Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.2, Avaya Aura® Session Manager R6.2 and Avaya Session Border Controller for Enterprise to Support Tele2 VoIP Connect SIP Trunking Service – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Tele2 VoIP Connect SIP Trunking Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Session Border Controller for Enterprise. Tele2 is a member of the DevConnect Global SIP 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.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Tele2 VoIP Connect Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Session Border Controller for Enterprise (Avaya SBCE). Customers using this Avaya SIP-enabled enterprise solution with the Tele2 VoIP Connect Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Session Border Controller for Enterprise. The enterprise site was configured to use the VoIP Connect service provided by Tele2.

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

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DDI numbers assigned by Tele2. Incoming PSTN calls were made to H.323, SIP and analogue telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via Tele2 to PSTN destinations.
- Outgoing calls from the enterprise to the PSTN were made from H.323, SIP and analogue telephones.
- Calls using G.711A and G.711mu codec's.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
- DTMF transmission using RFC 2833 with successful Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones, and the Avaya Desktop Video Device (Avaya DVD) running Flare Experience.
- Call coverage and call forwarding for endpoints at the enterprise site.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Tele2 VoIP Connect service with the following observations:

- Outgoing calls from SIP phones failed initially and required a script on the Avaya SBCE to remove unused headers and shorten the length of the INVITE
- Although G.729 is supported by the Tele2 network, it is not present in the SDP and is only successfully negotiated for outgoing calls from an analogue or digital phone. With this restriction, G729 can't be considered to be supported and the only supported codecs are G.711A and G.711mu.
- No test call was made to the Emergency Services Operator as no test was booked.
- Calls to an extension with call forwarding to a PSTN number fail intermittently when a 504 "Gateway Timeout" is received from the network. This is thought to occur when there is no number in the P-Asserted-ID prompting a subsequent SS7 CLI request. Resolved with Avaya SBCE script to insert Diversion number in PAID.
- When the trunk is busy or the signalling link is unavailable and a 5xx message is sent from Communication Manager or Session Manager, the network continues to send INVITEs and the caller gets no indication of call failure for some time.

2.3. Support

For technical support on Tele2 products please contact the Tele2 support team at: www.tele2.nl/zakelijk/customer-service.html Telephone number: +31 (0) 900 – 240 1602

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to Tele2 VoIP Connect. Located at the Enterprise site are the Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones and Avaya 16xx series IP telephones (with H.323 firmware), Avaya A175 Desktop Video Device running Flare Experience, Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone running on a laptop PC configured for H.323.

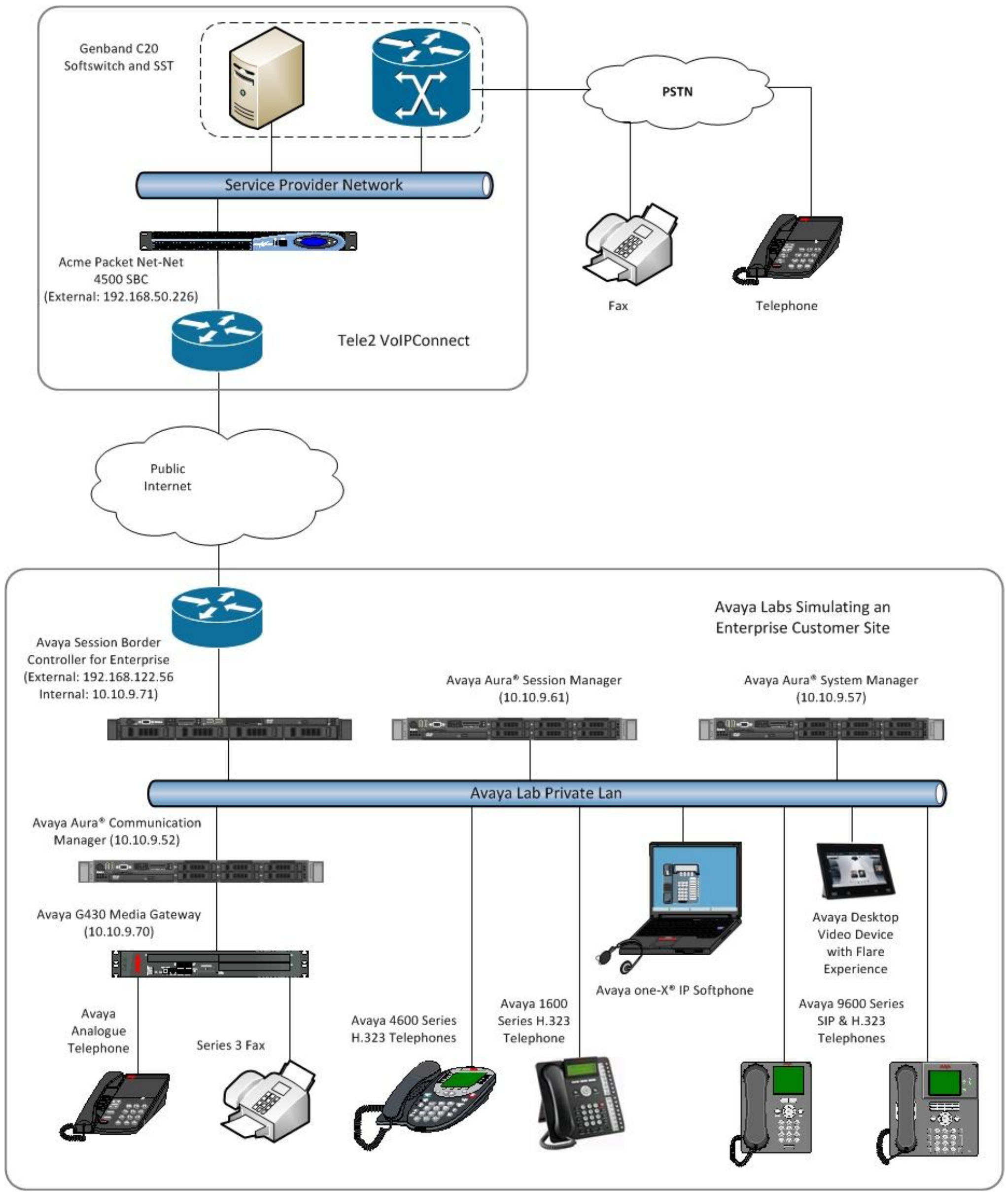


Figure 1: Tele2 VoIP Connect Solution Topology

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 Build R016x.02.0.823.0
Avaya G430 Media Gateway	FW 30.12.1
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 Build 6.2.0.0.620110
Avaya Aura® System Manager running on Avaya S8800 Server	R6.2 (System Platform 6.2.0.0.27, Template 6.2.12.0)
Avaya Session Border Controller running on Dell R210 V2 server	4.0.5.Q09
Avaya 1616 Phone (H.323)	1.301
Avaya 4621 Phone (H.323)	2.902
Avaya 9630 Phone (H.323)	3.103
Avaya A175 Desktop Video Device (SIP)	Flare Experience Release 1.1
Avaya 9630 Phone (SIP)	R2.6 SP6
Avaya one–X® Communicator (H.323) on Lenovo T510 Laptop PC	6.1.3.08-SP3-Patch2-35791
Analogue Phone	N/A
Tele2	
Acme Packet SBC Net-Net 4500	SCX6.2.0 MR-8 Patch 4 (Build 1005)
Nortel/Genband CS2K	SWC00012_PPC3_V125

5. Configure Avaya Aura ® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP signalling associated with the Tele2 VoIP Connect service. For incoming calls, the Session Manager receives SIP messages from the Avaya SBCE and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Tele2 network. 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. The general installation of the Avaya S8800 Servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

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. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the Tele2 network, and any other SIP trunks used.

```
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 3
             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 0
                       Maximum Administered SIP Trunks: 24000 20
  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
```

On **Page 4**, verify that the **IP Trunks** field is set to **y.**

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

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                        ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? y              Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? y                 Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                 Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM100** and **10.10.9.61** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
SM100               10.10.9.61
Sipera-SBC          10.10.9.71
default             0.0.0.0
procr               10.10.9.52
procr6              ::
```

5.3. Administer IP Network Region

Use the **change ip-network-region 1** command to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra**- and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the Avaya SBCE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** is used.

```
change ip-network-region 1                                        Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: default
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
```

5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form, **Section 5.3.** Enter the list of audio codecs eligible to be used in order of preference. For the interoperability test the codecs fully supported by Tele2 were configured, namely **G.711A**, and **G.711MU**.

```
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.711MU            n          2        20
 3:
```

The Tele2 VoIP Connect service supports T.38 for transmission of fax. Navigate to **Page 2** to configure T.38 by setting the **Fax Mode** to **t.38-standard** as shown below.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



                Mode                Redundancy
    FAX         t.38-standard        0
    Modem       off                  0
    TDD/TTY     US                   3
    Clear-channel   n                0
```

5.5. Administer SIP Signaling Groups

The signaling group (and trunk group) will be used for inbound and outbound PSTN calls to the Tele2 VoIP Connect service. During test, this was configured to use **TCP** and port **5060** to facilitate tracing and fault analysis. It is recommended however, to use TLS (Transport Layer Security) and the default TLS port of 5061 for security. Configure the **Signaling Group** using the **add signaling-group x** command, where **x** is an available signaling group, as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tcp**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signaling group as network region **1**)
- Leave **Far-end Domain** blank (allows the CM to accept calls from any SIP domain on the associated trunk)
- Set **Direct IP-IP Audio Connections** to **y**
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.

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

 Group Number: 1               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


   Near-end Node Name: procr                 Far-end Node Name: SM100
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1

Far-end Domain:
                                             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
```

5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group x** command, where **x** is an available trunk group. On **Page 1** of this form:

- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan (in the test system the dial plan includes 1 as a three digit dac – not shown)
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **public-netwrk**
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the **Number of Members** supported by this SIP trunk group

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

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: Group 1                     COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

On **Page 2** of the trunk-group form, the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed upon with Tele2 to prevent unnecessary SIP messages during call setup.

```
Add trunk-group 1                                                Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

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

 Disconnect Supervision - In? y  Out? y
```

On **Page 3**, set the **Numbering Format** field to **public**. This allows delivery of CLI in E.164 format with a leading "+".

```
add trunk-group 1                                                      Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

On **Page 4** of this form:

- Set **Send Transferring Party Information** to **y** to ensure that the transferring party number is sent. This information is used by the Tele2 network for call transfer.
- Set **Send Diversion Header** to **y** to ensure that the Diversion header is sent. This information is used by the Tele2 network for call forwarding.
- Set **Support Request History** to **n** to remove the History Info header. This information is not used and increases the size of the INVITE unnecessarily.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Tele2
- Set **Always Use re-INVITE for Display Updates** to **y** as the most effective method employed by Communication Manager of modifying an existing dialogue

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

                               Mark Users as Phone? n
                     Prepend '+' to Calling Number? n
           Send Transferring Party Information? y
                          Network Call Redirection? 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? y
            Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
                                     Enable Q-SIP? n
```

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number. In the test configuration, individual stations were mapped to send numbers allocated from the Tele2 DDI range supplied. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Note that the digits identifying the DDI range are not shown.

```
change public-unknown-numbering 0                                    Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext             Trk       CPN             CPN
Len Code            Grp(s)    Prefix          Len
                                                  Total Administered: 8
 4  2000            1         31207nnnnn0     11     Maximum Entries: 9999
 4  2291            1         31207nnnnn1     11
 4  2296            1         31207nnnnn2     11    Note: If an entry applies to
 4  2316            1         31207nnnnn3     11    a SIP connection to Avaya
 4  2346            1         31207nnnnn4     11    Aura(R) Session Manager,
 4  2396            1         31207nnnnn5     11    the resulting number must
 4  2400            1         31207nnnnn6     11    be a complete E.164 number.
 4  2601            1         31207nnnnn7     11
```

5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the Tele2 VoIP Connect service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

```
change feature-access-codes                                          Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *69
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 7
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
```

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to national, international and some Operator numbers. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

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

          Dialed            Total      Route     Call   Node  ANI
          String           Min  Max   Pattern    Type   Num   Reqd
    0                      8    14     1         pubu         n
    00                     13   17     1         pubu         n
    00353                  10   14     1         pubu         n
    0044                   12   14     1         pubu         n
    01                     7    14     1         pubu         n
    0800                   11   11     1         pubu         n
    118                    5    6      1         pubu         n
```

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**. Numbering Plan Indictor (NPI) of the Calling Party Number is set to E.164 and Type of Numbering (TON) is set to international by using **Numbering Format** of **intl-pub**.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: all calls
                             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: 1    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                                intl-pub  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
```

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Tele2 can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by Tele2 for testing are assigned to the internal extensions of the test equipment configured within the Communication Manager. The **change inc-call-handling-trmt trunk-group 1** command is used to translate numbers **+31207nnnnn0** to **+31207nnnnn9** to the 4 digit extension by deleting **all** of the incoming digits and inserting the extension number. Note that the significant digits beyond the city code have been obscured.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    12 +31207nnnnn0     all 2000
 public-ntwrk    12 +31207nnnnn1     all 2396
 public-ntwrk    12 +31207nnnnn2     all 2346
 public-ntwrk    12 +31207nnnnn3     all 2296
 public-ntwrk    12 +31207nnnnn4     all 2601
 public-ntwrk    12 +31207nnnnn5     all 2316
 public-ntwrk    12 +31207nnnnn6     all 2400
 public-ntwrk    12 +31207nnnnn7     all 6103
 public-ntwrk    12 +31207nnnnn8     all 2501
 public-ntwrk    12 +31207nnnnn9     all 2291
```

5.10. EC500 Configuration

When EC500 is enabled on the Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2396. Use the command **change off-pbx-telephone station mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386nnnnnnn**)
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing
- Set the **Config Set** to **1**

```
change off-pbx-telephone station-mapping 2396                   Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 1601             EC500         -     0035386nnnnnnn   1          1
                                -
```

Save Communication Manager changes by entering **save translation** to make them permanent.

