Avaya Solution & Interoperability Test Lab

Application Notes for Configuring TDC Business Trunk with Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.3 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between TDC Business Trunk and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.3, Avaya Session Border Controller for Enterprise 6.3 and various Avaya endpoints.

TDC Business Trunk 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 TDC Business Trunk and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.3, Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.3 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with TDC Business 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 TDC Business 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.

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from softphones. Two Avaya soft phones were used in testing: Avaya one-X® Communicator (1XC) and Avaya Communicator 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 Communicator for Windows was used in testing as a simple SIP endpoint for basic inbound/outbound calls.
- SIP transport using TCP and UDP as supported.

- 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.
- Various call types including: long distance, international, outbound toll-free, 11414, 1177, 118118 and 112 services.
- Codec G.711A, G.729A, and G.711MU.
- 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).
- Use of SIP RE-INVITE for call transfer.
- Use of the Diversion Header for call forward.
- Call Center scenarios.
- Fax T.38.
- Mobility EC500.
- DTMF - RFC2833.
- Additional MEX call testing. With TDC Business Trunk, MEX calls from MEX enabled mobile phones are tromboned in the Avaya PBX and returned as normal Business Trunk calls. The MEX implementation relies on IN triggers on the PSTN side which prefixes the called number with a routing number used for routing the call towards the Avaya PBX.

Items not supported included the following:

- Registration and Authentication.

Items not tested included the following:

- SIP Refer in Call Transfer. TDC Business Trunk was not sure 100% to support the SIP Refer. Therefore, the SIP Re-Invite was tested in Call Transfer.

2.2. Test Results

Interoperability testing of TDC Business Trunk was completed with successful results for all test cases with the exception of the limitation described below.

- **TDC sent the SIP OPTIONS included the Max-Forward = 0, and Avaya responded with "483 Too Many Hops"** - The OPTIONS request is simply a keep-alive message. As long as TDC received some kind of reply, TDC treated the connection to be open. Of course the value of Max-Forward could be increased, but since it did not cause any problem during compliance testing, TDC preferred to keep the same configuration, as it has been the most usual.

- **Avaya sent the SIP OPTIONS, and TDC responded "404 Called User Unknown" -** As long as Avaya received some kind of reply, Avaya treated the connection to be alive.
- **Anonymous outbound call from Avaya PBX to PSTN failed** - In this call scenario, Avaya set Privacy header as "id" as well as sent FROM header with "anonymous" for user's Name and ID number. But TDC rejected this call because the system needed a Privacy header with "id" and a valid ID number instead of an anonymous ID number to trust with 3GPP specifications. In order to fix this, TDC has a workaround to replace the anonymous string by the identity of the pilot user and when doing so also this user has to be assigned a phone number – 46104925878. These anonymous calls may be used but charging for these calls cannot be done on individual basis.
- **Call was dropped between the active phones in a conference if the Avaya IP phone disconnected the conference** – On a call scenario was when an Avaya IP phone hosted a conference among phones, and then the Avaya IP phone disconnected the conference, the call was dropped between active phones in the conference. The issue is under investigation.
- **The inbound Fax T.38 call was failed** – In order to communicate with inbound Fax T.38, TDC should send the packet MPS (MultiPage Signal),….to keep on communicating with FAX T.38 for sending pages, but TDC did not send this packet. As the result, the inbound Fax T.38 call failed with multi-pages faxes only.
- **Call from Mobile Extension (MEX) mobile A to any MEX Fixed network numbers or to any MEX Fixed extension numbers, the MEX Fixed number A was always displayed in full length number instead of extension number** - This is the configuration of SIP manipulation on Avaya SBCE to replace the MEX mobile by MEX fixed number.

2.3. Support

For technical support on the TDC Business Trunk system, please use the support link at http://www.tdc.se/, or call the customer support number at 020-832 832.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to TDC Business 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.

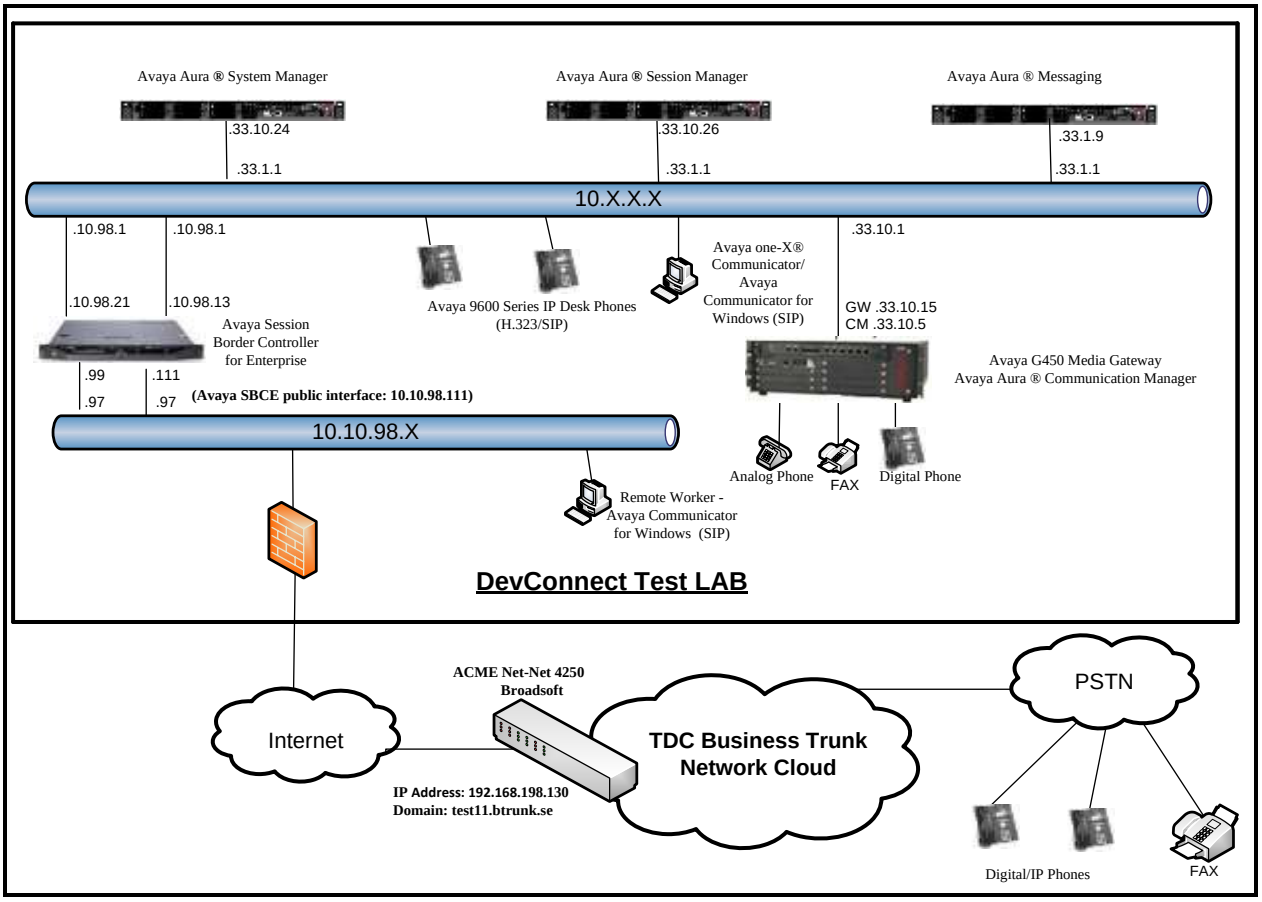

Figure 1: Avaya IP Telephony Network and TDC Business Trunk

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 Avaya S8300 Server	6.3.10 (R016x.03.0.124.0-22147)
Avaya G450 Media Gateway – MM711AP Analog – MM712AP Digital – MM710AP	36.14 HW46 FW096 HW10 FW014 HW05 FW020
Avaya Aura® Session Manager running on Avaya S8800 Server	6.3.13 (6.3.13.631303)
Avaya Aura® System Manager running on Avaya S8800 Server	6.3.13 (Build No 6.3.0.8.5682 – Patch 6.3.8.5108 Software Update Revision No: 6.3.13.10.3336)
Avaya Aura® Messaging running on Avaya S8800 Server	6.2 SP2
Avaya Session Border Controller for Enterprise running on Dell R210 V2 Server	6.3.2-08-5478
Avaya 9630 IP Deskphone (SIP)	Avaya one-X® Deskphone SIP Edition 2.6.12.1
Avaya 9640 IP Deskphone (H.323)	Avaya one-X® Deskphone Edition 3.242A
Avaya 9630 IP Deskphone (H.323)	Avaya one-X® Deskphone Edition 3.220A
Avaya Communicator for Windows	2.1.1.74
Avaya one-X® Communicator (H.323 & SIP)	6.2.6-03 FP6
Avaya Digital Telephones (1408D)	N/A
Nortel Symphony 2000 Analog telephone	N/A
HP Officejet 4500 Fax	N/A
TDC Business Trunk Components	
Equipment/Software	**Release/Version**
ACME Net-Net 4250	Firmware SC6.1.0 MR-9 Patch 3 (Build 967)
Broadsoft	R20SP1

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.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for TDC Business Trunk. It is assumed the general installation of Communication Manager, Avaya Media Gateway and Session Manager has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged 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 24000 SIP trunks are available and 136 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: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 1
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 41000 0
                   Maximum Video Capable IP Softphones: 18000 5
                      Maximum Administered SIP Trunks: 24000 136
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                            Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

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

On **Page 3**, verify that **ARS** is set to **y**.

```
display system-parameters customer-options                    Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? n
        Analog Trunk Incoming Call ID? n                      CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? n                        CAS Main? n
Answer Supervision by Call Classifier? n                 Change COR by FAC? n
                                ARS? y  Computer Telephony Adjunct Links? n
                 ARS/AAR Partitioning? y  Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                      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 3

On **Page 5**, verify that **Private Networking** and **Processor Ethernet** are set to **y**.

```
display system-parameters customer-options                    Page   5 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? y               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 5

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? y
                                    Trunk-to-Trunk Transfer: all
              Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
```

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.

```
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: 1
          International Access Code: 011

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 of Communication Manager **(procr**) and Session Manager (**SM63**). 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
DevAAM                  10.33.10.9
SM63                    10.33.10.26
default                 0.0.0.0
procr                   10.33.10.5
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. For the compliance test, ip-codec-set 1 was used for this purpose. TDC Business Trunk supports the **G.711A**, **G.729**, **G.711MU** 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.711A          n            2        20
 2: G.729           n            2        20
 3: G.711MU         n            2        20
```

Figure 8: IP-Codec-Set Form – Page 1

On **Page 2**, to enable fax t.38, set the **FAX Mode** to **t.38-standard**.

```
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            EMC: 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 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 **bvwdev7.com**. This name appears in the From header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable IP-IP Direct Audio (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region 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: bvwdev7.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

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: 19660

      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: 10.33.10.5
          Subnet Mask: /24
```

Figure 11: IP-Interface Form

5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups between Communication Manager and Session Manager. The signaling groups are used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group **20** was used for both outbound and inbound calls. It was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the value of **tcp** (Transmission Control Protocol). The transport method specified here is used between Communication Manager and Session Manager. TLS (Transport Layer Security) is the recommended setting, but TCP was used during testing to aid in debugging.
- 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 **SM63**. 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 TCP, as **5080**.
- 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 **bvwdev7.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 Media Gateway will not remain in the media path of all calls between the SIP trunk and the endpoint.
- Set the **Alternate Route Timer** to **6**. This defines the number of seconds the 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: tcp
       Q-SIP? n
    IP Video? n                                    Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+'to Outgoing Calling/Alerting/Diverting/connected Public Numbers? y
Remove '+'from Incoming Called/Calling/Alerting/Diverting/connected Numbers? n

  Near-end Node Name: procr                 Far-end Node Name: SM63
 Near-end Listen Port: 5080               Far-end Listen Port: 5080
                                       Far-end Network Region: 1
                                 Far-end Secondary Node Name:
Far-end Domain: bvwdev7.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 12: Signaling-Group

5.8. Trunk Group

Use the **add trunk-group** command to create trunk groups for the signaling groups created in **Section 5.7**. For the compliance test, trunk group **20** was used for both outbound and inbound calls. 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**).
- 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: 10
```

Figure 13: 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 re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

```
add trunk-group 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 14: Trunk-Group – Page 2

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. The compliance test used 11 digit numbering format. Thus, **Numbering Format** was set to **private** and the **Numbering Format** field in the route pattern was set to **unk-unk** (see **Section 5.10**).

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: private
                                              UUI Treatment: service-provider

                                               Replace Restricted Numbers? y
                                              Replace Unavailable Numbers? y


                                  Modify Tandem Calling Number: no


 Show ANSWERED BY on Display? y
```

Figure 15: Trunk-Group – Page 3

On **Page 4**, the **Network Call Redirection** field can be set to **n** (default setting) so that the SIP REFER is not sent. TDC Business SIP Trunk was not sure 100% to support the SIP Refer. Therefore, the SIP Re-Invite was tested in Call Transfer instead (see **Section 2.1**).

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been re-directed. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

```
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? n
          Build Refer-To URI of REFER From Contact For NCR? n

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

                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            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 16: Trunk-Group – Page 4

5.9. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.8**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs), 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 private-numbering entry can be applied for all extensions. In this compliance testing, all stations with a 4-digit extension beginning with **58** will send the calling party number as the **Private Prefix** plus the extension number.

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

Ext  Ext             Trk         Private          Total
Len  Code            Grp(s)      Prefix           Len
 4   58              20          4610492           11     Total Administered: 11
                                                         Maximum Entries: 540
```

Figure 17: Private-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 **9** is used as the ARS access code. Enterprise callers will dial **9** to reach an "outside line". This common configuration is illustrated below. Use the **change dialplan analysis** command to define a **Dialed String** beginning with **9** of **Total Length 1** as a feature access code (**fac**).

```
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

    0890        7    ext
    112         3    ext
    11414       5    ext
    1177        4    ext
    118118      6    ext
    18          4    ext
    58          4    ext
    613962     10    ext
    8           4    ext
    9           1    fac
    *           4    dac
    #           4    dac
```

Figure 18: Dialplan–Analysis Form

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

```
change feature-access-codes                                    Page   1 of  11
                                FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated 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: *100
    Auto Route Selection (ARS) - Access Code 1: 9     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 19: Feature–Access-Codes Form

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **9**. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to **Route Pattern 20** which contains the SIP trunk to the service provider (as defined next).

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

          Dialed          Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
     001                  10   17    20        pubu          n
     087                   5   10    20        pubu          n
     089                   5   10    20        pubu          n
     10494                 5   10    20        pubu          n
     1303                 11   11    20        pubu          n
     1416                 11   11    20        pubu          n
     1613                 11   11    20        pubu          n
     1800                 11   11    20        pubu          n
     463                  10   13    20        pubu          n
     9                     5    7    20        pubu          n
```

Figure 20: 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 **unk-unk** since private 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                                 unk-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 21: Route–Pattern 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 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**. As an example, use the **change inc-call-handling-trmt trunk-group 20** to convert incoming DID numbers +4610492XXXX to 4 digit extension XXXX by deleting **8** of the incoming digits. The incoming DID number **+46104925878** is converted to **8000** by deleting 12 of incoming digits for voicemail testing purpose. The incoming DID number **+222, +222010492, +2225872** are converted to corresponding numbers by deleting and inserting the appropriated digits for MEX call testing purposes.

```
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       12         +4610492         8
 public-ntwrk       12         +46104925878     12  8000
 public-ntwrk       14         +222             4   9
 public-ntwrk       14         +222010492       10
 public-ntwrk       8          +2225872         8   5872
 public-ntwrk       17         +222             4   9
```

Figure 22: Inc-Call-Handling-Trmt Form

5.12. Avaya Aura® Communication Manager Stations

In the sample configuration, four digit station extensions were used with the format 58XX. Use the **add station 5871** command to add an Avaya H.323 IP telephone.

- Enter **Type**: **9640**, **Name**: **5871**, **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 5871                                          Page   1 of   5
                                    STATION

Extension: 5871                         Lock Messages? n                BCC: 0
     Type: 9640                           Security Code: 1234             TN: 1
     Port: S000012                       Coverage Path 1: 1              COR: 1
     Name: 5871                          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: 5871
           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 23: Add-Station Form

5.13. 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.

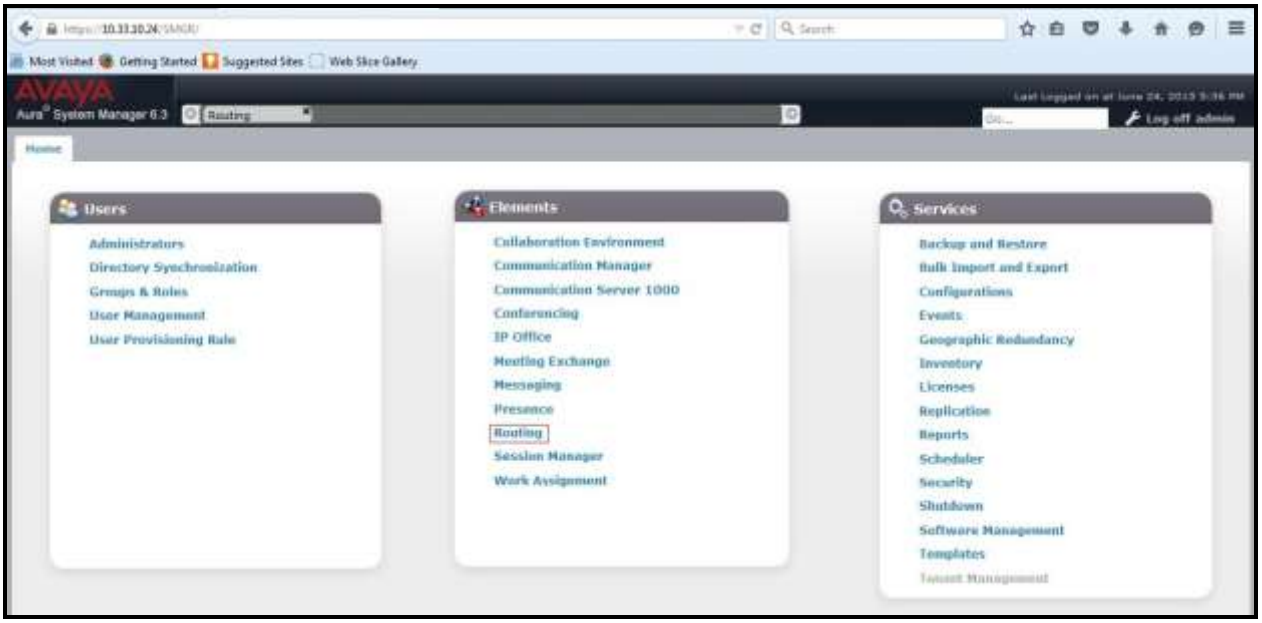

Figure 24: System Manager Home Screen

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.

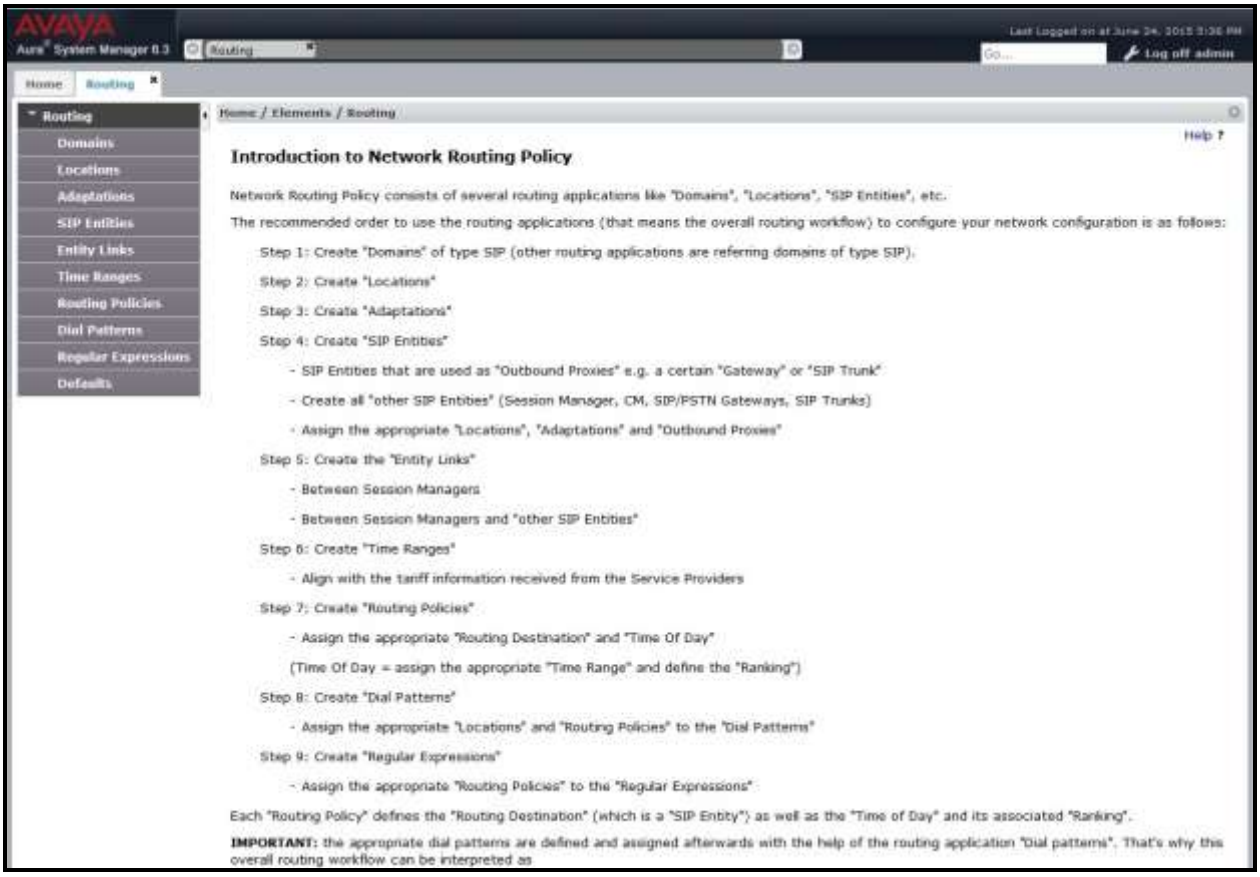

Figure 25: Network Routing Policy

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 **bvwdev7.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 26: 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**, 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.

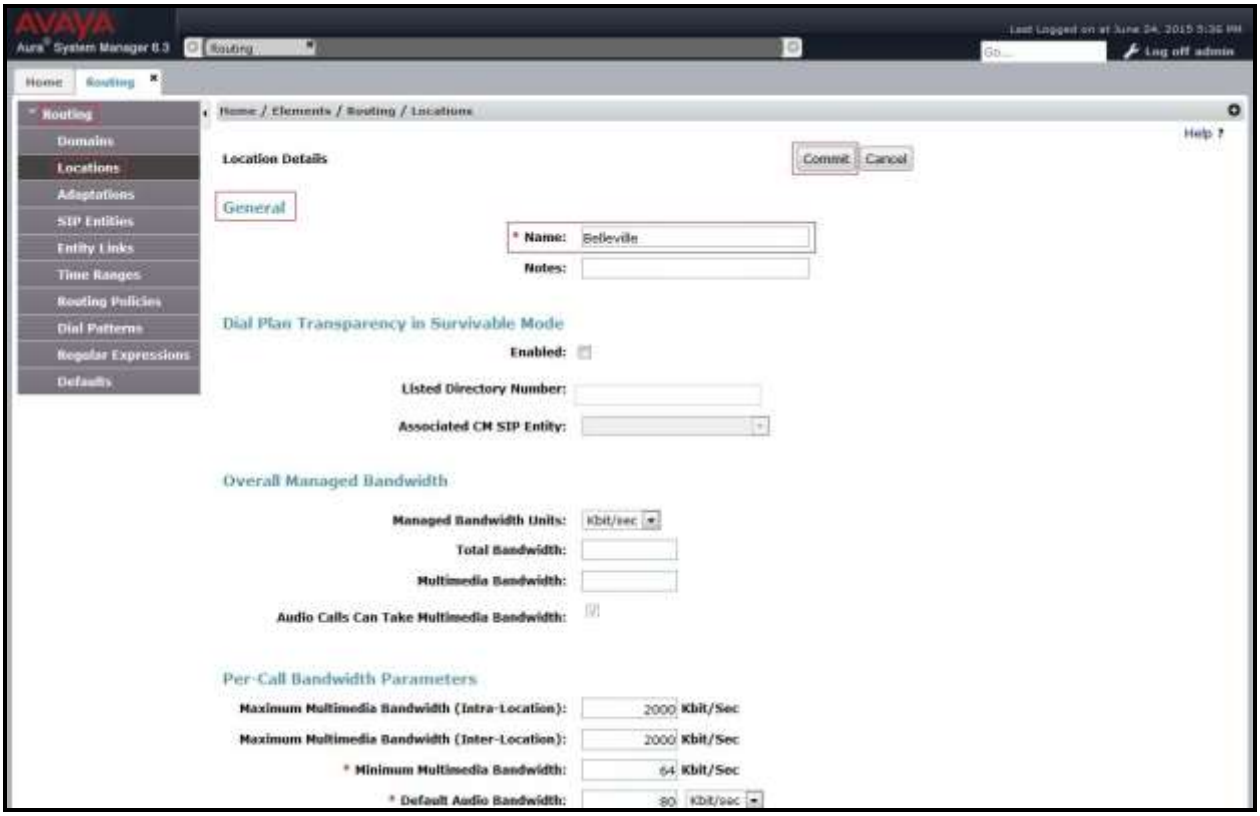

Figure 27: Location Configuration

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

- **IP Address Pattern:** 10.33.*, 10.10.98.*.
- Click **Commit** to save.

Figure 28: 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 **Other** for Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. Adaptation module was 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**.
- **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 **SM63**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.10.26**. The user will need to select the specific values for the **Location** and **Time Zone**.

