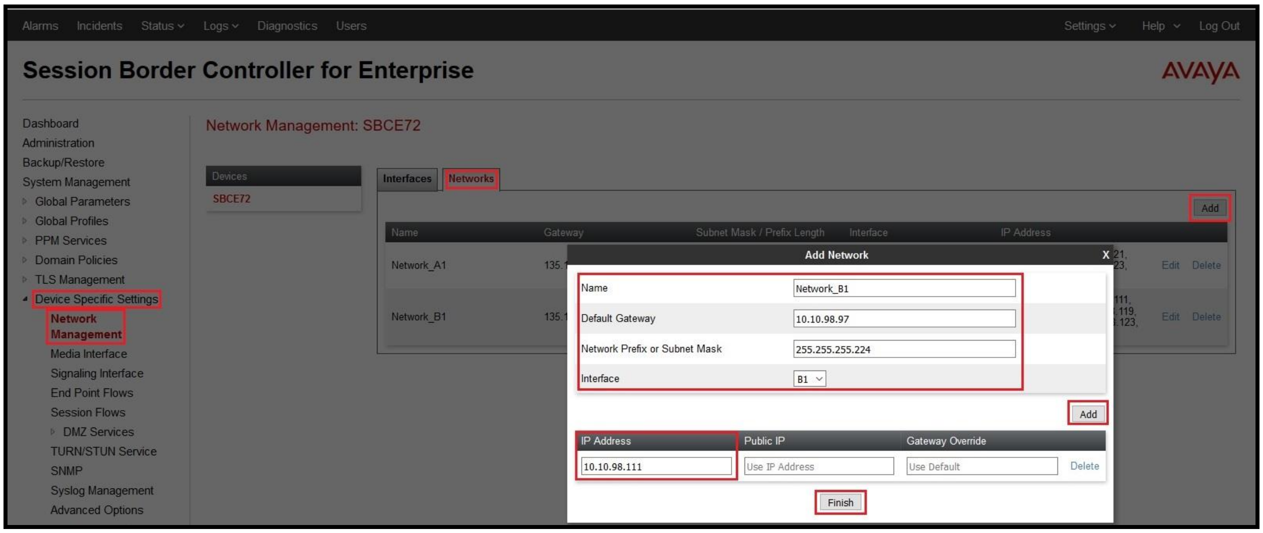

Figure 74: Network Management – Outside Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Select the **Interfaces** tab
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state

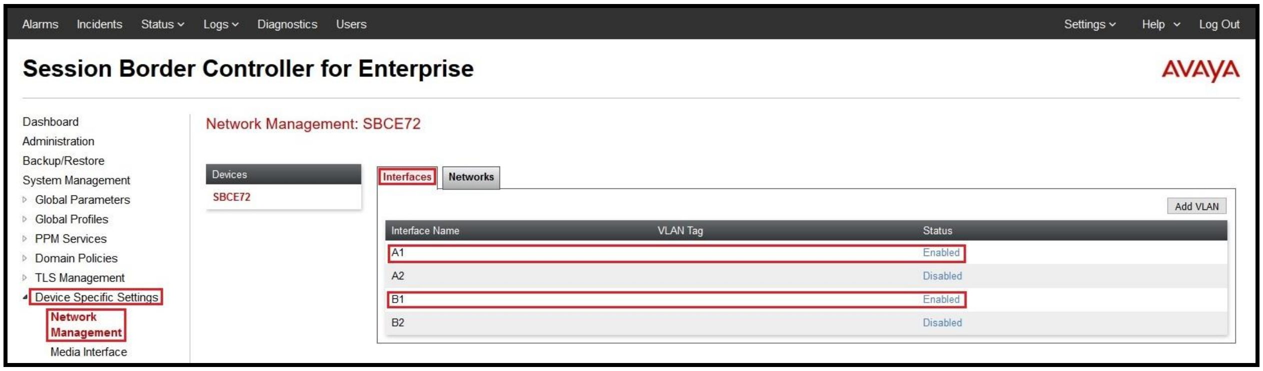

Figure 75: Network Management – Interface Status

7.4.2. Create Media Interfaces

Media Interfaces define the IP addresses and port ranges in which the Avaya SBCE will accept media streams on each interfaces. The default media port range on the Avaya SBCE can be used for inside port.

From the menu on the left-hand side, **Device Specific Settings → Media Interface**

- Select the **Add** button and enter the following:
  - **Name**: **InsideMedia1**
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Session Manager)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
  - **Name**: **OutsideMedia1**
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward TELUS)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)

Figure 76: Media Interface

7.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**

- Select the **Add** button and enter the following:
  - **Name**: **OutsideUDP**
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward TELUS)
  - **UDP Port**: **5060**
  - Click **Finish** (not shown)

From the menu on the left-hand side, select **Device Specific Settings → Signaling Interface**

- Select the **Add** button and enter the following:
  - **Name**: **InsideTLS**
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Session Manager)
  - **TLS Port**: **5061**
  - **TLS Profile**: **AvayaSBCServer71**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
  - Click **Finish** (not shown)

Note: For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 the same as TELUS used. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061.

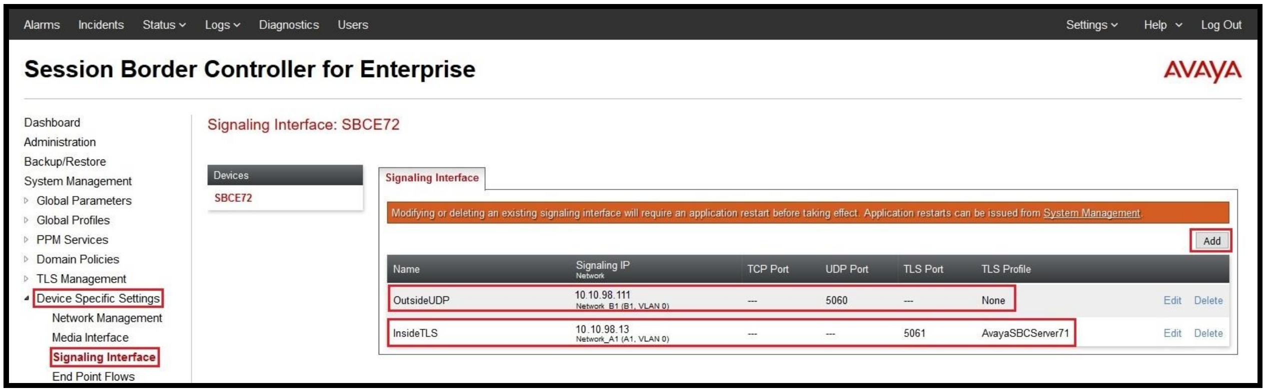

Figure 77: Signaling Interface

7.4.4. Configuration Server Flows

Server Flows allow an administrator to categorize trunk-side signaling and apply a policy.

7.4.4.1 Create End Point Flows – SMVM Flow

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**

- Select the **Server Flows** tab
- Select **Add**, enter **Flow Name**: **SMVM Flow**
  - **Server Configuration**: **SMVM** (see **Section 7.2.4**)
  - **URI Group**: *
  - **Transport: ***
  - **Remote Subnet: ***
  - **Received Interface**: **OutsideUDP** (see **Section 7.4.3**)
  - **Signaling Interface**: **InsideTLS** (see **Section 7.4.3**)
  - **Media Interface**: **InsideMedia1** (see **Section 7.4.2**)
  - **Secondary Media Interface**: **None**
  - **End Point Policy Group**: **SMVM_SP4** (see **Section 7.3.2**)
  - **Routing Profile**: **SMVM_To_SP4** (see **Section 7.2.7**)
  - **Topology Hiding Profile**: **SP4_To_SMVM** (see **Section 7.2.8**)
  - Leave other parameters as default
  - Click **Finish**