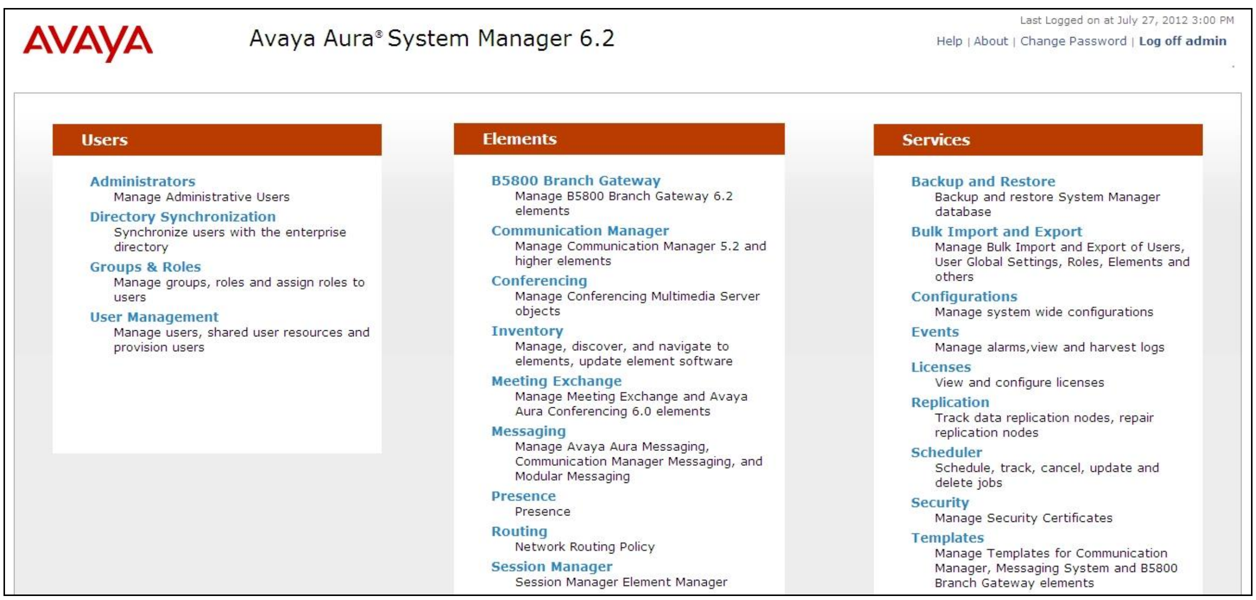
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured via the System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager
- Administer SIP Extensions

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN >/SMGR**, where <**FQDN**> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the Home tab will be presented with menu options shown below.

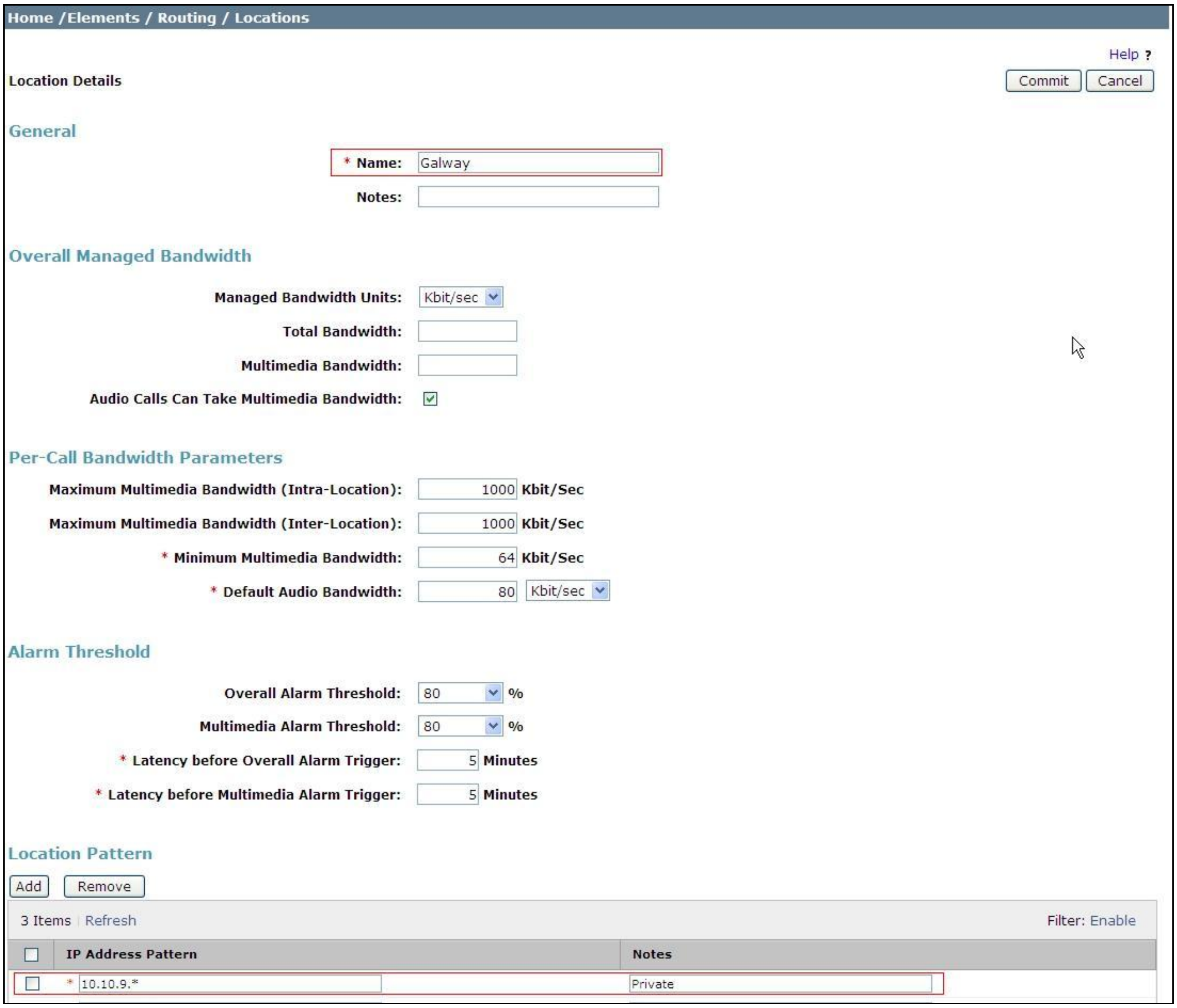


6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **avaya.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes.

6.3. Administer Locations

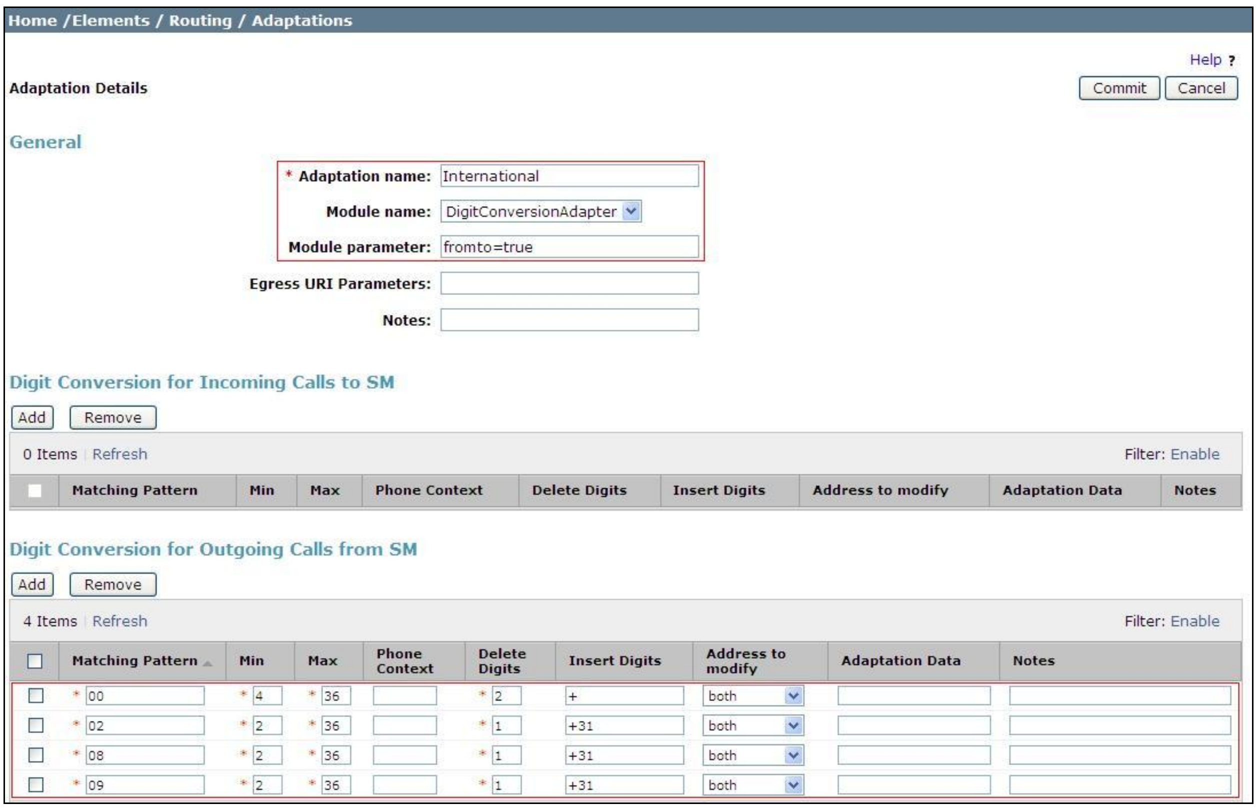
Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the test enterprise.



6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. Additionally, the called and calling party numbers can also be modified using **Digit Conversion** when **fromto=true** is entered in the **Module Parameters**. The example shown was used in test to convert the called numbers in the Request URI to E.164 format with leading zero according to the standard used by Tele2. In addition, the To header is converted to the same format to be consistent with the calling party numbers in the From header.

DigitConversionAdaptor is used and leading zeros are analysed. Both national and international numbers are converted with national numbers requiring the prefixing of the country code. The two leading zeros of the international number are removed and replaced with a "+".The single leading zero of the national number are removed and replaced with a "+31"These rules are applied to the destination addresses.



Home /Elements / Routing / Adaptations

Help ?