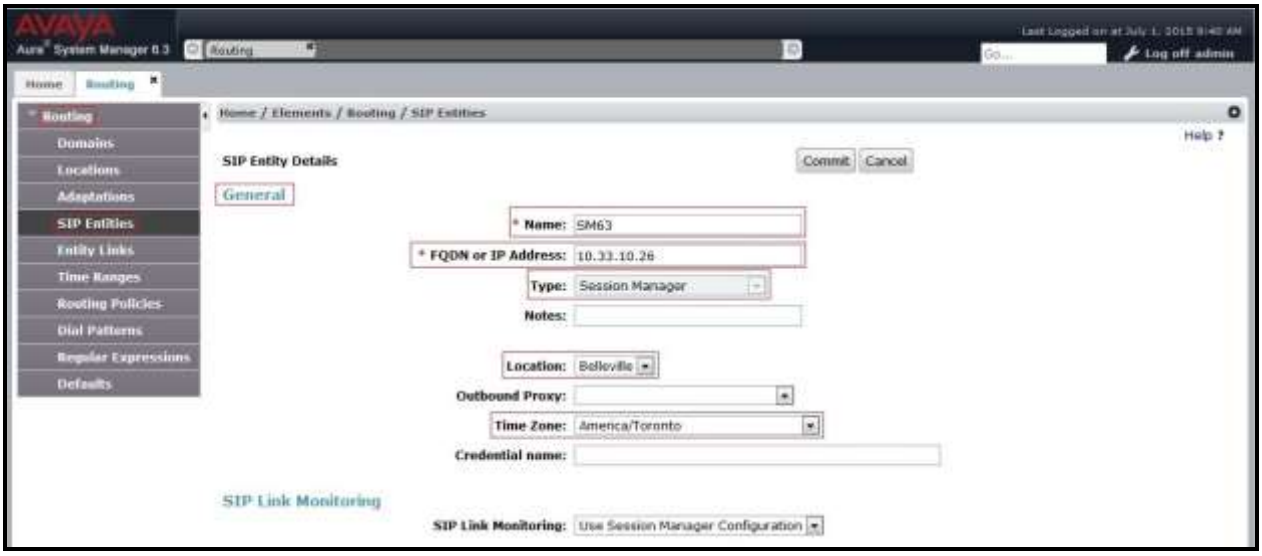

Figure 29: Session Manager SIP Entity

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

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

- **Port:** Port number on which 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 **5080** with **TCP** for connecting to Communication Manager, port **5060** with **TCP** for connecting Avaya SIP telephones and SIP soft clients, port **5060** with **UDP** for connecting to Avaya SBCE.

Figure 30: 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 **SP3_CM63_TCP_5080**. 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 **10.33.10.5**. Note that **CM** was selected for **Type**. The **Location** field is set to **Belleville** which is the Location that includes the subnet where Communication Manager resides. The user will need to select the specific values for the **Location** and **Time Zone.**

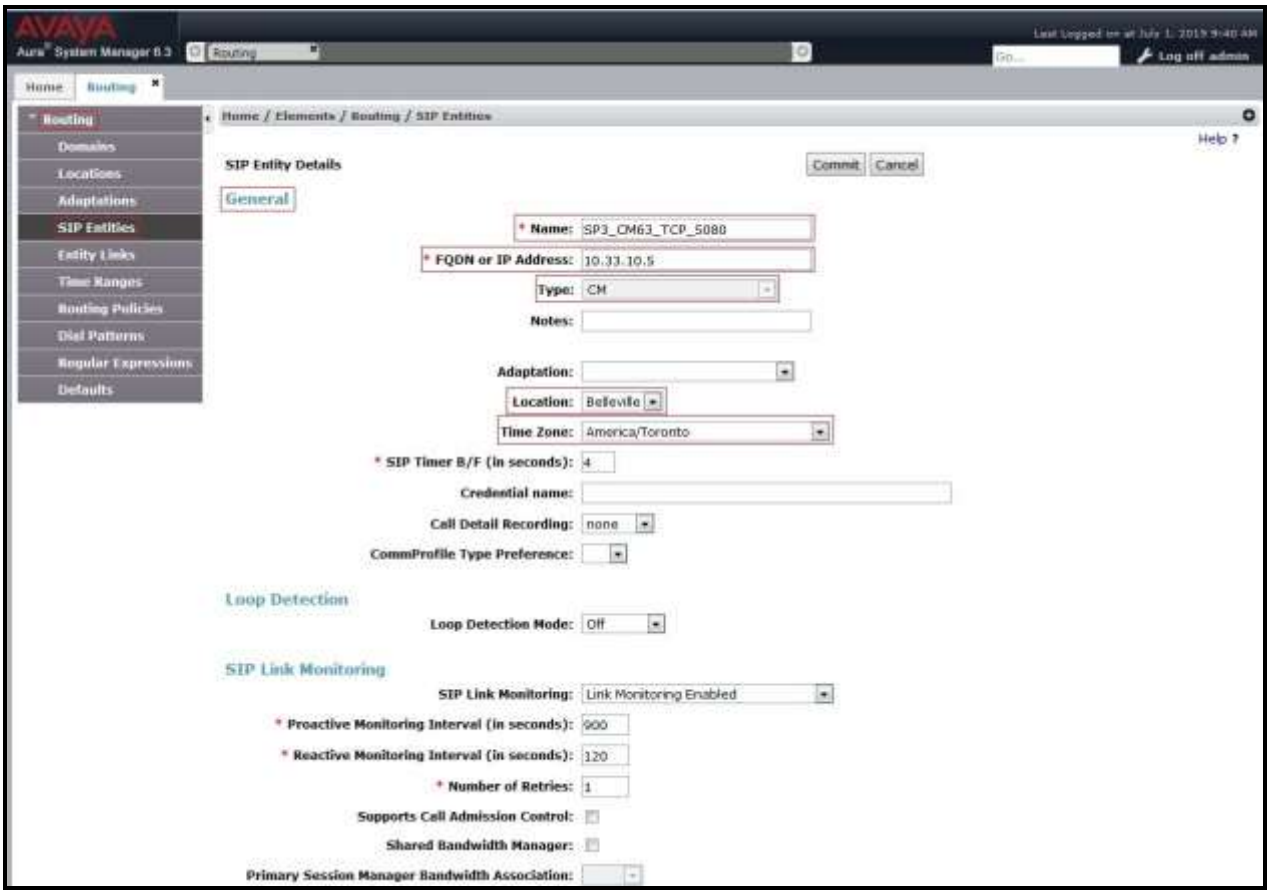

Figure 31: Communication Manager SIP Entity

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 **Other** was selected for **Type**. The **Location** field is set to **Belleville** which includes the subnet where the Avaya SBCE resides. The user will need to select the specific values for the **Location** and **Time Zone.**

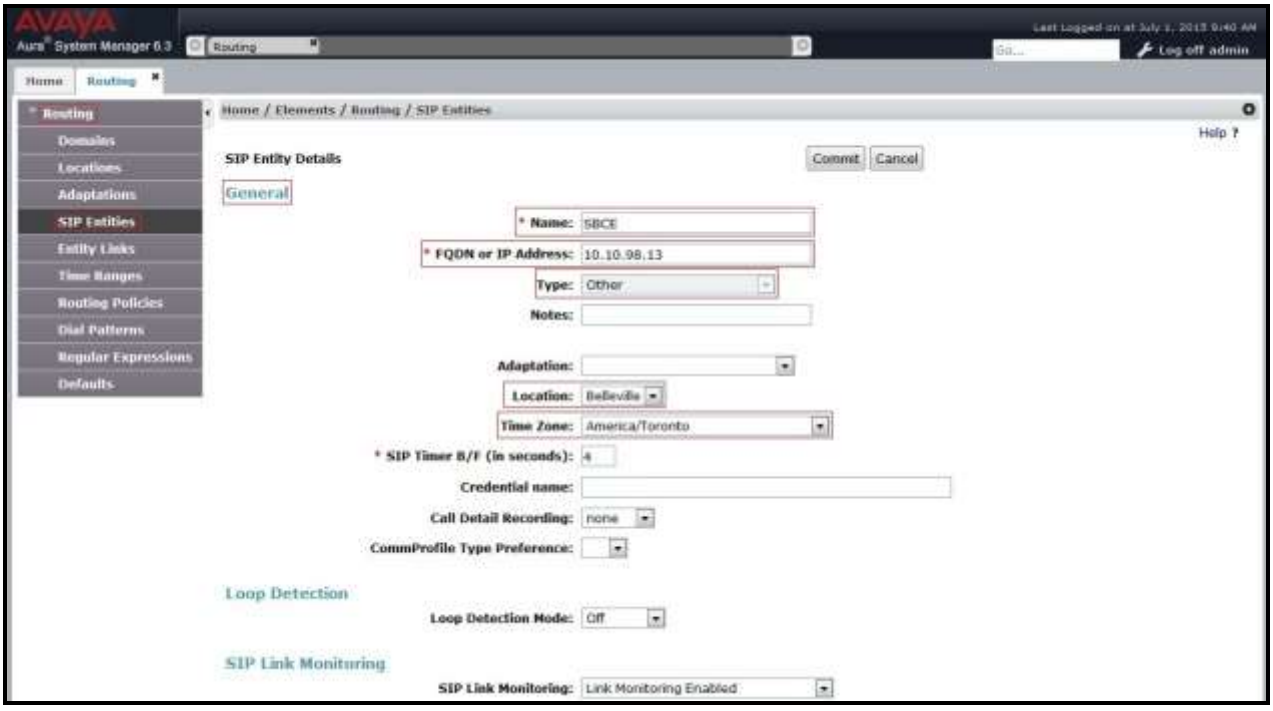

Figure 32: Avaya SBCE SIP Entity

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 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. (Ex: For the Communication Manager Entity Link, this must

match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**).

- **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. (Ex: For the Communication Manager Entity Link, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**).
- **Trusted**: Check this box. **Note**: If this box is not checked, 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**.

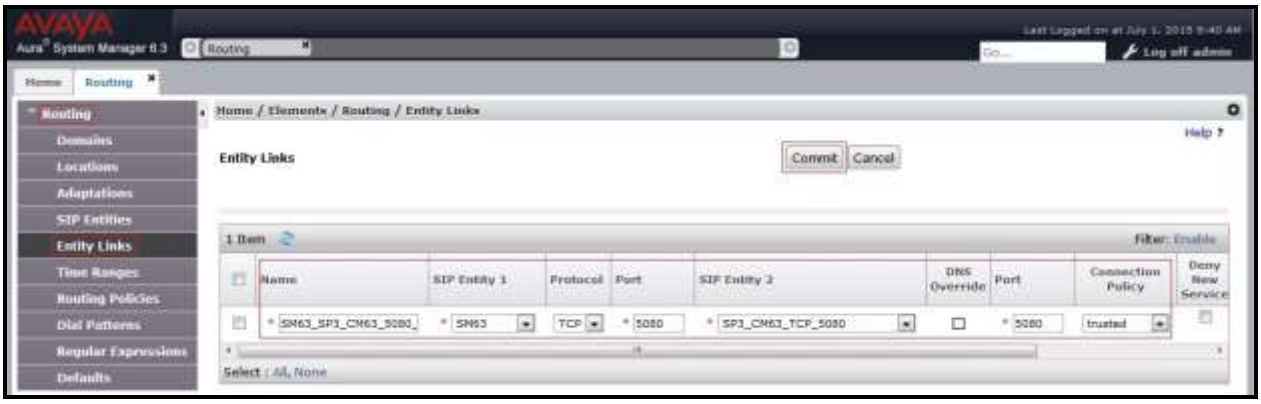

Figure 33: Communication Manager Entity Link

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** and **7.2.6**.

Figure 34: Avaya SBCE Entity Link

6.6. Configure Time Ranges

Time Ranges is configured for time-based-routing. In order to add a Time Ranges, 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 35: 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 **TDC_Inbound_To_CM63** associated with incoming PSTN calls from TDC Business Trunk to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **SP3_CM63_TCP_5080**.

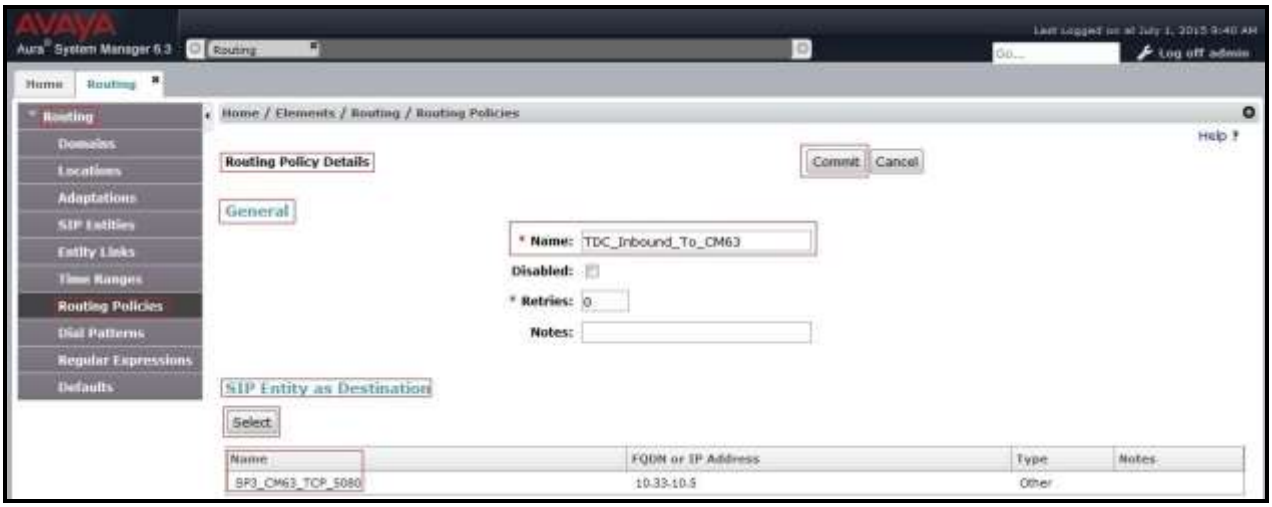

Figure 36: Routing to Communication Manager

The following screen shows the **Routing Policy Details** for the policy named **TDC_Outbound_To_SP3**, associated with outgoing calls from Communication Manager to the PSTN via TDC Business Trunk through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.

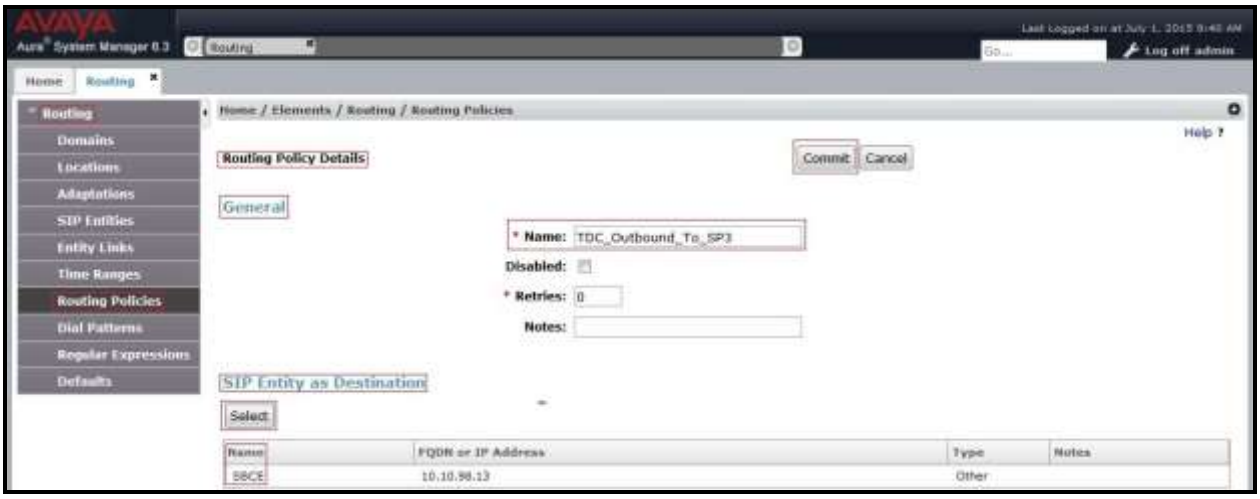

Figure 37: Routing to TDC Business Trunk

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 TDC Business 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 **1303** and have a destination SIP Domain of **bvwdev7.com** uses Routing Policy Name **TDC_Outbound_To_SP3** as defined in **Section** Error! Reference source not found..

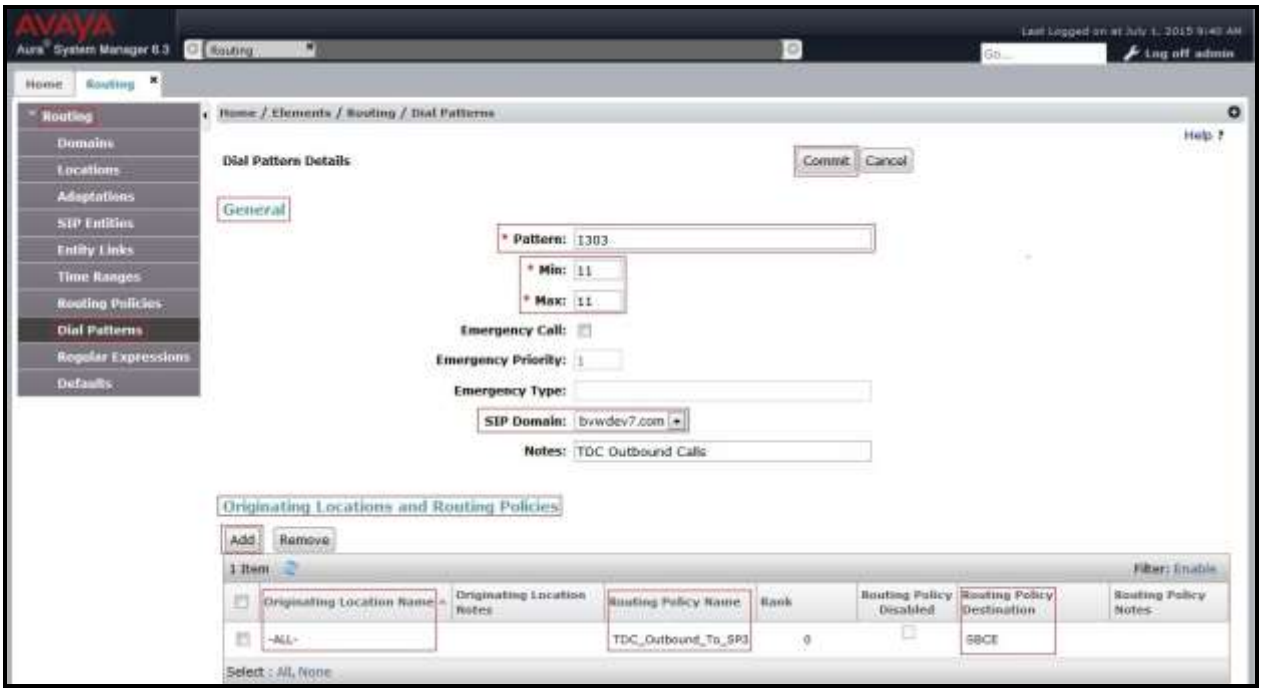

Figure 38: Dial Pattern_1303

Note that with the above Dial Pattern, TDC Business SIP Trunk did not restrict outbound calls to specific US 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 12-digit numbers that start with **+4610** use Routing Policy Name **TDC_Inbound_To_CM63** as defined in **Section** Error! Reference source not found.. This Dial Pattern matches the DID numbers assigned to the enterprise by TDC Business Trunk.

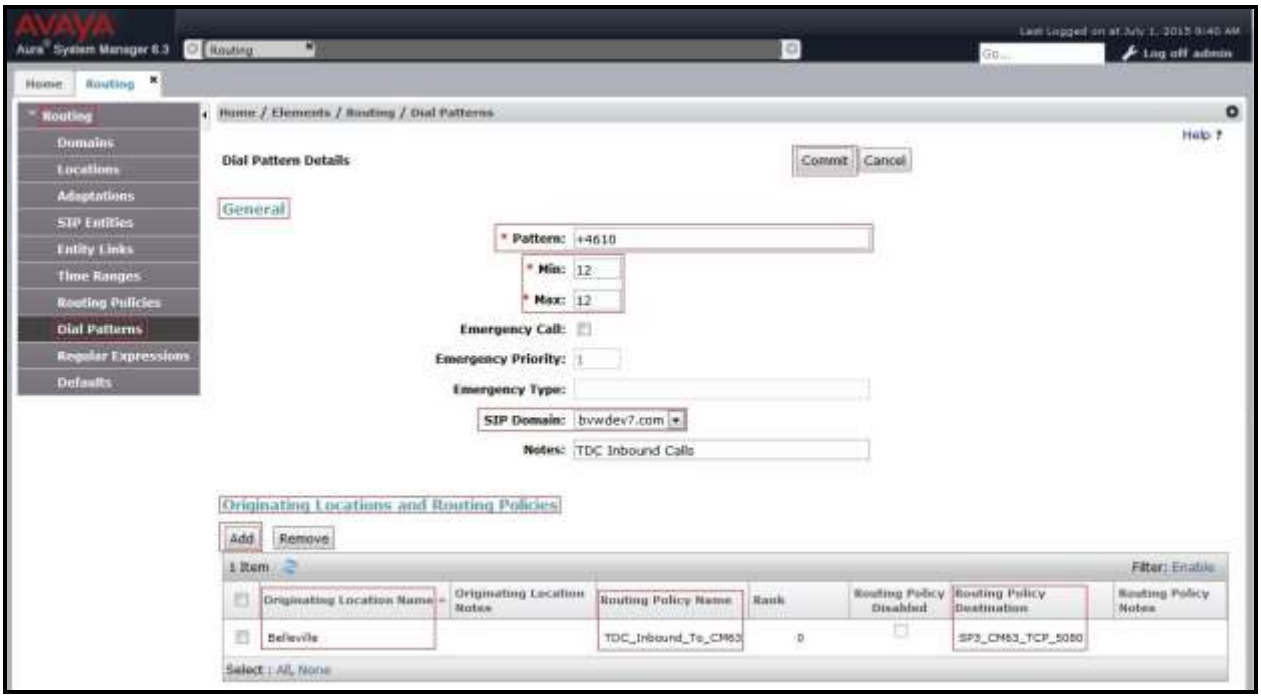

Figure 39: Dial Pattern_+4610

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

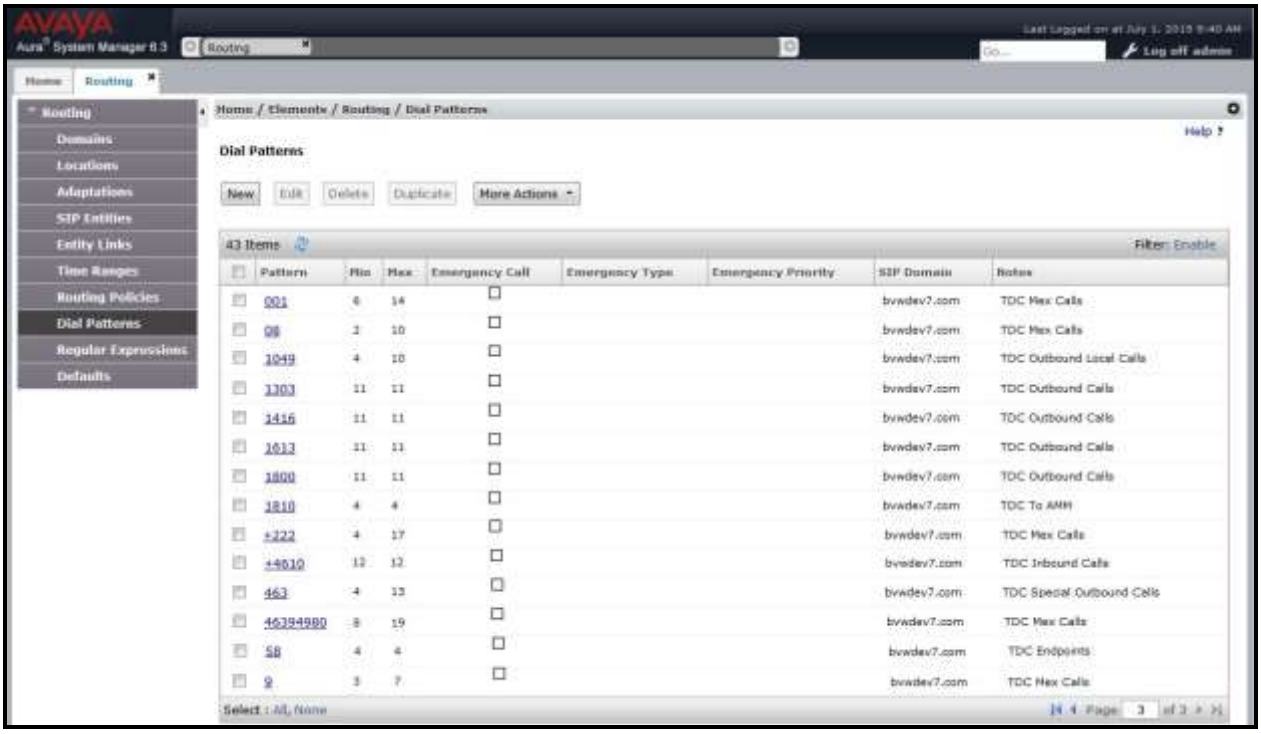

Figure 40: Dial Pattern List

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 TDC Business Trunk system.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the TDC Business Trunk 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 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**.

Figure 41: Avaya SBCE Login

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

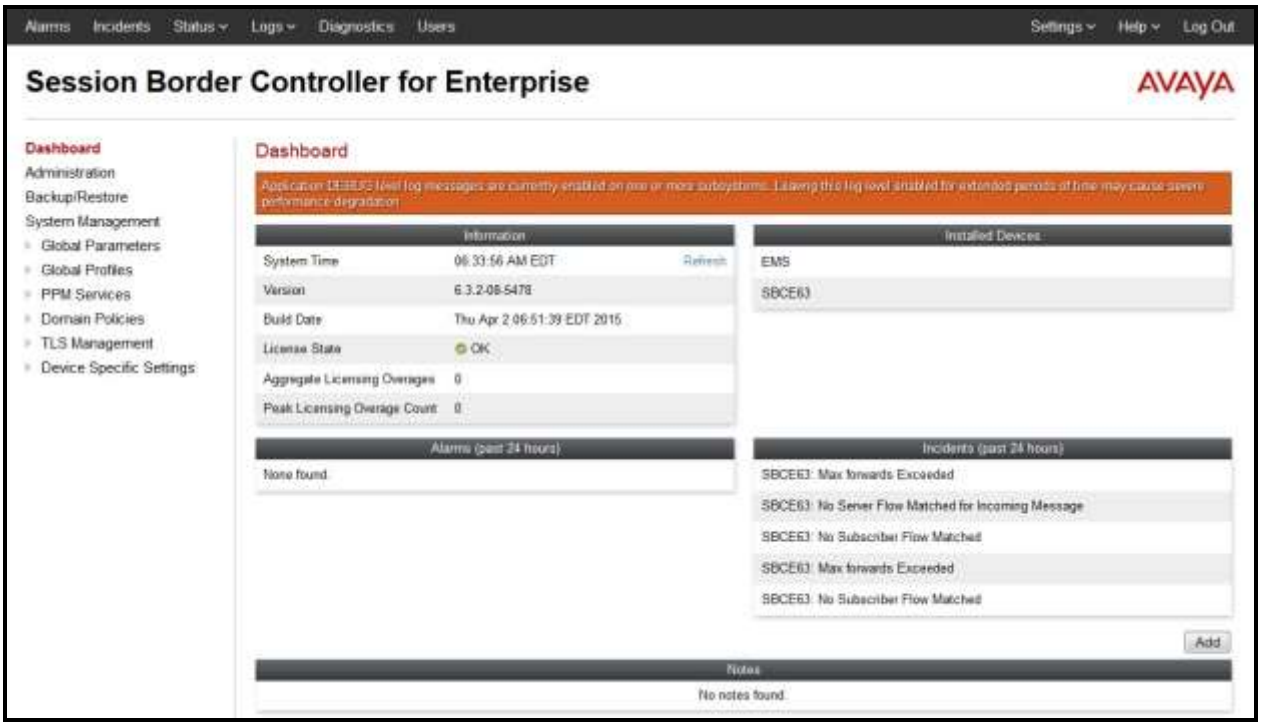

Figure 42: Avaya SBCE Dashboard

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 **SBCE63** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.

