Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R7.0.1, Avaya Aura® Session Manager R7.0.1 and Avaya Session Border Controller for Enterprise R7.1 to support Orange Business Services BTIP/BT SIP Trunking - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Orange Business Services BTIP/BT SIP Trunking and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server.

Orange Business Services BTIP/BT SIP Trunking provides PSTN access via a SIP Trunk connected to the Orange Business Services Voice over Internet Protocol (VoIP) network as an alternative to legacy analogue or digital trunks.

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

Orange Business Services is a member of the 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.

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Orange Business Services BTIP/BT SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R7.0.1; Avaya Aura® Session Manager R7.0.1; Avaya Session Border Controller for Enterprise R7.1; Endpoints as described in **Section 3**. Note that the shortened names Communication Manager, Session Manager and Avaya SBCE will be used throughout the remainder of the document. Customers using this Avaya SIP-enabled enterprise solution with Orange Business Services BTIP/BT 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 customer.

For simplicity, Orange Business Services will be referred to as "Orange", and its BTIP/BT SIP Trunking service as "SIP Trunking" in the remainder of this document."

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 Avaya SBCE. The enterprise site was configured to connect to the Orange SIP Trunking service.

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 PSTN phones using the Orange SIP Trunking service, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the Orange SIP Trunking service to PSTN destinations, calls made from SIP and H.323 telephones.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator and Avaya Equinox for Windows soft phones.
- Calls using the G.711A Law and G.729A 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 Voice Mail/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 between the Avaya SBCE and the SIP and H.323 telephones.

- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by Orange SIP Trunking requiring Avaya response and sent by Avaya requiring Orange SIP Trunking response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Orange SIP Trunking service with the following observations:

- Occasionally outbound calls via the French gateway (Devil+) were rejected with “500 Internal Server Error” causing them to overflow to the alternative SBC. This is assumed to be a characteristic of the test environment and not an interoperability issue.
- Occasionally calls, though successful, would be marked with a major alarm in the Orange CDR Repository due to a timing issue. Typically, a “100 Trying” would not be received within 500ms of the INVITE being sent. This was due to network delays in the test environment and is not considered to be an interoperability issue.
- When making an inbound call that was not answered, Communication Manager sent a “480 Temporarily Unavailable” message after 3 minutes and at approximately the same time, a CANCEL message was sent by the network. Neither of these messages was received at the other end and it became apparent that they were being dropped by the Avaya Lab VPN server. This was resolved by configuration of the VPN server.
- When making an outbound call to a busy number, the network returned “480 Temporarily Not Available” instead of “486 Busy Here”. This is assumed to be a characteristic of the PSTN interconnect used in the test environment and not an interoperability issue. Calls to busy local numbers received the correct response.
- Calls to short code numbers were correctly formatted and routed but could not be completed in the test environment. The network returned “502 Bad Gateway”
- When calls outbound calls to PSTN numbers were put on hold on the PSTN phone, the network did not provide any indication in signalling that the call was on hold. This did not affect call handling and is listed merely as an observation.
- In the initial testing of long duration call hold, it was observed that the media path was not restored when the call was resumed. Call hold indication was turned off on Communication Manager as the Service Provider commented that it is not required and is unnecessary signalling. Following this change, the media path was restored successfully after long duration call hold.
- Although calls to and from one-X Communicator connected via SIP were successful, the default Payload Type for DTMF in one-X Communicator is 120 and the value used by the Orange SIP Trunking network is 101. If required, the Payload Type can be changed by adding the following lines in the config.xml file located in the one-x Communicator application folder (it's usually located at "C:\Users\<user name>\AppData\Roaming\Avaya\Avaya one-X Communicator"):
    - <parameter>
    - <name>DTMFPayloadType</name>
    - <value>101</value>
    - </parameter>

- When transferring or conferencing one-X Communicator calls in “Other Phone” mode and connected via SIP as opposed to H.323, no ringback was heard on leg 2 of the call. This is not considered to be an interoperability issue as this softphone functions effectively when connected via H.323 and also for SIP in “Computer Mode”. If this is observed in the network, it should be raised as a one-X Communicator fault.
- The media on long duration inbound calls was lost after 50 minutes. Communication Manager was sending an UPDATE message that was not received by the network, and when it didn’t receive a response, Communication Manager was rejecting the next OPTIONS message with a “481 Transaction Does Not Exist” message. The UPDATE message was being dropped by the Avaya Lab VPN server. This was resolved by configuration of the VPN server.

Items not tested include the following:

- No Inbound Toll-Free access was available for testing
- No test call was made to Emergency Services as a test call was not booked with the Emergency Services Operator.
- Remote Worker is not currently tested in Europe.

2.3. Support

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

For technical support on the Orange SIP Trunking service, please contact Orange Business Talk at
http://www.orange-business.com/en/products/business-talk

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to Orange SIP Trunking. Located at the enterprise site is an Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series IP telephones (with SIP and H.323 firmware), Avaya 1600 series IP telephone (with H.323 firmware), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Avaya Equinox for Windows running on laptop PCs.