Adaptation Details

Commit Cancel

General

* Adaptation name: International

Module name: DigitConversionAdapter

Module parameter: fromto=true

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

Digit Conversion for Outgoing Calls from SM

Add Remove

4 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
	* 00	* 4	* 36		* 2	+	both		
	* 02	* 2	* 36		* 1	+31	both		
	* 08	* 2	* 36		* 1	+31	both		
	* 09	* 2	* 36		* 1	+31	both		

6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity. Under **General**:

- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **Gateway** for the Avaya SBCE SIP entity
- In the **Adaptation** field select the appropriate adaptation defined in **Section 6.4**, in test **International** was selected for the Avaya SBCE to convert called party numbers to E.164 format with a leading "+"
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

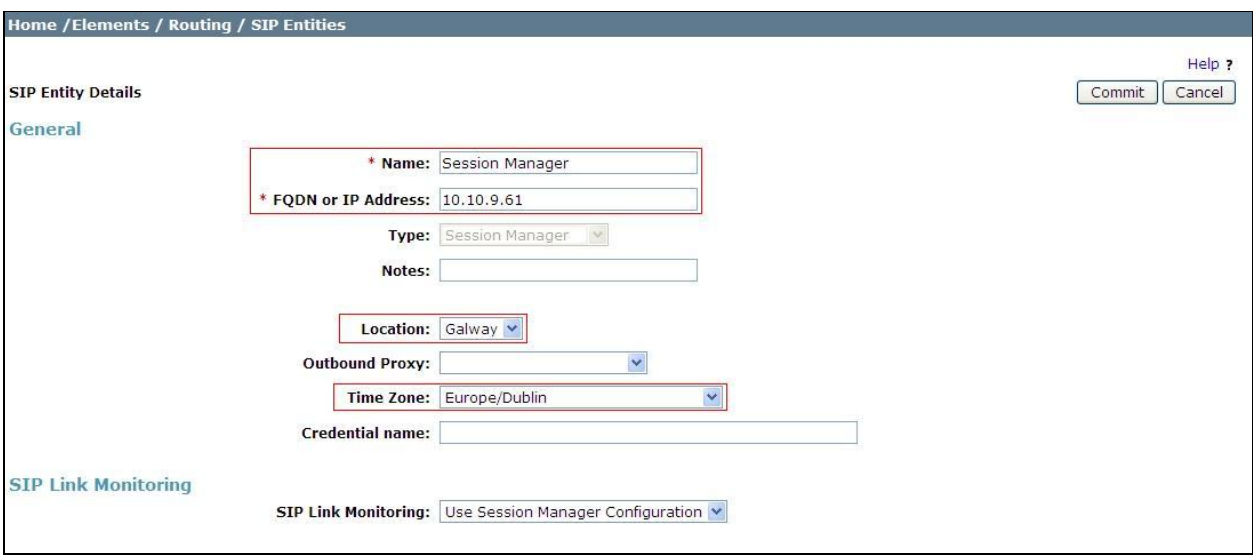
In this configuration there are three SIP Entities:

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

Note: Messaging is installed in the test system and is used for coverage tests but is not described in this Application Note.

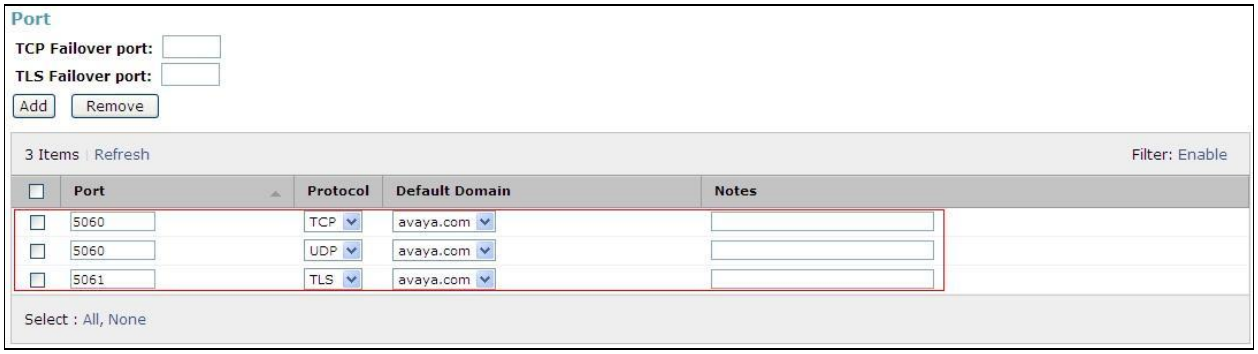
6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface.



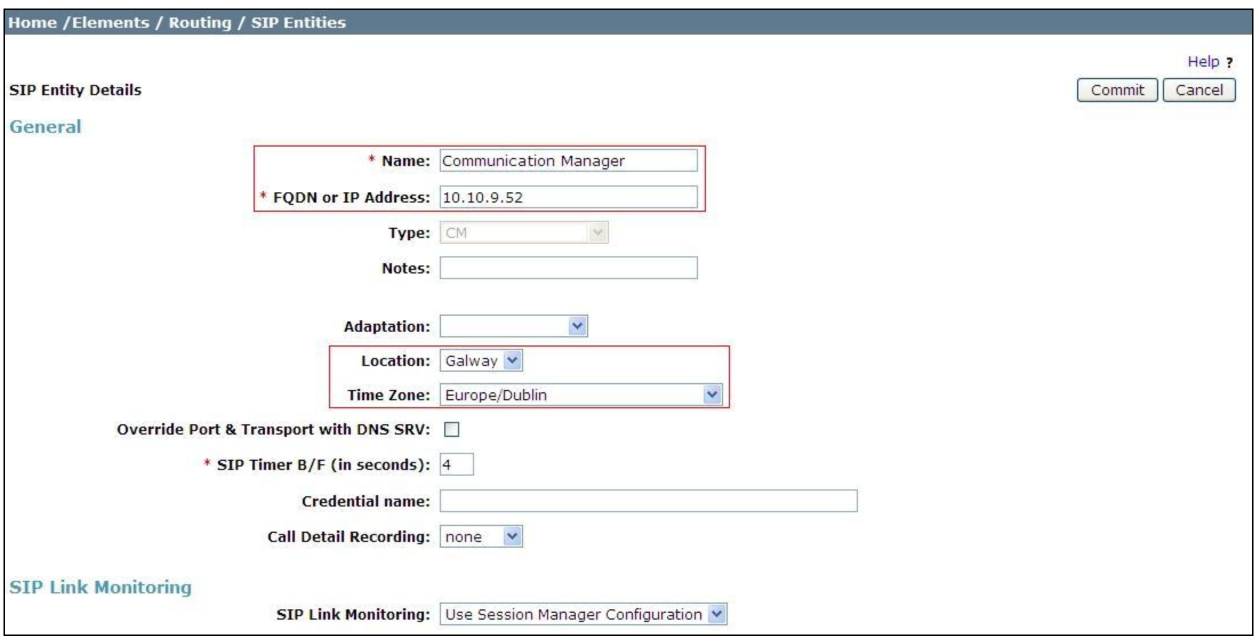
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these, scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field enter the port number on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol to be used for SIP requests
- In the **Default Domain** field, from the drop down menu select **avaya.com** as the default domain



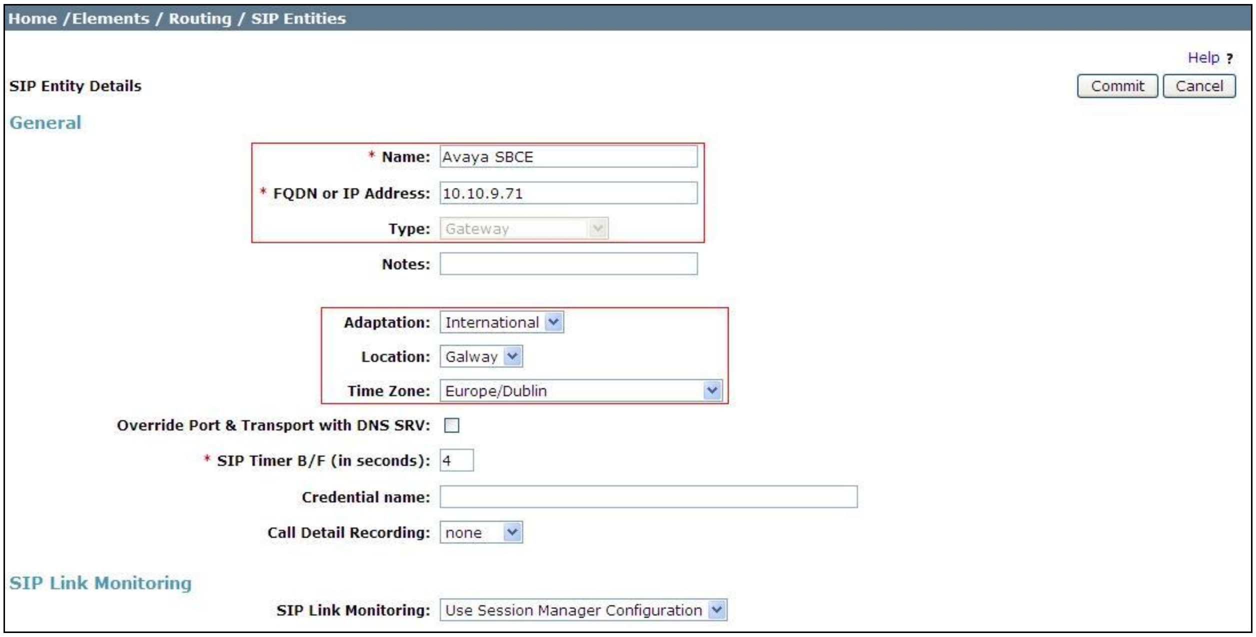
6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling.



6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Session Border Controller for Enterprise. The **FQDN or IP Address** field is set to the IP address of the Session Border Controller for Enterprise private network interface.

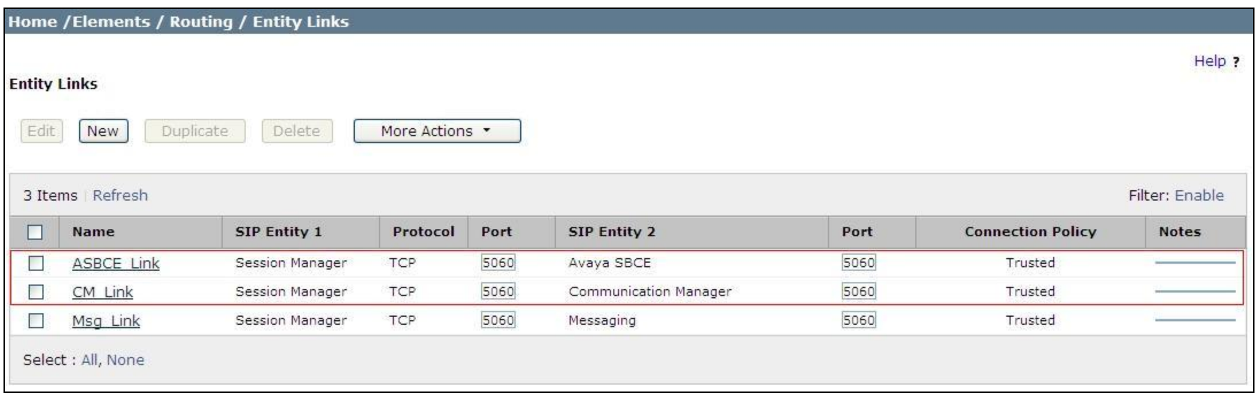


6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select the name given to the Session Manager Entity, in this case **Session Manager**
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- In the **Connection Policy** field enter **Trusted** to make the other system trusted
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in this configuration.


Home / Elements / Routing / Entity Links

Help ?

Entity Links

Edit | New | Duplicate | Delete | More Actions

3 Items | Refresh   Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
ASBCE_Link	Session Manager	TCP	5060	Avaya SBCE	5060	Trusted	
CM_Link	Session Manager	TCP	5060	Communication Manager	5060	Trusted	
Msg_Link	Session Manager	TCP	5060	Messaging	5060	Trusted	

Select : All, None

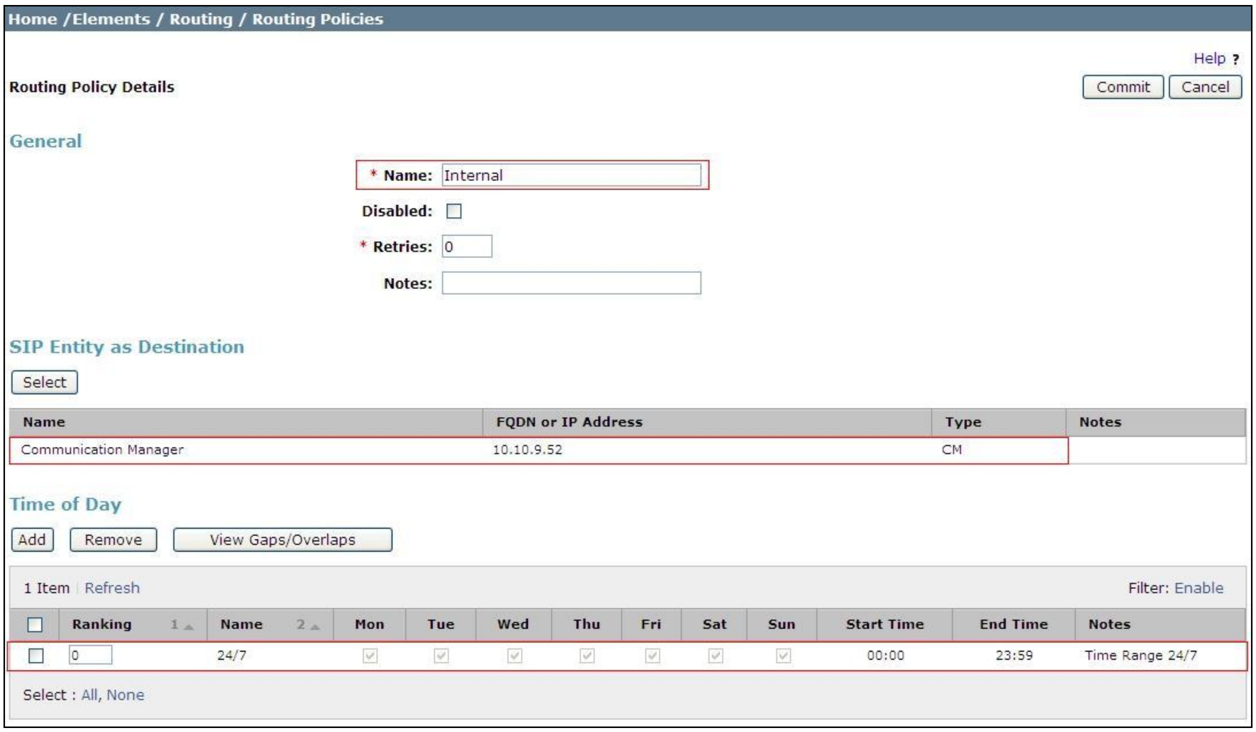
6.7. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