Figure 43: 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 corresponded to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**.

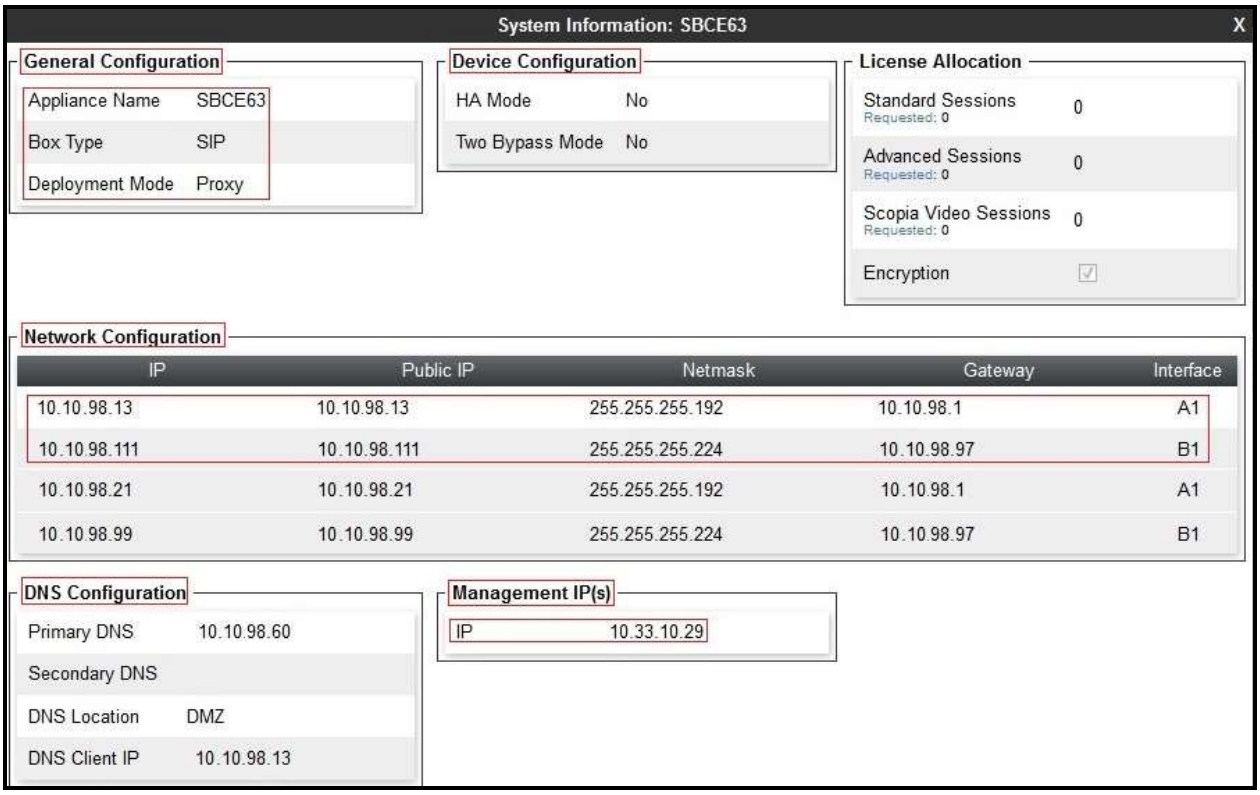

Figure 44: Avaya SBCE System Information

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**: **SM63** and click **Finish** (not shown).

From the list of **Interworking Profiles**, click on **SM63** to edit.

- On the **General** tab, set **T.38 Support** to **Yes** (TDC Business Trunk supports Fax T.38). Other options can be left at default.
- On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** tabs, all options can be left at default. Click **Finish** (not shown).

The following screen shows that Session Manager server interworking profile (named: **SM63**) was added.

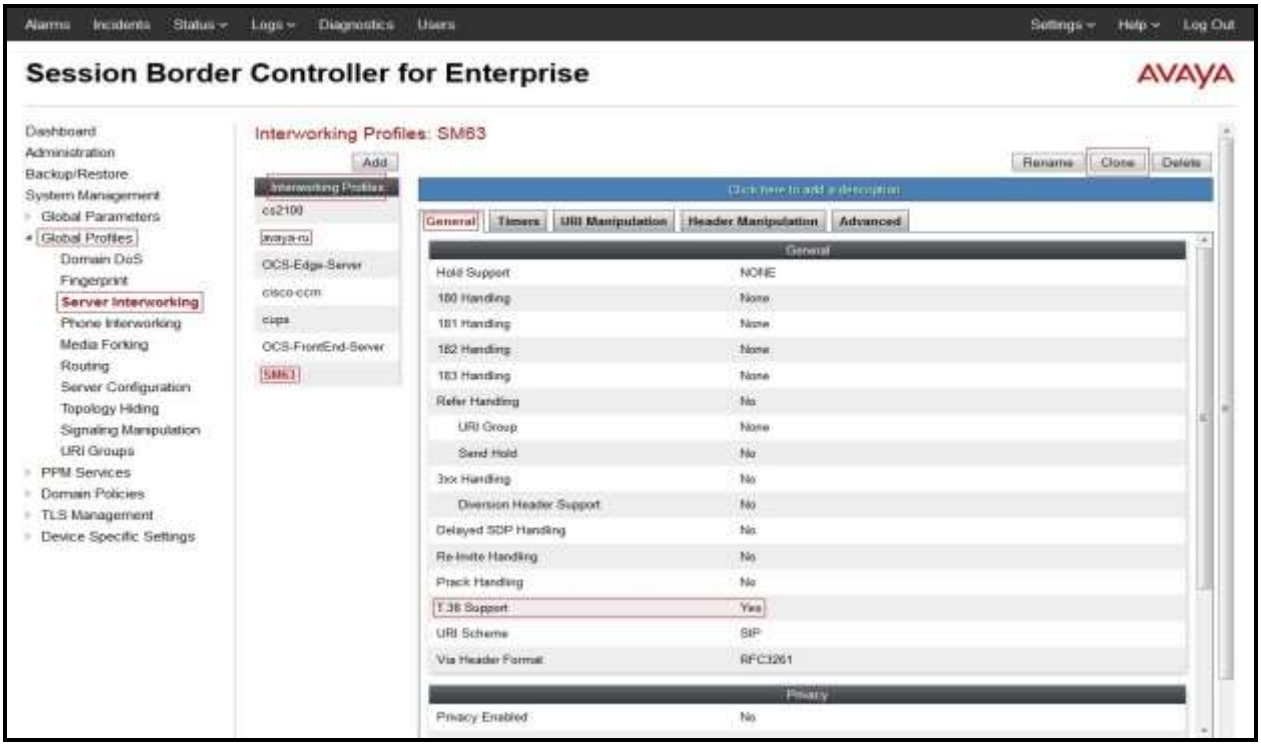

Figure 45: Server Interworking – Avaya site

7.2.2. Configure Server Interworking Profile – TDC Business 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).

From the list of **Interworking Profiles**, click on **SP4** to edit.

- On the **General** tab, click on **Edit** button (not shown) and set **T.38 Support** to **Yes** (TDC Business Trunk supports Fax T.38). Click **Next** button (not shown) to leave other options at default.
- Click **Finish** (not shown).

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

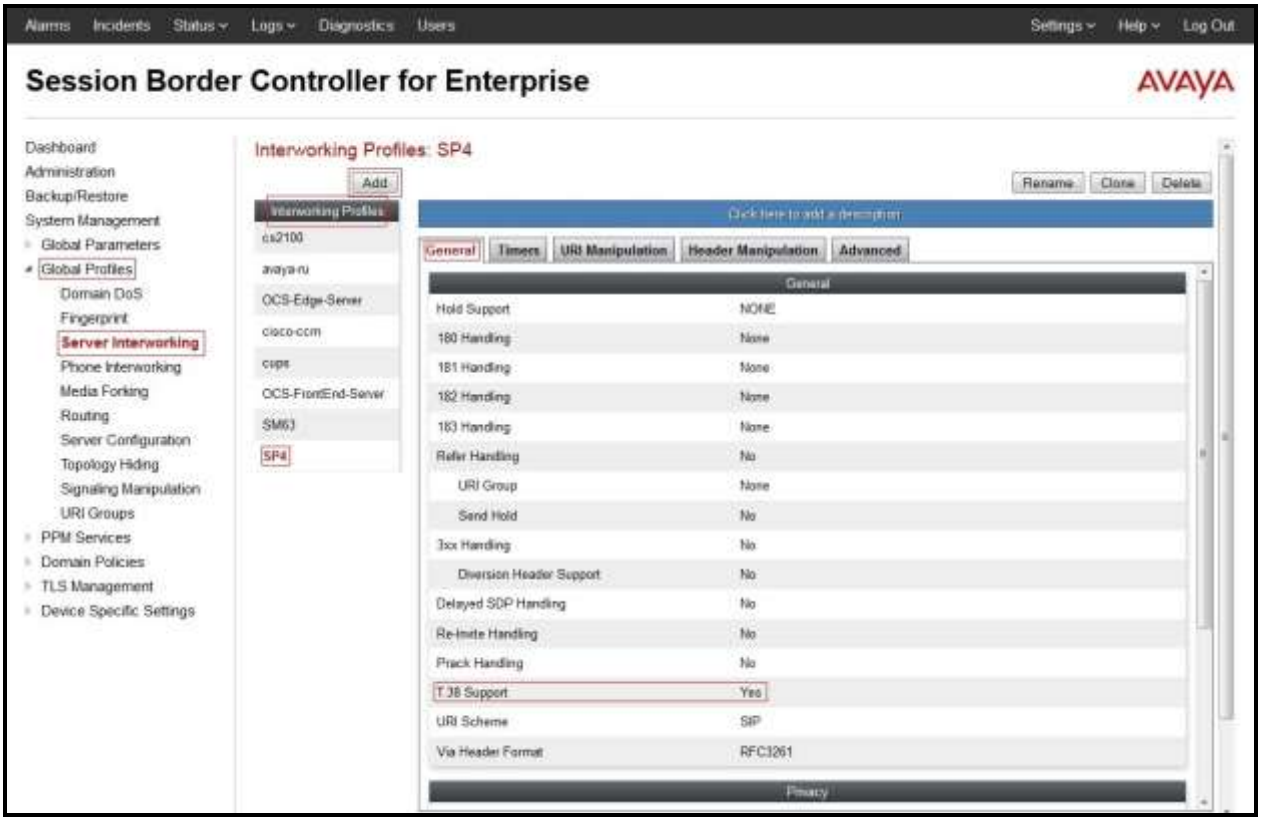

Figure 46: Server Interworking – TDC Business Trunk site

- On the **URI Manipulation** tab, click **Add** button to create the URI manipulation to add the prefix "**+**" sign in front of user number for any outbound calls. When a URI [user@domain] matches the following: **Domain Regex** as **10.33.10.5** or **bvwdev7.com**, do this with the user section: **User Action → Add prefix[Value]**, enter **User Values 1**: **+** (Not shown).

Note: TDC Business Trunk requires numbers to be given in E.164 with leading plus for all fields. This applies for both Request-URI, To- and From-header as well as for example the Diversion-header.

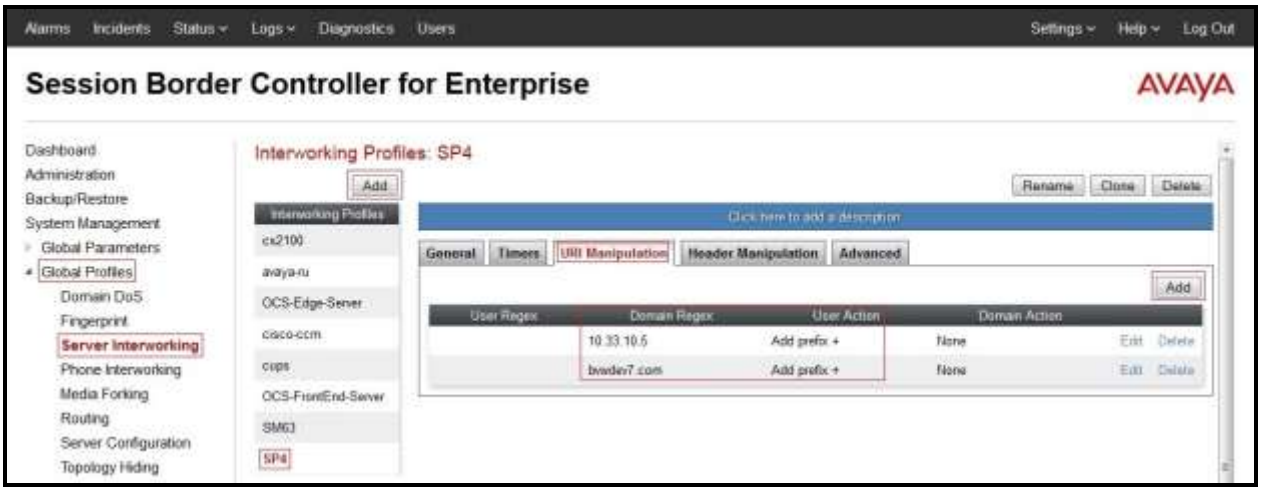

Figure 47: Server Interworking – TDC Business Trunk site - URI Manipulation

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**. In the script editing window, enter the text exactly as shown in the screenshot on the next page to perform the following:
  - Edit script to replace Mex enabled mobile number on From/Contact headers by Mex fixed number for incoming calls.
  - Edit the script to replace "++" by "+" on SIP headers for outgoing calls.
  - Click **Save** (not shown).

Note: The script is used for the additional TDC Mex testing purposes. See **Appendix B** in **Section 13** for the reference of this sigma script.

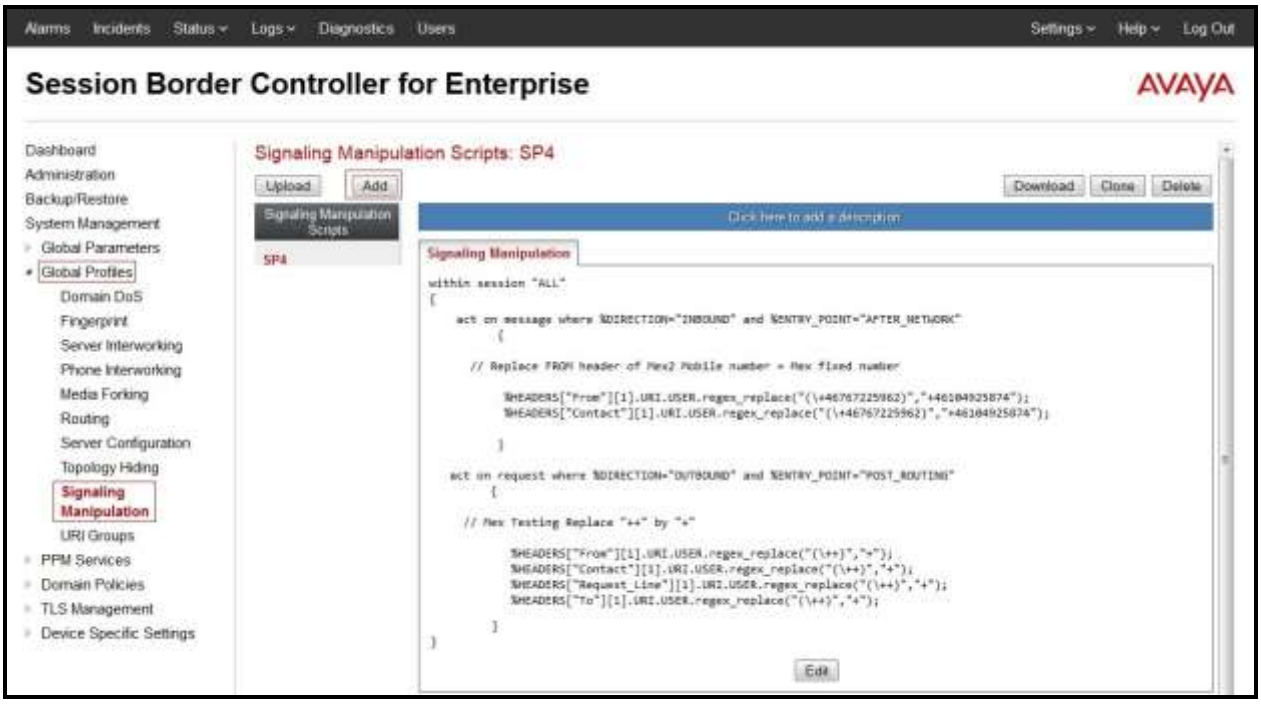

Figure 48: Signaling Manipulation

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 UDP 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**: **SM63**.

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

- **Server Type**: Select **Call Server**.
- **IP Address/FQDNs**: **10.33.10.26** (Avaya Aura Session Manager IP Address).
- **Port**: **5060**.
- **Transport**: **UDP**.
- Click **Finish** (not shown).

Figure 49: Server Configuration – General - Avaya site

On the **Advanced** tab:

- Select **SM63** for **Interworking Profile** (see **Section 7.2.1**).
- Click **Finish** (not shown).

Figure 50: Server Configuration – Advanced - Avaya site

7.2.5. Configure Server – TDC Business 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**: **192.168.198.130** (TDC Business Trunk Signaling Server IP Address).
- **Port**: **5060**.
- **Transport**: **UDP**.
- Click **Finish** (not shown).

Figure 51: Server Configuration – General - TDC site

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

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

Figure 52: Server Configuration – Advanced - TDC 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_SM63** (not shown).

- **Load Balancing**: **Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address.
- **Priority/Weight**: **1**.
- **Server Configuration**: **SM63** (see **Section 7.2.4**).
- **Next Hop Address**: **10.33.10.26:5060 (UDP)** (Avaya Session Manager IP address).
- Click **Finish**.

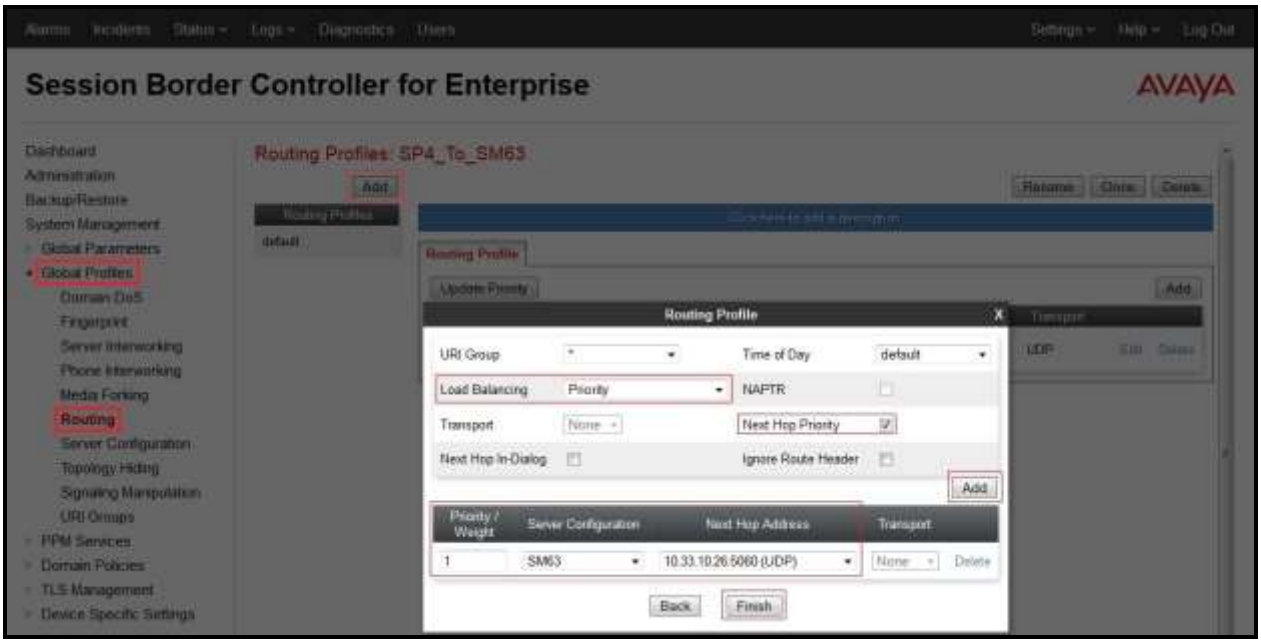

Figure 53: Routing to Session Manager

7.2.7. Configure Routing – TDC Business 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**: **SM63_To_SP4** (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**: **192.168.198.130:5060 (UDP)** (TDC Signaling Server IP address).
- Click **Finish**.

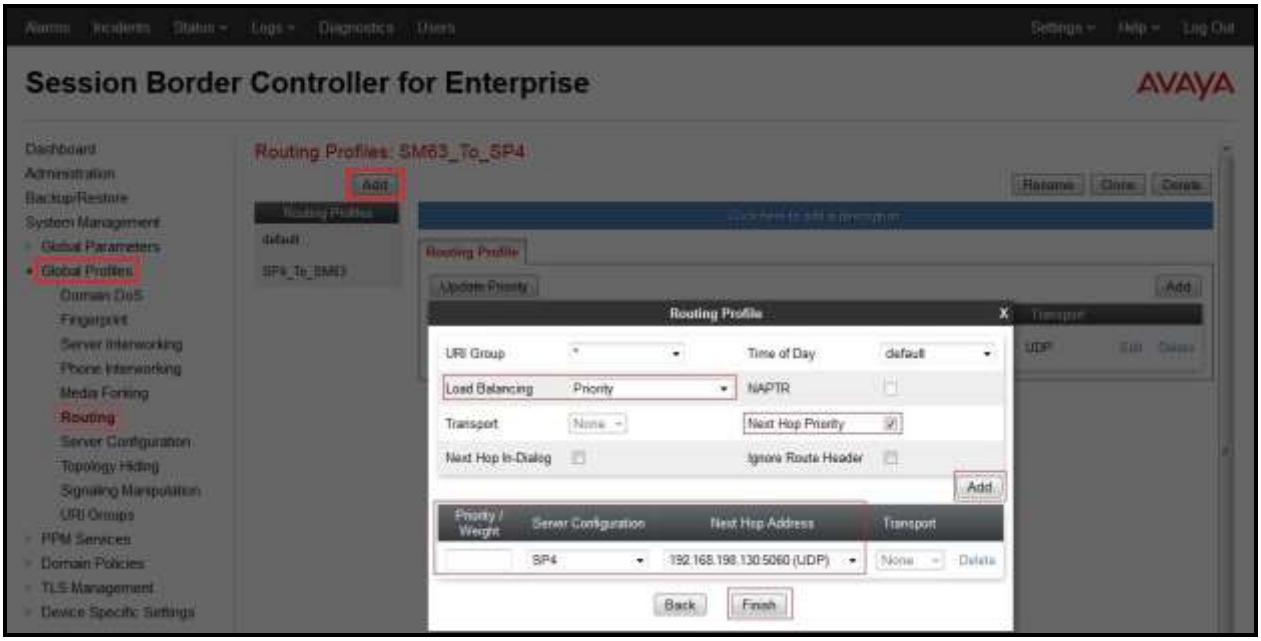

Figure 54: Routing to TDC Business Trunk

7.2.8. Configure Topology Hiding – Avaya site

The **Topology Hiding** screen allows 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 **Add** button to enter **Profile Name**: **SP4_To_SM63**.

- For the Header **From,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
    In the **Overwrite Value** column: **bvwdev7.com**
- For the Header **To,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev7.com**
- For the Header **Request-Line,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev7.com**

Click **Finish** (not shown).

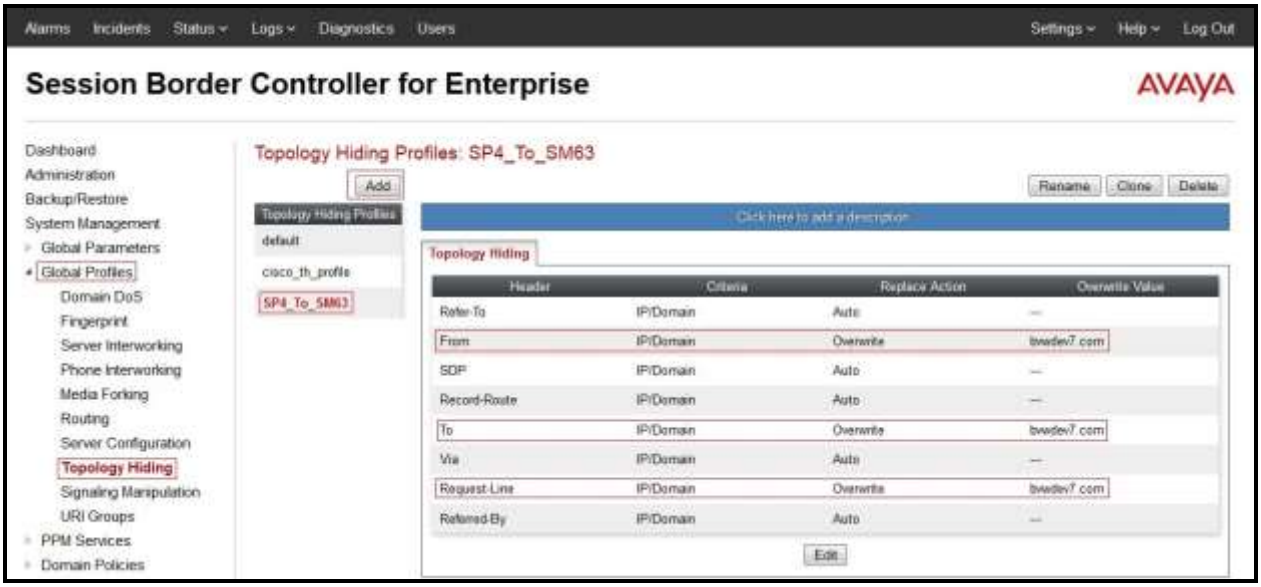

Figure 55: Topology Hiding Session Manager

7.2.9. Configure Topology Hiding – TDC Business Trunk site

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

Select **Add** button to enter **Profile Name**: **SM63_To_SP4**.