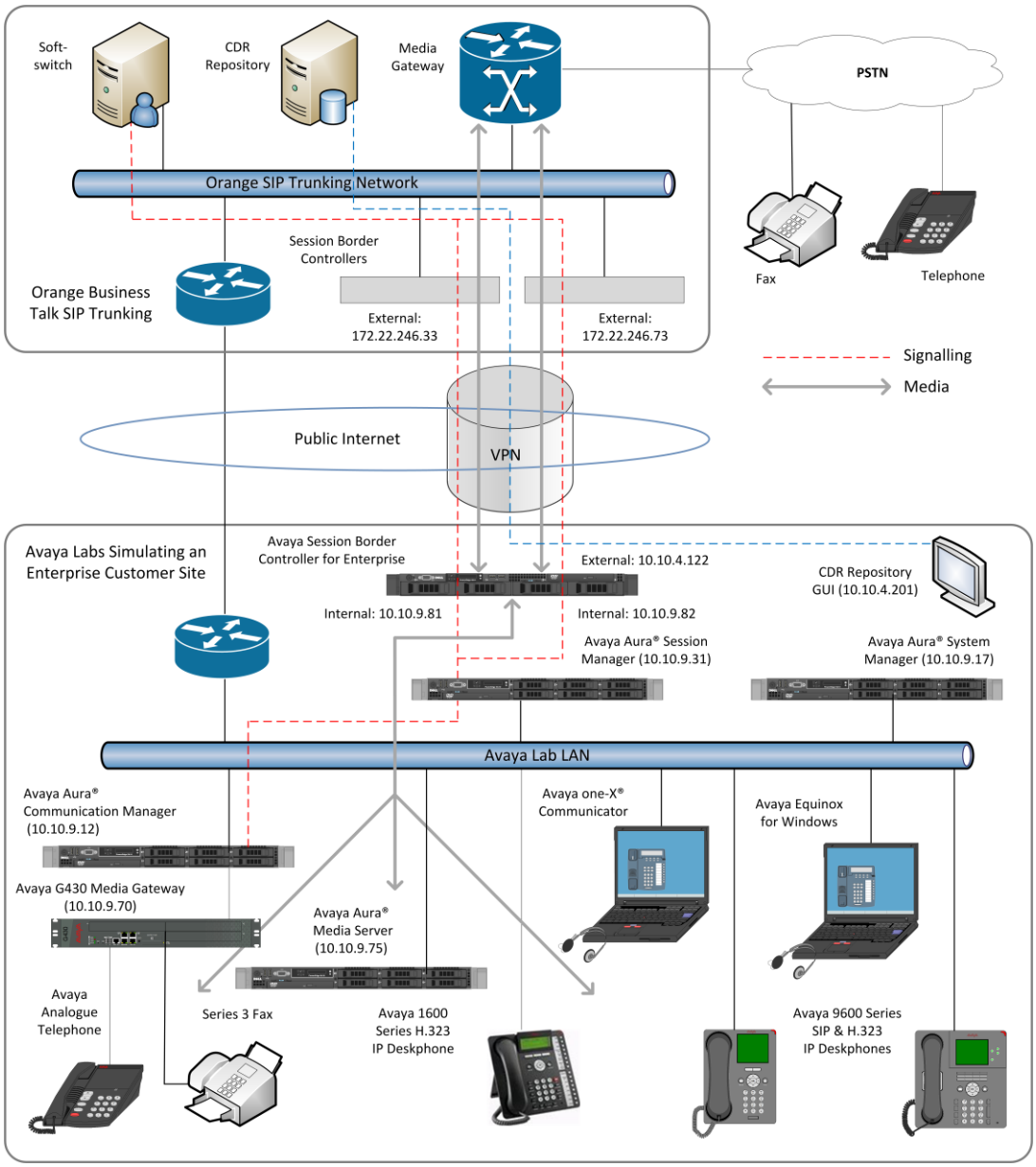


Figure 1: Test Setup of Orange SIP Trunking to Avaya Enterprise

Note: A standard IPSec tunnel was used to connect the Avaya Lab to the Orange SIP Trunking in the test environment. In production, Orange BVPN would be used.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Session Manager	7.0.1.2.701230
Avaya Aura® System Manager	7.0.1.2.086224 – SP2
Avaya Aura® Communication Manager	7.0.1.2.0 0-23523 – FP1 SP2
Avaya Session Border Controller for Enterprise	7.1.0.2-01-13249 – SP2
Media Server	7.8.0.268
Avaya G430 Media Gateway	37.41.0
Avaya IP Handsets: SIP 96x0 SIP 9608 H.323 96x0 H.323 9608 H.323 1616	 2.6.10 7.0.1.4 r6 3.2.7B 6.6.4.01 1.3.10
Avaya One-X Communicator	6.2.12.04 – SP12
Avaya Equinox for Windows	3.0.2.11
Avaya 2400 Series Digital Handsets	N/A
Analogue Handset	N/A
Analogue Fax	N/A
Orange SIP Trunking	
a-sbc: Oracle SBC	SCZ720m6p9
Session Router: Oracle SR	SCZ730m2p3
Application Server: Atos	Inap2SIPv2
French GW Call server: Italtel	release 5.3
International GW Call server: Italtel	release 5.4

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 Orange SIP Trunking. For incoming calls, 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 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 Orange SIP Trunking 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 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 Orange SIP Trunking and any other SIP trunks used.

```
display system-parameters customer-options                      Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 4000  0
           Maximum Concurrently Registered IP Stations: 2400  3
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  0
                       Maximum Administered SIP Trunks: 4000  20
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

On **Page 5**, verify that **IP Trunks** field is set to **y**.