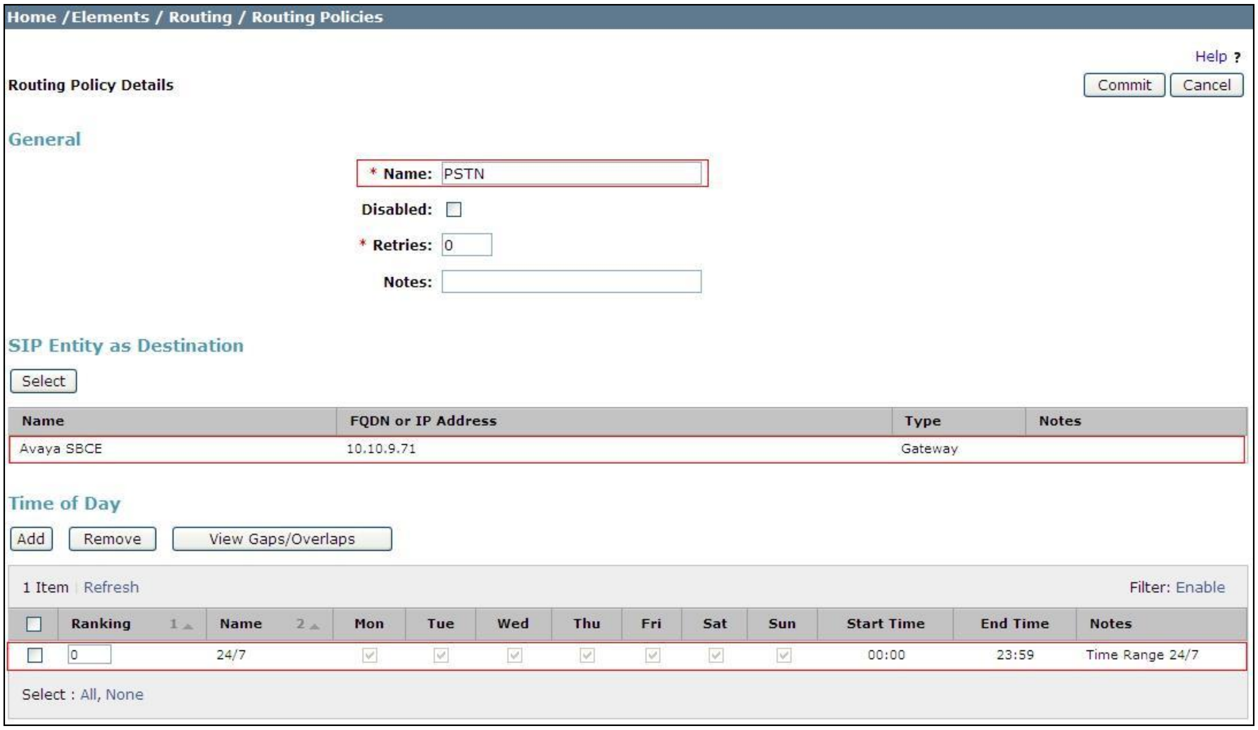
Under **General**:

- Enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies
- Under **Time of Day**, click **Add**, and then select the time range

The following screen shows the routing policy for Communication Manager.



The following screen shows the routing policy for the Session Border Controller.



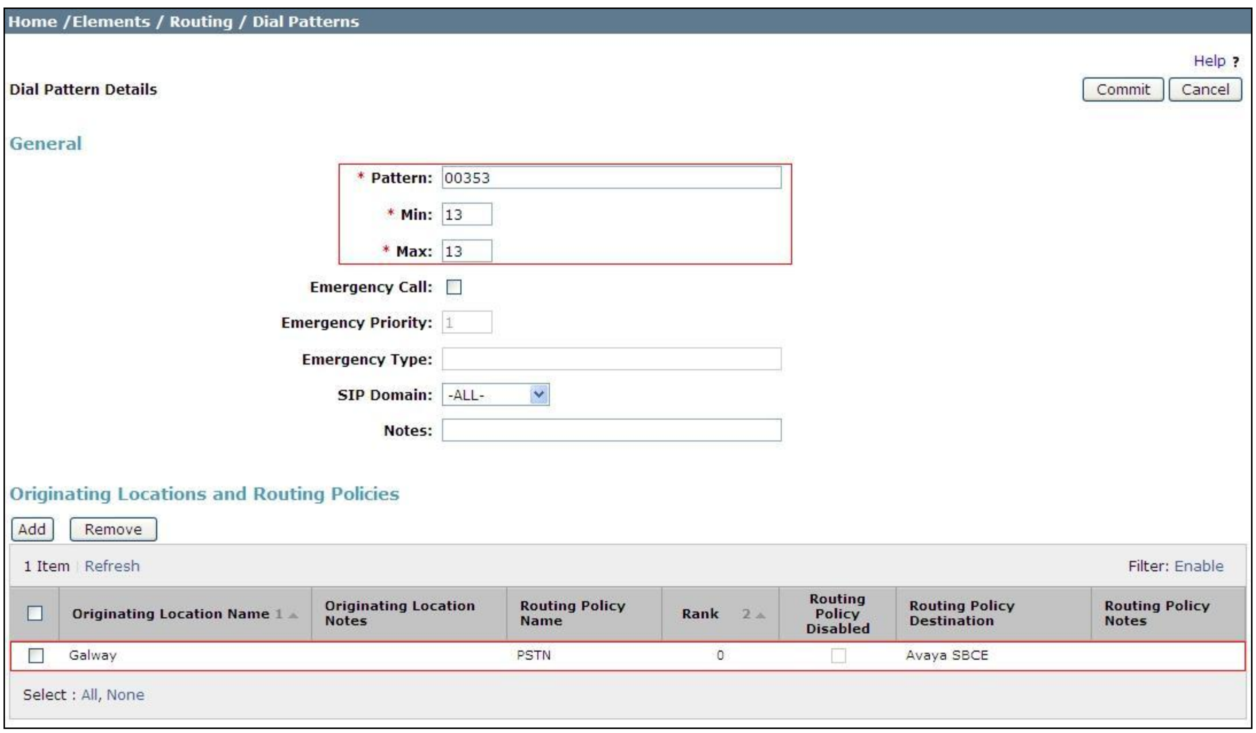
6.8. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

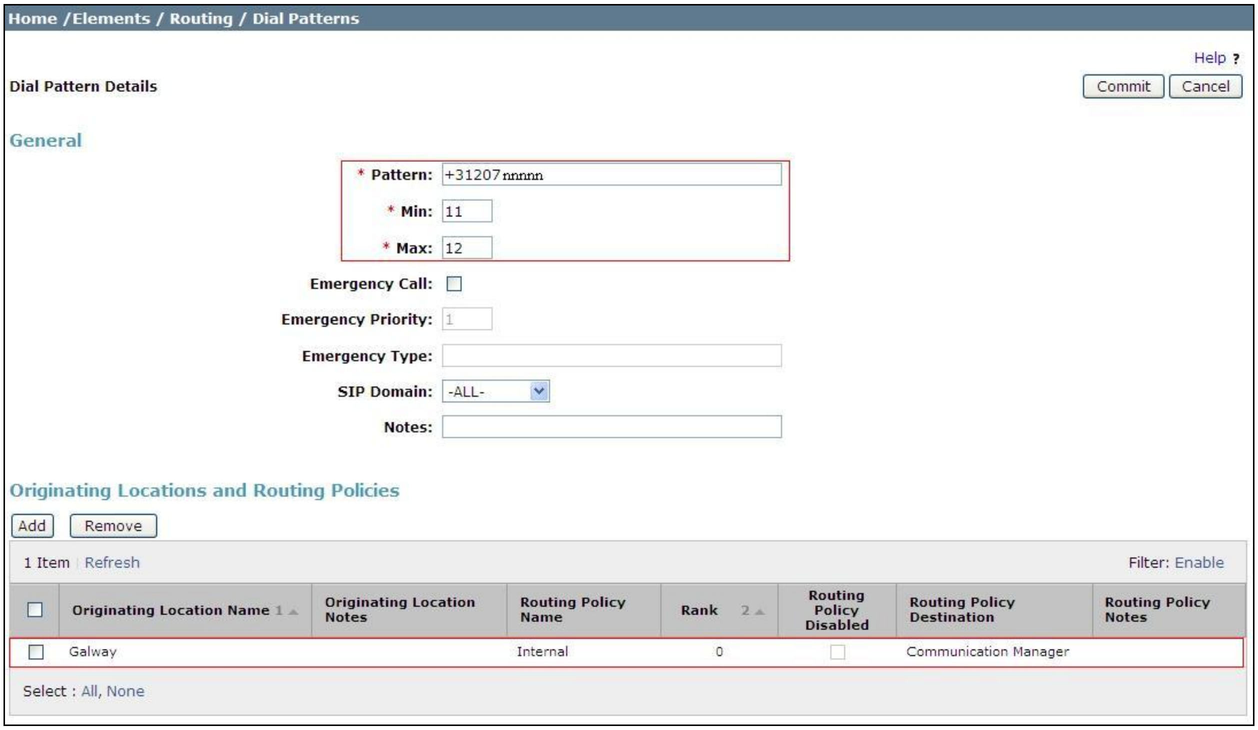
Under **General**:

- In the **Pattern** field enter a dialled number or prefix to be matched
- In the **Min** field enter the minimum length of the dialled number
- In the **Max** field enter the maximum length of the dialled number
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**

Under **Originating Locations and Routing Policies**, click **Add**. In the resulting screen (not shown), under **Originating Location** select **ALL** and under **Routing Policies** select one of the routing policies defined in **Section 6.7**. Click the **Select** button to save. The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the PSTN via the Tele2 VoIP Connect service.



The following screen shows the test dial pattern configured for Communication Manager. Note that the number format received from Tele2 was E.164 with leading +. The least significant digits have been obscured.



6.9. Administer Application for Avaya Aura® Communication Manager

From the Home tab, select **Session Manager** from the menu. In the resulting tab from the left panel menu, select **Application Configuration → Applications** and click **New**.

- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Communication Manager
- In the **CM System for SIP Entity** field select the SIP entity for the Communication Manager

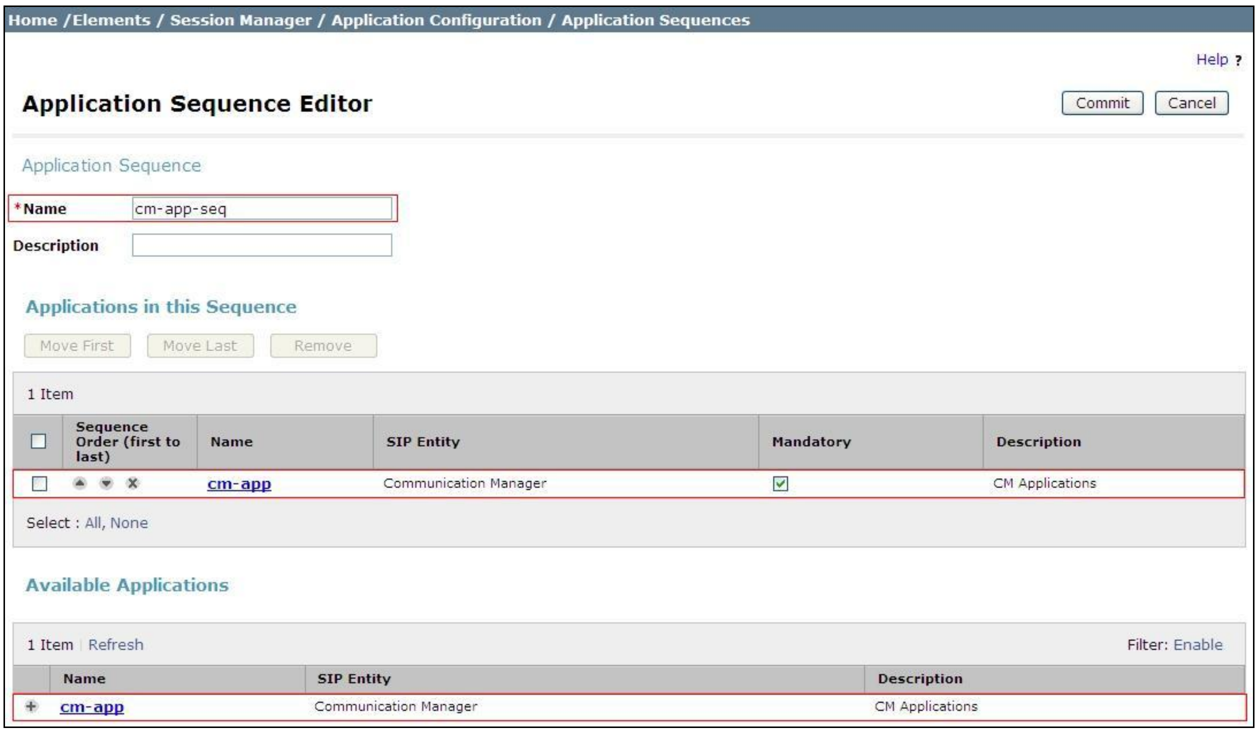
Select **Commit** to save the configuration.