- For the Header **From,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **test11.btrunk.se**
- For the Header **To,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **test11.btrunk.se**
- For the Header **Request-Line,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **test11.btrunk.se**

Click **Finish** (not shown).

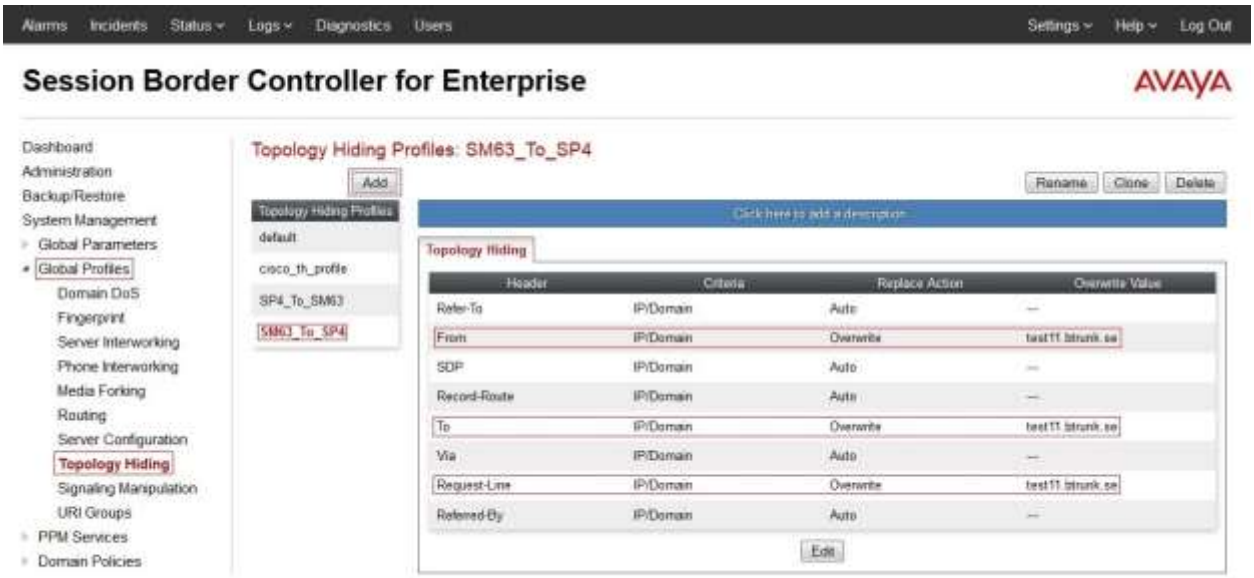

Figure 56: Topology Hiding TDC Business Trunk

7.3. 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, and ToD, 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**: **SM63_SP4_PolicyG**.
  - **Application Rule**: **default**.
  - **Border Rule**: **default**.
  - **Media Rule**: **default-low-med**.
  - **Security Rule**: **default-med**.
  - **Signaling Rule**: **default**.
  - **Time of Day**: **default**.
- Select **Finish** (not shown).

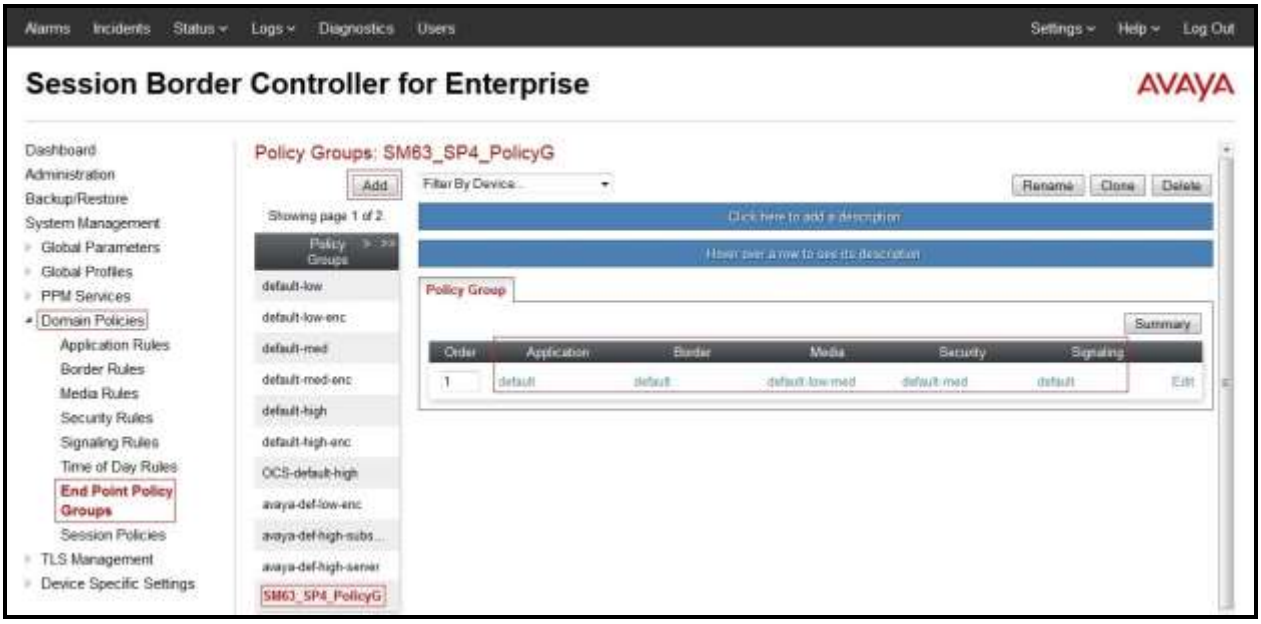

Figure 57: Endpoint Policy – Avaya site

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

- Select **Add**.
- Enter **Group Name**: **SP4_PolicyG**.
  - **Application Rule**: **default**.
  - **Border Rule**: **default**.
  - **Media Rule**: **default-low-med**.
  - **Security Rule**: **default-med**.
  - **Signaling Rule**: **default**.
  - **Time of Day**: **default**.
- Select **Finish** (not shown).

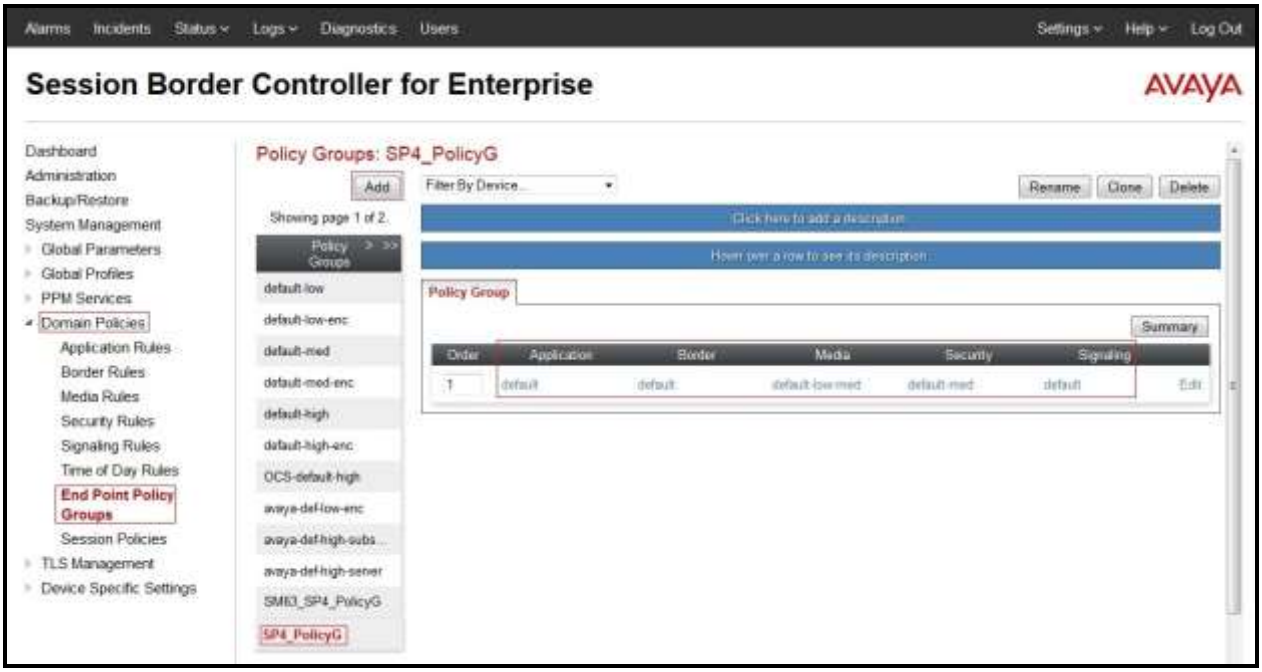

Figure 58: Endpoint Policy – TDC Business Trunk site

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

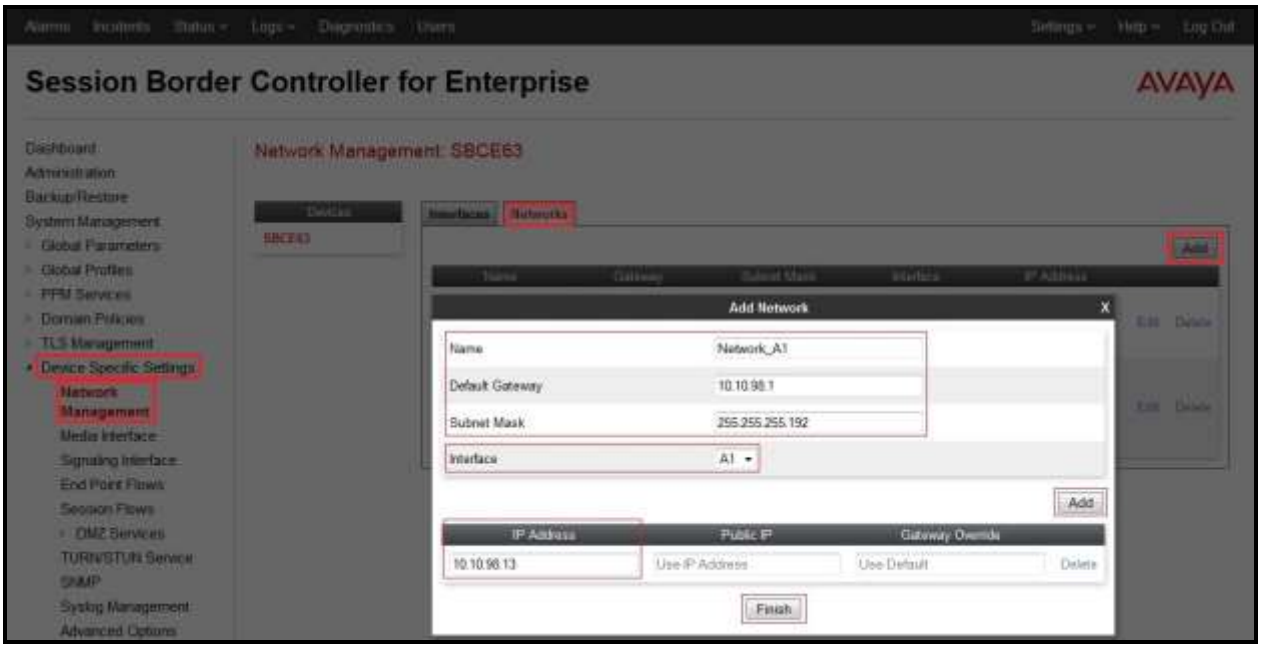

Figure 59: Network Management – Inside Interface

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 of outside interface as followings:
  - **Name**: **Network_B1**.
  - **Default Gateway**: **10.10.98.97**.
  - **Subnet Mask**: **255.255.255.224**.
  - **Interface**: **B1** (This is Avaya SBCE outside interface).
  - Click **Add** button to add **IP Address** for outside interface: **10.10.98.111**.
  - Click **Finish** button to save the changes.

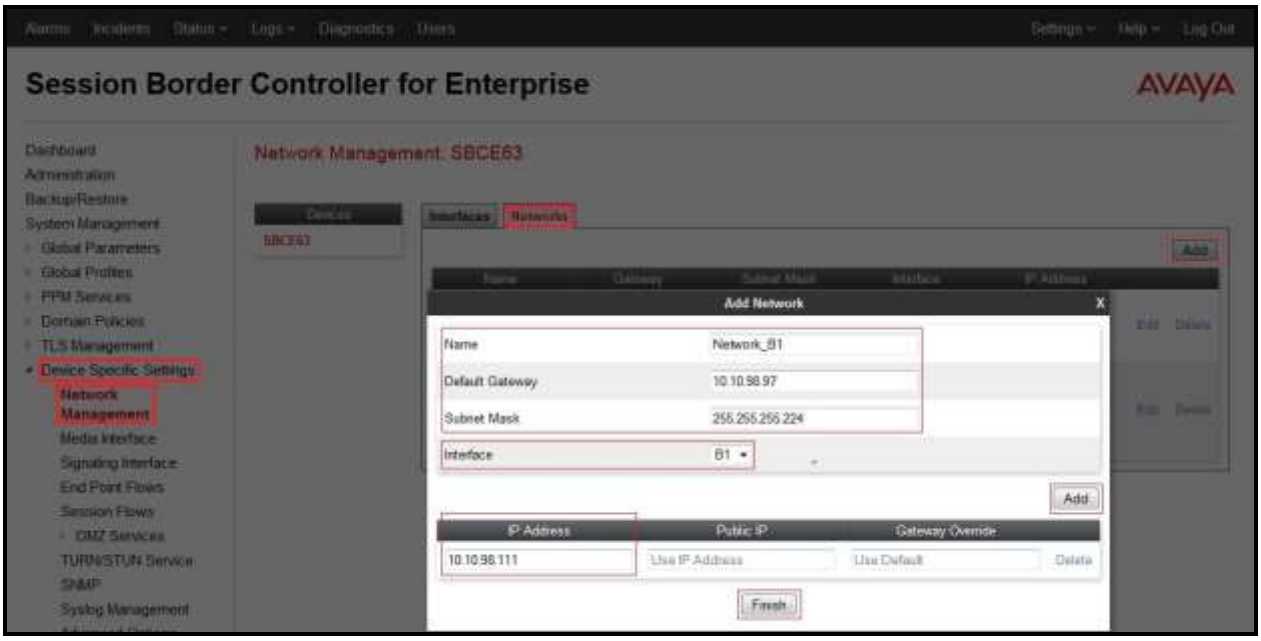

Figure 60: Network Management – Outside Interface

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

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

Figure 61: Network Management – Interface Status

7.4.2. Create Media Interfaces

Media Interfaces define the type of signaling on the ports. The default media port range on the Avaya can be used for both inside and outside ports.

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

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

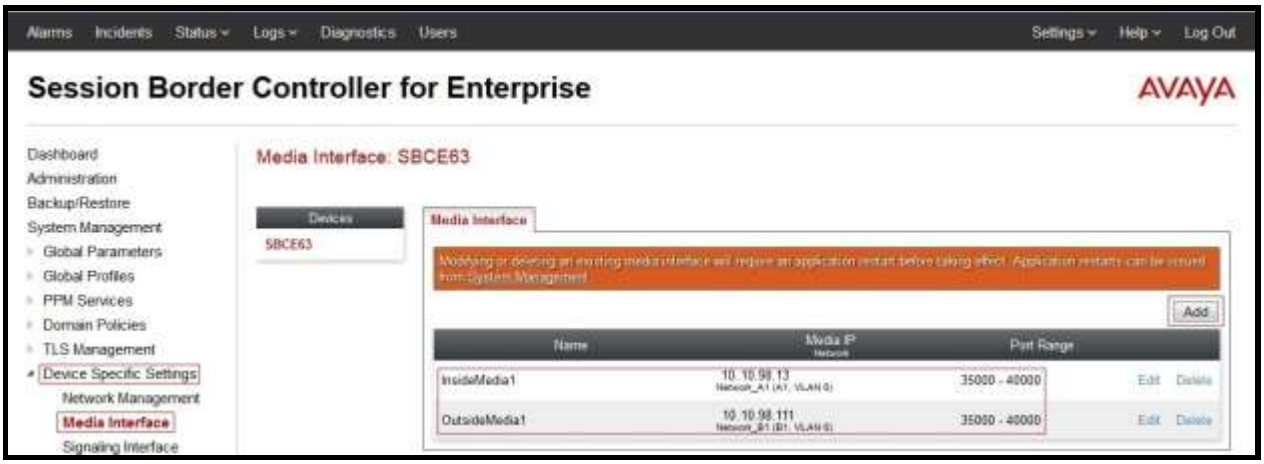

Figure 62: Media Interface

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 **Add** button and enter the following:
  - **Name**: **InsideUDP1**.
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Avaya Session Manager).
  - **UDP Port**: **5060**.
  - Click **Finish** (not shown).

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

- Select **Add** button and enter the following:
  - **Name**: **OutsideUDP1**.
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward TDC Business SIP trunk).
  - **UDP Port**: **5060**.
  - Click **Finish** (not shown).

Note: For the internal interface, the Avaya SBCE was configured to listen for UDP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 as same as TDC Business Trunk used.

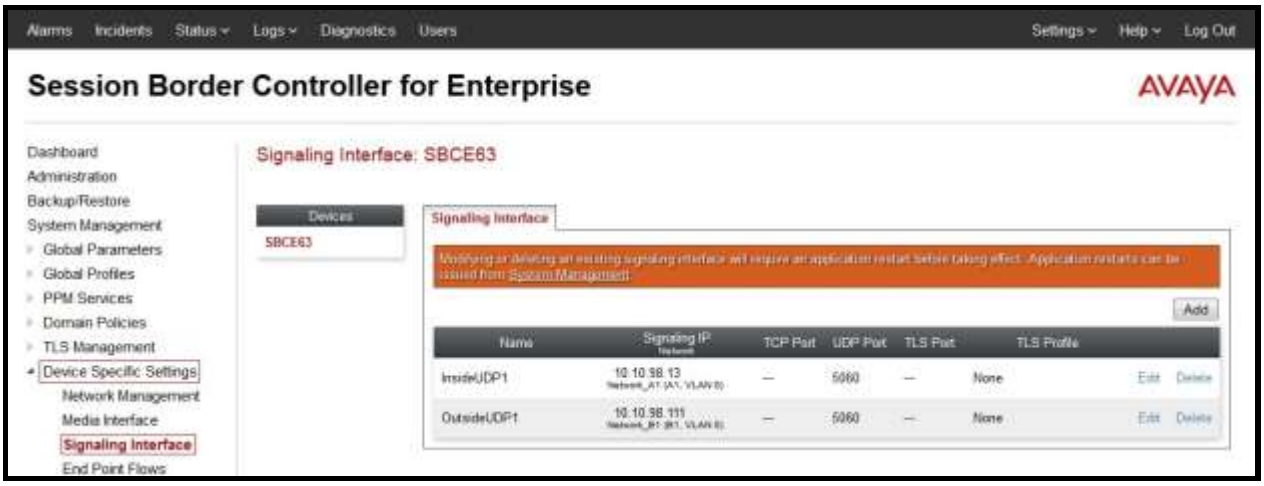

Figure 63: Signaling Interface

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 – SM63 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**: **SM63_Flow**.
  - **Server Configuration**: **SM63** (see **Section 7.2.4**).
  - **URI Group**: *****.
  - **Transport: ***.
  - **Remote Subnet: ***.
  - **Received Interface**: **OutsideUDP1** (see **Section 7.4.3**).
  - **Signaling Interface**: **InsideUDP1** (see **Section 7.4.3**).
  - **Media Interface**: **InsideMedia1** (see **Section 7.4.2**).
  - **End Point Policy Group**: **SM63_SP4_PolicyG** (see **Section 7.3**).
  - **Routing Profile**: **SM63_To_SP4** (see **Section 7.2.7**).
  - **Topology Hiding Profile**: **SP4_To_SM63** (see **Section 7.2.8**).
  - Click **Finish**.

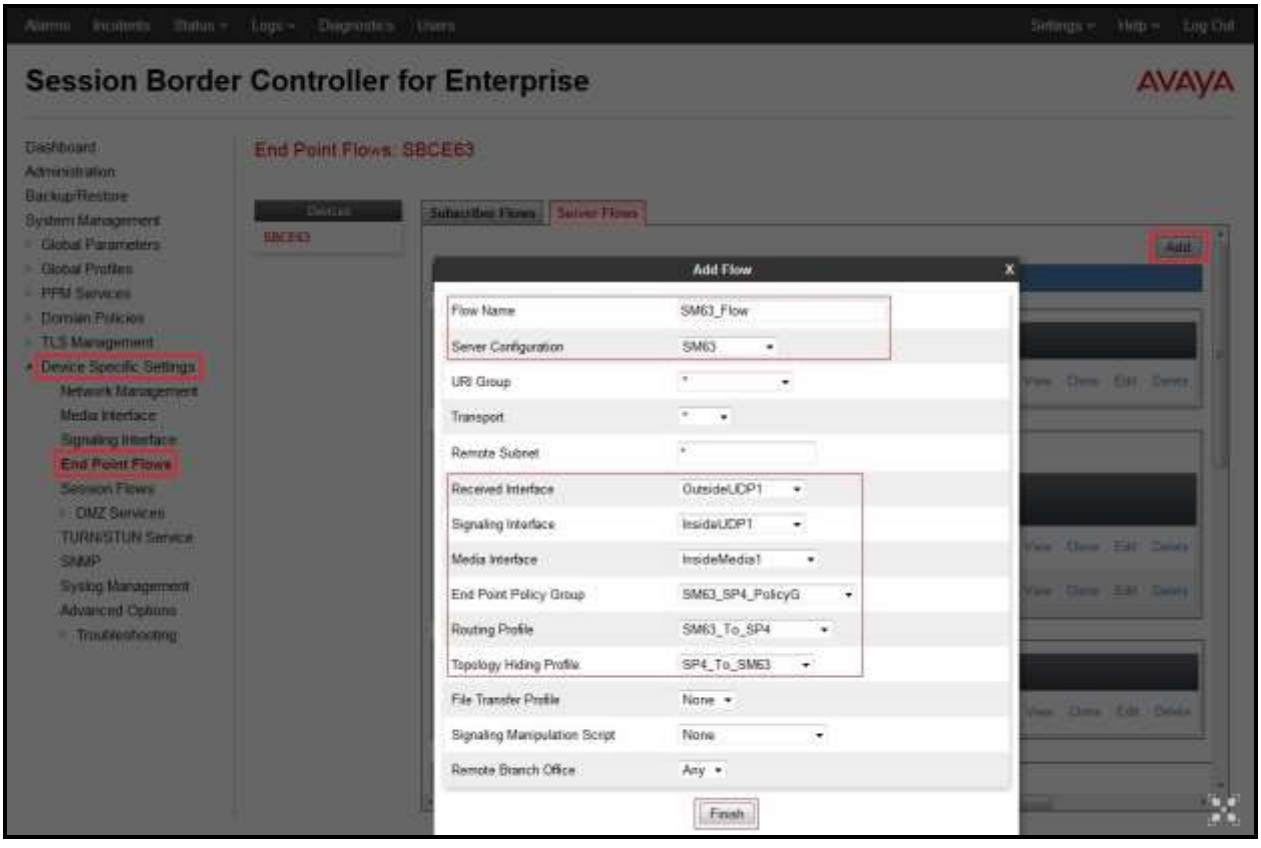

Figure 64: End Point Flow to TDC Business Trunk

7.4.4.2 Create End Point Flows – TDC Business 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**: **InsideUDP1** (see **Section 7.4.3**).
  - **Signaling Interface**: **OutsideUDP1** (see **Section 7.4.3**).
  - **Media Interface**: **OutsideMedia1** (see **Section 7.4.2**).
  - **End Point Policy Group**: **SP4_PolicyG** (see **Section 7.3**).
  - **Routing Profile**: **SP4_To_SM63** (see **Section 7.2.6**).
  - **Topology Hiding Profile**: **SM63_To_SP4** (see **Section 7.2.9**).
  - Click **Finish**.

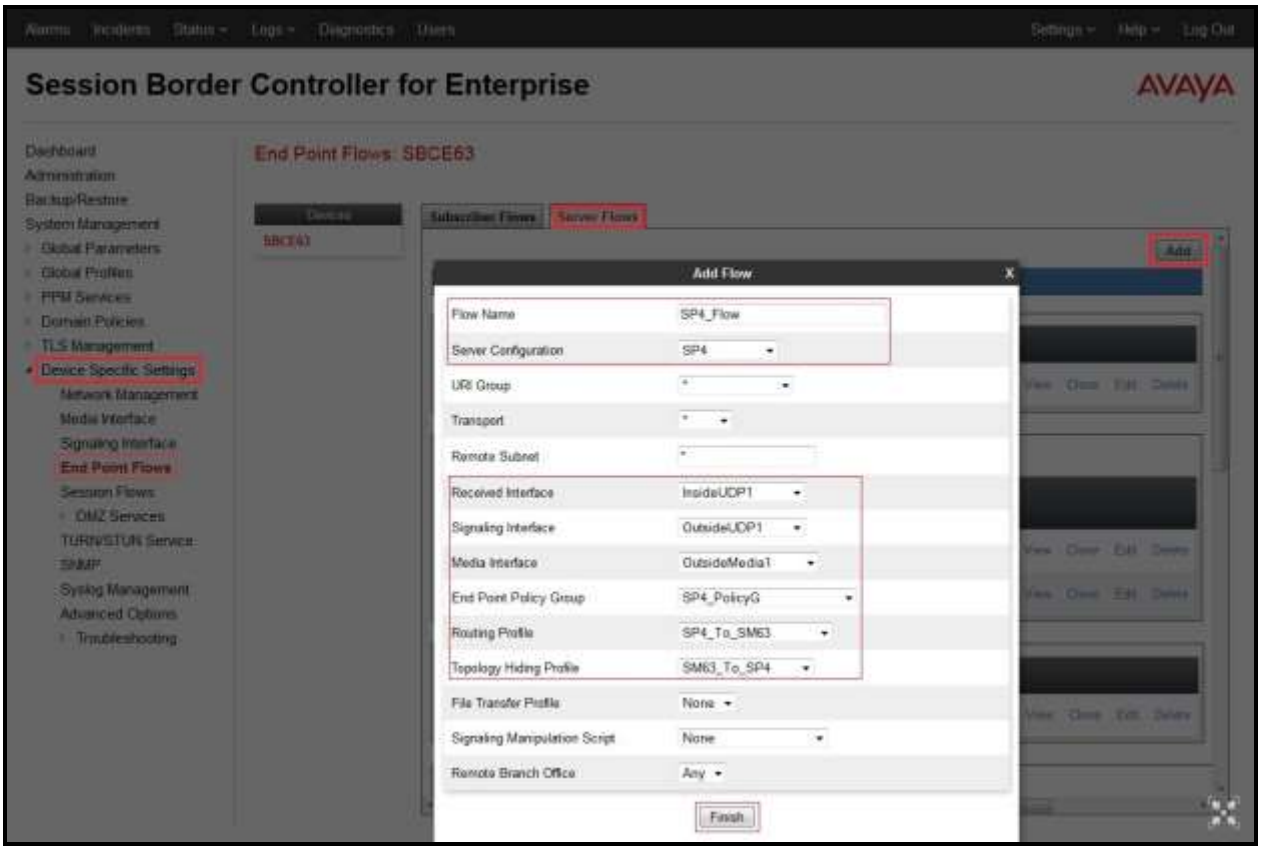

Figure 65: End Point Flow from TDC Business Trunk

8. TDC Business Trunk Configuration

TDC Business Trunk is responsible for the network configuration of the TDC Business Trunk service. TDC Business Trunk will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. TDC Business Trunk will provide the IP address of the TDC Business Trunk SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. TDC Business Trunk also provides the TDC 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 TDC Business Trunk and the enterprise is a static IP 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. Enter the following commands using 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 -x** – 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.
    - **Command Line Interface: /tmp/traceSBC**. The tool updates the database directly based on which trace mode is selected.
        - The first option is recommended when traceSBC is used off-line. These debugs can be enabled by the customers through the GUI, they can send the log files, and traceSBC can parse them off-line.
        - The second option is recommended for live captures. When the tool starts, it checks the database to see if debug logging is already enabled. If yes, the tool automatically starts processing the files.