```
display system-parameters customer-options                      Page   5 of  12
                                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 Session Manager using the **change node-names ip** command. In this case, **Session_Manager** and **10.10.9.31** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** IP address as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```
change node-names ip
                                    IP NODE NAMES
    Name               IP Address
AMS                  10.10.9.75
Session_Manager      10.10.9.31
default              0.0.0.0
procr                10.10.9.12
procr6               ::
```

5.3. Administer IP Network Region

Use the **change ip-network-region n** command where **n** is the chosen value of the configuration for the SIP Trunk. 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 direct media is used on a PSTN call, 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 **2** is used.
- Define the port range for RTP media using **UDP Port Min** and **UDP Port Max** as required. It can be left at default values as this is the range used for media between Communication Manager and the Avaya SBCE. During testing, it was set to the same range of **16384** to **32767** used between the Avaya SBCE and Orange SIP Trunking.
- The rest of the fields can be left at default values.

```
change ip-network-region 2                                      Page   1 of  20
                              IP NETWORK REGION
  Region: 2
Location:         Authoritative Domain: avaya.com
    Name: Trunk                 Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 16384                     IP Audio Hairpinning? n
   UDP Port Max: 32767
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 34
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
```

Note: In the test configuration, ip-network-region 1 was used within the enterprise and ip-network-region 2 was used for the SIP Trunk.

5.4. Administer IP Codec Set

Use the **change ip-codec set n** command where **n** is the codec set specified in the IP Network Region form in **Section 5.3**. Orange SIP Trunking supports either **G.711A** or **G.729A** but not both in order of preference. Most of the compliance testing was carried out with **G.711A**.

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

                           IP CODEC SET
    Codec Set: 2

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

Orange SIP Trunking supports T.38 for transmission of fax. Navigate to **Page 2** and define T.38 fax as follows:

- Set the **FAX - Mode** to **t.38-standard**
- Leave **ECM** at default value of **y**.

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

                           IP CODEC SET

                               Allow Direct-IP Multimedia? n



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

Note: **Redundancy** can be used to send multiple copies of T.38 packets which can help the successful transmission of fax over networks where packets are being dropped. This was not experienced in the test environment and **Redundancy** was left at the default value of **0**.

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to Orange SIP Trunking. During testing, this was configured to use TCP and port 5060. Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to required protocol. Note that TLS is recommended for security and was used for the SIP Trunk to Session Manager for SIP endpoints. For the Lab connection to Orange SIP Trunking however, **tcp** was used.
- Set **Peer Detection Enabled** to **y** allowing 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 Session Manager interface (node name **Session_Manager** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** as required, during testing, **5060** was used. These must correspond to those used on the Session Manager Entity Links (See **Section 6.6**).
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3** (logically establishes the far-end for calls using this signalling group as region **2**).
- Leave **Far-end Domain** blank (allows Communication Manager to accept calls from any SIP domain on the associated trunk).
- Set **DTMF over IP** to **rtp--payload** which uses telephone events according to RFC 2833 for DTMF transmission.
- Set **Direct IP-IP Audio Connections** to **y** to avoid unnecessary use of resources.
- Set **Initial IP-IP Direct Media** and **H.323 Station Outgoing Direct Media** to **y**. This initiates direct media when the call is set up without the need for shuffling.

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

 Group Number: 2              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
      IP Video? n                                   Enforce SIPS URI for SRTP? n
  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
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                  Far-end Node Name: Session_Manager
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 2

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? n                   Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? y            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 n** command, where **n** is an available trunk group for the SIP Trunk. 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.
- The **Direction** is set to **two-way** to allow incoming and outgoing calls.
- Set the **Service Type** field to **public-netwrk** if the Diversion header is to be supported.
- Specify the signalling 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 2                                                Page   1 of  21
                                TRUNK GROUP

Group Number: 2                    Group Type: sip           CDR Reports: y
  Group Name: SIP_Trunk                   COR: 1        TN: 1        TAC: 102
   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: 2
                                                   Number of Members: 10
```

On **Page 2** of the trunk-group form, the **Preferred Minimum Session Refresh Interval (sec)** field should be set to **600** as specified in the Orange configuration guide. This value sets the SIP Min-SE header to 1200. Note that during testing a value of **800** was used to avoid clashes with session refresh messages from the Orange SIP Trunking test environment.

```
add trunk-group 2                                                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): 800

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

On **Page 3** of this form:

- Set the **Numbering Format** field to **public** as Orange use E.164 numbering with preceding "+" in the SIP messages.
- Set **Hold/Unhold Notifications** to n as this is not required with Orange SIP Trunking and results in unnecessary signalling.

```
change trunk-group 2                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                       Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? n
                                  Modify Tandem Calling Number: no
```

On **Page 4** of this form:

- Set **Mark Users as Phone** to **n**. Note that during testing this was set to **y** for consistency with the Orange SIP Trunking test environment.
- Set **Network Call Redirection** to **n** as SIP "302 Moved Temporarily" and REFER are not supported by Orange.
- Set **Send Diversion Header** to **n** in line with Orange SIP Trunking configuration guidelines.
- Set **Support Request History** to **y** in line with Orange SIP Trunking configuration guidelines.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Orange (this Payload Type is not applied to calls from some SIP end-points).
- Leave other fields at default settings.

```
change trunk-group 2                                          Page   4 of  21
                              PROTOCOL VARIATIONS

                                        Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

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


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                               Enable Q-SIP? n
```

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number E.164 format. Communication Manager automatically prefixes a "+" to the numbers when this table is used. These calling party numbers are sent in the SIP From, Contact and PAI headers. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network.