6.10. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel, navigate to **Session Manager → Application Configuration → Application Sequences** and click on **New**.

- In the **Name** field enter a descriptive name
- Under **Available Applications**, click the + sign in front of the appropriate application instance. When the screen refreshes, the application should be displayed under the **Applications in this Sequence** heading.

Select **Commit**.

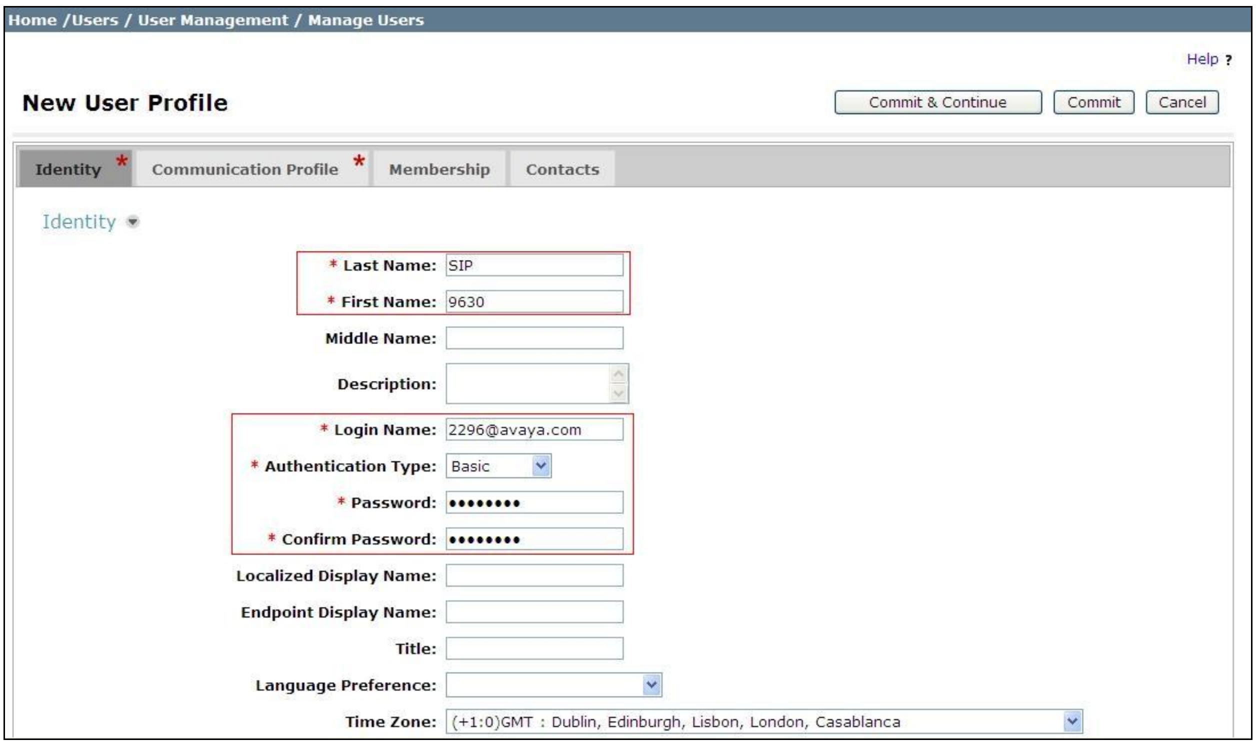


6.11. Administer SIP Extensions

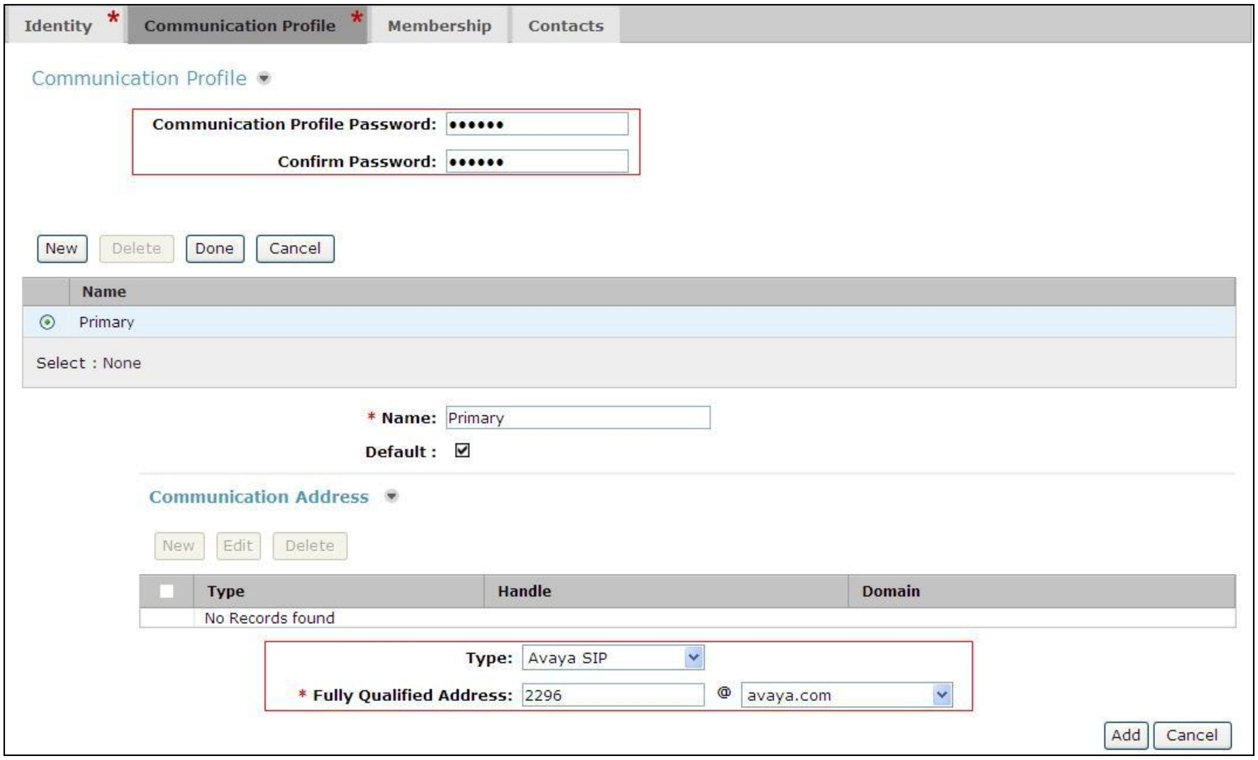
SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the Home tab, select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of **user@domain** (e.g. **2296@avaya.com**) which is used to create the user's primary handle
- The **Authentication Type** should be **Basic**
- In the **Password/Confirm Password** fields enter an alphanumeric password

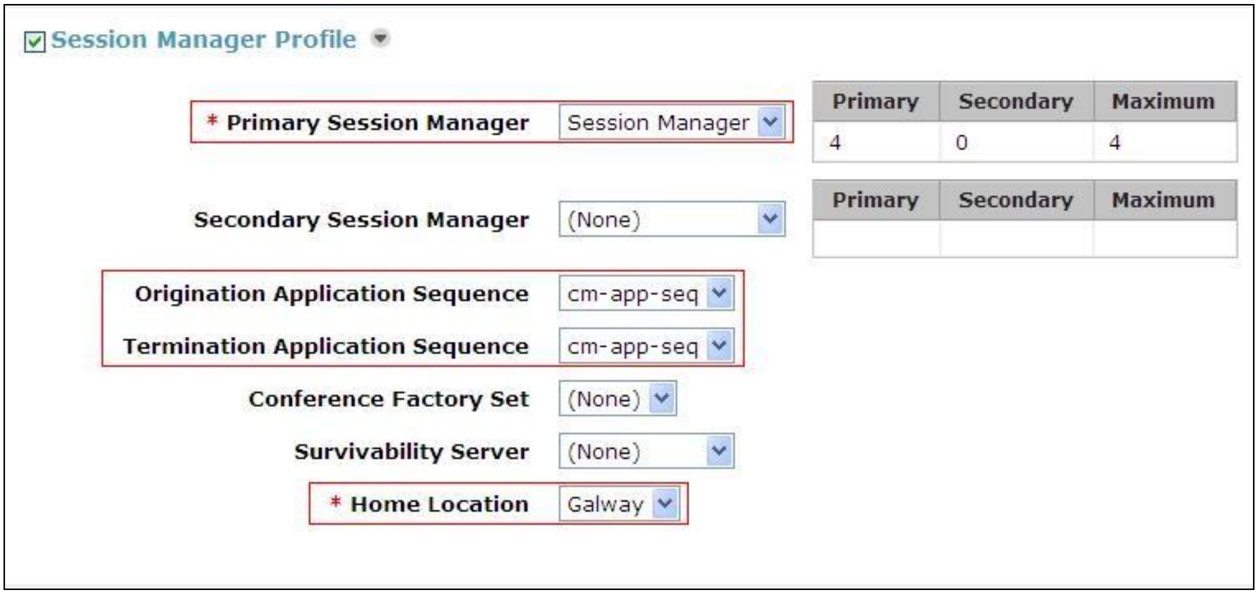


On the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it, then expand the **Communication Address** section and click **New**. For the **Type** field, select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.



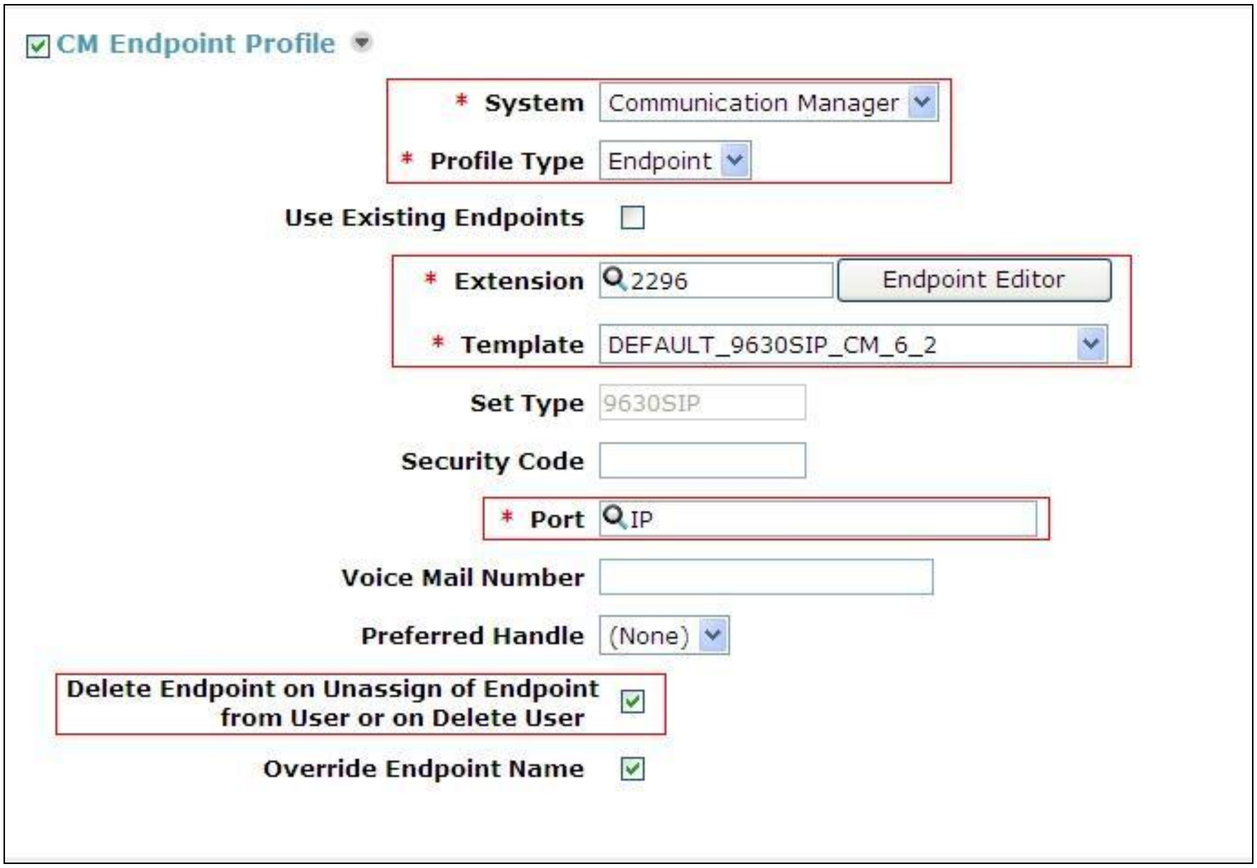
Expand the **Session Manager Profile** section.