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 TDC Business Trunk. This solution successfully passed compliance testing via the Avaya DevConnect Program. Please refer to **Section 2.2** for any exceptions or workarounds.

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 6.3, Issue 7, September 2014
[2] *Maintaining and Troubleshooting Avaya Aura® Session Manager,* Release 6.3, Issue 7, March 2015
[3] *Administering Avaya Aura® System Manager,* Release 6.3.10, Issue 6, Febuary 2015

Avaya Aura® Communication Manager

[4] *Administering Avaya Aura® Communication Manager,* Document ID 03-300509, Release 6.3, Issue 8, May 2013
[5] *Programming Call Vectoring Features in Avaya Aura® Call Center Elite,* Release 6.3, Issue 1, May 2013

Avaya Phones

[6] *Avaya one-X® Deskphone SIP 9621G/9641G User Guide for 9600 Series IP Telephones,* Document ID 16-603596, Issue 1, August 2012
[7] *Avaya one-X® Deskphone H.323 9608 and 9611G User Guide,* Document ID 16-603593, Issue 3, February 2012
[8] *Avaya one-X® Deskphone SIP for 9640/9640G IP Telephone User Guide*, Document ID 16-602403, June 2013
[9] *Avaya one-X® Deskphone H.323 for 9630 and 9630G IP Deskphone User,* Document ID 16-300700, June 2013
[10] *Avaya one-X® Communicator Overview and Planning*, Release 6.2 FP6, April 2015
[11] *Administering Avaya Communicator for Android, iPad, and Windows,* Release 2.1, Issue 4, August 2014

Avaya Aura® Messaging

[12] *Administering Avaya Aura® Messaging 6.2*, Issue 2.2, May 2013
[13] *Implementing Avaya Aura® Messaging 6.2*, Issue 2, January 2013

Avaya Session Border Controller for Enterprise

Product services for Avaya SBCE may be found at:
http://www.sipera.com/products-services/esbc

[14] *Avaya Session Border Controller for Enterprise Overview and Specification,* Release 6.3 Issue 3, October 2014
[15] *Administering Avaya Session Border Controller for Enterprise,* Release 6.3, Issue 4, October 2014

IETF (Internet Engineering Task Force) SIP Standard Specifications

[16] *RFC 3261 SIP: Session Initiation Protocol, http://www.ietf.org/*
[17] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/*

Product documentation for TDC Business Trunk SIP Trunk may be found at: *http://www.tdc.se/*.

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 TDC Business 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 Communicator for Windows SIP softphone. Avaya 96x1 SIP Deskphones support SRTP, while Avaya one-X® Communicator and Avaya Communicator for Windows softphones support RTP.

Note: In this compliance testing, only Avaya Communicator for Windows 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.

The figure below illustrates the Remote Worker topology used in the reference configuration.

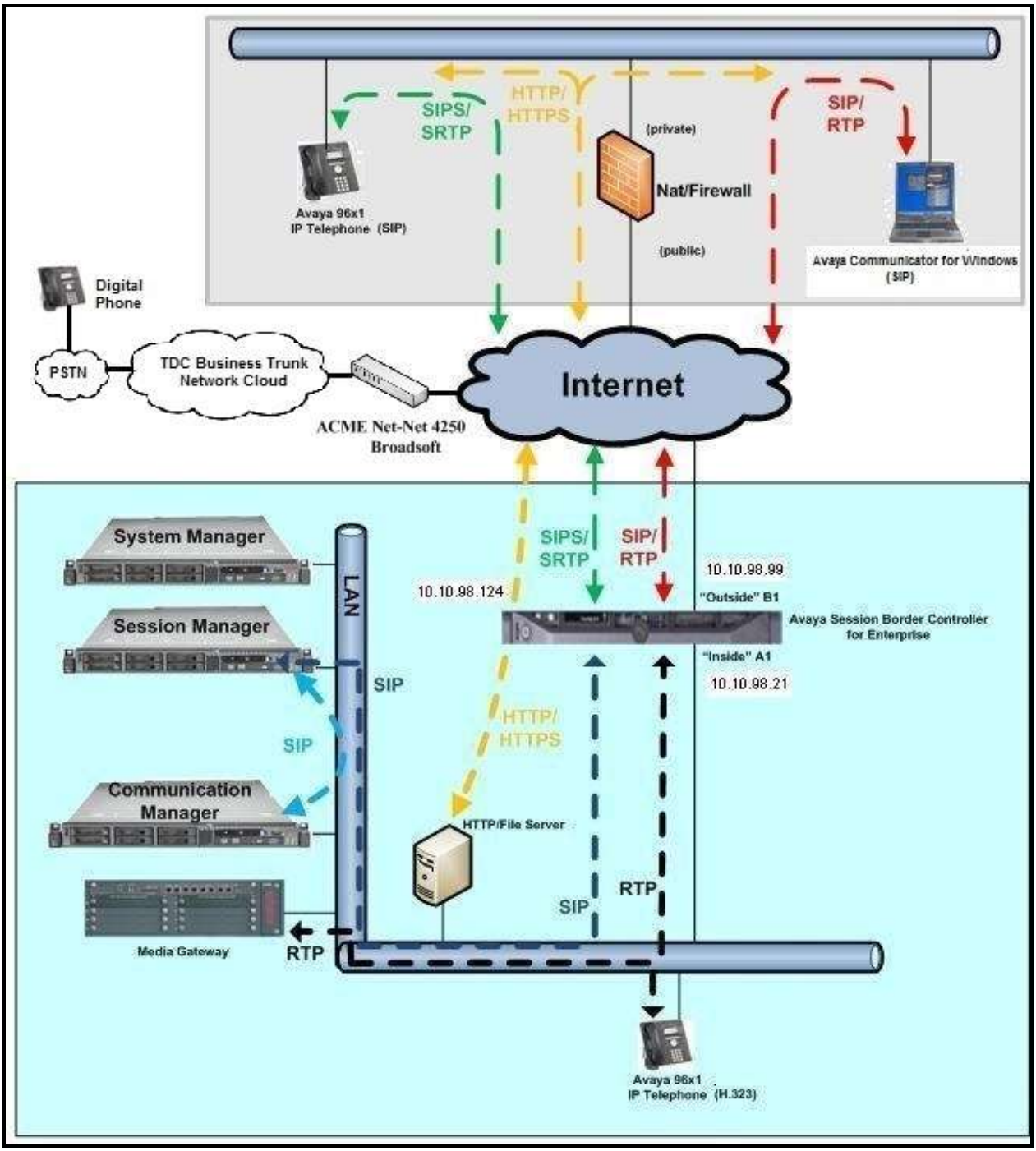

Figure 66: Avaya IP Telephony Network for Remote Worker

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 TDC Business Trunk (see **Section 7.4.1**).
- **10.10.98.21** 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 Trunk with TDC Business Trunk (see **Section 7.4.1**).
- **10.10.98.99** is the new Avaya SBCE "outside" address for Remote Worker access to Session Border Controller.
- **10.10.98.124** is the new Avaya SBCE "outside" address for file transfer access between the Remote Worker phone and the enterprise file server.

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 67: Network Management

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

Figure 68: 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 **Add** button and enter the following:
  - **Name**: **InsideMediaRW**.
  - **IP Address**: Select **Network_A1 (A1, VLAN0)** and **10.10.98.21** (Internal IP Address toward Session Manager).
  - **Port Range**: **35000 – 40000**.
  - Click **Finish** (not shown).
- Select **Add** button and enter the following:
  - **Name**: **OutsideMediaRW**.
  - **IP Address**: Select **Network_B1 (B1, VLAN0)** and **10.10.98.99** (External IP Address toward Remote Worker phones).
  - **Port Range**: **35000 – 40000**.
  - Click **Finish** (not shown).

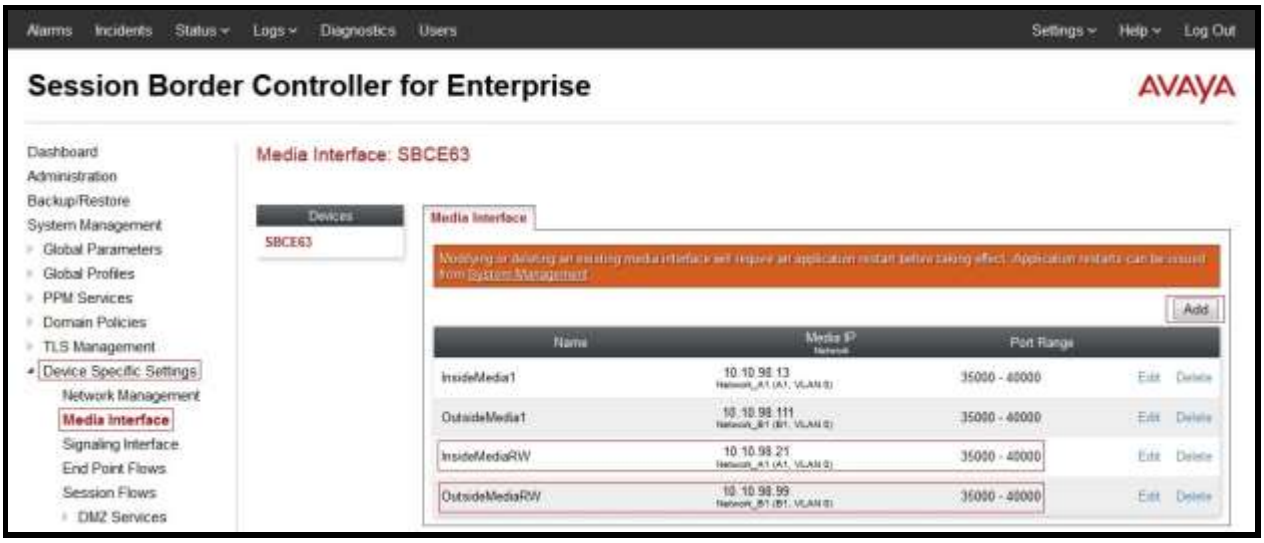

Figure 69: Media Interface

Note: Media Interface **OutsideMediaRW** is used in the Remote Worker Subscriber Flow (**Section 12.13.1**), and Media Interface **InsideMediaRW** is used in the Remote Worker Server Flow (**Section 12.13.2.1**).

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 **InsideSIPRW** using the parameters:

- **IP Address**: Select **Network_A1 (A1, VLAN0)** and **10.10.98.21** (Internal IP Address toward Session Manager).
- **TCP Port**: **5060**.
- Click on **Finish** (not shown).

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

- **IP Address:** Select **Network_B1 (B1, VLAN0)** and **10.10.98.99** (External IP Address toward Remote Worker phones).
- **TCP Port**: **5060**.
- Click on **Finish** (not shown).

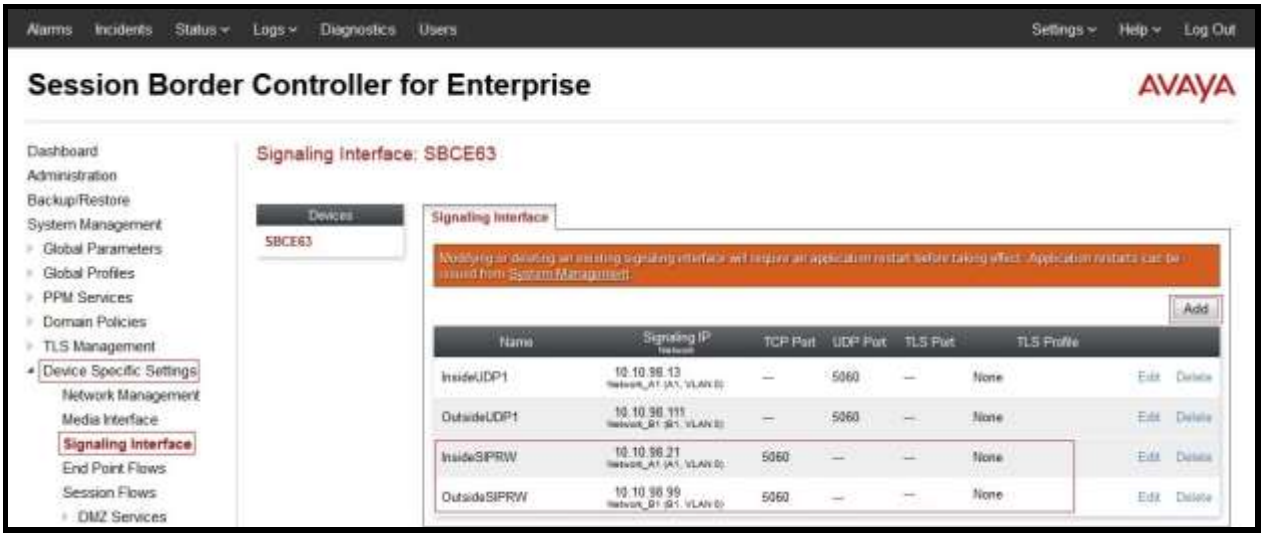

Figure 70: Signaling Interface

Note: Signaling Interface **OutsideSIPRW** is used in the Subscriber Flows (**Section 12.13.1**), and in the Remote Worker Server Flow (**Section 12.13.2.1**). Signaling Interface **InsideSIPRW** is used in the Remote Worker Server Flow (**Section 12.13.2.1**).

12.4. Server Interworking Configuration on Avaya SBCE

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

- Select **Interworking Profile**s as **SM63**.
- On the **Advanced** tab, click **Edit** button, verify that **Topology Hiding: Change Call-ID** must be **No** and **Avaya Extensions** should be **Yes**. Otherwise, calls to Remote Worker will fail.
- Click **Finish** (not shown).

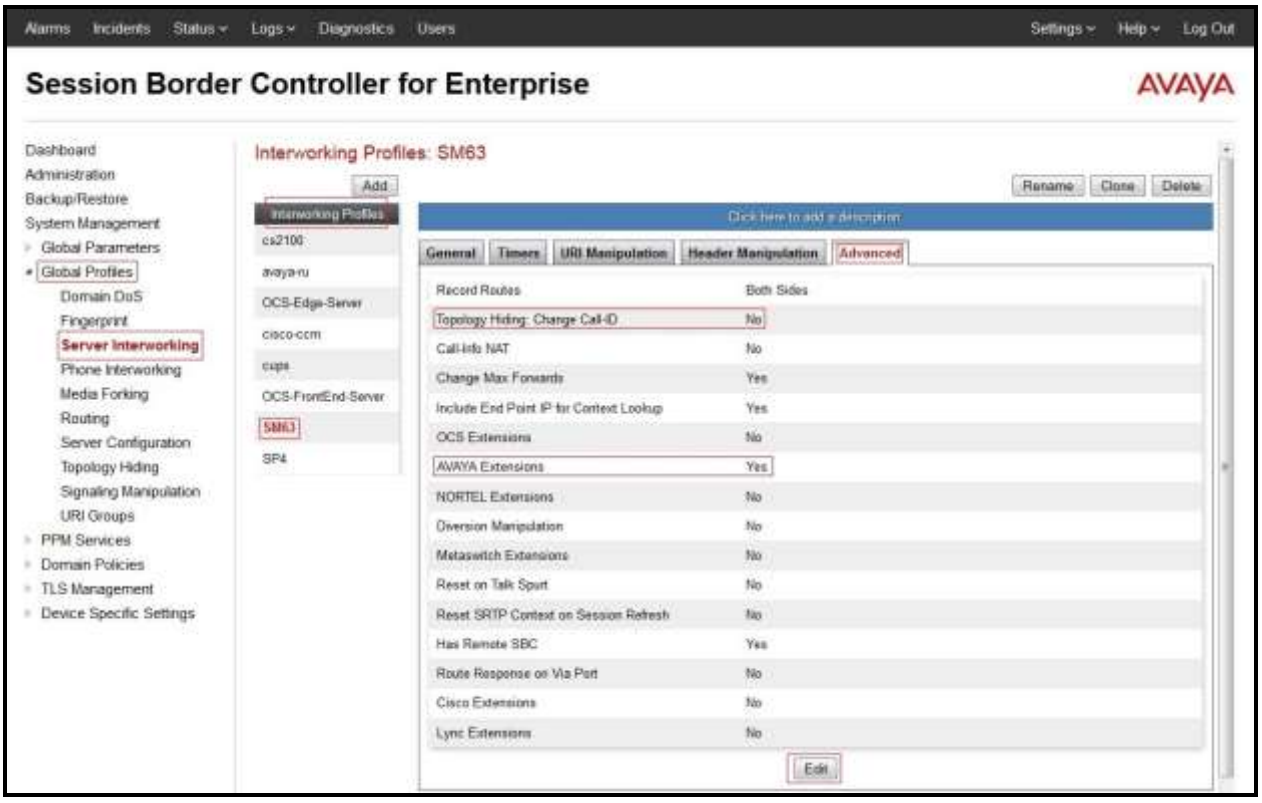

Figure 71: Server Interworking for Remote Worker

12.5. Server Configuration on Avaya SBCE

Note: **10.33.10.26** is the IP address of Session Manager in the reference configuration (see **Section 7.2.4**).

The following screens show the **Server Configuration** for the Profile **SM63** created previously for SIP Trunking with TDC Business Trunk in **Section 7.2.4** for Session Manager. The configuration includes TCP (5060) transport protocol which is also used for the Remote Worker configuration.

From the menu on the left-hand side, select **Global Profiles → Server Configuration**
Select **Server Profiles** as **SM63** to edit the existing Server Configuration SM63.

- On the **General** tab, click **Edit** button to add the following:
- **IP Address/FQDNs**: **10.33.10.26** (Avaya Aura Session Manager IP Address).
- **Port**: **5060**.
- **Transport**: **TCP**.
- Click **Finish** (not shown).

Figure 72: Server Configuration for Remote Worker

Note: This Server Configuration is used by the Routing Profile defined in **Section 12.6** and the Server Flows defined in **Section 12.13.2.2**.

12.6. Routing Profile on Avaya SBCE

The Routing Profile **To_SM_RW** is created for access to Session Manager.

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

Enter **Profile Name**: **To_SM_RW** (not shown).

- **Load Balancing**: **Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address.
- **Priority/Weight**: **1**.
- **Server Configuration**: **SM63** (see **Section 12.5**).
- **Next Hop Address**: **10.33.10.26:5060 (TCP)** (IP address of Session Manager).
- Click **Finish**.

The Routing Profile **To_SM_RW** is used in the Subscriber Flows (**Section 12.13.1**).

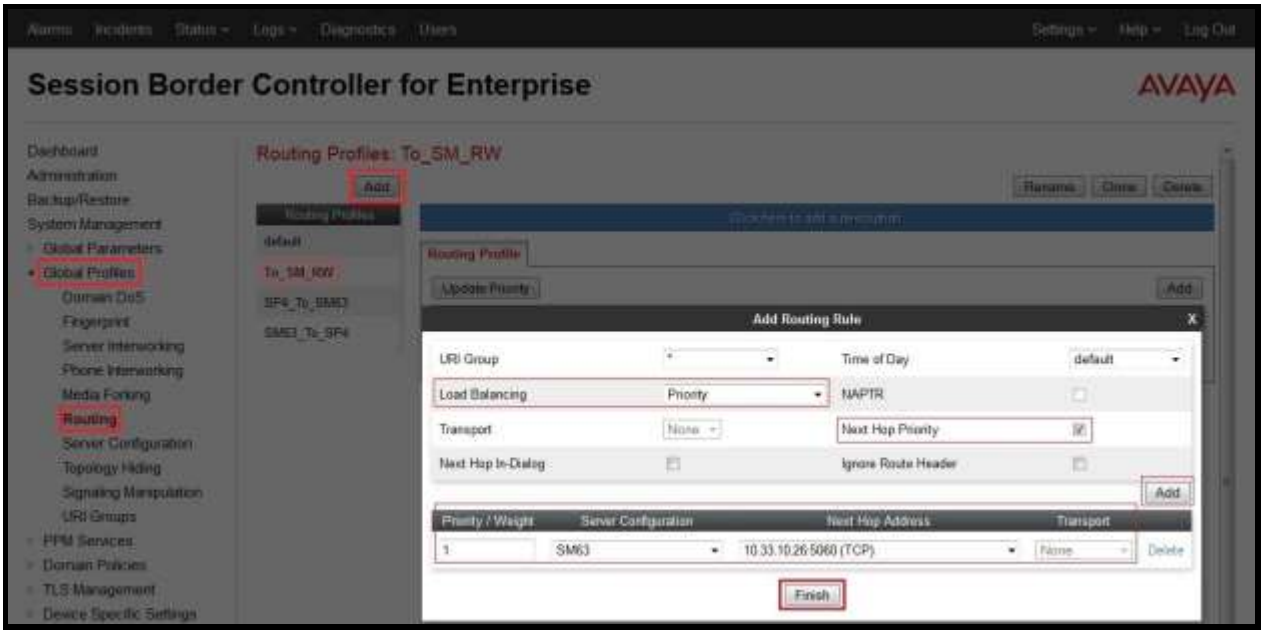

Figure 73: Remote Worker Routing to SM

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 12.13.2.1**.

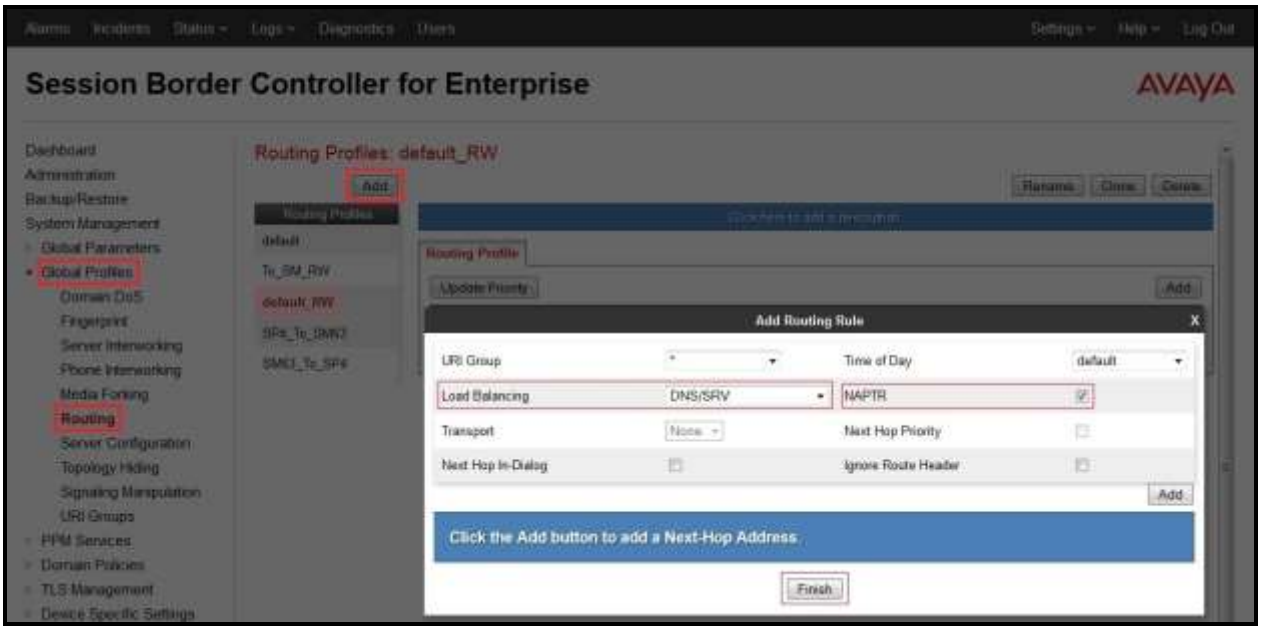

Figure 74: Remote Worker Default Routing

12.7. User Agent on Avaya SBCE

User Agents are created for each type of endpoint tested. In this compliance testing, Avaya Communicator for Windows will be 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**: **Avaya Communicator**.
- Enter **Regular Expression**: **Avaya Flare**.*.
- Click on **Finish** (not shown).