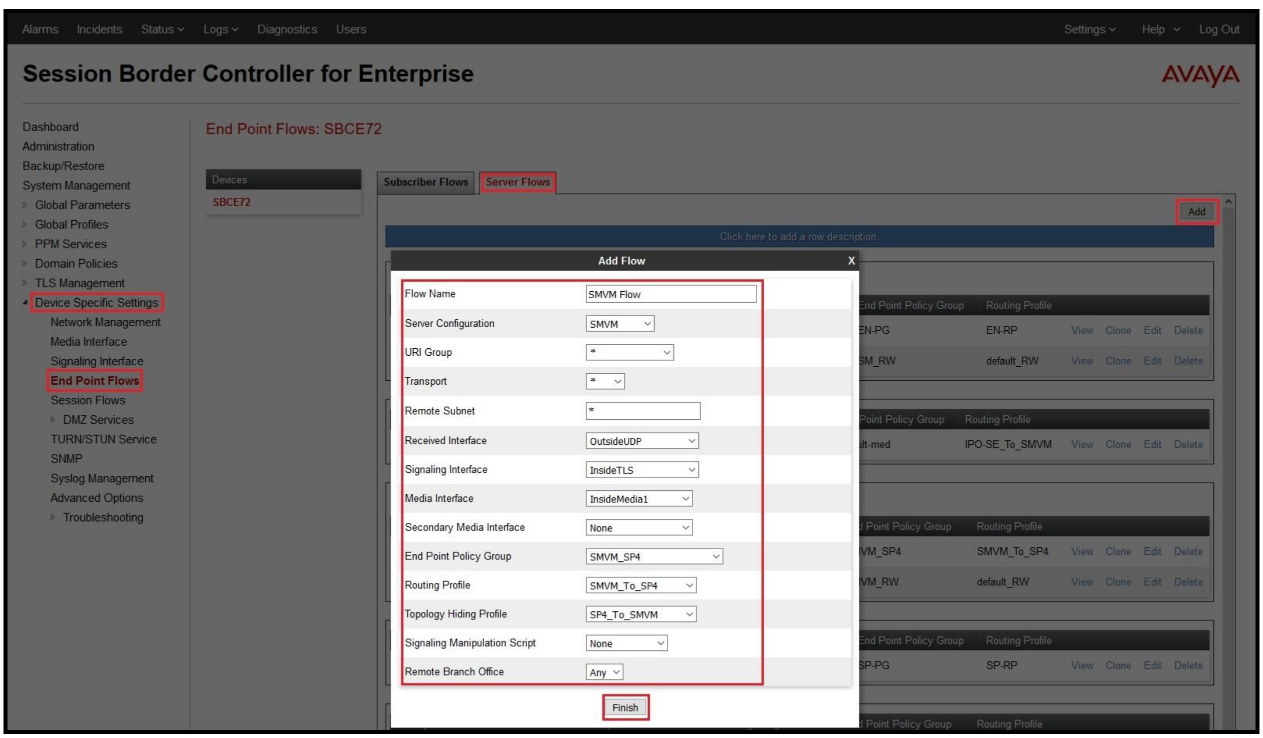

Figure 78: End Point Flow 1

7.4.4.2 Create End Point Flows – TELUS SIP Trunk Flow

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**

- Select the **Server Flows** tab
- Select **Add**, enter **Flow Name**: **SP4 Flow**
    - **Server Configuration**: **SP4** (see **Section 7.2.5**)
    - **URI Group**: *
    - **Transport: ***
    - **Remote Subnet: ***
    - **Received Interface**: **InsideTLS** (see **Section 7.4.3**)
    - **Signaling Interface**: **OutsideUDP** (see **Section 7.4.3**)
    - **Media Interface**: **OutsideMedia1** (see **Section 7.4.2**)
    - **Secondary Media Interface**: **None**
    - **End Point Policy Group**: **SMVM_SP4** (see **Section 7.3.2**)
    - **Routing Profile**: **SP4_To_SMVM** (see **Section 7.2.6**)
    - **Topology Hiding Profile**: **SMVM_ To_SP4** (see **Section 7.2.8**)
    - Leave other parameters as default
    - Click **Finish**

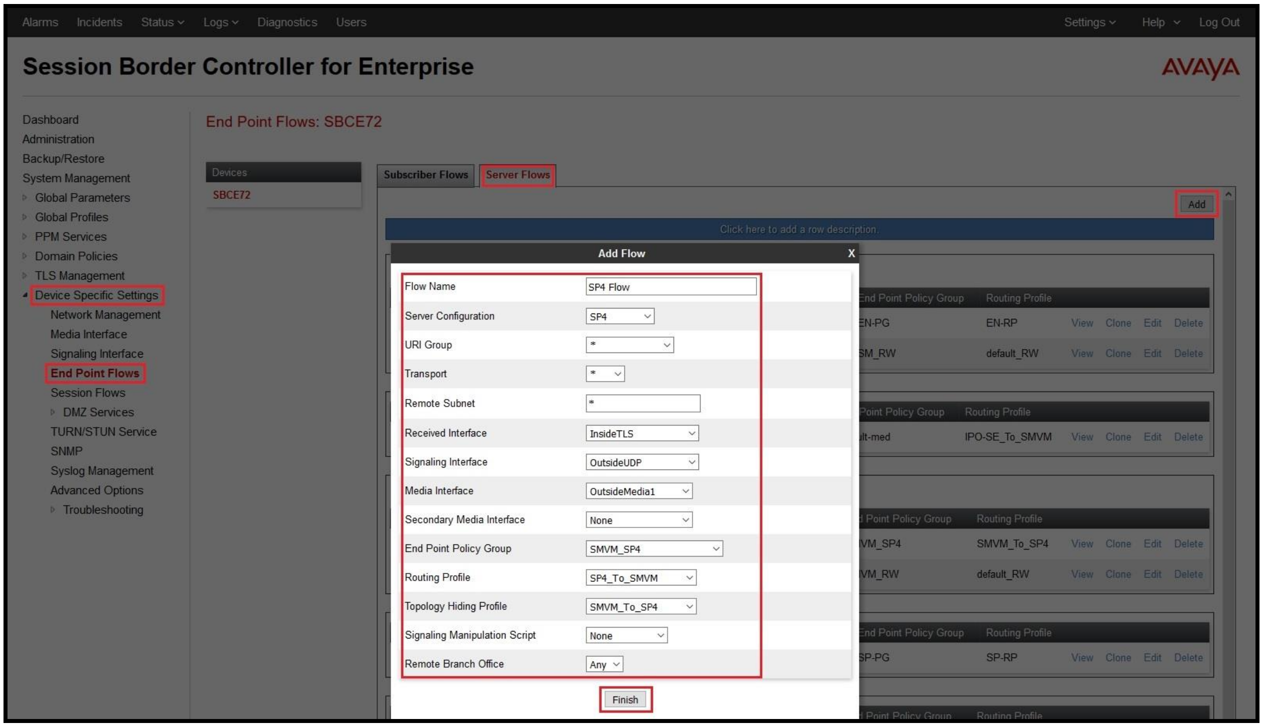

Figure 79: End Point Flow 2

8. TELUS SIP Trunk Configuration

TELUS is responsible for the network configuration of the TELUS SIP Trunk service. TELUS will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. TELUS will provide the IP address of the TELUS SIP Trunk SIP signaling/SBC IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. TELUS also provides the TELUS SIP Specification document for reference. This information is used to complete configurations for Communication Manager, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between TELUS SIP Trunk and the enterprise is a static IP address configuration.

9. Verification Steps

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

Verification Steps:

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

Troubleshooting:

1. Communication Manager: Enter the following commands using the Communication Manager System Access Terminal (SAT) interface.
    - **list trace station** <extension number> - Traces calls to and from a specific station.
    - **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
    - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
    - **status trunk-group** <trunk-group number> - Displays trunk-group state information.
    - **status signaling-group** <signaling-group number> - Displays signaling-group state information.
2. Session Manager:
    - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.
    - **traceSM** – Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.
3. Avaya SBCE: Debug logging can be started in two different ways:
    - **GUI** of the SBC: **Device Specific Settings → Troubleshooting → Debugging**.
        - SIP only: enable LOG_SUB_SIPCC subsystem under SSYNDI process.
        - CALL PROCESSING: enable all subsystems under SSYNDI process.
        - PPM: enable all subsystems under CONFIG_PROXY process.

      The log files are stored at: /usr/local/ipcs/log/ss/logfiles/elog/SSYNDI.
    - **Command Line Interface**: Login with root user and enter the command: **#traceSBC**. The tool updates the database directly based on which trace mode is selected.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to TELUS. This solution successfully passed compliance testing via the Avaya DevConnect Program. Please refer to **Section 2.2** for any exceptions or workaround.

11. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya, including the following, is available at:
http://support.avaya.com/

Avaya Aura® Session Manager/System Manager

[1] *Administering Avaya Aura® Session Manager*, Release 7.1.3, Issue 4, May 2018
[2] *Administering Avaya Aura® System Manager,* Release 7.1.3, Issue 14, June 2018

Avaya Aura® Communication Manager

[3] *Administering Avaya Aura ®Communication Manager*, Release 7.1.3, Issue 7, May 2018

Avaya Phones

[4] *Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones H.323,* Issue 2, March 2018
[5] *Installing and Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones SIP*, Issue 3, March 2018
[6] *Avaya one-X® Communicator Release 6.2 SP12 Patch10 Release Notes, Issue 1.0, January 2018*
[7] *Equinox™ Client (Windows) Release 3.3.4 (SP4), Release Notes, Issue 1.0, June 2018*

Avaya Session Border Controller for Enterprise

[8] *Administering Avaya Session Border Controller for Enterprise*, Release 7.2, Issue 3, September 2017

IETF (Internet Engineering Task Force) SIP Standard Specifications

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

Product documentation for TELUS SIP Trunking may be found at:
http://www.Telus.com/business/voice-networks/ip-trunking

12. Appendix A – Remote Worker Configuration

This section describes the process for connecting remote Avaya SIP endpoints on the public Internet, access through the Avaya SBCE to Session Manager on the private enterprise. It builds on the Avaya SBCE configuration described in previous sections of this document.

In the reference configuration, an existing Avaya SBCE is provisioned to access the TELUS SIP Trunk Services (see **Section 2.1** of this document). The Avaya SBCE also supports Remote Worker configurations, allowing remote SIP endpoints (connected via the public Internet) to access the private enterprise.