- Make sure the **Session Manager** check box is checked
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field
- Select the appropriate application sequence from the drop-down menu in the **Origination Application Sequence** field configured in **Section 6.9**
- Select the appropriate application sequence from the drop-down menu in the **Termination Application Sequence** field configured in **Section 6.9**
- Select the appropriate location from the drop-down menu in the **Home Location** field



Expand the **Endpoint Profile** section.

- Select the Communication Manager SIP Entity from the **System** drop-down menu
- Select **Endpoint** from the drop-down menu for **Profile Type**
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- For the **Port** field select **IP**
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box
- Select **Commit** to save changes and the System Manager will add the Communication Manager user configuration automatically



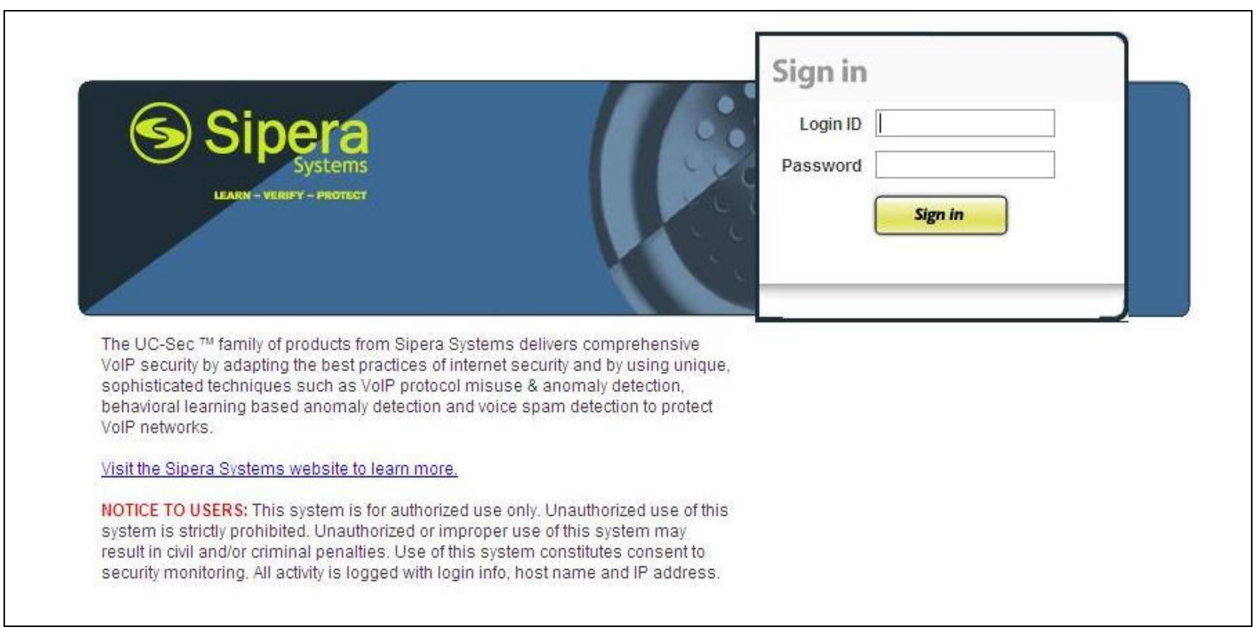
7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Session Border Controller for Enterprise. At the time of writing the Avaya Session Border Controller for Enterprise was badged as the Sipera E-SBC (Enterprise Session Border Controller) developed for Unified Communications Security (UC-Sec). The Avaya Session Border Controller for Enterprise is administered using the UC-Sec Control Center.

7.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. Select the **UC-Sec Control Center.**

Log in with the appropriate credentials.

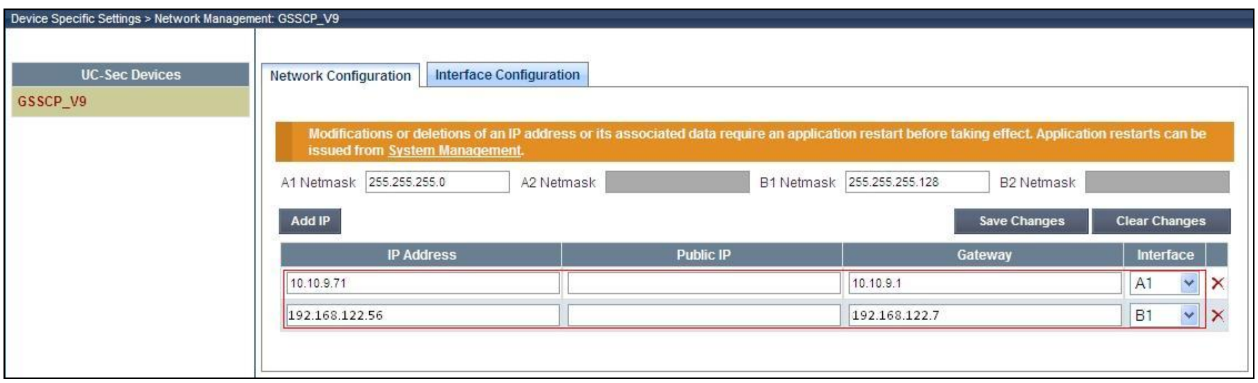


7.2. Define Network Information

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have multiple IP addresses, but these can only be assigned to one interface.

To define the network information, navigate to **Device Specific Settings → Network Management** in the **UC-Sec Control Center** menu on the left hand side and click on **Add IP**. Enter details in the blank box that appears at the end of the list

- Define the internal IP address with screening mask and assign to interface **A1**
- Select **Save Changes** to save the information
- Click on **Add IP**
- Define the external IP address with screening mask and assign to interface **B1**
- Select **Save Changes** to save the information
- Click on **System Management** in the main menu
- Select **Restart Application** indicated by an icon in the status bar (not shown)



Select the **Interface Configuration** tab and click on **Toggle State** to enable the interfaces.

7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

7.3.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Signaling Interface** in the **UC-Sec Control Center** menu on the left hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here

- Select **Add Signaling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal signalling interface
- For **Signaling IP**, select an **internal** signalling interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is used for the Session Manager
- Select **Add Signaling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external signalling interface
- For **Signaling IP**, select an **external** signalling interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is used for Tele2

7.3.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Media Interface** in the **UC-Sec Control Center** menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface
- For **Media IP**, select an **internal** media interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external media interface
- For **Media IP**, select an **external** media interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the Tele2 SBC

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the Tele2 SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the **UC-Sec Control Center** menu on the left hand side. To define Server Interworking for the Session Manager, highlight the **avaya-ru** profile which is a factory setting appropriate for Avaya equipment and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown)

- In the **Clone Name** field enter a descriptive name for the Session Manager and click **Finish** – in test **ASM9** was used
- Select **Edit** and enter details in the pop-up menu.
- Check the **T.38** box
- Change the **Hold Support** RFC to **RFC2543** then click **Next** and **Finish**

To define Server Interworking for the Tele2 SBC, highlight the previously defined profile for the Session Manager and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown)

- In the **Clone Name** field enter a descriptive name for server interworking profile for the Tele2 SBC and click **Finish** – in test **Tele2_Trunk** was used
- Select **Edit** and enter details in the pop-up menu
- Check the **T.38** box
- Select **Next** three times and **Finish**

7.5. Define Signalling Manipulation

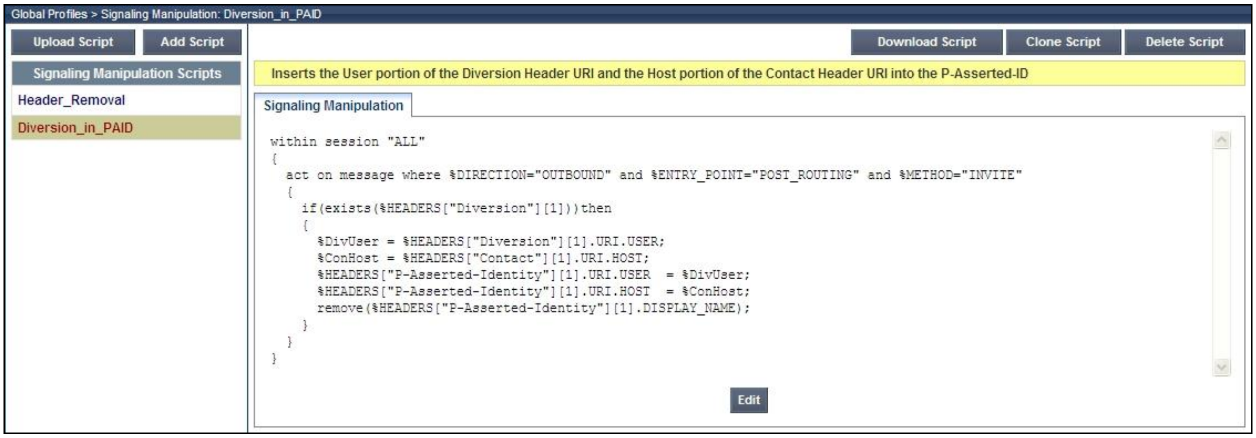
Signalling manipulation is required in some cases to ensure effective interworking. During test, some issues were found in the interworking between Tele2 VoIP Connect service and the enterprise that were resolved using signalling manipulation**.** The first issue is that call forwarding to a PSTN number was failing intermittently with a SIP 504 “Gateway Timeout” message from the network. This was happening when no number was present in the P-Asserted-ID field and subsequently the CLI was missing from the SS7 signalling causing a request for CLI from the far end. The solution was to take the number from the Diversion header and insert it into the P-Asserted-ID.

The second issue is that calls from SIP phones were failing, apparently because of additional information in the INVITE. The solution was to remove unused headers from the INVITE.

To define the signalling manipulation to take the user portion of the Diversion header and insert it into the P-Asserted-ID header, navigate to **Global Profiles → Signaling Manipulation** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Script** and enter a title and the script in the script editor. The title in the example is **Diversion_in_PAID**. The script text is as follows:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and
%METHOD="INVITE"
  {
    if(exists(%HEADERS["Diversion"][1]))then
    {
      %DivUser = %HEADERS["Diversion"][1].URI.USER;
      %ConHost = %HEADERS["Contact"][1].URI.HOST;
      %HEADERS["P-Asserted-Identity"][1].URI.USER  = %DivUser;
      %HEADERS["P-Asserted-Identity"][1].URI.HOST  = %ConHost;
      remove(%HEADERS["P-Asserted-Identity"][1].DISPLAY_NAME);
    }
  }
}
```

Once entered and saved, the script appears as shown in the following screenshot:

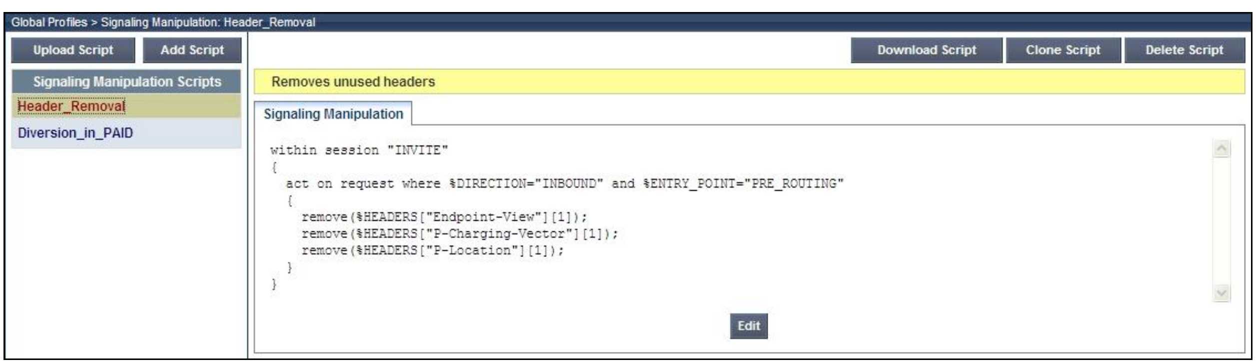


Note: This script relies on the existence of the Diversion header. This is included for the forwarded calls by configuration of the Communication Manager as described in **Section 5.6**

To define the signalling manipulation to remove the unused headers, navigate to **Global Profiles → Signaling Manipulation** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Script** and enter a title and the script in the script editor. The script text is as follows:

```
within session "INVITE"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Endpoint-View"][1]);
    remove(%HEADERS["P-Charging-Vector"][1]);
    remove(%HEADERS["P-Location"][1]);
  }
}
```

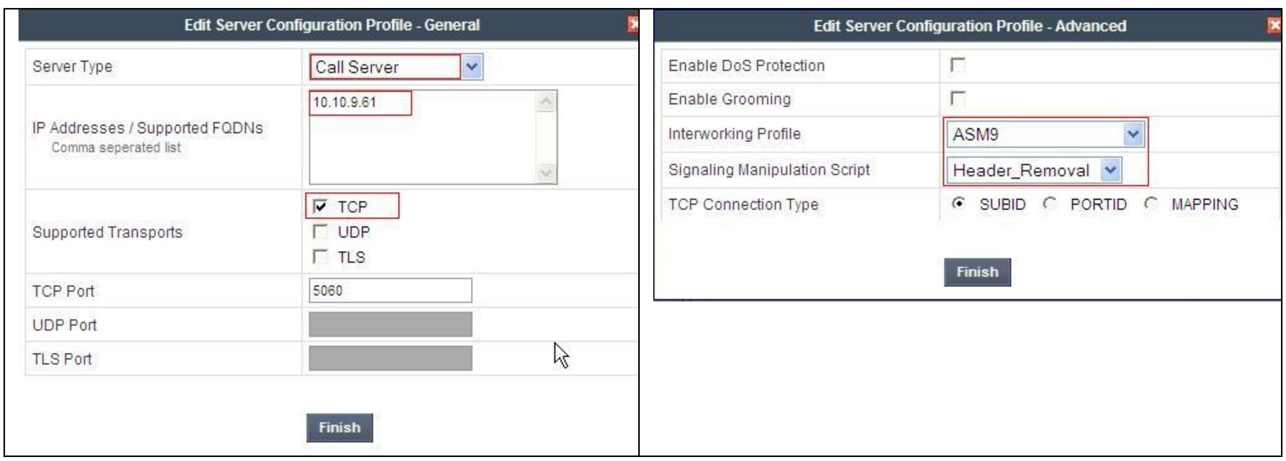
Once entered and saved, the script appears as shown in the following screenshot:



7.6. Define Servers

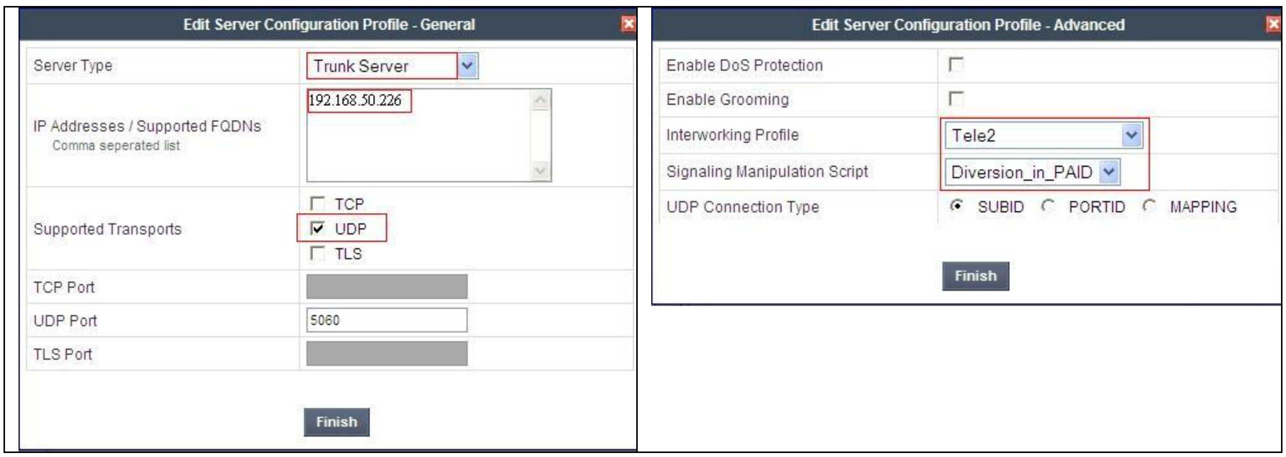
Servers are defined for each server connected to the Avaya SBCE. In this case, the Tele2 SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the Session Manager, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next** (not shown)
- Select **Call Server** from the **Server Type** drop down menu
- In the **IP Addresses / Supported FQDNs** box, type the Session Manager SIP interface address which is the same as that defined on the Communication Manager in **Section 5.2**
- Check **TCP** in **Supported Transports**
- Define the **TCP** port for SIP signalling, **5060** is used for the Session Manager
- Click **Next** three times then select the **ASM9** Session Manager interworking profile defined in **Section 7.4** from the **Interworking Profile** drop down menu
- Select the **Header Removal** script defined in **Section 7.5** from the **Signalling Manipulation Script** drop down menu



To define the Tele2 SBC as a Trunk Server, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for the Tele2 SBC and click **Next** (not shown)
- Select **Trunk Server** from the **Server Type** drop down menu,
- In the **IP Addresses / Supported FQDNs** box, type the IP address of the Tele2 SBC
- Check **UDP** in **Supported Transports**
- Define the **UDP** port for SIP signaling, **5060** is used for Tele2
- Click **Next** three times then select the **Tele2** SBC interworking profile defined in **Section 7.4** from the **Interworking Profile** drop down menu
- Select the **Diversion_in_PAID** script defined in **Section 7.5** from the **Signalling Manipulation Script** drop down menu

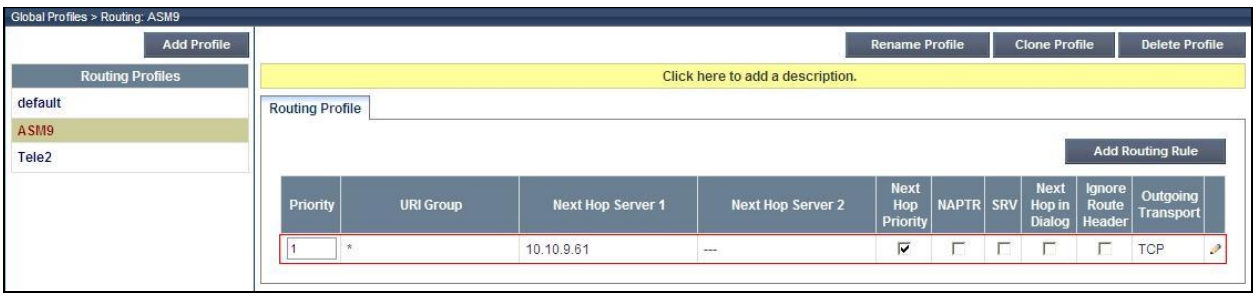


7.7. Define Routing

Routing information is required for routing to the Session Manager on the internal side and the Tele2 SBC on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used. To define routing to the Session Manager, navigate to **Global Profiles → Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu (not shown).

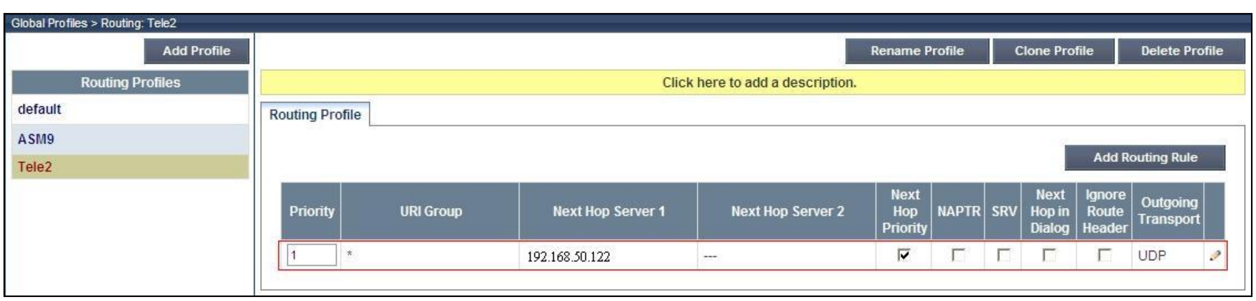
- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- Enter the Session Manager SIP interface address and port in the **Next Hop Server 1** field
- Select **TCP** for the **Outgoing Transport**
- Click **Finish**

Note: Port is not required in the next hop IP address if default value 5060 is used.



To define routing to the Tele2 SBC, navigate to **Global Profiles → Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Tele2 SBC and click **Next**
- Enter the Tele2 SBC IP address and port in the **Next Hop Server 1** field
- Select **UDP** for the **Outgoing Transport**
- Click **Finish**



7.8. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**; this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from the Session Manager. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for the Session Manager, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- If the **Record-Route and Via** Headers aren't shown, click on **Add Header** and **s**elect from the **Header** drop down menu
- For both of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **Request-Line**, **From**, **To** and **SDP** Headers aren't shown, click on **Add Header** and **s**elect from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten)
- For each of the headers leave the **Replace Action** at the default value of **Auto**

Note: The use of **Auto** results in an IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used where appropriate, and the required domain names entered in the **Overwrite Value** field. Different domain names could be used for the enterprise and the Tele2 network.

To define Topology Hiding for the Tele2 SBC, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the Tele2 SBC and click **Next**
- If the **Request-Line** header isn't shown, click on **Add Header** and **s**elect from the **Header** drop down menu
- Select the required action from the **Replace Action** drop down menu, **Auto** was used for test
- If the **Record-Route and Via** Headers aren't shown, click on **Add Header** and **s**elect from the **Header** drop down menu
- For both of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **From**, **To** and **SDP** Headers aren't shown, click on **Add Header** and **s**elect from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten)
- For each of the headers leave the **Replace Action** at the default value of **Auto**

7.9. Signalling Rules

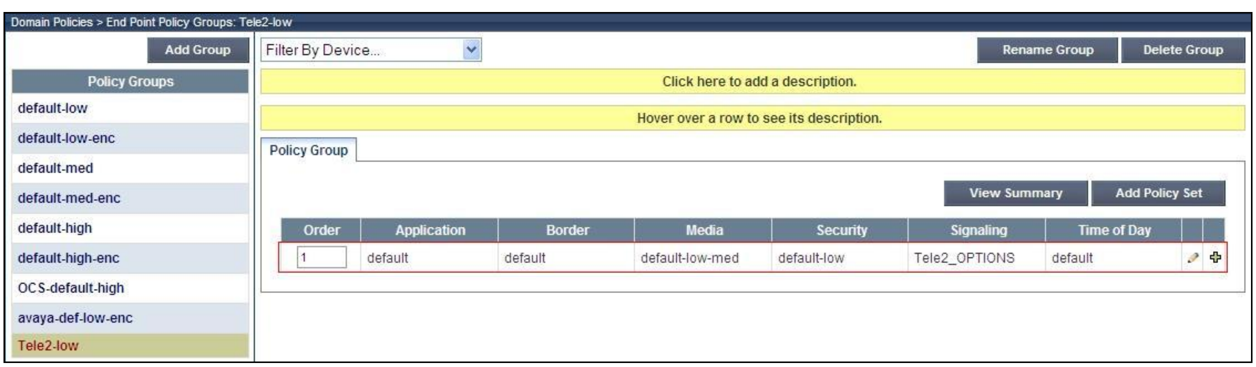
Signalling rules are a mechanism on the Avaya SBCE to handle any unusual signalling scenarios that may be encountered for a particular Service Provider. In the case of Tele2 the network is sending OPTIONS messages that are being passed on to the Session Manager which is not responding with a 200OK. A signalling rule is required to block the OPTIONS with a 200 OK which means the response is coming from the Avaya SBCE rather than the Session Manager

To define the signalling rule, navigate to **Domain Policies →Signalling Rules** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Rule** and enter details in the **Signalling Rule** pop-up box

- In the **Rule Name** field enter a descriptive name for the Tele2 signalling rule and click **Next** and **Next** again, then **Finish**
- Click on the **Requests** tab
- Click on the **Add In Request Control**
- Select **OPTIONS** from the **Method Name** drop down menu
- Select **Block with** from the **In Dialog Action** drop down menu
- Define the response code as **200** and the text field as **OK**
- Select **Block with** from the **Out of Dialog Action** drop down menu
- Define the response code as **200** and the text field as **OK**
- Click **Finish**

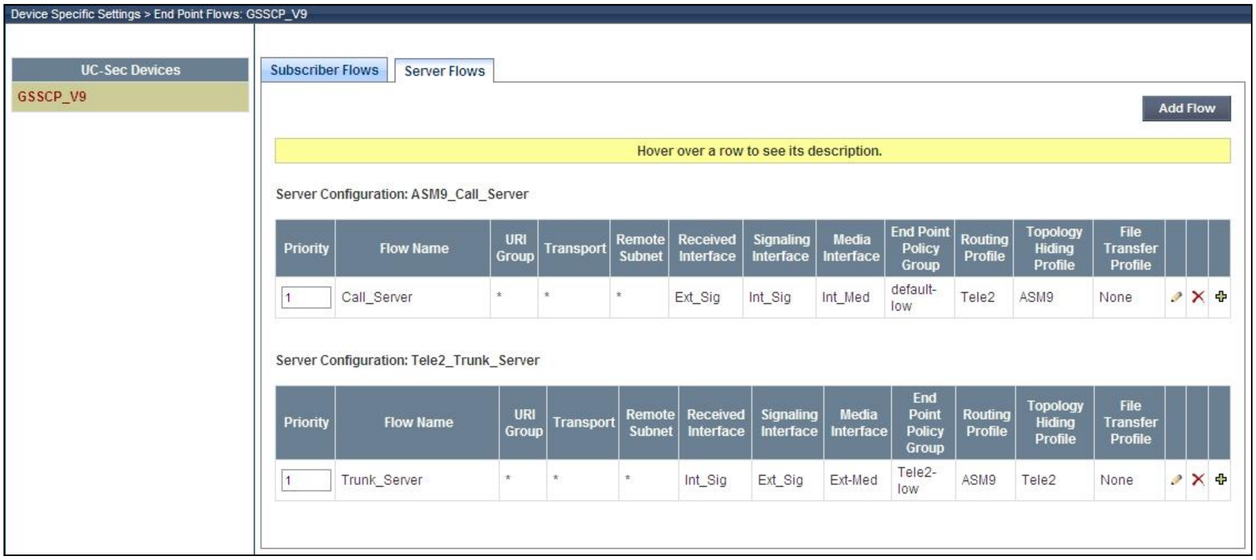
An End Point Policy Group is required to implement the signalling rule. To define this, navigate to **Domain Policies → End Point Policy Groups** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Group** and enter details in the **Policy Group** pop-up box

- In the **Group Name** field enter a descriptive name for the Tele2 Policy Group, in this case **Tele2-low**, and click **Next**
- Leave the **Application**, **Border**, **Media**, **Security** and **Time of Day** fields at their default values
- In the **Signaling** drop down menu, select the recently added signalling rule for Tele2 (**Tele2_OPTIONS)**
- In the **Time of Day** drop down menu, select **default**



7.10. Server Flows

Server Flows combine the previously defined profiles into an outgoing flow from the Session Manager to the Tele2 SBC and an incoming flow from the Tele2 SBC to the Session Manager. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to the Tele2 SBC and vice versa. The information for all Server Flows is shown on a single screen on the Avaya SBCE.



To define Server Flows, navigate to **Device Specific Settings → End Point Flows**. Click on the **Server Flows** tab and define Server Flows for both the Call Server (Session Manager) and Trunk Server (Tele2 SBC)

Define the Trunk Server as follows:

- In the **Name** field enter a descriptive name for the outgoing server flow to the Tele2 SBC
- In the **Server Configuration** drop-down menu, select the **Tele2_Trunk_Server** defined in **Section 7.6**
- In the **Received Interface** drop-down menu, select the **Int_Sig** internal SIP signalling interface defined in **Section 7.3**
- In the **Signaling Interface** drop-down menu, select the **Ext_Sig** external SIP signalling interface defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the **Ext-Med** external media interface defined in **Section 7.3**
- In the **End Point Policy Group** drop-down menu, select the **Tele2-low** policy group defined in **Section 7.9**
- In the **Routing Profile** drop-down menu, select the **ASM9** routing profile of the Session Manager defined in **Section 7.7**
- In the **Topology Hiding Profile** drop-down menu, select the **Tele2** topology hiding profile of the Tele2 SBC defined in **Section 7.8** and click **Finish**

Server Configuration: Tele2_Trunk_Server

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile
1	Trunk_Server	*	*	*	Int_Sig	Ext_Sig	Ext-Med	Tele2-low	ASM9	Tele2	None

Define the Call Server as follows:

- In the **Name** field enter a descriptive name for the incoming server flow to the Session Manager
- In the **Server Configuration** drop-down menu, select the **ASM9_Call_Server** defined in **Section 7.6**
- In the **Received Interface** drop-down menu, select the **Ext_Sig** external SIP signalling interface defined in **Section 7.3**
- In the **Signaling Interface** drop-down menu, select the **Int_Sig** internal SIP signalling interface defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the **Int_Med** internal media interface defined in **Section 7.3**
- In the **Routing Profile** drop-down menu, select the **Tele2** routing profile of the Tele2 SBC defined in **Section 7.6**
- In the **Topology Hiding Profile** drop-down menu, select the **ASM9** topology hiding profile of the Session Manager defined in **Section 7.7** and click **Finish**

Server Configuration: ASM9_Call_Server

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile
1	Call_Server	*	*	*	Ext_Sig	Int_Sig	Int_Med	default-low	Tele2	ASM9	None

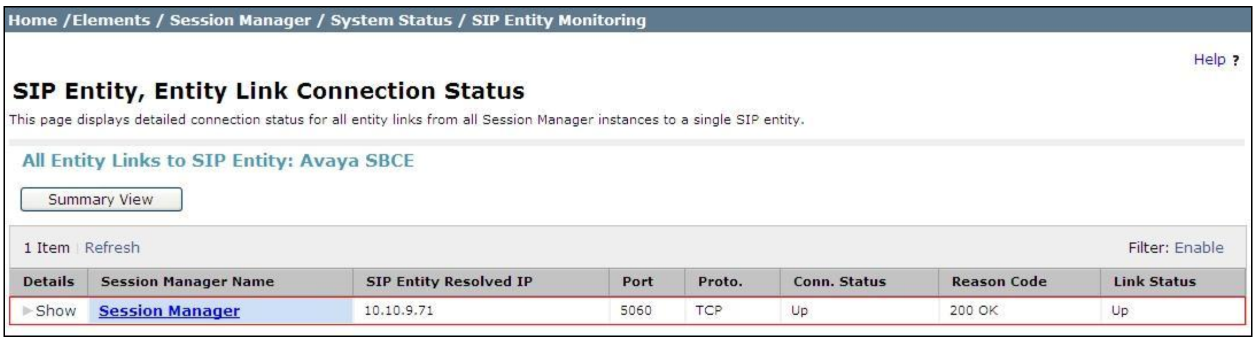
8. Tele2 Configuration

The configuration required by Tele2 to allow the tests to be carried out is not covered in this document and any further information required should be obtained through the local Tele2 representative.

9. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager Home Tab click on Session Manager and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**. The screenshot shows the status of the Entity Link for the Avaya SBCE

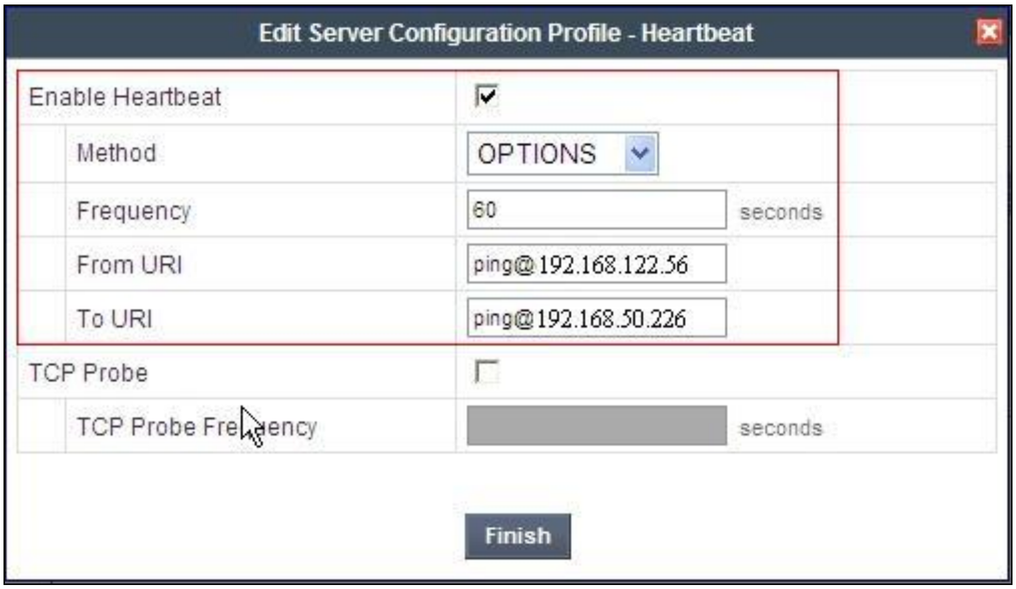


2. From the Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/idle**.