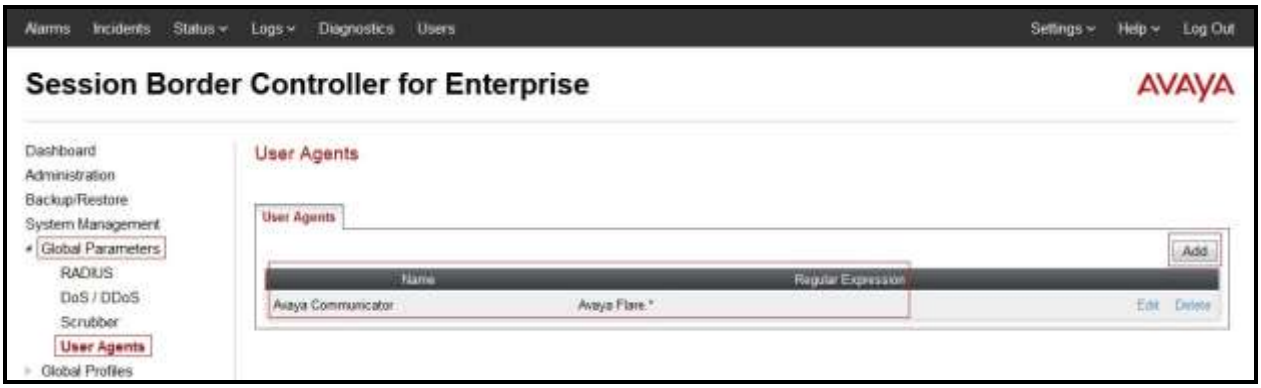

Figure 75: User Agents for Remote Worker

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

```
INVITE sip: 91303XXX9042@bvwdev7.com SIP/2.0
From: sip:5872@bvwdev7.com;tag=-59f03c7f529fb7c152aa3fd4_F0950710.10.98.136
To: sip: 91303XXX9042@bvwdev7.com
CSeq: 24 INVITE
Call-ID: 18_a7e80-49279ea452aa365c_I@10.33.5.58
Contact: <sip:5872@10.10.98.21:5060;transport=tcp;subid_ipcs=592904751>
Record-Route: <sip:10.10.98.21:5060;ipcs-line=3472;lr;transport=tcp>
Record-Route: <sip:10.10.98.99:5060;ipcs-line=3472;lr;transport=tcp>
Allow:
INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE,PRACK
Supported: eventlist, 100rel, replaces
User-Agent: Avaya Flare Engine/ 2.0.0 (Engine GA-2.0.0.24; Windows NT 6.1, 64-bit)
Max-Forwards: 69
Via: SIP/2.0/TCP 10.10.98.21:5060;branch=z9hG4bK-s1632-001362762279-1--s1632-
Via: SIP/2.0/TCP 10.10.98.136:5060;branch=z9hG4bK18_a7e80-312c149e52aa3fe8_I09507
Accept-Language: en
Content-Type: application/sdp
Content-Length: 340
```

Figure 76: Output of trace for User Agent

Note: The User Agent is defined in its associated **Subscriber Flows** in **Section 12.13.1**.

12.8. Relay Services on Avaya SBCE

Relay Services are used to define how file transfers (e.g., phone firmware upgrades and configuration data), are routed to the Remote Worker endpoints. Both HTTP and HTTPS protocols are supported.

In the reference configuration, HTTP protocol is used for file exchanges between the Remote Worker phones and an HTTP file server located in the enterprise. For completeness, HTTP configuration is shown below.

From the menu on the left-hand side, select **Device Specific Settings → DMZ Services → Relay Services**

On the **Application Relay** tab, click on the **Add** button and enter the following:

- Set **Service Type**: **HTTP**.
- Set the **Remote Domain** to the domain **bvwdev7.com**, previously specified for SIP Trunking with TDC Business Trunk in Communications Manager (see **Section 5.5**) and in Session Manager (see **Section 6.2**).
- Set the **Remote IP:Port** to the IP address of the enterprise file server (e.g., **10.10.98.60:80**) used to provide the firmware updates and configuration data for the Remote Worker endpoints.
- Set the **Remote Transport**: **TCP**.
- Set the **Published Domain** to **bvwdev7.com**.
- Set **Listen IP:Port** to the IP address of the Avaya SBCE's external IP address designated for file transfers (**Network_B1 (B1, VLAN 0)** and **10.10.98.124:80**).
- Set the **Listen Transport** to **TCP**.
- Set the **Connect IP** to the internal IP address of the Avaya SBCE used for Remote Worker (**Network_A1 (A1, VLAN 0)** and **10.10.98.21**).
- Click on **Finish** (not shown).

Figure 77: Relay Services Setup

12.9. Mapping Profiles on Avaya SBCE

A Mapping Profile is defined for Personal Profile Manager (PPM) data between the Remote Worker endpoints and Session Manager. The following screen shows the mapping profile **RW** created in the sample configuration. This enables the remote Avaya SIP endpoints to send and receive PPM information to and from Session Manager via the Avaya SBCE.

From the menu on the left-hand side, select **PPM Services → Mapping Profiles**

- Click on the **Add** button and enter the following:
- Enter **Profile Name** (e.g., **RW**), and click on **Next** (not shown).
- Select **Server Type**: **Session Manager**.
- In **Server Configuration** field, select **SM63** (not shown) from the drop down menu and in **Server Address** field, select **10.33.10.26:5060 (TCP)** from the drop down menu (see **Section 12.5**).
- Select **SBCE Device**: **SBCE63**.
- In **Signaling Interface** field, select **OutsideSIPRW (10.10.98.99)** from the drop down menu (see **Section 12.3**).
- In **Mapped Transport** field, select **TCP (5060)** from the drop down menu.
- Click **Finish** (not shown).

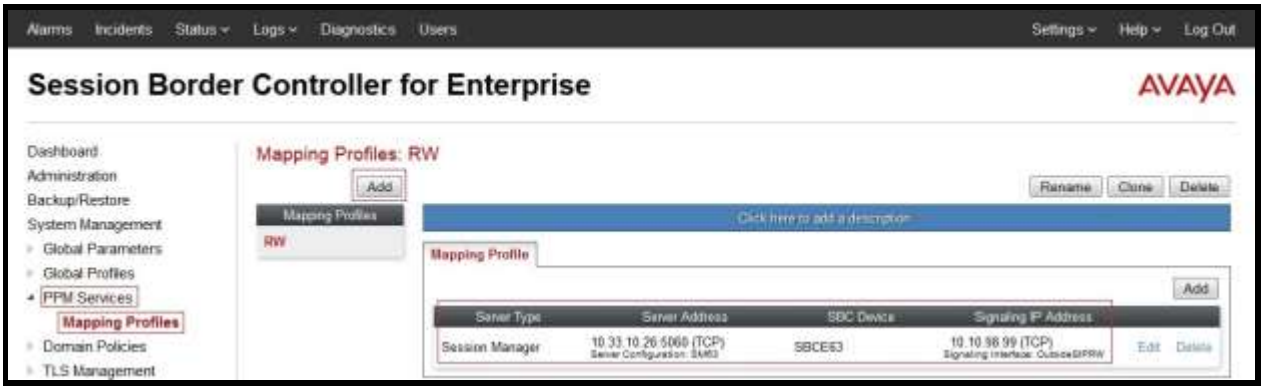

Figure 78: Mapping Profiles - PPM Services Setup

12.10. Application Rules on Avaya SBCE

The following section describes Application Rule **RemoteWorker_AR,** used in this Remote Worker settings. 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., **RemoteWorker_AR**) and click **Finish** (not shown).
- Click on **RemoteWorker_AR** from **Application Rules**, then click **Edit** button:
- In the **Voice** 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).

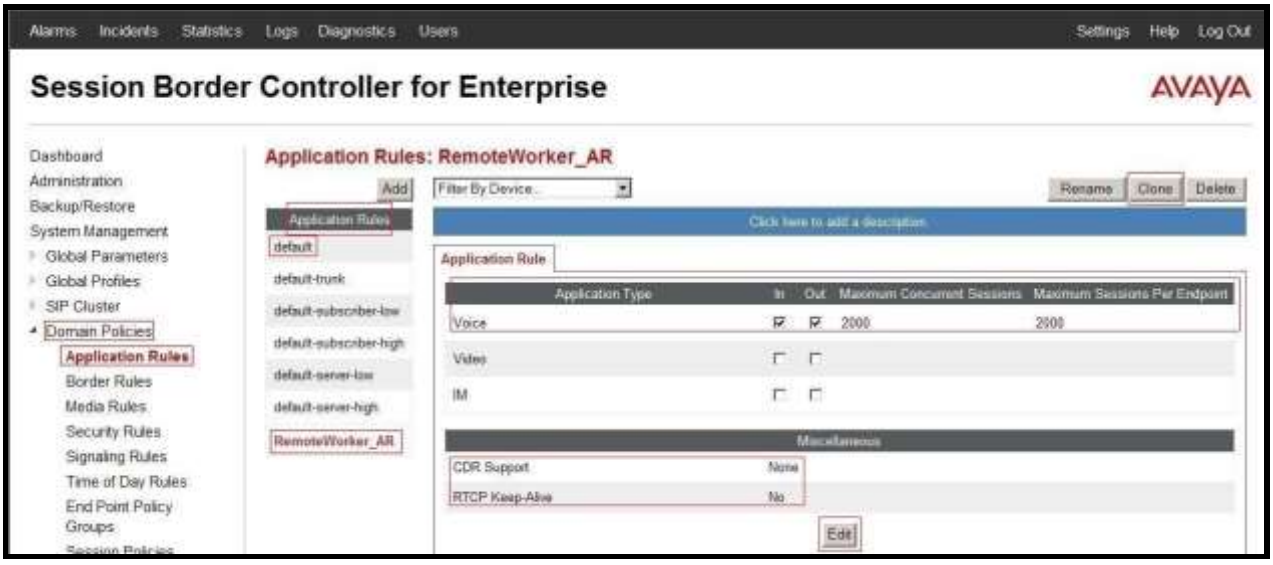

Figure 79: Remote Worker Application Rule

Note: The rule **RemoteWorker_AR** is assigned to the End Point Policy Groups in **Section 12.12**.

12.11. Media Rules on Avaya SBCE

The following section describes **Media Rule**: The existing rule **default-low-med** was used for the Remote Worker. Note that rule has **Interworking** in **Media Encryption** tab checked..

As described above the **default-low-med** rule was previously used and is shown here for completeness.

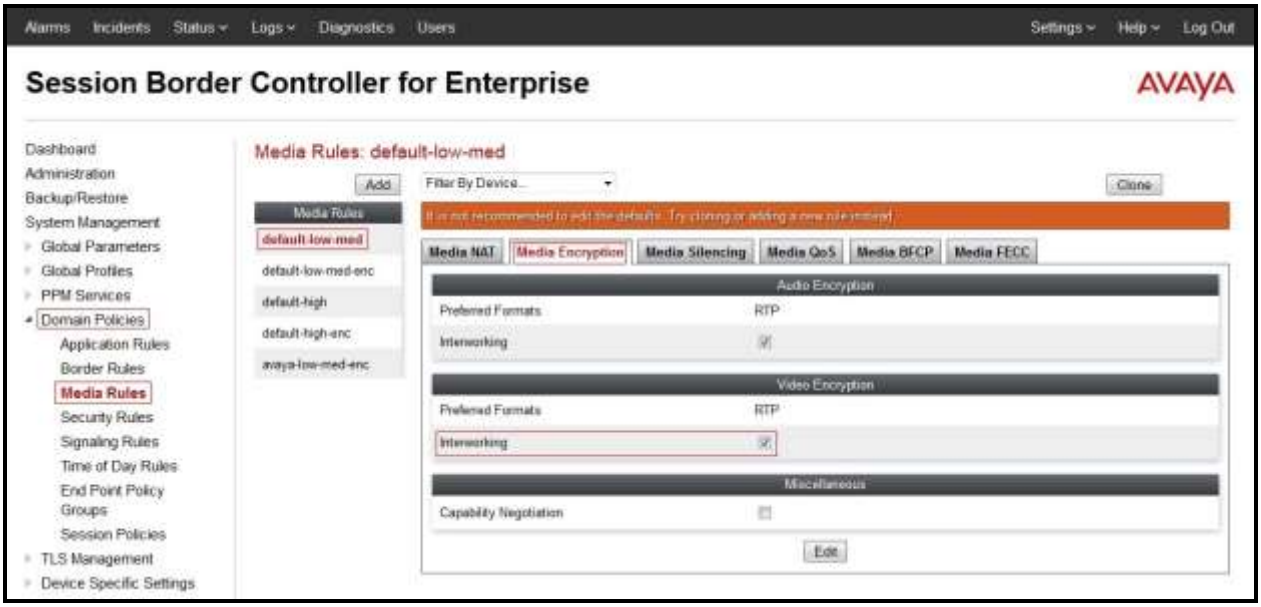

Figure 80: Default-Low-Med Media Rule

Note: The rule **default-low-med** is assigned to the End Point Policy Groups in **Section 12.12**.

12.12. End Point Policy Groups on Avaya SBCE

Two new End Point Policy Groups are defined for Remote Worker: **SM_RW**, and **RemoteUser_RTP**.

In addition, the End Point Policy Group **SP4_PolicyG** was previously created for SIP Trunking with TDC Business Trunk (see **Section 7.3**) and is shown here for completeness.

The End Point Policy Group **SP4_PolicyG** is used in the Server Flow defined in the **Section 12.13.2.2**.

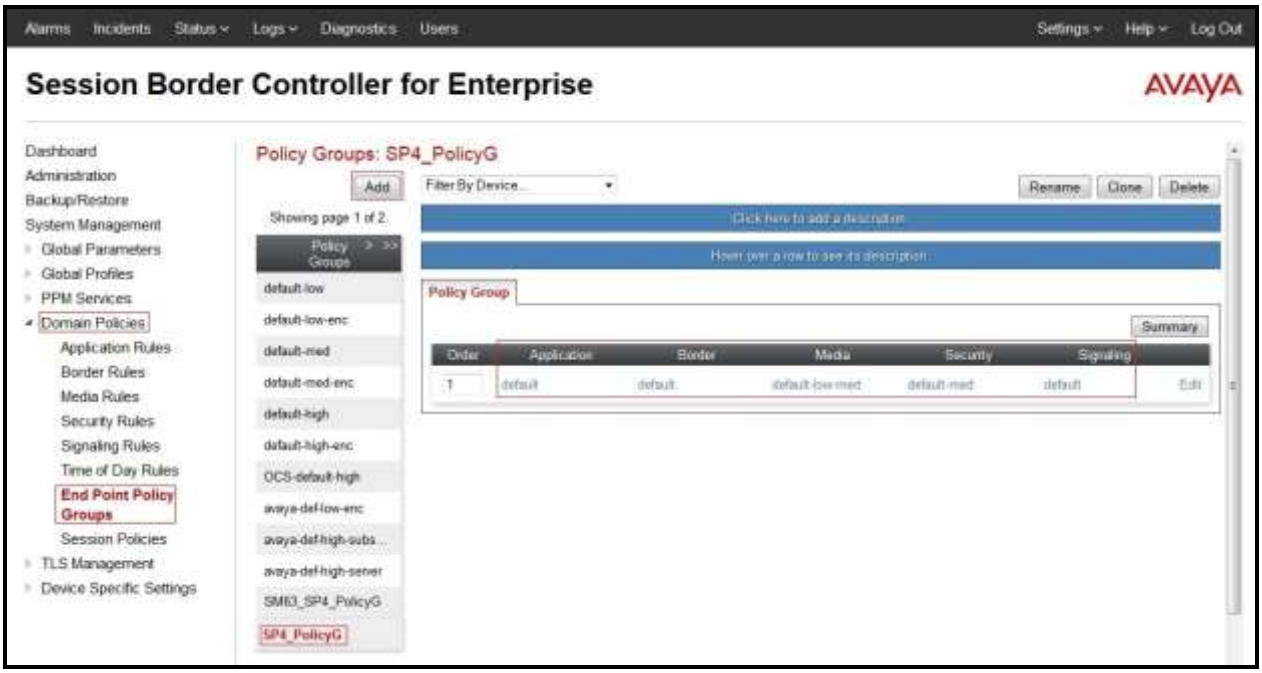

Figure 81: TDC Business Trunk End Point Policy

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

- Enter a name (e.g., **SM_RW**), and click on **Next** (not shown).
- The **Policy Group** window will open. Enter the following:
  - **Application Rule** = **RemoteWorker_AR** (**Section 12.10**).
  - **Border Rule** = default.
  - **Media Rule** = **default-low-med** (**Section 12.11**).
  - **Security Rule** = default-low.
  - **Signaling Rule** = default.
  - **Time of Day Rule** = default.
- Click on **Finish** (not shown).

The End Point Policy Group **SM_RW** is used in the Subscribe Flows **Flare** in **Section 12.13.1**.

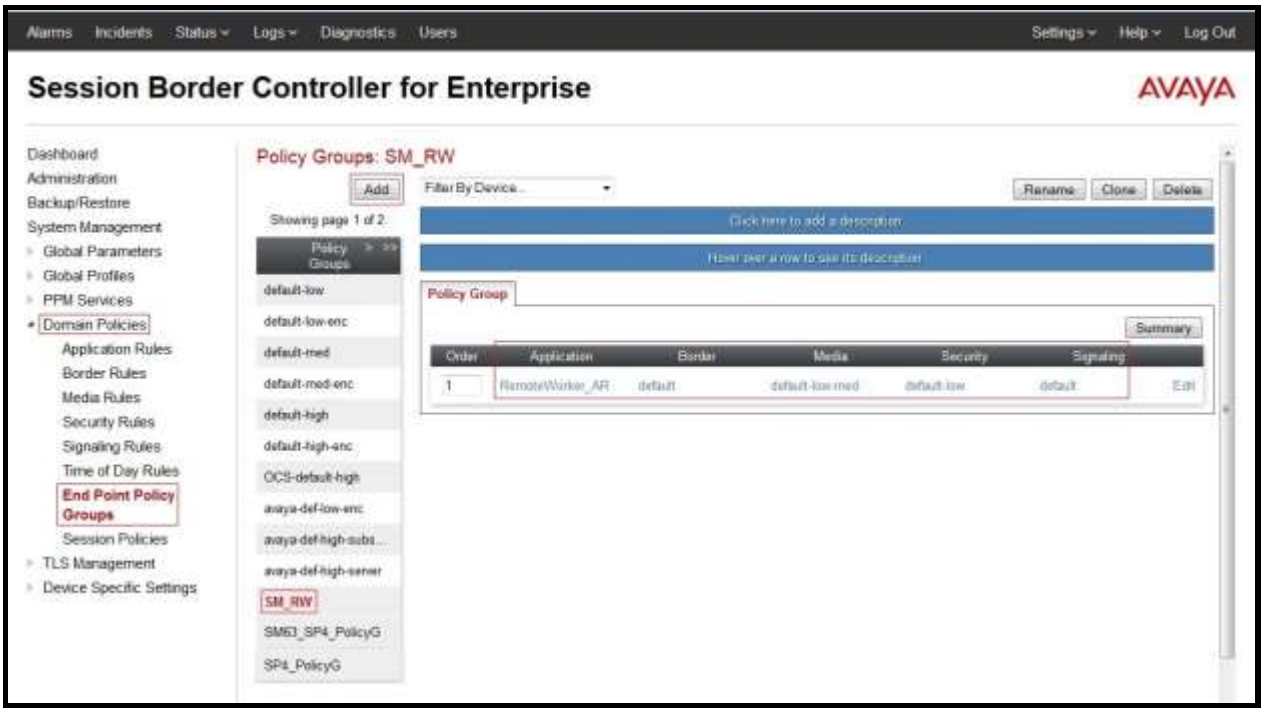

Figure 82: Remote Worker End Point Policy

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

- Enter a name (e.g., **RemoteUserRTP**), and click on **Next** (not shown).
- The **Policy Group** window will open. Enter the following:
  - **Application Rule** = **RemoteWorker_AR** (**Section 12.10**).
  - **Border Rule** = default.
  - **Media Rule** = **default_low_med** (**Section 12.11**).
  - **Security Rule** = default-low.
  - **Signaling Rule** = default.
  - **Time of Day Rule** = default.
- Click on **Finish** (not shown).

The End Point Policy Group **RemoteUserRTP** is used in the Server Flows **SM63_RemoteWorker** defined in the **Section 12.13.2.1**.

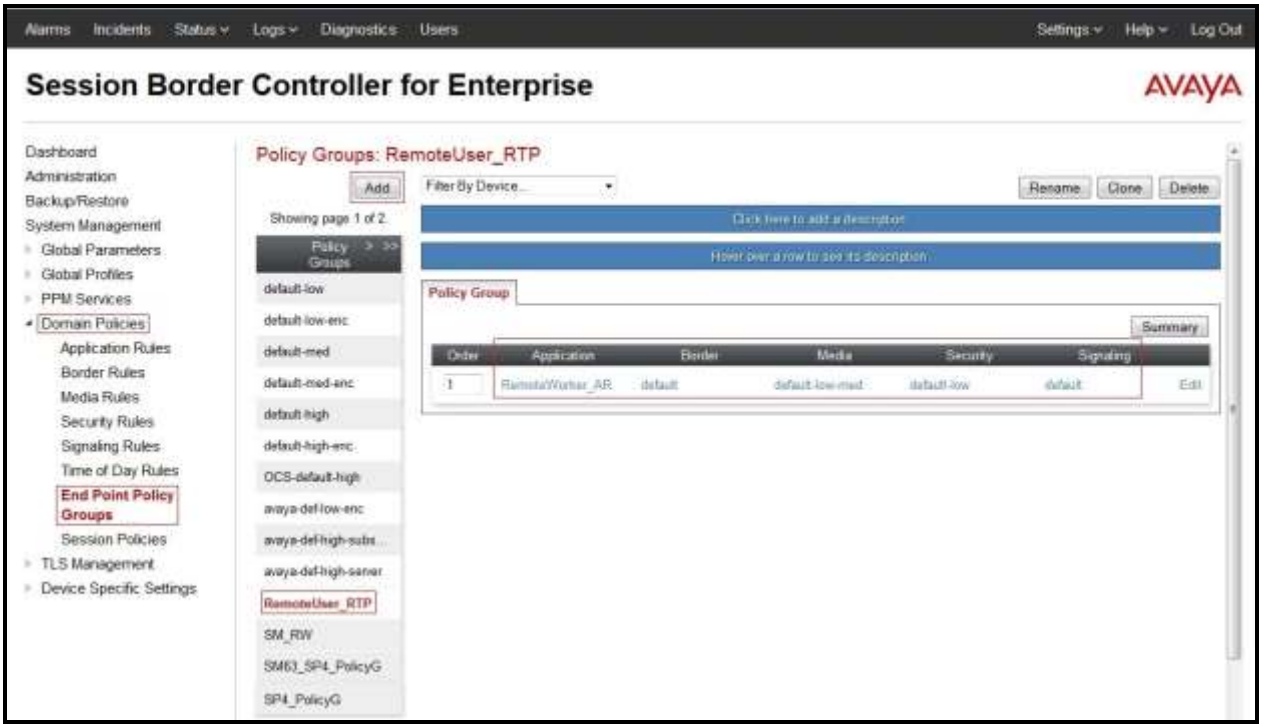

Figure 83: Remote Worker End Point Policy - RTP

12.13. End Point Flows on Avaya SBCE

12.13.1. Subscriber Flow

The **Subscriber Flow** is defined for Remote Workers associated with the **User Agent** previously created: **Avaya Communicator**.

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

On **Subscriber Flows** tab, click on **Add** button and enter the following:

- Enter a **Flow Name** (e.g., **Flare**).
- **URI Group** = * (default).
- **User Agent** = **Avaya Communicator** (see **Section 12.7**).
- **Source Subnet** = ***** (default).
- **Via Host** = ***** (default).
- **Contact Host** = ***** (default).
- **Signaling Interface** = **OutsideSIPRW** (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.

- **User Agent** = **Avaya Communicator**.
- **Media Interface** = **OutsideMediaRW** (see **Section 12.2**).
- **End Point Policy Group = SM_RW** (see **Section 12.12**).
- **Routing Profile = To_SM_RW** (see **Section 12.6**).
- **Topology Hiding Profile** = **None**.
- **Phone Interworking Profile** = **Avaya-Ru**.
- **TLS Client Profile** = **None**.
- **RADIUS Profile = None**.
- **File Transfer Profile** = **None**.
- **Signaling Manipulation Script** = **None**.