```
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: 6
 4  2             1                          4        Maximum Entries: 240
 4  2000          2         332960nnnn1      11
 4  2291          2         332960nnnn3      11    Note: If an entry applies to
 4  2316          2         332960nnnn4      11    a SIP connection to Avaya
 4  2391          2         332960nnnn2      11    Aura(R) Session Manager,
 4  2400          2         332960nnnn5      11    the resulting number must
                                                   be a complete E.164 number.

                                                   Communication Manager
                                                   automatically inserts
                                                   a '+' digit in this case.
```

Note: During testing the extension numbers were reformatted to international numbers for Trunk Group 2 only. The numbers were analysed for Trunk Group 1 but not reformatted.

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 Orange SIP Trunking network. 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: 8
    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 with leading **0**. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. The example shows international numbers with country code **353** for Ireland and area code **91** for Galway. Calls are sent to **Route Pattern 12**. Note also an entry for country code **33** with no international prefix digits, this was used during testing for EC500 as described in **Section 5.10**.

```
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    12    11       pubu         n
    00                    13   15    12       pubu         n
    0035391               13   13    12       pubu         n
    1                     3    4     10       pubu         n
    118                   5    6     10       pubu         n
    3                     4    4     10       pubu         n
    33                    11   11    13       pubu         n
```

Use the **change route-pattern n** command, where **n** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **12** is used to route **International** calls to trunk group **2**. **Numbering Format** is applied to CLI and is used to set TDM signalling parameters such as type of number and numbering plan indicator. This doesn't have the same significance in SIP calls and during testing it was set to **intl-pub**.

```
change route-pattern 12                                        Page   1 of   3
                    Pattern Number: 12     Pattern Name: International
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                                  Dgts                                  Intw
 1: 2    0                         0   p64                               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 Sub  Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
 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
```

Note: In the test environment, the **Inserted Digits** field in **route-pattern 12** was used to prefix the dialled number with +64 (**p64**) for the international gateway. In route-pattern 13, this field was set to p6400 to include the international dialling prefix for EC500 (see **Section 5.10**).

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to Communication Manager extensions. The incoming digits sent in the INVITE message from Orange SIP Trunking can be manipulated as necessary to route calls to the desired extension. Use the **change inc-call-handling-trmt trunk-group x** command where **x** is the Trunk Group defined in **Section 5.6**.

In the example shown, 13 digits numbers are received in E.164 format with a "+" prefix used in SIP to indicate an international number. The preceding "+" and all digits are deleted and the extension number is inserted. Note that some of the DDI digits have been obscured.

```
change inc-call-handling-trmt trunk-group 2                    Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    12 +332960nnnn1     12  2000
 public-ntwrk    12 +332960nnnn2     12  2391
 public-ntwrk    12 +332960nnnn3     12  2291
 public-ntwrk    12 +332960nnnn4     12  2316
 public-ntwrk    12 +332960nnnn5     12  2400
 public-ntwrk
```

5.10. EC500 Configuration

When EC500 is enabled on a 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 2291. Use the command **change off-pbx-telephone station-mapping x** where **x** is a Communication Manager station.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** if required by the routing configuration, none was required during testing.
- For the **Phone Number** enter the phone that will also be called (e.g. **3314094nnnn**).
- Set the **Trunk Selection** to **ars** so that the ARS table will be used for routing.
- Set the **Config Set** to **1**.