Supported endpoints are Avaya 96x1 SIP Deskphones, Avaya one-X® Communicator SIP softphone and Avaya Equinox™ for Windows SIP softphone.

Note: In the compliance testing, only Avaya one-X® Communicator SIP softphone was used to test as the remote worker.

Standard and Advanced Session Licenses are required for the Avaya SBCE to support Remote Workers. Contact an authorized Avaya representative for assistance if additional licensing is required. The settings presented here illustrate a sample configuration and are not intended to be prescriptive.

12.1. Network Management on Avaya SBCE

The following screen shows the **Network Management** of the Avaya SBCE. The Avaya SBCE is configured with three “outside” IP addresses assigned to physical interface B1, and two “inside” addresses assigned to physical interface A1.

Note: A SIP Entity in Session Manager was not configured for the Avaya SBCE’s internal IP address used for Remote Worker. This keeps the Remote Worker interface untrusted in Session Manager, thereby allowing Session Manager to properly challenge user registration requests.

These are the IP addresses used in the reference configuration:

- **10.10.98.13** is the Avaya SBCE “inside” address previously provisioned for SIP Trunking with TELUS (see **Section 7.4.1**)
- **10.10.98.34** is the new Avaya SBCE “inside” address for Remote Worker access to Session Manager
- **10.10.98.111** is the Avaya SBCE “outside” address previously provisioned for SIP Trunking with TELUS (see **Section 7.4.1**)
- **10.10.98.123** is the new Avaya SBCE “outside” address for Remote Worker access to Session Border Controller

From the menu on the left-hand side, select **Device Specific Settings → Network Management**

- Enter the above **IP Addresses** and **Gateway Addresses** for both the Inside and the Outside interfaces
- Select the physical interface used in the **Interface** column accordingly

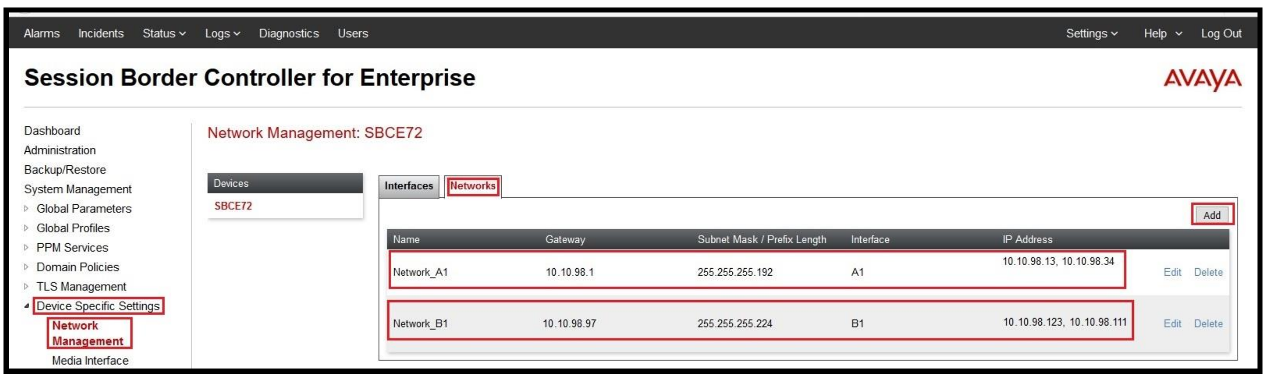

Figure 80: Network Management

On the **Interfaces** tab, verify that Interfaces **A1** and **B1** are both set to **Enabled** as previously configured for the TELUS SIP Trunk access in **Section 7.4.1**.

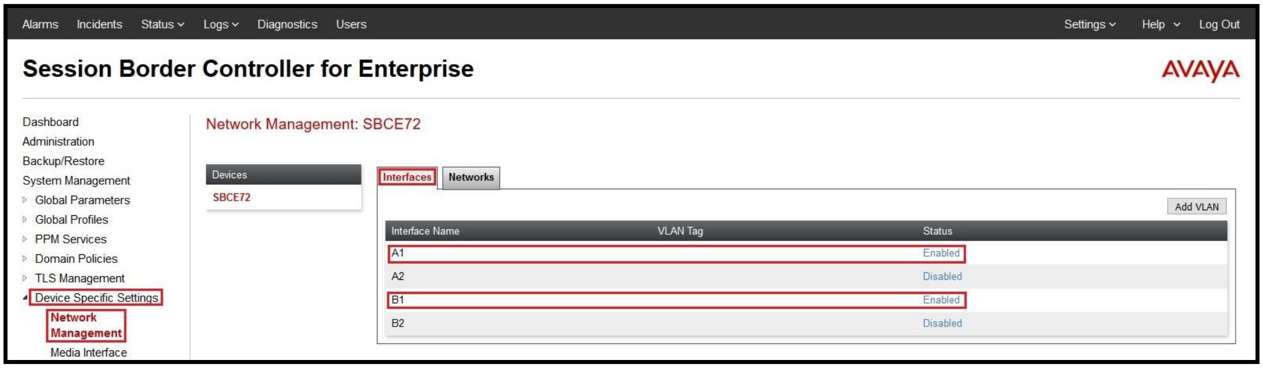

Figure 81: Network Interface Status

12.2. Media Interface on Avaya SBCE

From the menu on the left-hand side, select **Device Specific Settings → Media Interface**

- Select the **Add** button and enter the following:
  - **Name**: **InsideMedRW**
  - **IP Address**: Select **Network_A1 (A1, VLAN0)** and **10.10.98.34** (Internal IP Address toward Session Manager)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
  - **Name**: **OutsideMedRW**
  - **IP Address**: Select **Network_B1 (B1, VLAN0)** and **10.10.98.123** (External IP Address toward Remote Worker phones)
  - **Port Range**: **35000 – 40000**
  - Click **Finish** (not shown)

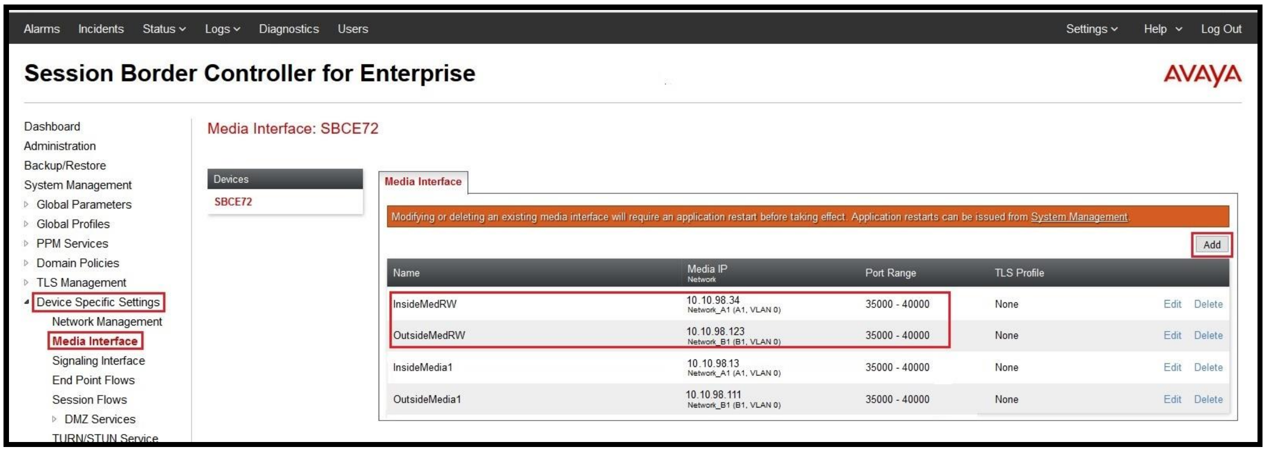

Figure 82: Media Interface

Note: Media Interface **OutsideMedRW** is used in the Remote Worker Subscriber Flow (**Section 12.8.1**), and Media Interface **InsideMedRW** is used in the Remote Worker Server Flow (**Section 12.8.2.1**).