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

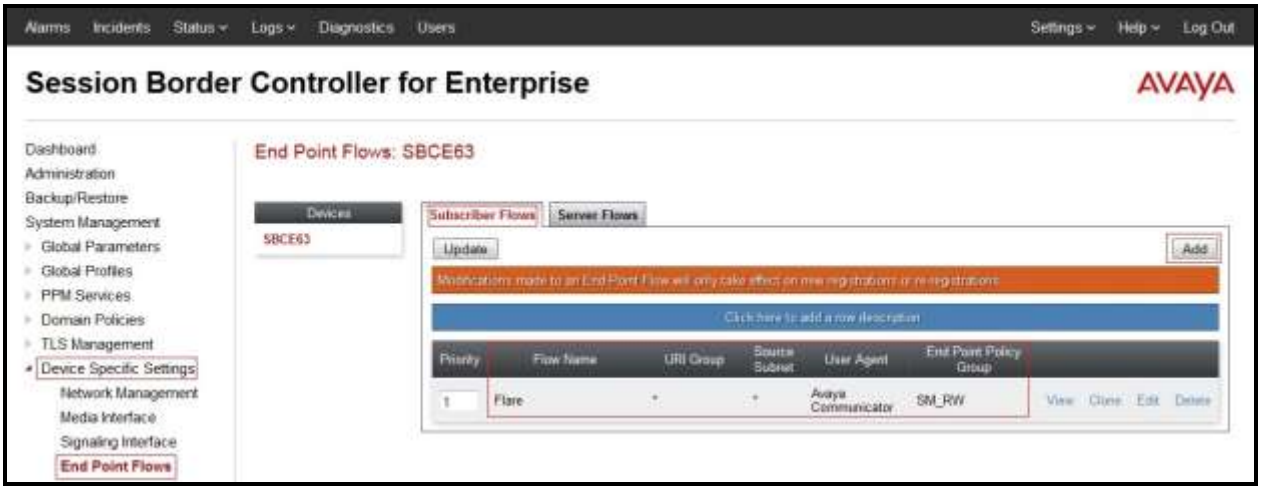

Figure 84: Remote Worker Subscriber Flows – Flare 1

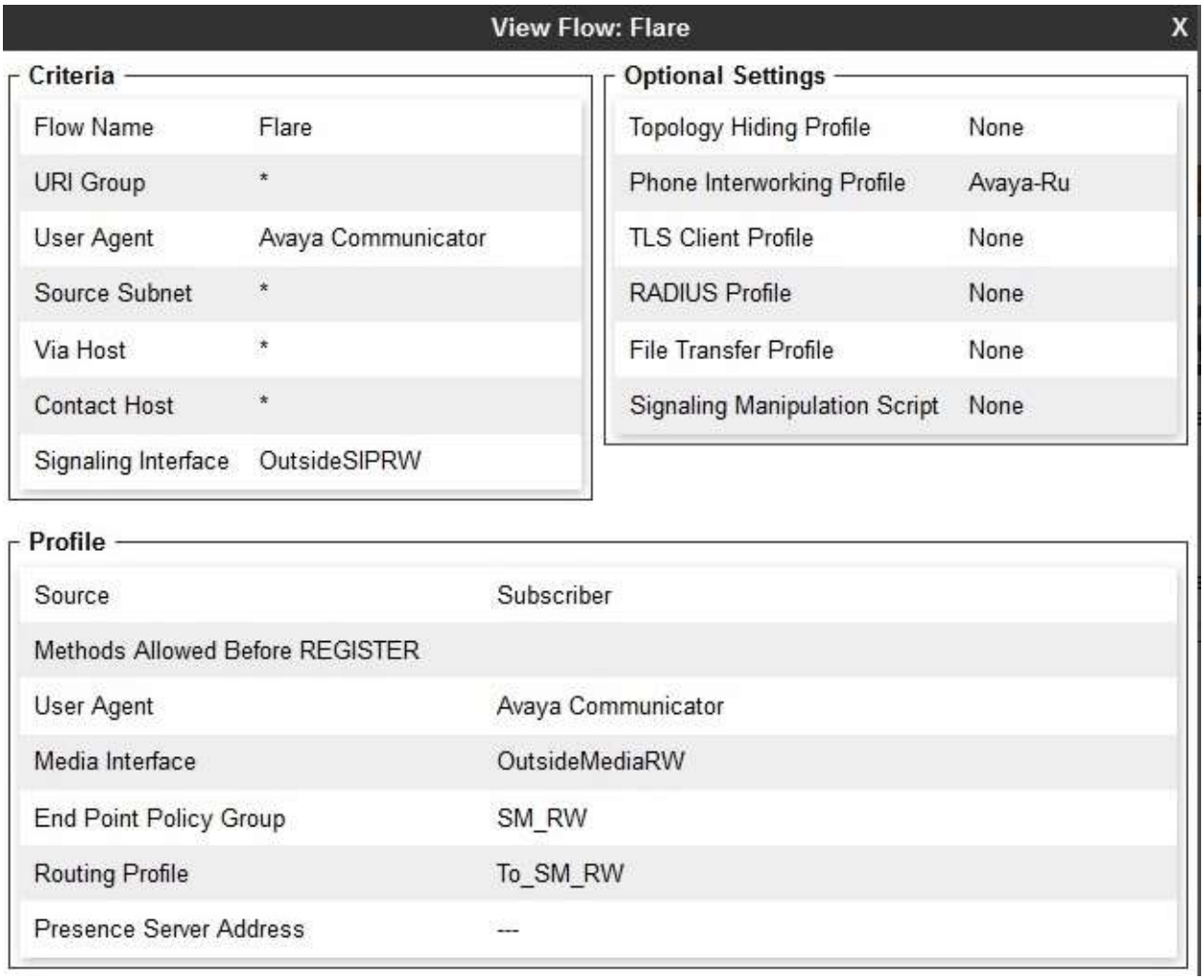

Figure 85: Remote Worker Subscriber Flows – Flare 2

12.13.2. Server Flow on Avaya SBCE

The following screens show the new **Server Flow** settings for Remote Worker access to Session Manager. Two examples of Server Flows are defined for Remote Worker.

12.13.2.1 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 **Add button** (not shown) to enter the following:

- **Name = SM63_RemoteWorker**.
- **Server Configuration** = **SM63** (see **Section 12.5**).
- **URI Group** = ***** (default).
- **Transport** = ***** (default).
- **Remote Subnet** = ***** (default).
- **Received Interface** = **OutsideSIPRW** (see **Section 12.3**).
- **Signaling Interface** = **InsideSIPRW** (see **Section 12.3**).
- **Media Interface** = **InsideMediaRW** (see **Section 12.2**).
- **End Point Policy Group** = **RemoteUser_RTP** (see **Section 12.12**).
- **Routing Profile** = **default_RW** (see **Section 12.6**).
- **Topology Hiding Profile** = **None** (default).
- **File Transfer Profile** = **None** (default).
- **Signaling Manipulation Script = None** (default).
- **Remote Branch Office** = **Any** (default).

Click **Finish** (not shown).

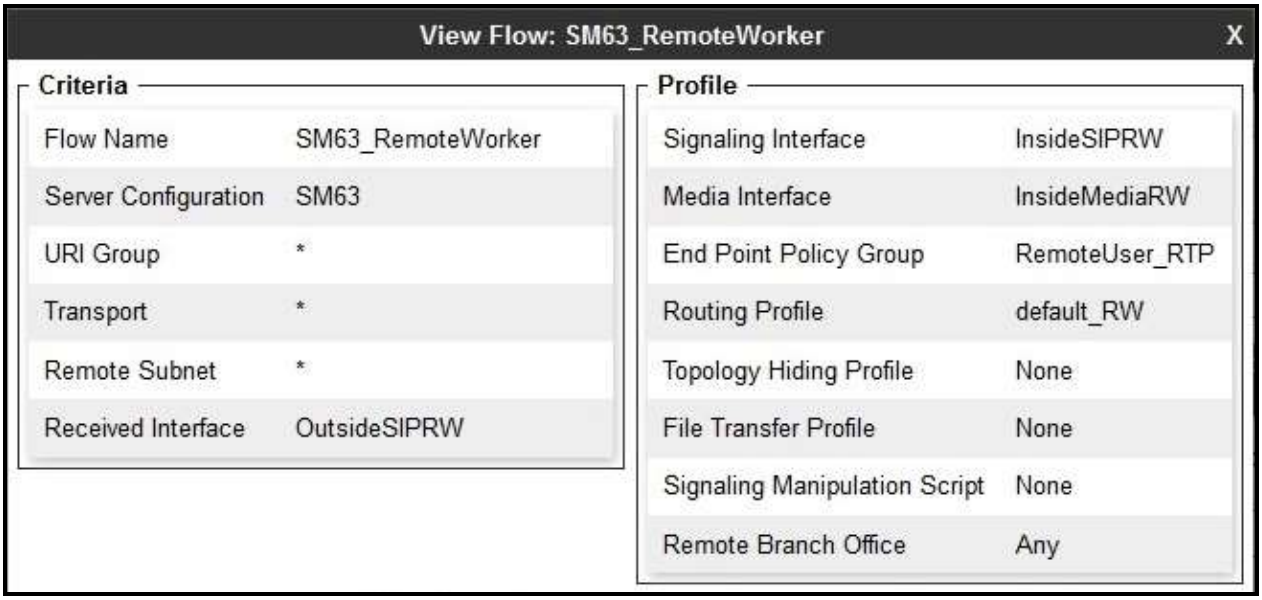

Figure 86: Remote Worker Server Flow

12.13.2.2 Trunking Server Flow on Avaya SBCE

The TDC Business Trunk Server Flow is defined in **Section 7.4.4.2** of this document.

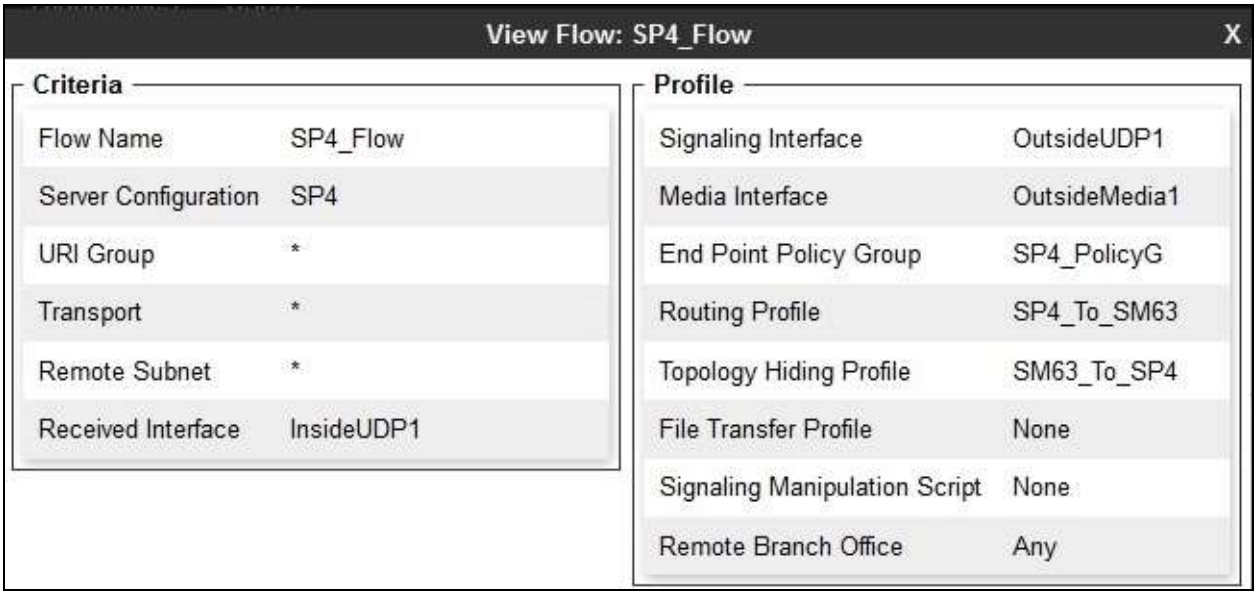

Figure 87: Trunking Server Flow

12.14. System Manager

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

Select **Rule Sets** as **Rule Set for SM63,** click **Edit** button.

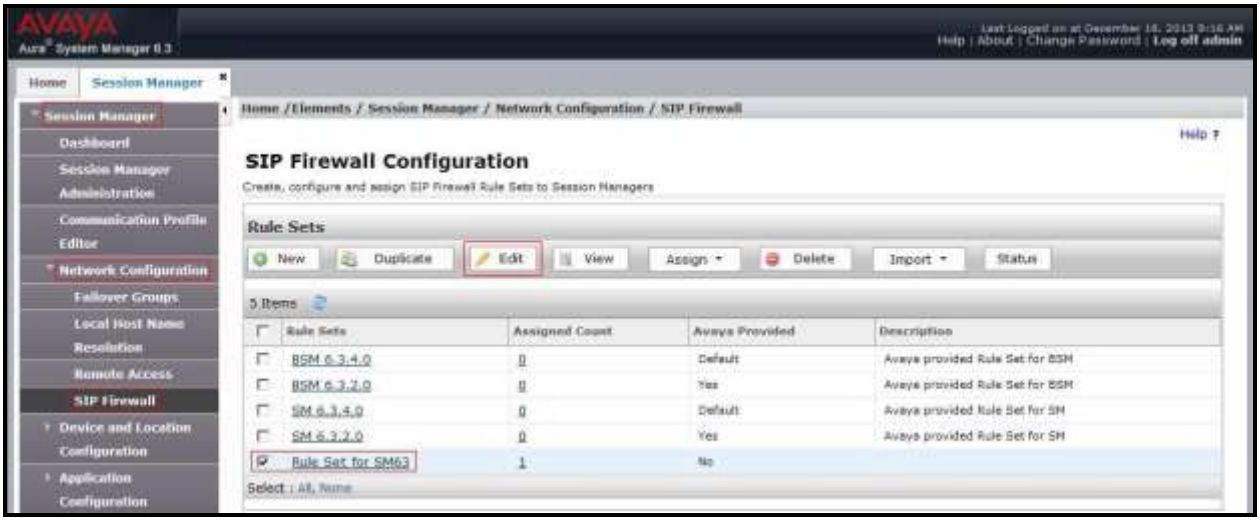

Figure 88: Session Manager – SIP Firewall Configuration - Rules

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 (**10.33.10.21**, see **Section 12.1**).
- In the **Mask** field, enter the appropriate mask (e.g., **255.255.255.0**).
- Select **Apply As Current**.

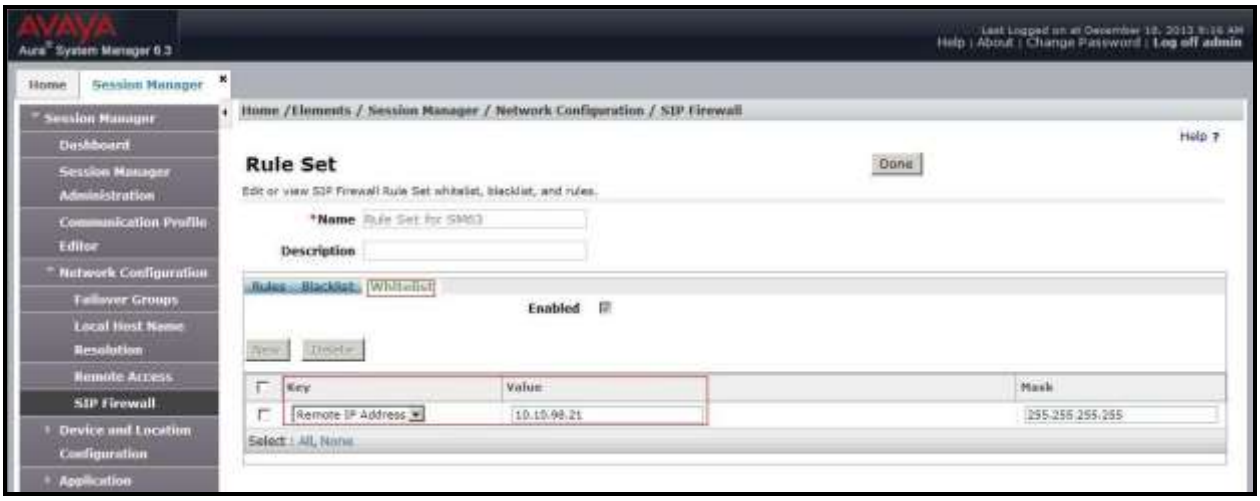

Figure 89: Session Manager – SIP Firewall Configuration - Whitelist

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

Select the **Session Manager instances** as **SM63**, and select **Edit**.

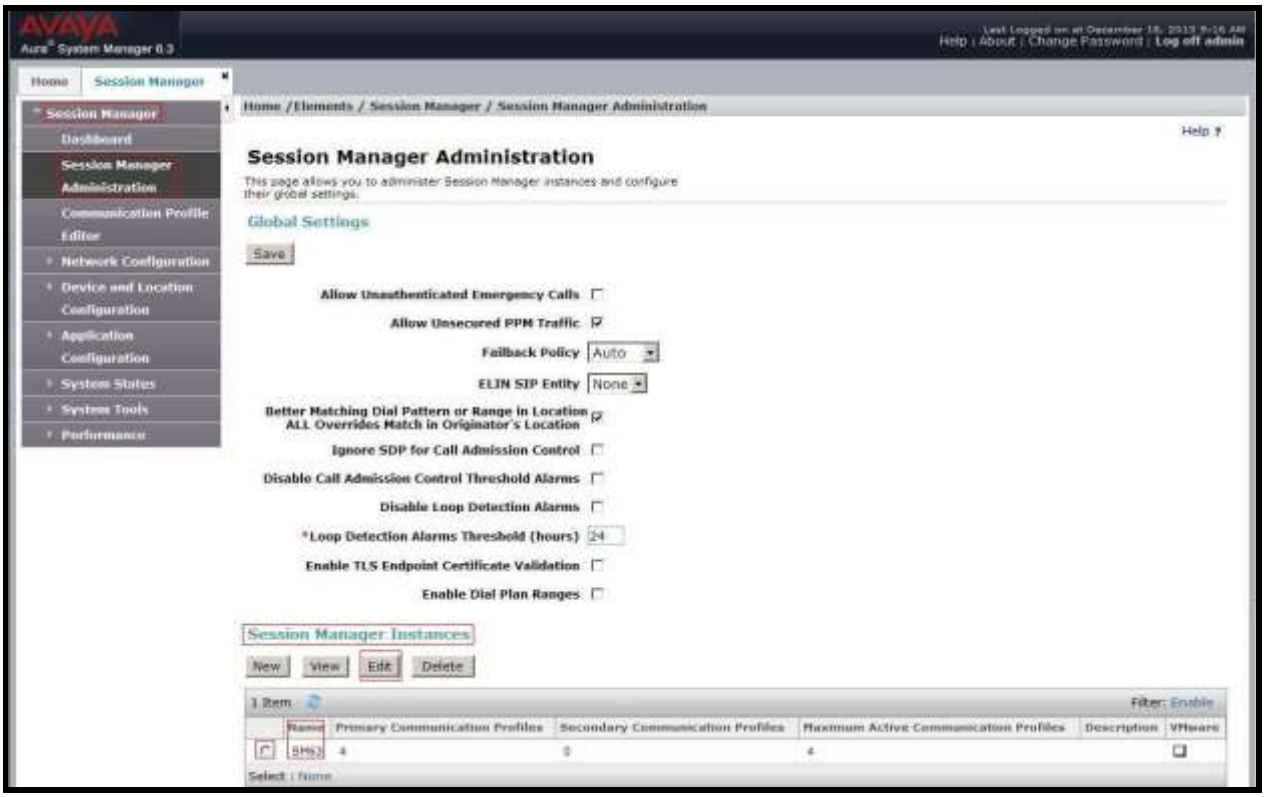

Figure 90: Session Manager – Edit Instance

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

- Uncheck the **Limited PPM Client Connections** and **PPM Packet Rate Limiting** options.
- Select **Return** (not shown).

Figure 91: Session Manager – Disable PPM limit

12.15. Remote Worker Client Configuration

The following screens illustrate Avaya Communicator for Windows 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 Communicator Settings** and click on **Server**. Set **Server address** parameter to the outside interface of the Avaya SBCE defined for Remote Worker telephony, **10.10.98.99** (see **Section 12.1**). Set **Server port**: **5060** and **Transport type**: **TCP**. The **Domain** is set to **bvwdev7.com**. The other fields are default. Click **OK** to submit the settings.

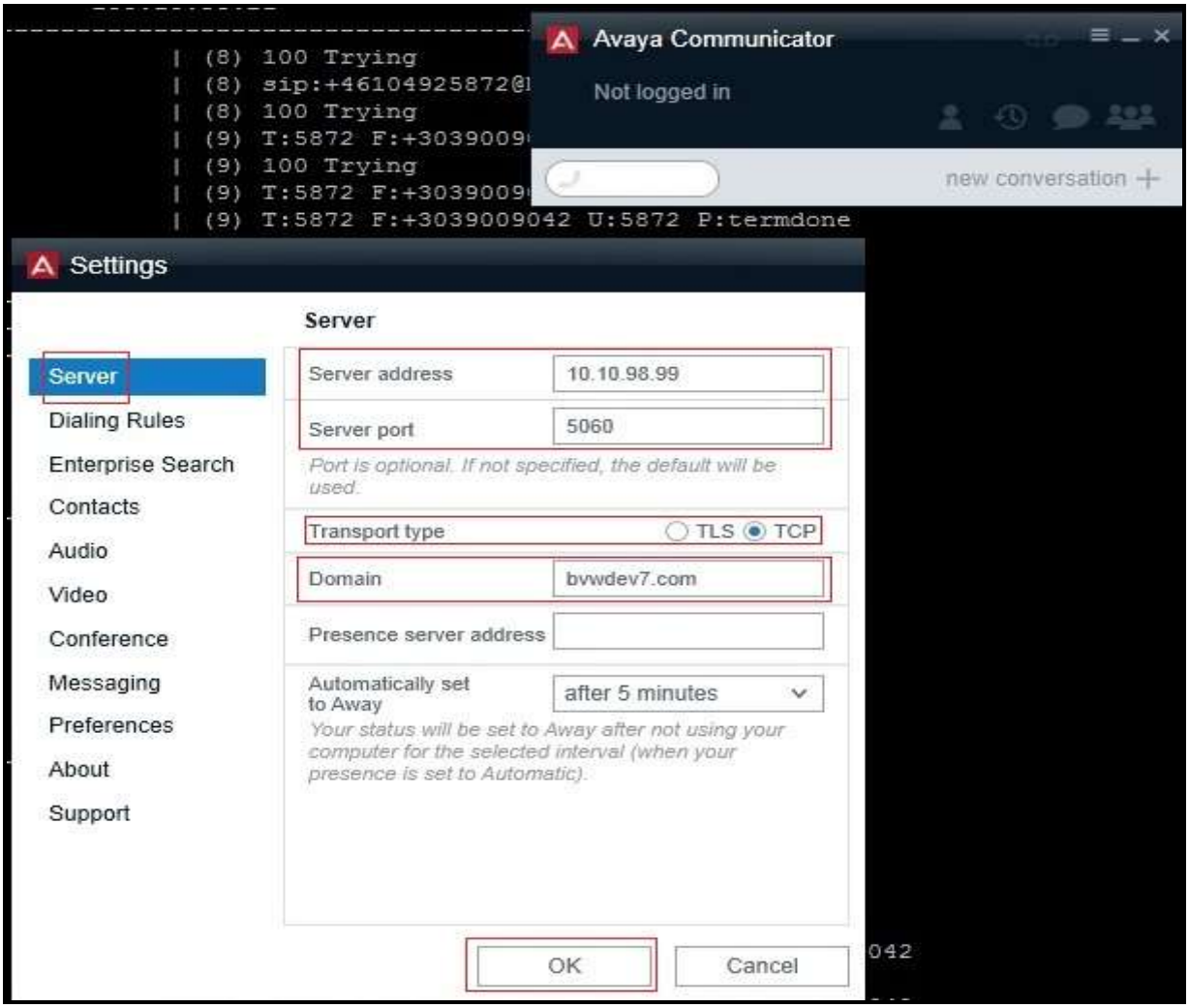

Figure 92: Avaya Communicator for Windows - SIP Global Settings

13. Appendix B: 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"
                {

     // Replace FROM header of Mex2 Mobile number = Mex fixed number


%HEADERS["From"][1].URI.USER.regex_replace("(\+46767225962)","+46104925874");

%HEADERS["Contact"][1].URI.USER.regex_replace("(\+46767225962)","+46104925874");

 %HEADERS["From"][1].URI.USER.regex_replace("(\+46767225921)","+46104925872");

%HEADERS["Contact"][1].URI.USER.regex_replace("(\+46767225921)","+46104925872");

                }

  act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
                {

    // Mex Testing Replace "++" by "+"

          %HEADERS["From"][1].URI.USER.regex_replace("(\++)","+");
          %HEADERS["Contact"][1].URI.USER.regex_replace("(\++)","+");
          %HEADERS["Request_Line"][1].URI.USER.regex_replace("(\++)","+");
          %HEADERS["To"][1].URI.USER.regex_replace("(\++)","+");

                }
}
```

14. Appendix C: MEX Testing

In this compliance testing, the below test extensions can only be used in Sweden to be able to trigger IN services.

Mex 1 fixed number = +46104925874 (Mex1 enabled mobile= +46767225962) extension 5874.
Mex 2 fixed number = +46104925872 (Mex2 enabled mobile= +46767225921) extension 5872.

R1 number: +222 and Prefix: +46394980.

14.1. Inbound Call To Mex enabled Mobile

A calls to B (mex fixed number, which is routed to PBX).
After receiving the SIP Invite from TDC, the PBX should send a SIP re-Invite against the SIP trunk with the To-header user part that must contain a concatenation of PREFIX +46394980 and the Mex enabled mobile's number in international format.
The From-header user part is the original calling number generated by the PBX (the number to display on the Mex enabled mobile).

Example 1:

Assuming a call from +46767892721 to a Mex1 fixed number (+46104925874) associated with Mex1 enabled mobile +46767225962.

Firstly, TDC sent SIP Invite message to Avaya with the To- and From-headers might look like:
To: <sip:+2220104925874@test11.btrunk.se>
From: <sip:+46767892721@test11.btrunk.se>

Then, Avaya PBX sent SIP re-Invite to TDC with the To- and From-headers might look like:
To: <sip:+4639498046767225962@test11.btrunk.se>
From: <sip:+46104925872@test11.btrunk.se>

Example 2:

Assuming a call from Mex1 enabled mobile +46767225962 to a Mex2 fixed extension number (5872) associated with Mex1 enabled mobile +46767225921.

Firstly, TDC sent SIP Invite message to Avaya with the To- and From-headers might look like:
To: <sip:+2225872@test11.btrunk.se>
From: <sip:+46767225962@test11.btrunk.se>

Then, Avaya PBX sent SIP re-Invite to TDC with the To- and From-headers might look like:
To: <sip:+4639498046767225921@test11.btrunk.se>
From: <sip:+46104925874@test11.btrunk.se>

14.1.1. Configure Session Manager – Dial Pattern

There are two examples of dial patterns defined in this configuration: 46394980 and +222.

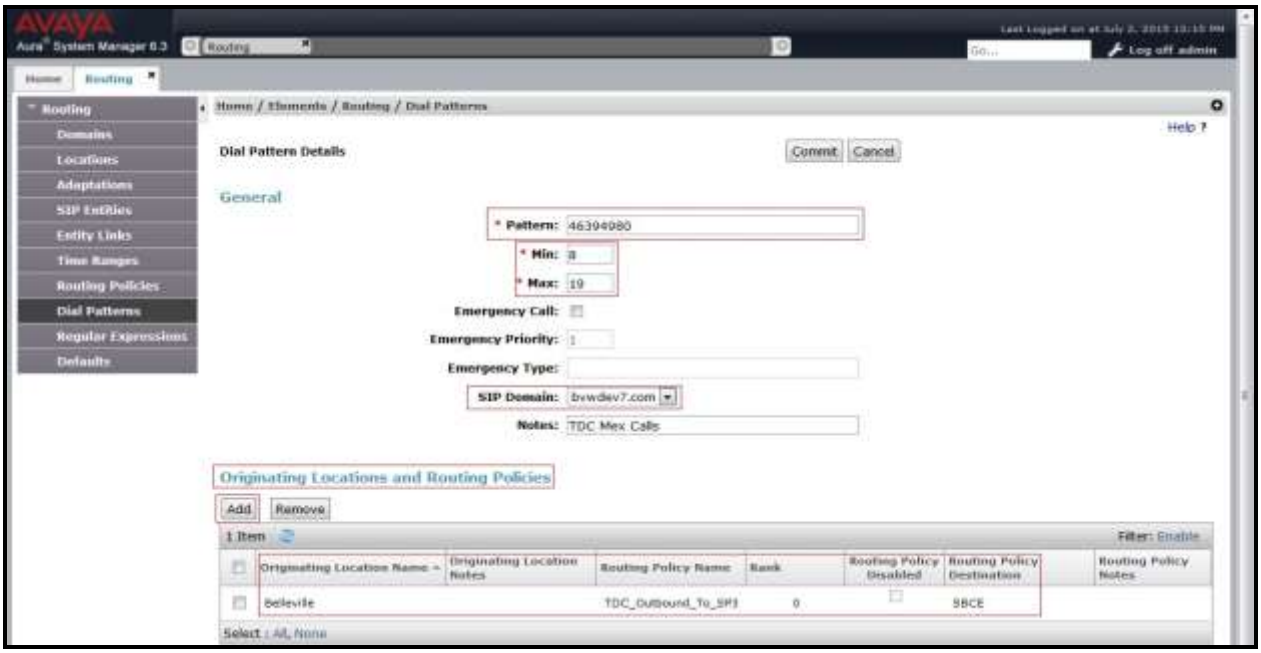

Figure 93: Dial Pattern_46394980

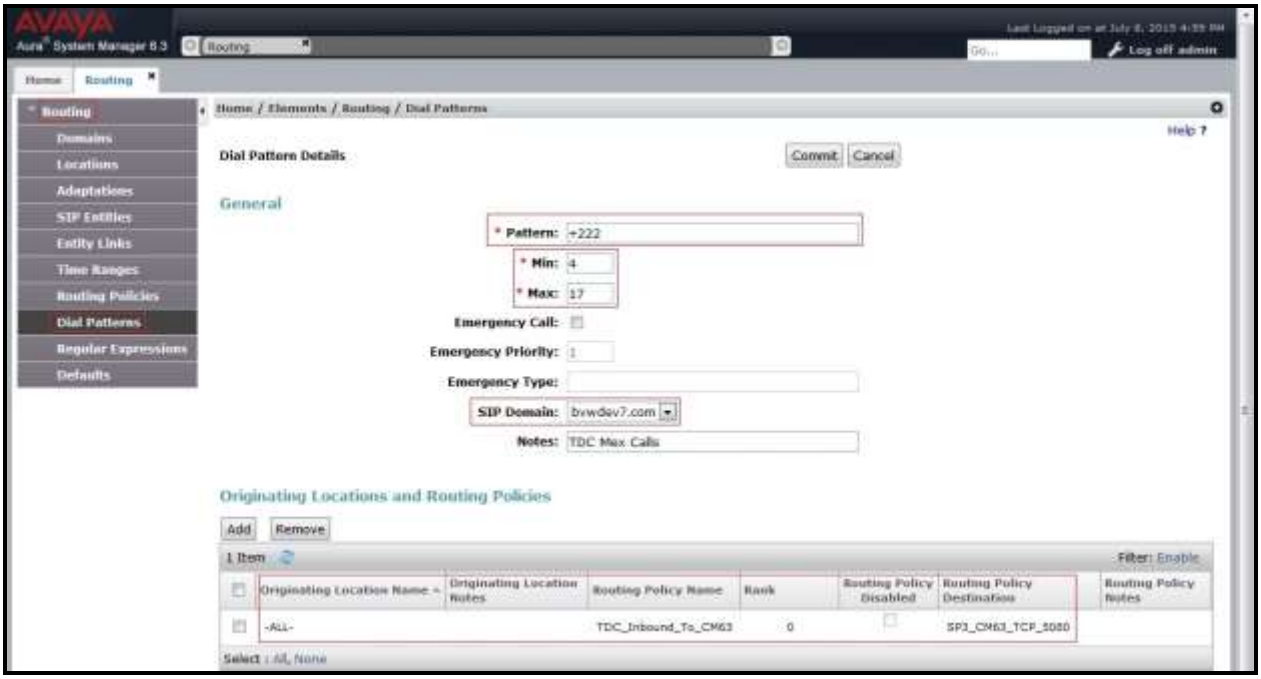

Figure 94: Dial Pattern_+222

14.1.2. Configure Communication Manager

1. Configure off-pbx- telephone station-mapping for extension 5874