```
change off-pbx-telephone station-mapping 2291                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                    Selection   Set     Mode
 2291            OPS           -     2291             aar        1
 2291            EC500         -     3314094nnnn      ars        1
```

Note: The **Phone Number** shown is an example. To use facilities such as Feature Name Extension (FNE) for calls coming in from EC500 mobile phones, the calling party number received by Communication Manager in the P-Asserted-Identity header must exactly match the

number specified in the above table. In the solution tested, a Session Manager Adaptation is used to insert the P-Asserted-Identity header as described in **Section 6.4**. The Adaptation uses the number in the From header as opposed to the default behaviour of using the number in the Contact header.

The From header received from Orange SIP Trunking is in E.164 format with leading "+". The leading "+" is ignored when matching the number for the FNE so the phone number can be specified in E.164 with no "+" or international dialling prefix. As there is no international dialling prefix, an ARS entry for the country code is required as described in **Section 5.8**.

Save Communication Manager configuration by entering **save translation**.

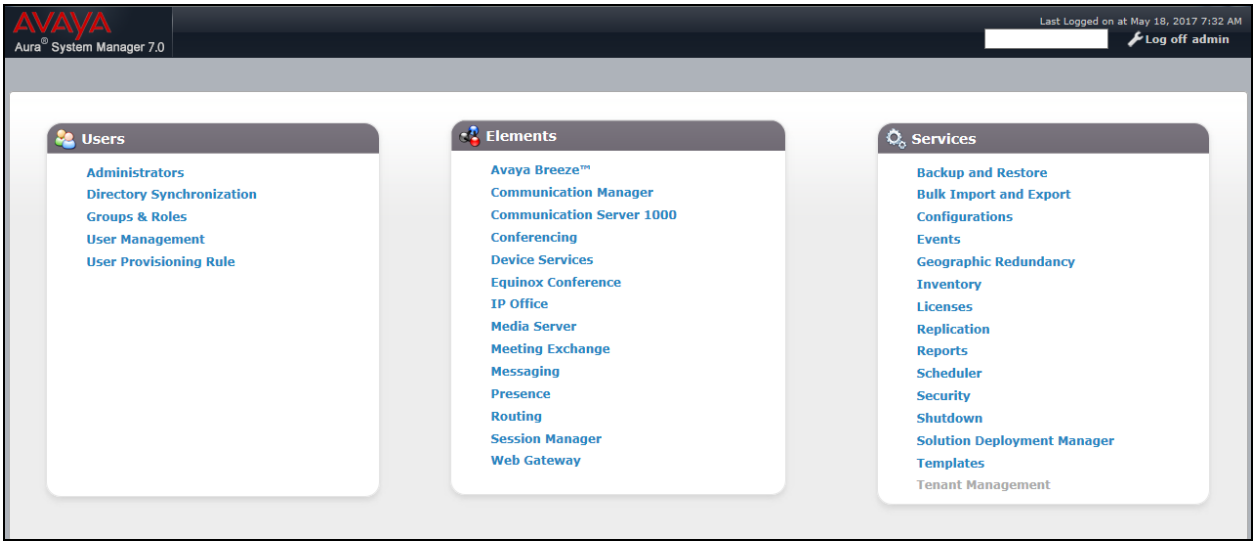
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured by opening a web browser to 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

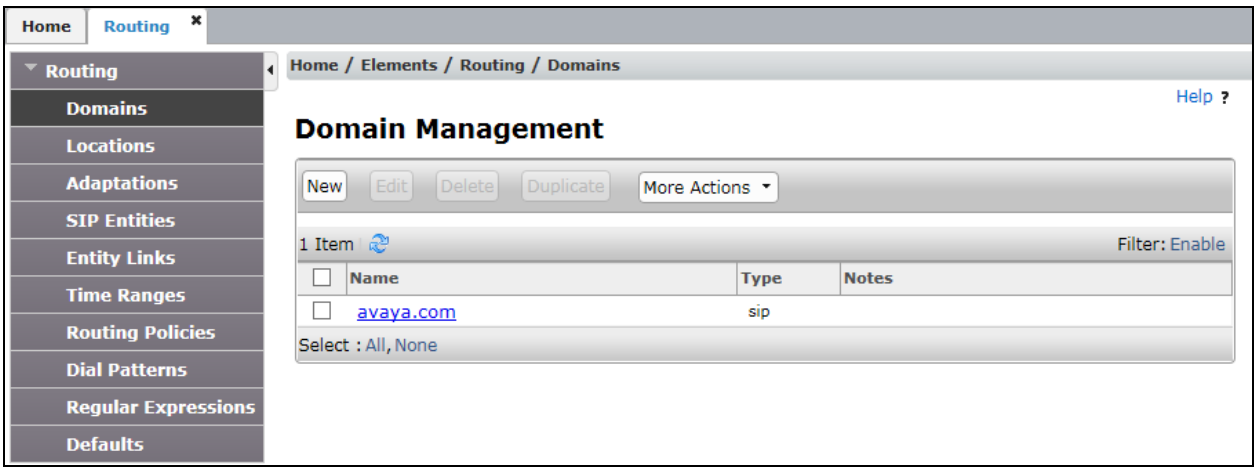
6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a web browser and 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** screen will be presented with menu options shown below.



6.2. Administer SIP Domain

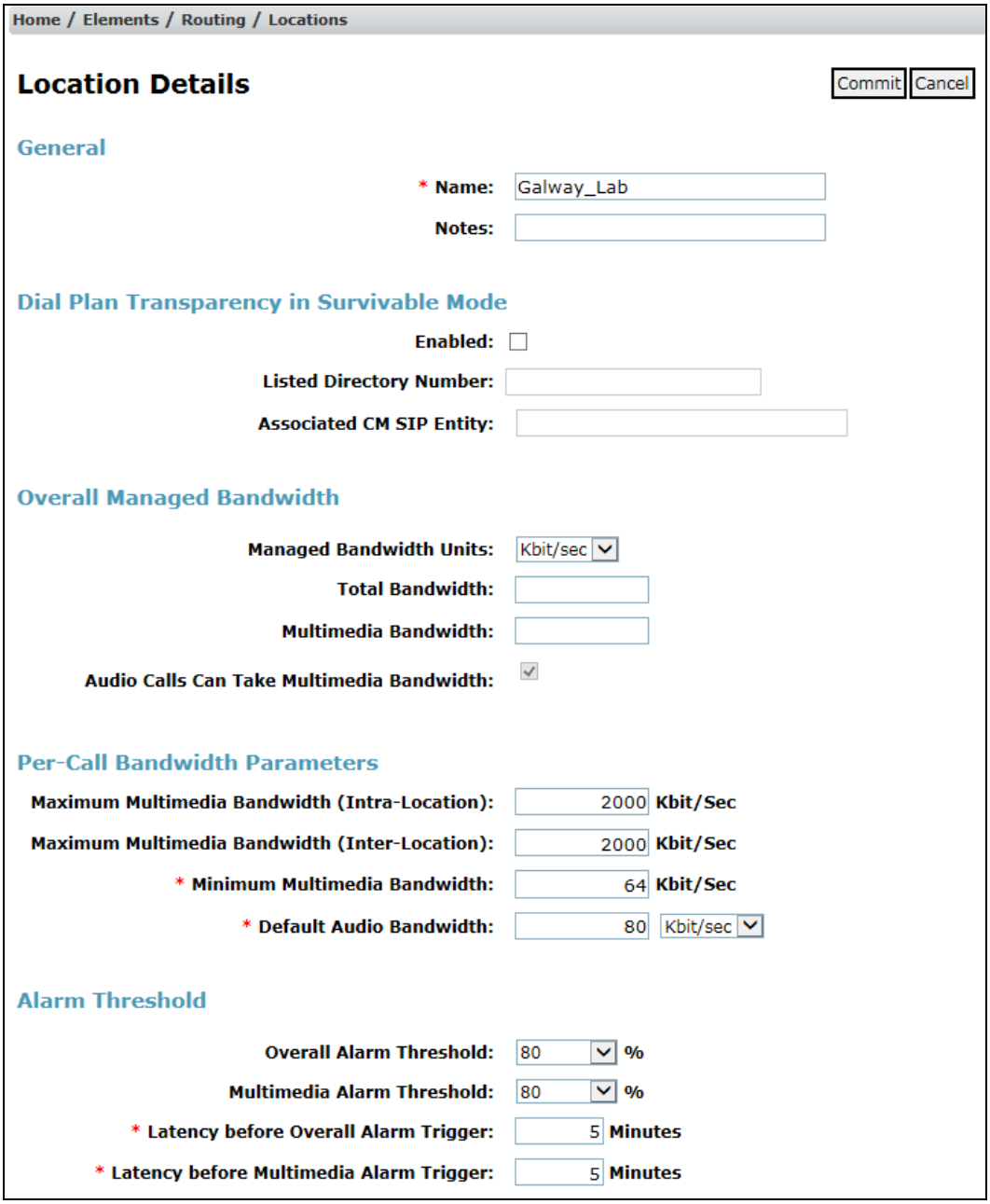