12.3. Signaling Interface on Avaya SBCE

The following screen shows the Signaling Interface settings. Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

Select the **Add** button to create Signaling Interface **InsideSIGRW** using the parameters:

- **IP Address**: Select **Network_A1 (A1, VLAN0)** and **10.10.98.34** (Internal IP Address toward Session Manager)
- **TLS Port**: **5061**
- **TLS Profile**: **AvayaSBCServer71**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use. Session Manager 7.1 includes SMGR signed certs, not the Avaya demo certificates
- Click on **Finish** (not shown)

Select the **Add** button to create Signaling Interface **OutsideSIGRW** using the parameters:

- **IP Address:** Select **Network_B1 (B1, VLAN0)** and **10.10.98.123** (External IP Address toward Remote Worker phones)
- **TLS Port**: **5061**
- **TLS Profile**: **AvayaSBCServer71**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use. Session Manager 7.1 includes SMGR signed certs, not the Avaya demo certificates
- Click on **Finish** (not shown)

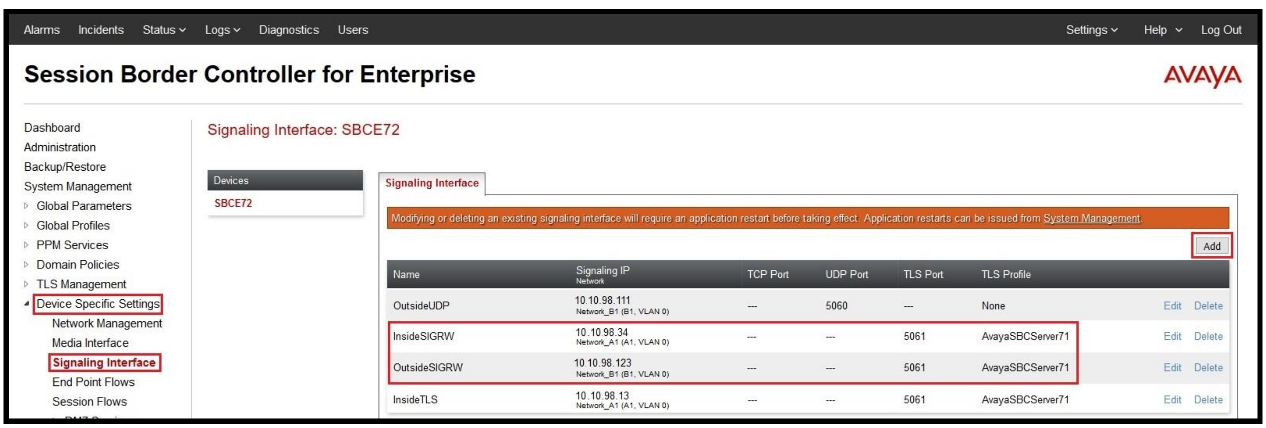

Figure 83: Signaling Interface

Note: Signaling Interface **OutsideSIGRW** is used in the Subscriber Flows (**Section 12.8.1**), and in the Remote Worker Server Flow (**Section 12.8.2.1**). Signaling Interface **InsideSIGRW** is used in the Remote Worker Server Flow (**Section 12.8.2.1**).

12.4. Routing Profile on Avaya SBCE

The Routing Profile **To_SMVM_RW** is created for routing the SIP traffic from Remote Worker to Session Manager via Avaya SBCE.
From the menu on the left-hand side, select **Global Profiles → Routing →Add**

Enter **Profile Name**: **To_SMVM_RW** (not shown)

- **Load Balancing**: **Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight**: **1**
- **Server Configuration**: **SMVM**
- **Next Hop Address**: **10.33.10.43:5061 (TLS)** (IP Address of Session Manager)
- Click **Finish**

The Routing Profile **To_SMVM_RW** is used in the Subscriber Flows (**Section 12.8.1**).

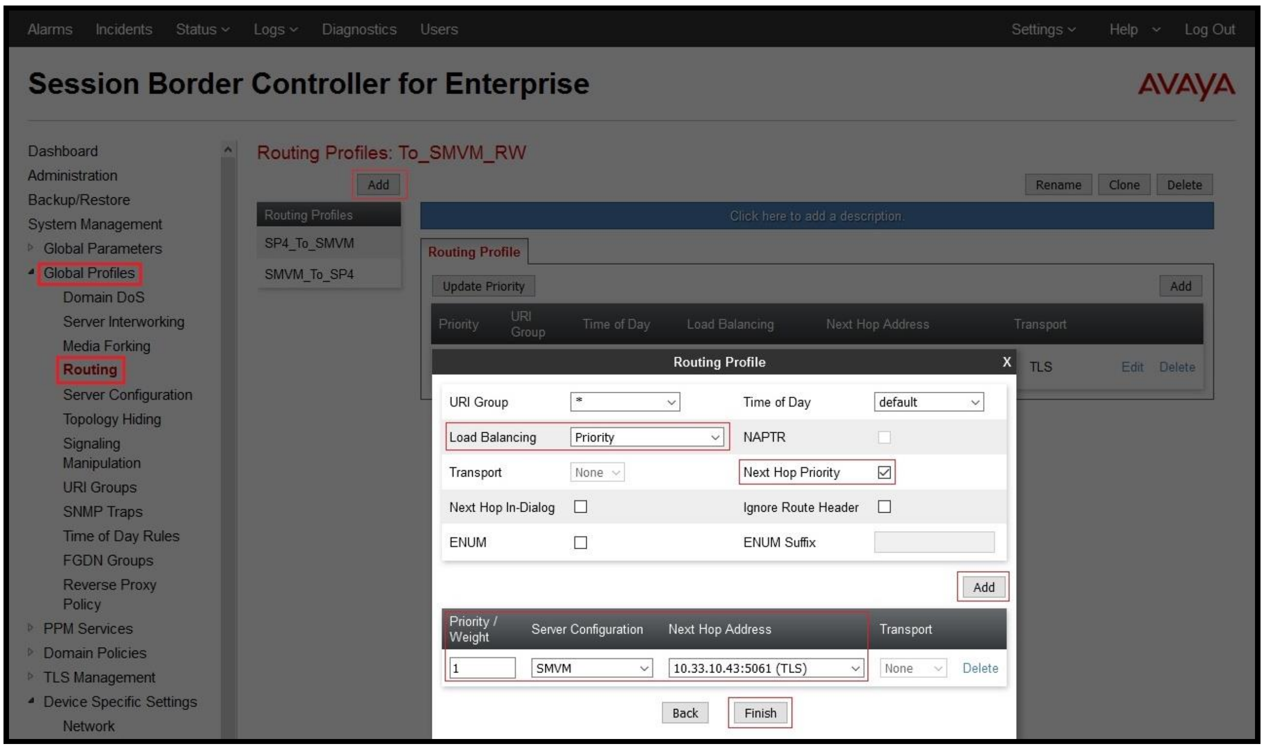

Figure 84: Remote Worker Routing to Session Manager

The Routing Profile default_RW is created for routing SIP traffic from Session Manager to Remote Worker via Avaya SBCE.
From the menu on the left-hand side, select **Global Profiles → Routing →Add**
Enter **Profile Name**: **default_RW**

- Check **Load Balancing**: **DNS/SRV**
- **NAPTR** box is checked
- Click **Finish**

The Routing Profile **default_RW** is used in the Remote Worker Server Flow in **Section 12.8.2.1**.

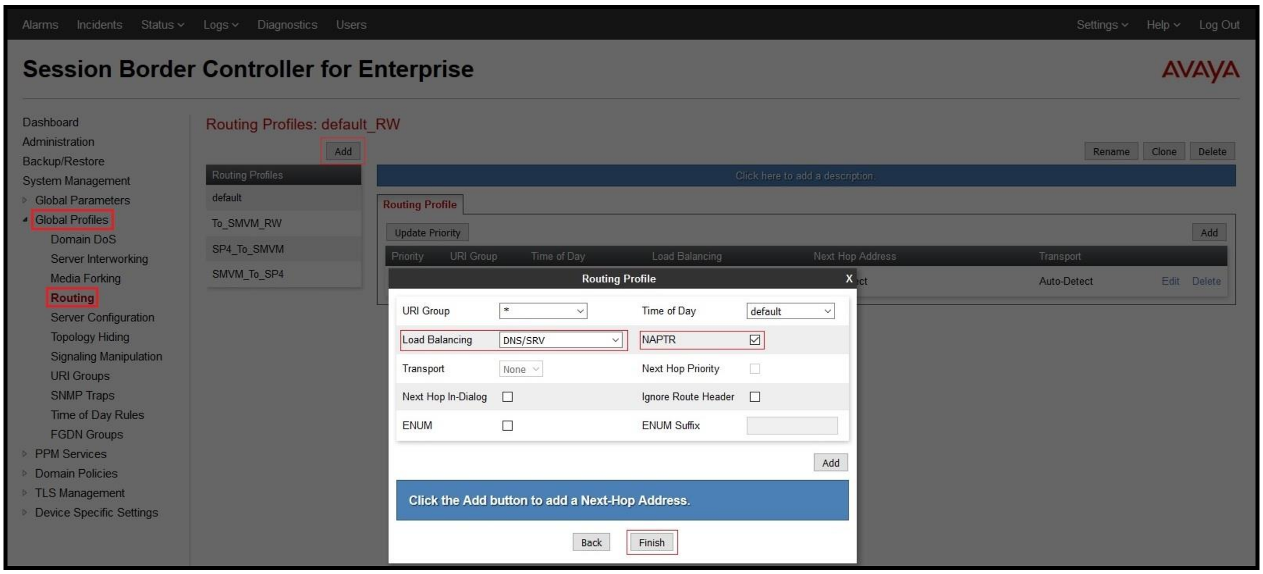

Figure 85: Remote Worker Default Routing

12.5. User Agent on Avaya SBCE

User Agents are created for each type of endpoints tested. In this compliance testing, Avaya one-X Communicator is used as the User Agent.