```
change off-pbx-telephone station-mapping 5874                    Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                    Selection   Set     Mode
 5874            EC500     4639 -     498046767225962   20         1
                           -
```

Figure 95: Station-Mapping_5874

2. Configure station 5874

```
change station 5874                                              Page   2 of   5
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                  Auto Answer: none
            CDR Privacy? n                             Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n                  Bridged Idle Line Preference? n
   Bridged Call Alerting? n                      Restrict Last Appearance? y
  Active Station Ringing: single
                                                        EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                    EC500 State: enabled
         Multimedia Mode: enhanced                 Audible Message Waiting? n
    MWI Served User Type:                        Display Client Redirection? n
              AUDIX Name:                       Select Last Used Appearance? n
                                                  Coverage After Forwarding? s
                                                    Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 5874          Always Use? n IP Audio Hairpinning? n
```

Figure 96: Station 5874 – Page 2

```
change station 5874                                          Page   4 of   5
                                    STATION
 SITE DATA
      Room:                                              Headset? n
      Jack:                                              Speaker? n
     Cable:                                             Mounting: d
     Floor:                                          Cord Length: 0
   Building:                                           Set Color:

ABBREVIATED DIALING
     List1:                    List2:                     List3:

BUTTON ASSIGNMENTS
 1: call-appr                            5:
 2: call-appr                            6:
 3: call-appr                            7:
 4: ec500      Timer? n                  8:
    voice-mail
```

Figure 97: Station 5874 – Page 4

3. Configure off-pbx- telephone station-mapping for extension 5872

```
change off-pbx-telephone station-mapping 5872                  Page   1 of   3
                 STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                    Selection   Set     Mode
 5872            EC500     4639 -     498046767225921   20         1
                           -
```

Figure 98: Station-Mapping_5872

4. Configure station 5872

```
change station 5872                                          Page   2 of   5
                                    STATION
FEATURE OPTIONS
          LWC Reception: spe              Auto Select Any Idle Appearance? n
         LWC Activation? y                          Coverage Msg Retrieval? y
  LWC Log External Calls? n                                 Auto Answer: none
            CDR Privacy? n                               Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? n                       Restrict Last Appearance? y
  Active Station Ringing: single
                                                        EMU Login Allowed? n
       H.320 Conversion? n          Per Station CPN - Send Calling Number?
      Service Link Mode: as-needed                    EC500 State: enabled
        Multimedia Mode: enhanced                 Audible Message Waiting? n
    MWI Served User Type:                       Display Client Redirection? n
            AUDIX Name:                        Select Last Used Appearance? n
                                                 Coverage After Forwarding? s
                                                   Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 5872          Always Use? n IP Audio Hairpinning? n
```

Figure 98: Station 5872 – Page 2

```
change station 5872                                          Page   4 of   5
                                    STATION
 SITE DATA
      Room:                                              Headset? n
      Jack:                                              Speaker? n
     Cable:                                             Mounting: d
     Floor:                                          Cord Length: 0
  Building:                                            Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                            5:
 2: call-appr                            6:
 3: call-appr                            7:
 4: ec500      Timer? n                  8:

    voice-mail
```

Figure 99: Station 5872 – Page 4

5. Configure incoming-call-handling

```
change inc-call-handling-trmt trunk-group 20                    Page   1 of  30
                     INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    17 +222             4   9
 public-ntwrk    14 +222010492       10
 public-ntwrk    14 +222             4   9
```

Figure 100: Incoming Call Handling

6. Configure Dialplan

```
change dialplan analysis                                        Page   1 of  12
                            DIAL PLAN ANALYSIS TABLE
                                  Location: all           Percent Full: 4

    Dialed       Total            Call
    String       Length           Type
     9             1               fac
```

Figure 101: Dialplan

7. Configure ARS

```
change ars analysis 463                                          Page   1 of   2
                           ARS DIGIT ANALYSIS TABLE
                                 Location: all            Percent Full: 0

   Dialed           Total     Route    Call   Node  ANI
   String          Min  Max  Pattern   Type   Num   Reqd
    463            10   13    20       pubu         n
```

Figure 102: ARS Analysis

14.2. Outbound Call from Mex enabled mobile

Mex enabled mobile calls to B (any PSTN numbers).
After receiving the SIP Invite from TDC, the PBX should send a SIP re-Invite against the SIP trunk with the To-header user part must contain PSTN number in international format and the From-header user part will be replaced by the MEX fixed number.

Example:

Assuming a call from Mex enabled mobile with number +46767225962 to PSTN 0016139675206 and R1 is using +222.

Firstly, TDC sent the SIP Invite to Avaya with To- and From-headers might look like:
To: <sip:+2220016139675206@test11.btrunk.se>
From: <sip:+46767225962@test11.btrunk.se>

Then, Avaya PBX sent SIP re-Invite to TDC with the To- and From-headers might look like:
To: <sip:+0016139675206@test11.btrunk.se>
From: <sip:+46104925874@test11.btrunk.se>

14.2.1. Configure Session Manager – Dial Pattern

There are examples of dial patterns defined in this configuration: +222, 001, and other dial patterns related to any PSTN numbers that user wish to call.

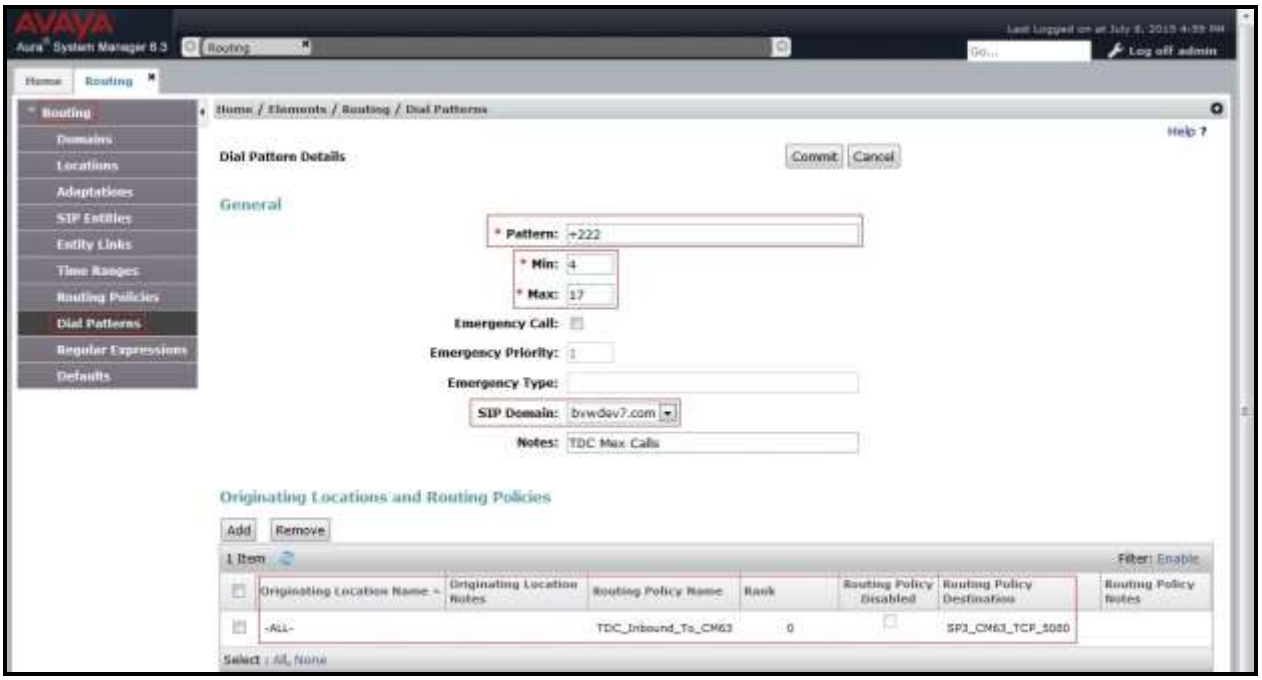

Figure 103: Dial Pattern_+222

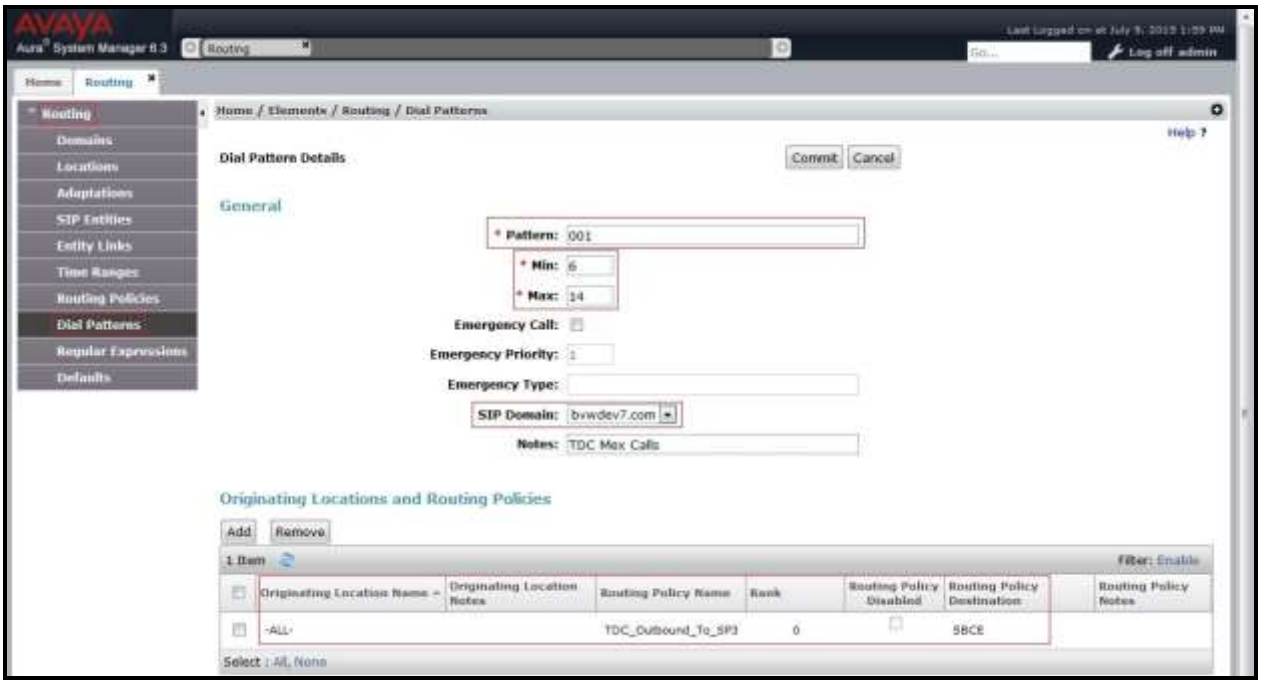

Figure 104: Dial Pattern_001

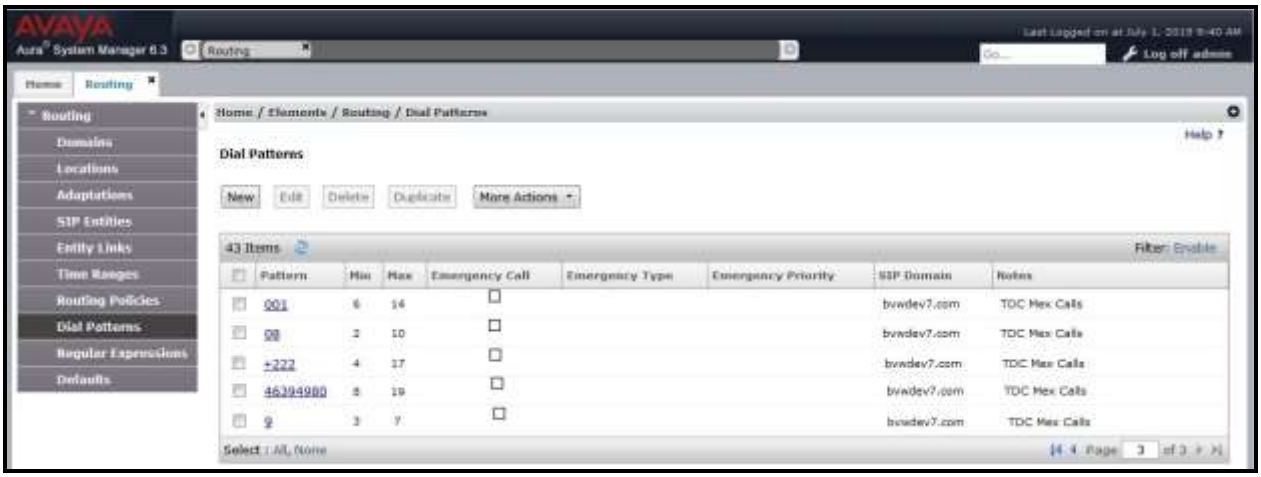

Figure 105: Dial Pattern_List

14.2.2. Configure Communication Manager

1. Configure incoming-call-handling

```
change inc-call-handling-trmt trunk-group 20                    Page   1 of  30
                     INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    17 +222             4   9
 public-ntwrk    14 +222010492       10
 public-ntwrk    14 +222             4   9
```

Figure 106: Dial Pattern_List

2. Configure Dialplan

```
change dialplan analysis                                        Page   1 of  12
                            DIAL PLAN ANALYSIS TABLE
                                  Location: all            Percent Full: 4

    Dialed       Total            Call
    String       Length           Type

     9             1              fac
```

Figure 107: Dialplan

3. Configure ARS

```
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
    001                   10   17    20       pubu         n
    087                    5   10    20       pubu         n
    089                    5   10    20       pubu         n
    463                   10   13    20       pubu         n
    9                      5    7    20       pubu         n
```

Figure 108: ARS Analysis

14.2.3. Configure Signaling Manipulation on Avaya SBCE

The below information is defined in **Section 7.2.3**. The script was used to replace Mex enabled mobile number on From/Contact headers by Mex fixed number for incoming calls and to replace "++" by "+" on SIP headers for outgoing calls.

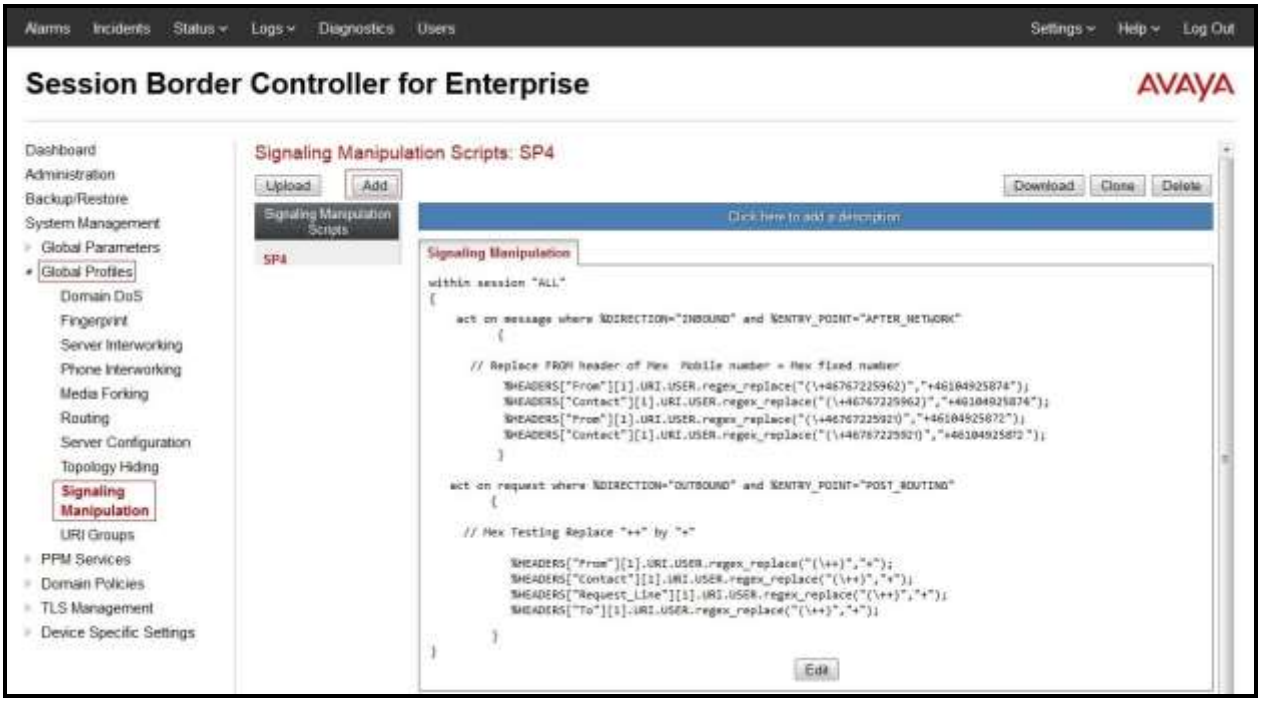

Figure 109: Signaling Manipulation for Mex Testing

15. Appendix D: Configure Special Numbers

Calls from PBX to Inquire, Emergency, Healthcare, or Police number services, service numbers are required a prefix/suffix before being sent to the TDC platform. The prefix/suffix needs to be added by the PBX. The prefix is always **463** and is required for the number series starting on 112, 1177, 11414, and 118118. The suffix is always **479** and is required for the number series starting on 112, 1177, 11414.

Example:

- Calling Inquire number 118118: The PBX sent +46379118118
- Calling Emergency number 112: The PBX sent +46379112479
- Calling Healthcare number 1177: The PBX sent +463791177479
- Calling Police number 11414: The PBX sent + 4637911414479.

15.1.1. Configure Communication Manager

1. Configure Dialplan

```
change dialplan analysis                                        Page   1 of  12
                            DIAL PLAN ANALYSIS TABLE
                                  Location: all            Percent Full: 4

    Dialed          Total         Call
    String          Length        Type

     9              1              fac
```

Figure 110: Dialplan

2. Configure ARS

```
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

    463             10   13    20        pubu          n
```

Figure 111: ARS Analysis

3. Configure Vector 1 for Inquire Number 118118

```
change vector 1                                                Page   1 of   6
                                  CALL VECTOR

    Number: 1                Name: Inquire_118118
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 silence
02 route-to     number 946379118118     with cov n if unconditionally
03 stop
04
```

Figure 112: Vector for 118118

4. Configure VDN for Inquire Number 118118

```
change vdn 118118                                              Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 11.81.18
                                 Name*: Inquire_118118
                           Destination: Vector Number        1
                     Attendant Vectoring? n
                    Meet-me Conferencing? n
                      Allow VDN Override? n
                                    COR: 1
                                    TN*: 1
                              Measured: none


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

Figure 113: VDN for 118118

5. Configure Vector 2 for Emergency Number 112

```
change vector 2                                                  Page   1 of   6
                                  CALL VECTOR

    Number: 2                Name: Emergency-112
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 silence
02 route-to     number 946379112479     with cov n if unconditionally
03 stop
04
05
06
```

Figure 114: Vector for 112

6. Configure VDN for Emergency Number 112

```
change vdn 112                                                   Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                              Extension: 112
                                  Name*: Emergency-112
                            Destination: Vector Number        2
                       Attendant Vectoring? n
                     Meet-me Conferencing? n
                       Allow VDN Override? n
                                     COR: 1
                                      TN*: 1
                                Measured: none


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

Figure 115: VDN for 112

7. Configure Vector 3 for Healthcare Number 1177

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

    Number: 3                Name: Healthcare_1177
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 silence
02 route-to     number 9463791177479    with cov n if unconditionally
03 stop
04
```

Figure 116: Vector for 1177

8. Configure VDN for Healthcare Number 1177

```
change vdn 1177                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                              Extension: 1177
                                  Name*: Healthcare_1177
                            Destination: Vector Number        3
                      Attendant Vectoring? n
                     Meet-me Conferencing? n
                       Allow VDN Override? n
                                     COR: 1
                                     TN*: 1
                               Measured: none


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

Figure 117: VDN for 1177

9. Configure Vector 4 for Police Number 11414

```
change vector 4                                                Page   1 of   6
                                  CALL VECTOR

    Number: 4                Name: Police-11414
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 silence
02 route-to     number 94637911414479   with cov n if unconditionally
03 stop
04
```

Figure 118: Vector for 11414

10. Configure VDN for Police Number 11414

```
change vdn 11414                                               Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                              Extension: 11414
                                  Name*: Police-11414
                            Destination: Vector Number        4
                      Attendant Vectoring? n
                     Meet-me Conferencing? n
                       Allow VDN Override? n
                                     COR: 1
                                     TN*: 1
                               Measured: none


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

Figure 119: VDN for 11414

15.1.2. Configure Session Manager – Dial Pattern

The example of dial pattern is defined in this configuration: **463**.

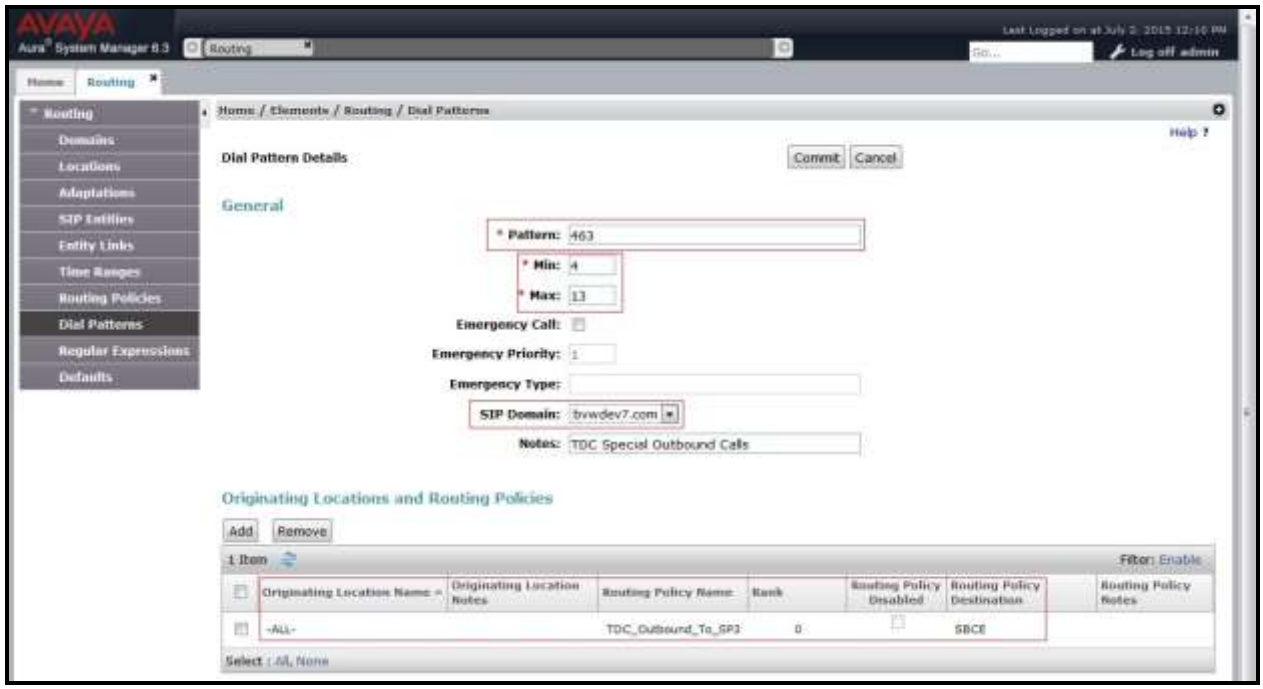

Figure 120: Dial Pattern_463

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.