To add the SIP domain that will be used with Session Manager, select **Routing** from the **Elements**, **Home** screen menu and in the resulting tab select **Domains** from the left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name of the enterprise site or a name agreed with Orange; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on Communication Manager. Refer to **Section 5.3** for details. In test, **avaya.com** was used. Optionally, a description for the domain can be entered in the **Notes** field. Click **Commit** to save changes.



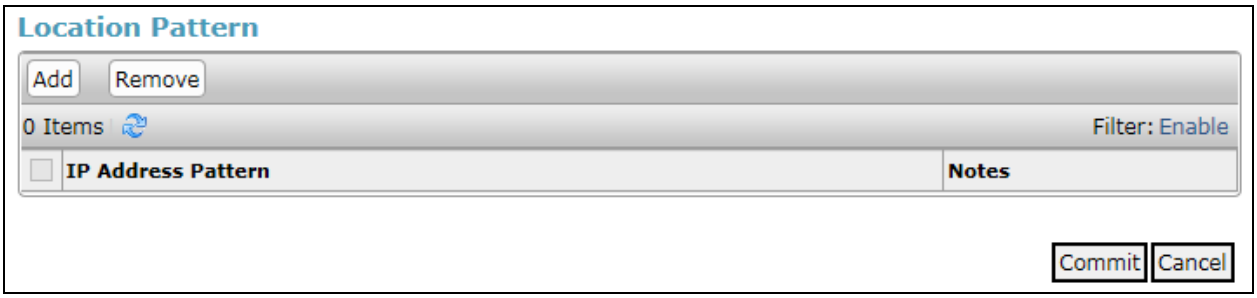
Note: If the existing domain name used in the enterprise equipment does not match that used in the network, a Session Manager Adaptation can be used to change it (see **Section 6.4**).

6.3. Administer Locations

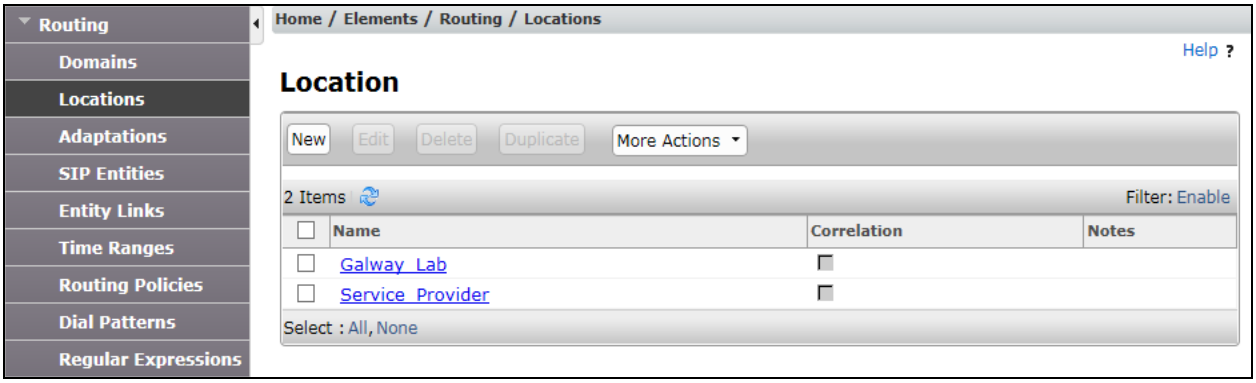
Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management and Session Manager routing. One location is added to the sample configuration for all of the enterprise SIP entities and another for Orange SIP Trunking. On the **Routing** tab select **Locations** from the left hand menu (not shown). Under **General**, in the **Name** field, enter an informative name for the location. Define bandwidth requirements, during testing these were left at default values.



The location pattern is a way of using subnets to further refine the location information, this may be useful for endpoints that could be logged in from different subnets. This was not used during testing. If required, 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.



A separate location was defined for Orange called **Service_Provider**. This was used in the Dial Patterns defined in **Section 6.8** to ensure that calls originating from Communication Manager to one of the DDI numbers assigned to Communication Manager would be routed via the SIP Trunk. This was useful for some test calls. The bandwidth parameters were left at default values and are not shown here.