```
status trunk 1

                              TRUNK GROUP STATUS

Member    Port     Service State       Mtce Connected Ports
                                       Busy

0001/001 T00001   in-service/idle     no
0001/002 T00002   in-service/idle     no
0001/003 T00003   in-service/idle     no
0001/004 T00004   in-service/idle     no
0001/005 T00005   in-service/idle     no
0001/006 T00006   in-service/idle     no
0001/007 T00007   in-service/idle     no
0001/008 T00008   in-service/idle     no
0001/009 T00009   in-service/idle     no
0001/010 T00010   in-service/idle     no
```

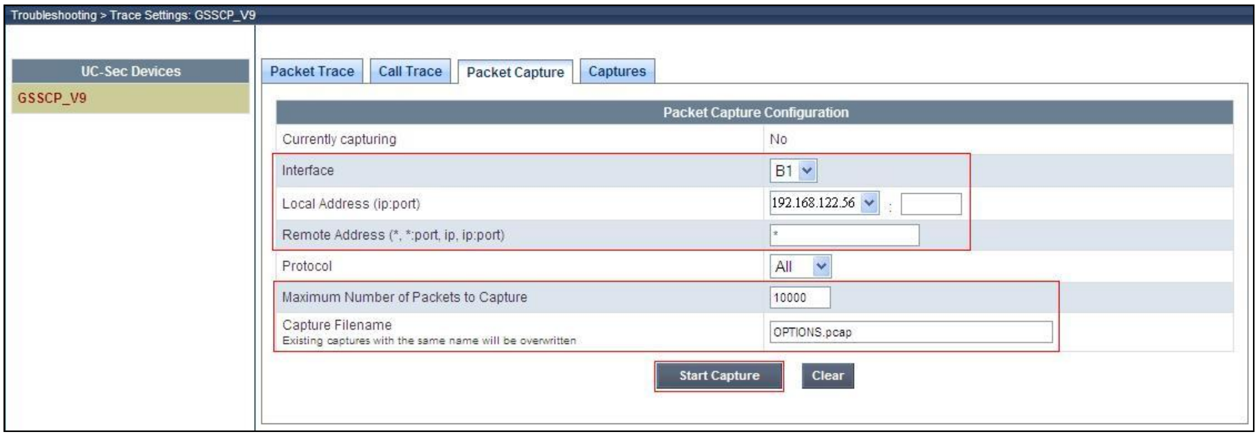
3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.

5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Should issues arise with the SIP trunk, check from the Avaya SBCE using OPTIONS. This is done by defining the heartbeat in the Server configuration then running a trace. To define the heartbeat, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side and click on the Trunk Server profile. Select the **Heartbeat** tab and click on **Edit**
   - Check the **Enable Heartbeat** box
   - Select **OPTIONS** from the **Method** drop down menu
   - Enter the **Frequency** in seconds, for convenience this can be set to the minimum value of **60** seconds
   - Enter the **From URI** in Fully Qualified Domain Name format
   - Enter the **To URI** in FQDN
   - Click on **Finish**



To define the trace, navigate to **Troubleshooting → Trace Settings** in the **UC-Sec Control Center** menu on the left hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu
- Select the signalling interface IP address from the **Local Address** drop down menu
- Enter the IP address of the Service Provider's SBC in the **Remote Address** field or enter a * to capture all traffic
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example
- Specify the filename of the resultant pcap file in the **Capture Filename** field
- Click on **Start Capture**



To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces. The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP 200 OK response will be seen from the Service Provider.

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 Tele2 VoIP Connect service. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. References

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

[1] *Installing and Configuring Avaya Aura® System Platform Release 6.2*, March 2012.

[2] *Administering Avaya Aura® System Platform Release 6.2*, February 2012.

[3] *Administering Avaya Aura® Communication Manager*, Release 6.2, February 2012.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, February 2012, Document Number 555-245-205.

[5] *Implementing Avaya Aura® System Manager Release 6.2*, March 2012.

[6] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473

[7] *Administering Avaya Aura® Session Manager*, February 2012, Document Number 03-603324.

[8] *Various Application Notes for the Avaya Session Border Controller for Enterprise*, March 2012

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

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.