From the menu on the left-hand side, select **Global Parameters → User Agents**
Click **Add** button to add the user agent:

- Enter **Name**: **one-X Communicator**
- Enter **Regular Expression**: **Avaya one-X Communicator.***
- Click on **Finish** (not shown)

Figure 86: User Agents for Remote Worker

The following abridged output of Session Manager trace shows the details of an INVITE from an Avaya one-X Communicator. The User-Agent shown in this trace will match User Agent **one-X Communicator** shown above with a **Regular Expression** of "**Avaya one-X Communicator.***". In this expression, "**.***" will match anything listed after the user agent name.

```
INVITE sip: 1613XXX7497@bvwdev.com SIP/2.0
From: sip:0309@bvwdev.com;tag=-59f03c7f529fb7c152aa3fd4_F0950710.10.98.79
To: sip: 1613XXX7497@bvwdev.com
CSeq: 24 INVITE
Call-ID: 18_a7e80-49279ea452aa365c_I@10.10.98.79
Contact: <sip:0309@10.10.98.79:5061;transport=tls;subid_ipcs=3784557512>;+avaya-cm-line=1
Allow:INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE,PRA
CK
Supported: eventlist, 100rel, replaces, vnd.avaya.ipo
User-Agent: Avaya one-X Communicator/6.2.12.22 (Engine GA-2.2.0.174; Windows NT 6.2, 32-bit) AVAYA-
SM-7.1.3.0.713014 Avaya CM/R017x.01.0.532.0
Max-Forwards: 69
Via: SIP/2.0/TLS 10.10.98.79:62151;branch=z9hG4bK18_a7e80-312c149e52aa3fe8_I09507
Accept-Language: en
Content-Type: application/sdp
Content-Length: 440
```

Figure 87: Output of trace for User Agent

Note: The User Agent is defined in its associated **Subscriber Flows** in **Section 12.8.1**.

12.6. Application Rules on Avaya SBCE

The following section describes Application Rule **RW_AR**, used in this Remote Worker setting. In a typical customer installation, set the **Maximum Concurrent Sessions** for the **Voice** application to a value slightly larger than the licensed sessions.

From the menu on the left-hand side, select **Domain Policies → Application Rules**

- Select **default** from **Application Rules** and click **Clone** button:
- Enter **Clone Name** (e.g., **RW_AR**) and click **Finish** (not shown)
- Click on **RW_AR** from **Application Rules**, then click **Edit** button:
- In the **Audio** field:
  - Check **In** and **Out**
  - Enter an appropriate value in the **Maximum Concurrent Sessions** field (e.g., **2000**), and the same value in the **Maximum Session Per Endpoint** field
  - Leave the **CDR Support** field at **None** and the **RTCP Keep-Alive** field unchecked (**No**)
  - Click on **Finish** (not shown)

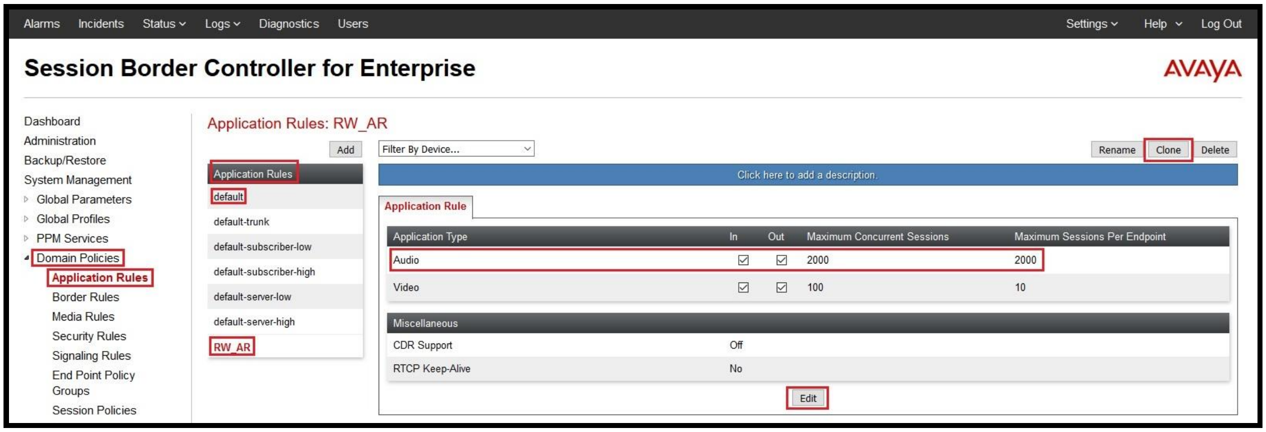

Figure 88: Remote Worker Application Rule

Note: The rule **RW_AR** is assigned to the End Point Policy Groups in **Section 12.7**.

12.7. End Point Policy Groups on Avaya SBCE

A new End Point Policy Groups is defined for Remote Worker: **SMVM_RW**.

To create the new **SMVM_RW** group, click on **Add**. Enter the following:

- Enter a name (e.g., **SMVM_RW**), and click on **Next** (not shown)
- The **Policy Group** window will open. Enter the following:
  - **Application Rule** = **RW_AR** (see **Section 12.6**)
  - **Border Rule** = **default**
  - **Media Rule** = **SMVM_SP4** (see **Section 7.3.1**)
  - **Security Rule** = **default-low**
  - **Signaling Rule** = **default**
- Click on **Finish** (not shown)

The End Point Policy Group **SMVM_RW** is used in the Subscriber Flow **one-X Communicator** in **Section 12.8.1** and Remote Worker Server Flow in **Section 12.8.2.1**.

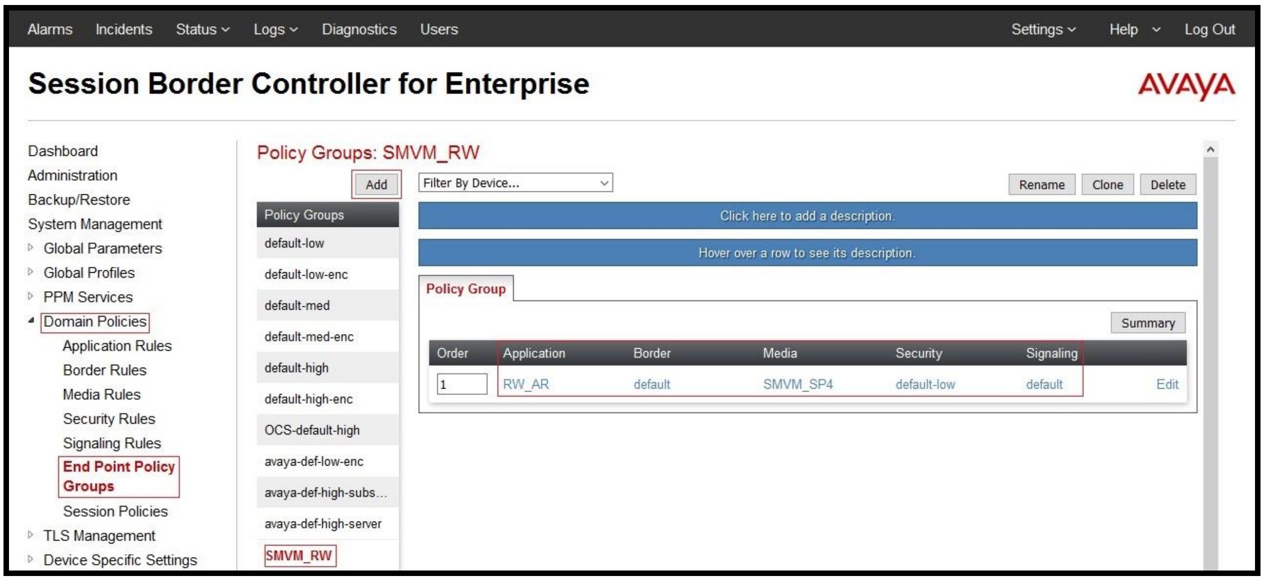

Figure 89: Remote Worker End Point Policy

12.8. End Point Flows on Avaya SBCE

12.8.1. Subscriber Flow

The **Subscriber Flow** is defined for Remote Workers associated with the **User Agent one-X Communicator** that was created in **Section 12.5**.The below subscriber flow is configured for Remote Worker to access Session Manager via Avaya SBCE.

From the menu on the left-hand side, select **Device Specific Settings → End Point Flows**
On the **Subscriber Flows** tab, click on the **Add** button and enter the following:

- Enter a **Flow Name** (e.g., **one-X Communicator**)

- **URI Group** = * (default)
- **User Agent** = **one-X Communicator** (see **Section 12.5**)
- **Source Subnet** = ***** (default)
- **Via Host** = ***** (default)
- **Contact Host** = ***** (default)
- **Signaling Interface** = **OutsideSIGRW** (see **Section 12.3**)

Click on **Next** (not shown) and the Profile window will open (not shown). Enter the following:

- **Source** = **Subscriber**
- **Methods Allowed Before REGISTER =** Leave as default
- **Media Interface** = **OutsideMedRW** (see **Section 12.2**)
- **Received Interface** = **None**.
- **End Point Policy Group = SMVM_RW** (see **Section 12.7**)
- **Routing Profile = To_SMVM_RW** (see **Section 12.4**)
- **TLS Client Profile** = **None**
- **Signaling Manipulation Script** = **None**
- **Presence Server Address** = Leave as blank

Click on **Finish** (not shown).