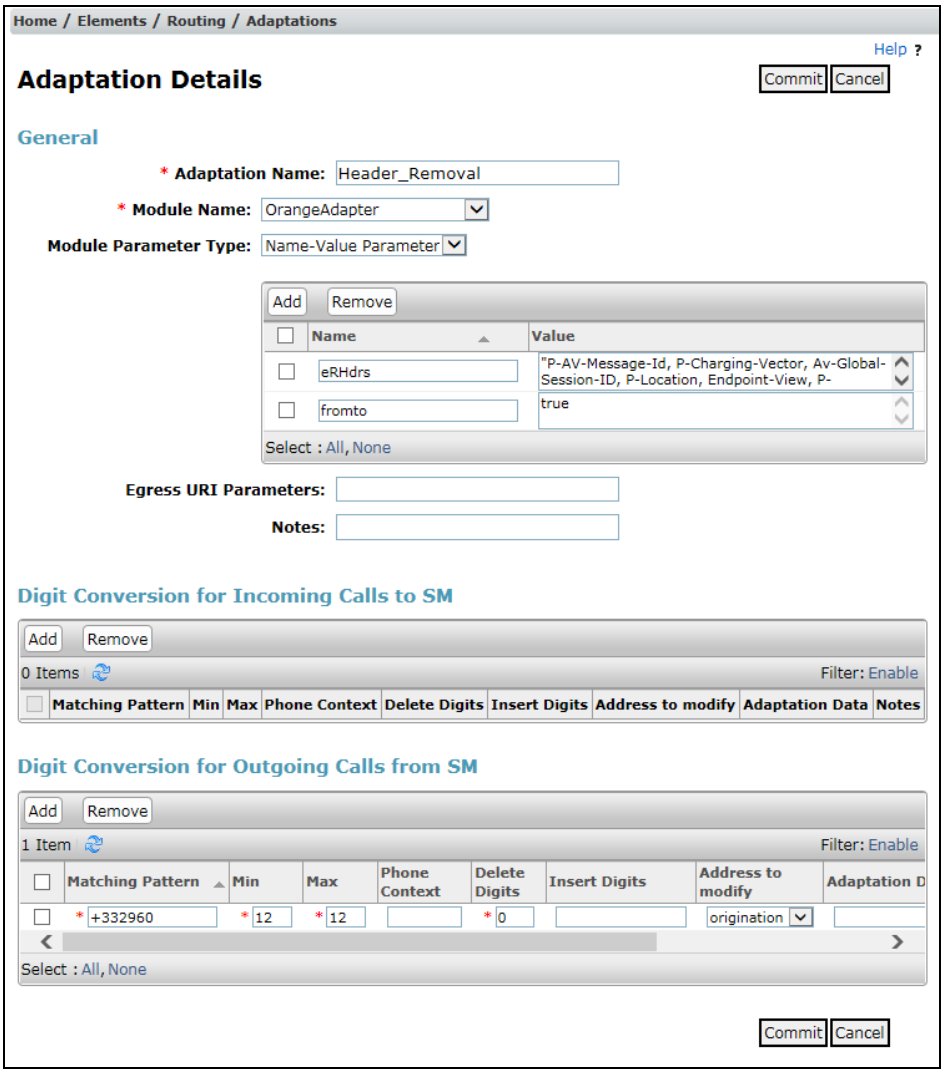


6.4. Administer Adaptations

Session Manager Adaptations can be used to alter parameters in the SIP message headers. An Adaptation was used during testing to remove Avaya proprietary headers from messages sent from Session Manager. This Adaptation also used the From header to create the P-Asserted-Identity header as opposed to the default behavior of using the Contact header. This is required for correct FNE functionality from an EC500 mobile phone (See **Section 5.10**).

Communication Manager and Session Manager make use of Avaya proprietary SIP headers to facilitate the full suite of Avaya functionality within the enterprise. These are not required on the SIP trunk however, and make the SIP messages unnecessarily large. A Session Manager Adaptation is used to remove proprietary headers. On the **Routing** tab select **Adaptations** from the left-hand menu. Click on **New** (not shown).

- In the **Adaptation Name** field, enter a descriptive title for the adaptation.
- In the **Module Name** drop down menu, select **OrangeAdapter**.
- In the **Module Parameter Type** drop down menu, select **Name-Value Parameter**.
- In the **Name** box, type **eRHdrs**.
- In the **Value** box, type the list of headers to be deleted. During testing, the following list was used: **"P-AV-Message-Id, P-Charging-Vector, Av-Global-Session-ID, P-Location, Endpoint-View, P-Conference, Alert-Info, Correlation-ID, Accept-Language"**.
- Scroll down and in the section **Digit Conversion for Outgoing Calls from SM**, click on **Add**. An additional row will appear (not shown) for digit manipulation.