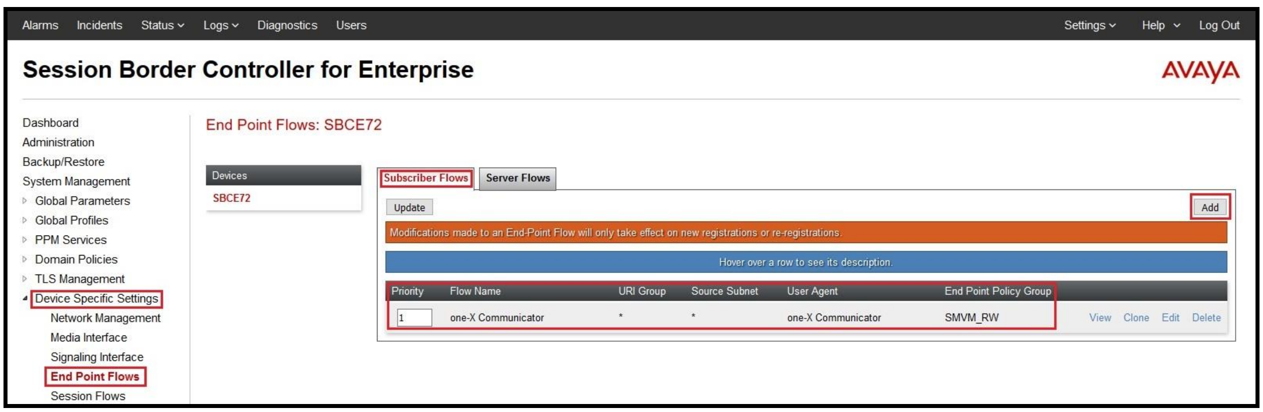

Figure 90: Remote Worker Subscriber Flows – 1

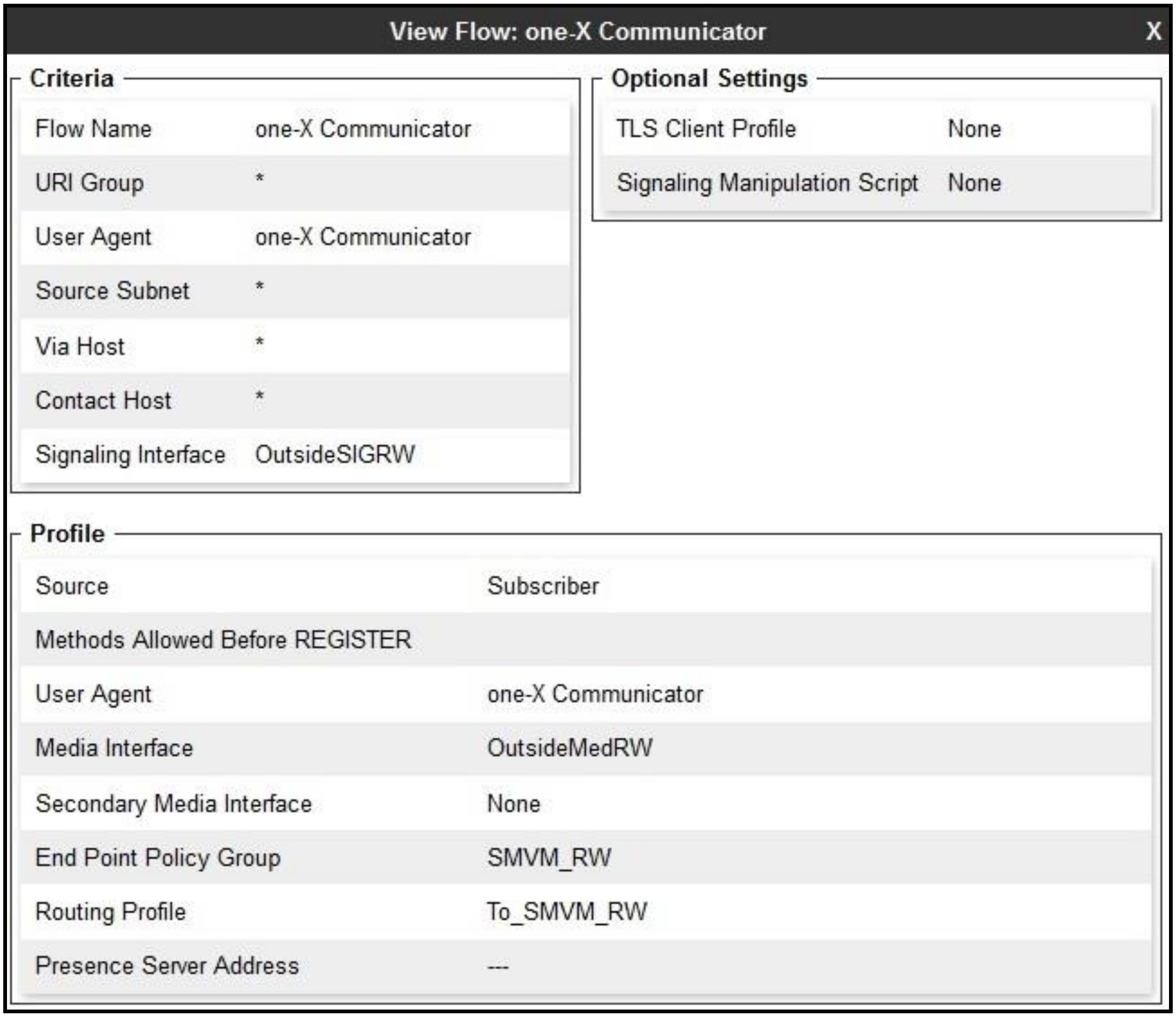

Figure 91: Remote Worker Subscriber Flows – 2

12.8.2. Server Flow on Avaya SBCE

The new Remote Worker Server Flow (**SMVM_RemoteWorker**) is configured for the SIP traffic flow from Session Manager to Remote Worker via Avaya SBCE. Two existing Trunking Server Flows (SMVM Flow in **Section 7.4.4.1** and SP4 Flow in **Section 7.4.4.2**) are also used for Remote Worker.

12.8.2.1 Remote Worker Server Flow

From the menu on the left-hand side, select **Device Specific Settings → Endpoint Flows**
Select the **Server Flows** tab and click the **Add** button (not shown) to enter the following:

- **Name = SMVM_RemoteWorker**
- **Server Configuration** = **SMVM** (see **Section 7.2.4**)
- **URI Group** = ***** (default)
- **Transport** = ***** (default)
- **Remote Subnet** = ***** (default)
- **Received Interface** = **OutsideSIGRW** (see **Section 12.3**)
- **Signaling Interface** = **InsideSIGRW** (see **Section 12.3**)
- **Media Interface** = **InsideMedRW** (see **Section 12.2**)
- **Secondary Media Interface** = **None**
- **End Point Policy Group** = **SMVM_RW** (see **Section 12.7**)
- **Routing Profile** = **default_RW** (see **Section 12.4**)
- **Topology Hiding Profile** = **None** (default)
- **Signaling Manipulation Script = None** (default)
- **Remote Branch Office** = **Any** (default)

Click **Finish** (not shown).

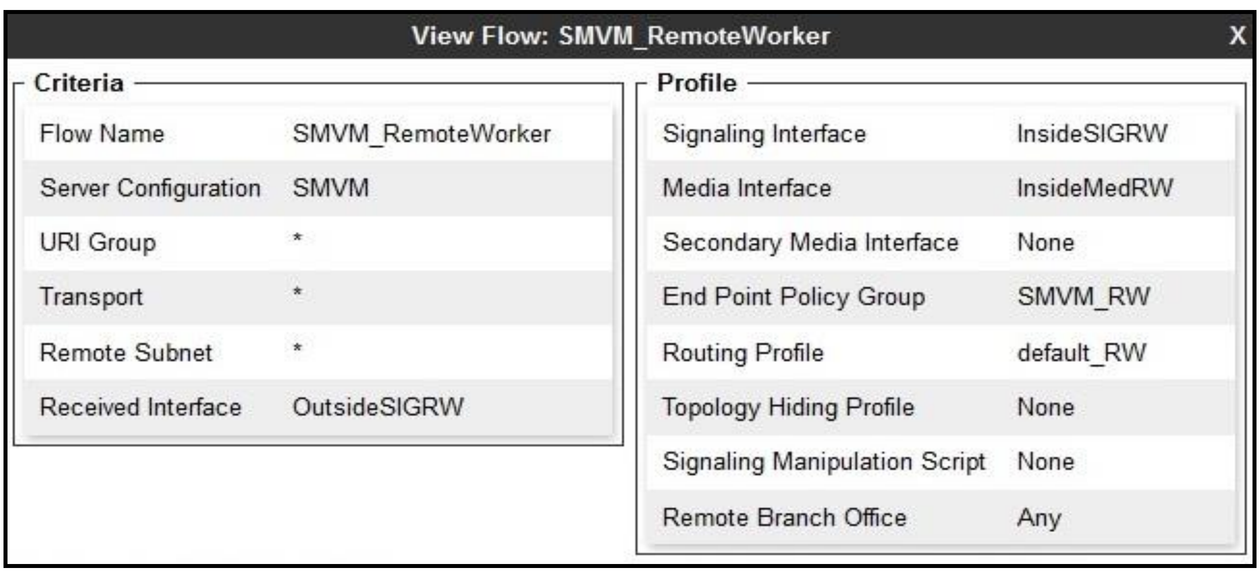

Figure 92: Remote Worker Server Flow

12.8.2.2 Trunking Server Flow

Two existing Trunking Server Flows (SMVM Flow in **Section 7.4.4.1** and SP4 Flow in **Section 7.4.4.2**) are also used for Remote Worker.

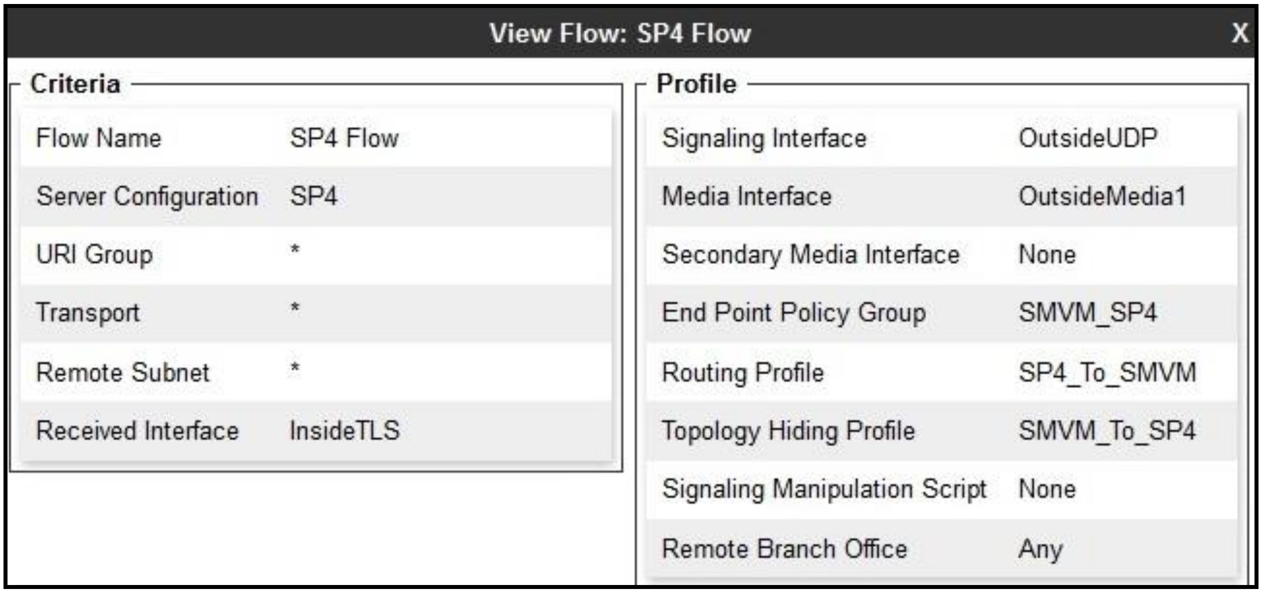

Figure 93: Trunking Server Flow – SP4 Flow

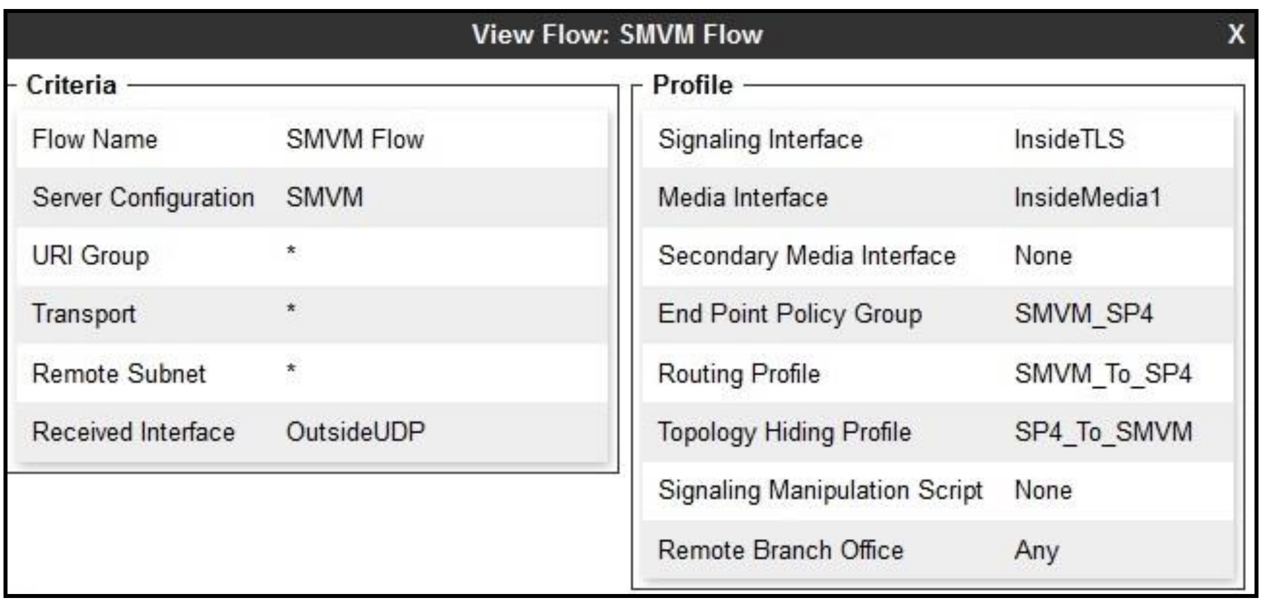

Figure 94: Trunking Server Flow – SMVM Flow

12.9. System Manager

12.9.1. Modify Session Manager Firewall: Elements → Session Manager → Network Configuration → SIP Firewall

Select **Rule Sets** as **Rule Set for SMVM,** click **Edit** button

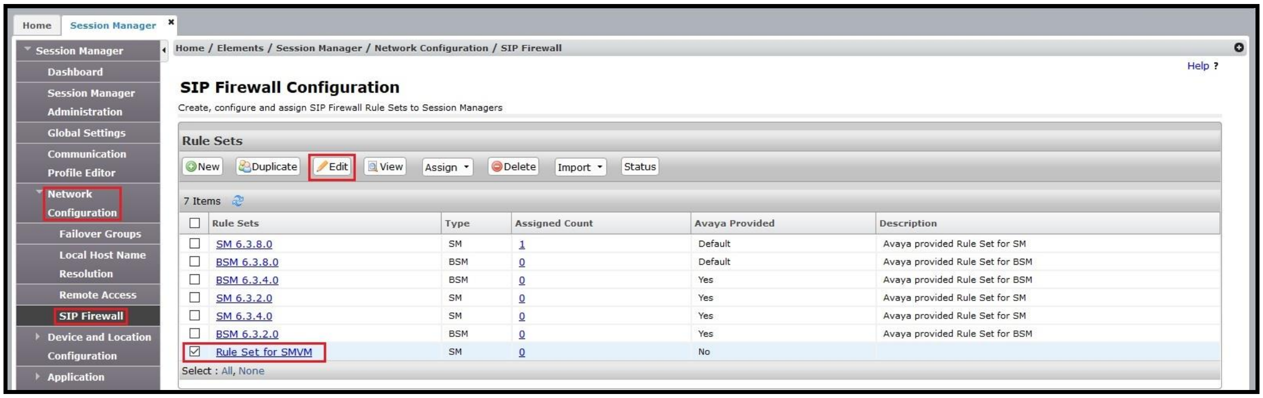

Figure 95: Session Manager – SIP Firewall Configuration - Rules

On **Whitelist** tab, select **New**

- In the **Key** field, select **Remote IP Address**
- In the **Value** field, enter internal Avaya SBCE IP address used for Remote Worker (**10.33.10.34** as defined in **Section 12.1**)
- In the **Mask** field, enter the appropriate mask (e.g., **255.255.255.255**)
- **Enabled** box is checked
- Select **Commit**

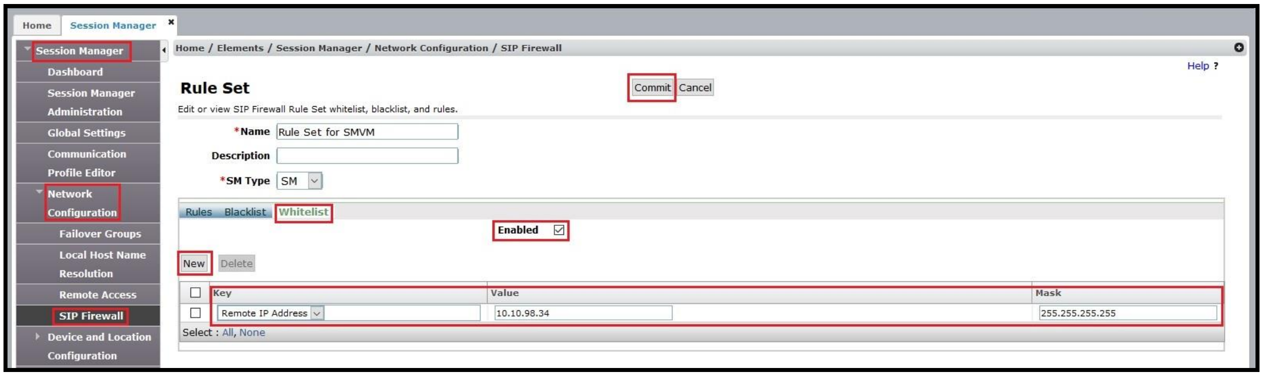

Figure 96: Session Manager – SIP Firewall Configuration - Whitelist

12.9.2. Disable PPM Limiting: Elements → Session Manager → Session Manager Administration

Select the **Session Manager Instance** named **bvwasm2**, and select **Edit**

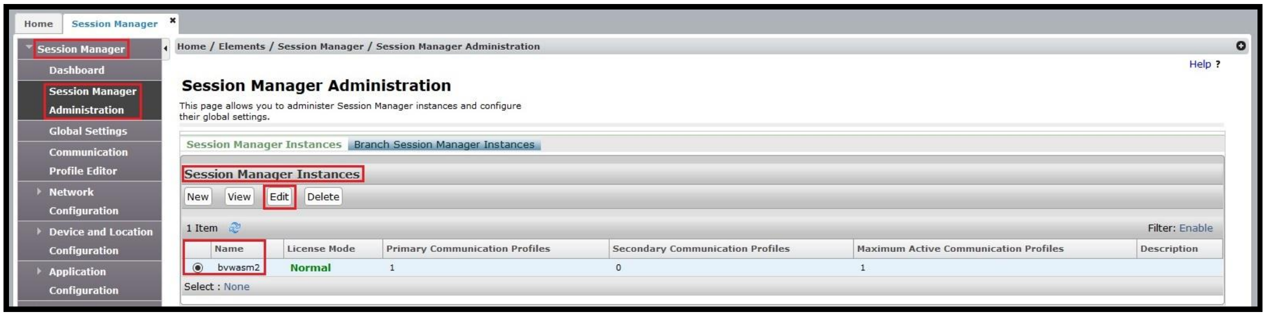

Figure 97: Session Manager – Edit Instance

The **Session Manager View** screen is displayed. Scroll down to the **Personal Profile Manager (PPM) – Connection Settings** section.

- Uncheck the **Limited PPM Client Connection** and **PPM Packet Rate Limiting** options
- Select **Commit** (not shown)

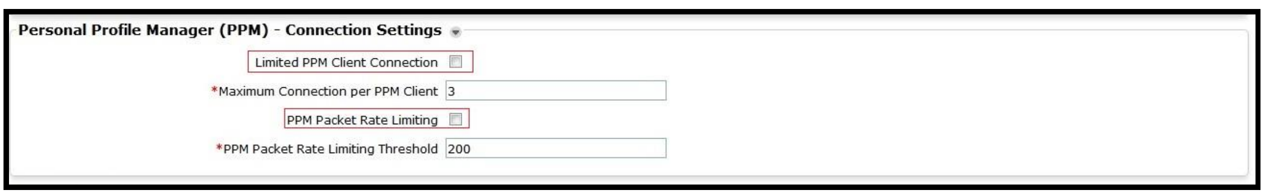

Figure 98: Session Manager – Disable PPM limit

12.10. Remote Worker Client Configuration

The following screen illustrates Avaya one-X® Communicator administration settings for the Remote Worker, used in the reference configuration (note that some screen formats may differ from endpoint to endpoint).

SIP Global Settings Screen

Launch to **Avaya one-X® Communicator settings** and click on **Telephony** under **Accounts**.
Select **Using** as **SIP**
Enter **Extension** and **Password**
Click **Add** button to add a server into **Server List**
Enter **Proxy Server** as **10.10.98.123** (see **Section 12.1**). Set **Transport Type**: **TLS and Port**: **5061**. Click **OK** to submit the changes.
Set the **Domain** to **bvwdev.com**.
The other fields are default. Click **OK** to submit the settings.

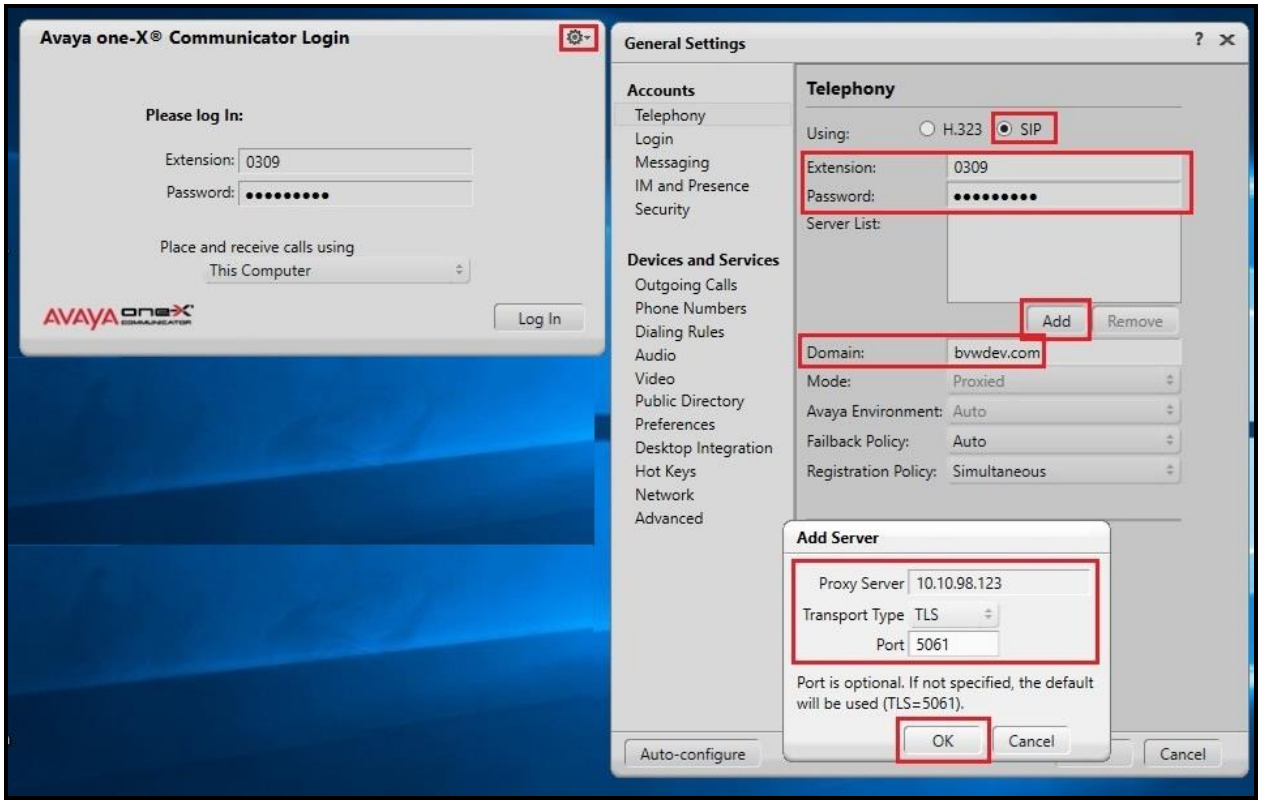

Figure 99: Avaya one-X Communicator - Settings

13. Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the SBCE, **Section 7.2.3**:

```
within session "ALL"
{
   act on message where %DIRECTION="INBOUND" and
%ENTRY_POINT="AFTER_NETWORK"
        {
//Modify the OPTIONS

%HEADERS["Request_Line"][1].regex_replace("sip:p587XXX0308@10.10.98.111:5060","sip:
587XXX0308@10.10.98.111:5060");
         }
 }
// Set Max-Forward Header to 0 in outbound SIP OPTION. This is optional for testing ONLY.
//within session "OPTIONS"
//{
//    act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
//       {
//          if (exists(%HEADERS["Max-Forwards"][1]))then
//          {
//          %HEADERS["Max-Forwards"][1]= "0";
//          }
//       }
//}
within session "ALL"
{
   act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
       {
//Remove plus sign
         %HEADERS["From"][1].URI.USER.regex_replace("\+","");
         %HEADERS["P-Asserted-Identity"][1].URI.USER.regex_replace("(\+)","");
         %HEADERS["Contact"][1].URI.USER.regex_replace("(\+)","");
         %HEADERS["Diversion"][1].URI.USER.regex_replace("(\+)","");
//Modify user of SIP URI in PAI header on Call Forward Off-net
            if (%HEADERS["Diversion"][1].regex_match("reason")) then
               {
              %HEADERS["P-Asserted-Identity"][1].URI.USER =
%HEADERS["Diversion"][1].URI.USER;
```

```
                }
//Remove unwanted Headers
        remove(%HEADERS["History-Info"][3]);
        remove(%HEADERS["History-Info"][2]);
        remove(%HEADERS["History-Info"][1]);
      }
}
```

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.