The screenshot shows how the calling party numbers in messages going to the Avaya SBCE were analysed for testing. There was no digit conversion required as called and calling party numbers were passed from Communication Manager in the required format. The calling party number was still analysed however, so that the header removal rule would be applied to all calls.

The **OrangeAdapter** module includes **DigitConversionAdpater** for simple digit conversion and provides the additional functionality of changing the way the P-Asserted-Identity header is populated where it is not received from the Service Provider. The default action is to use information in the Contact header. This module uses the From header instead which resolves issues with calls from EC500 mobiles as described in **Section 5.10**. The full functionality of the OrangeAdapter module is described in the Session Manager Administration Guide referenced in **Section 11**.

6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to 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 **SIP Trunk** for the Avaya SBCE SIP Entity.
- In the **Adaptation** field (not available for the Session Manager SIP Entity), select the appropriate Adaptation from the drop down menu.
- 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.

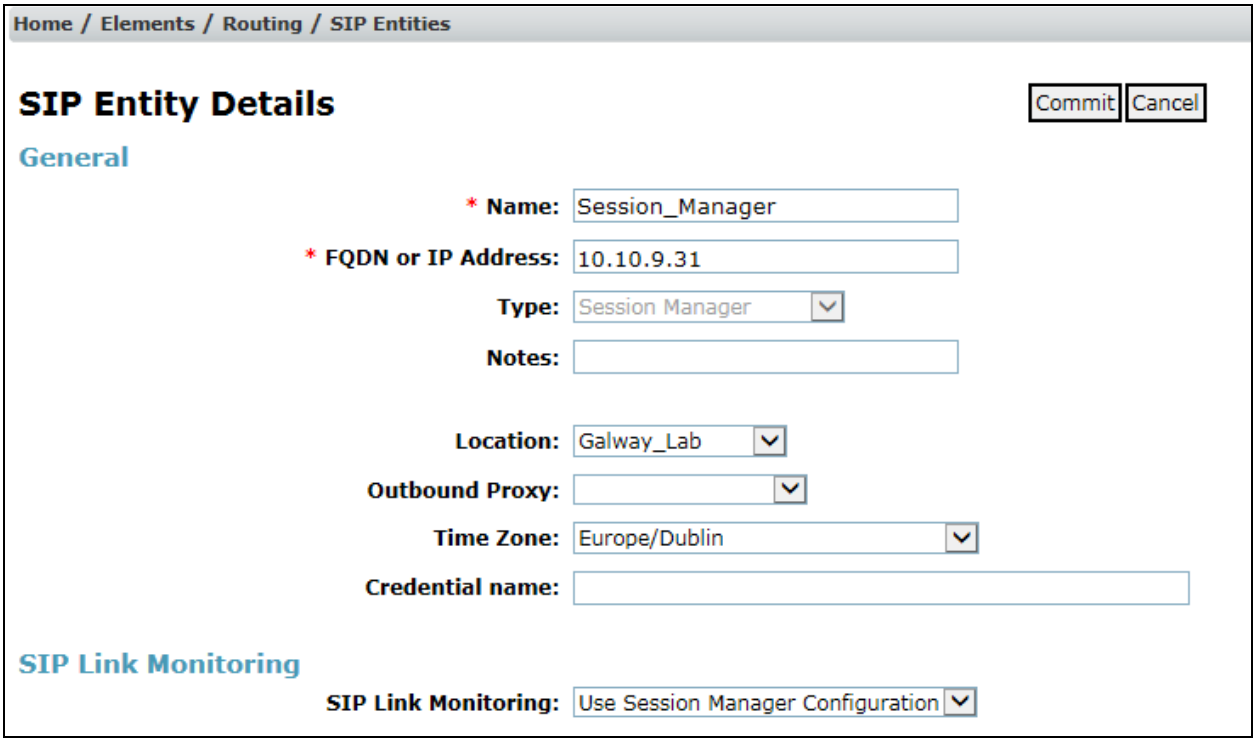
In this configuration there are four SIP Entities:

- Avaya Aura® Session Manager SIP Entity.
- Avaya Aura® Communication Manager SIP Entity for the SIP Endpoints.
- Avaya Aura® Communication Manager SIP Entity for the SIP Trunk.
- Avaya Session Border Controller for Enterprise (Avaya SBCE) SIP Entity for PSTN destinations.

There is also a SIP Entity for Avaya Aura® Messaging but that is not described in this document.

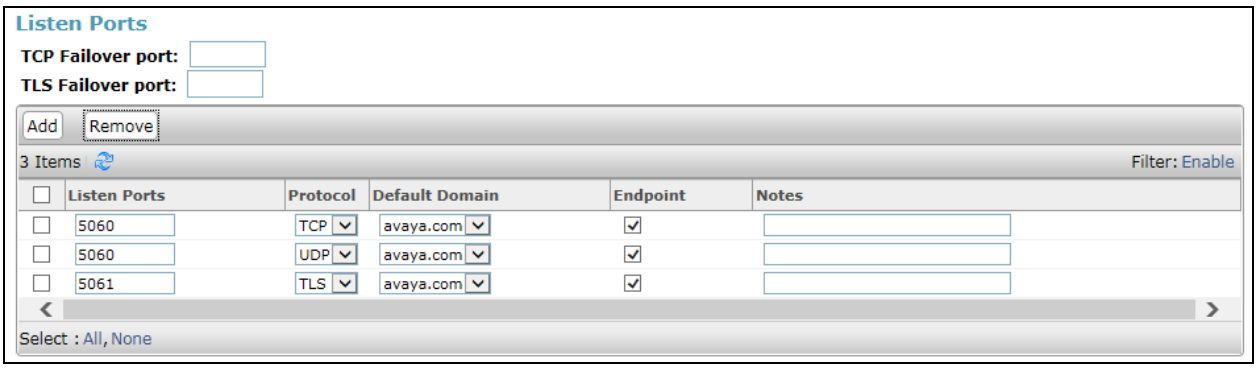
6.5.1. Avaya Aura® Session Manager SIP Entity

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.



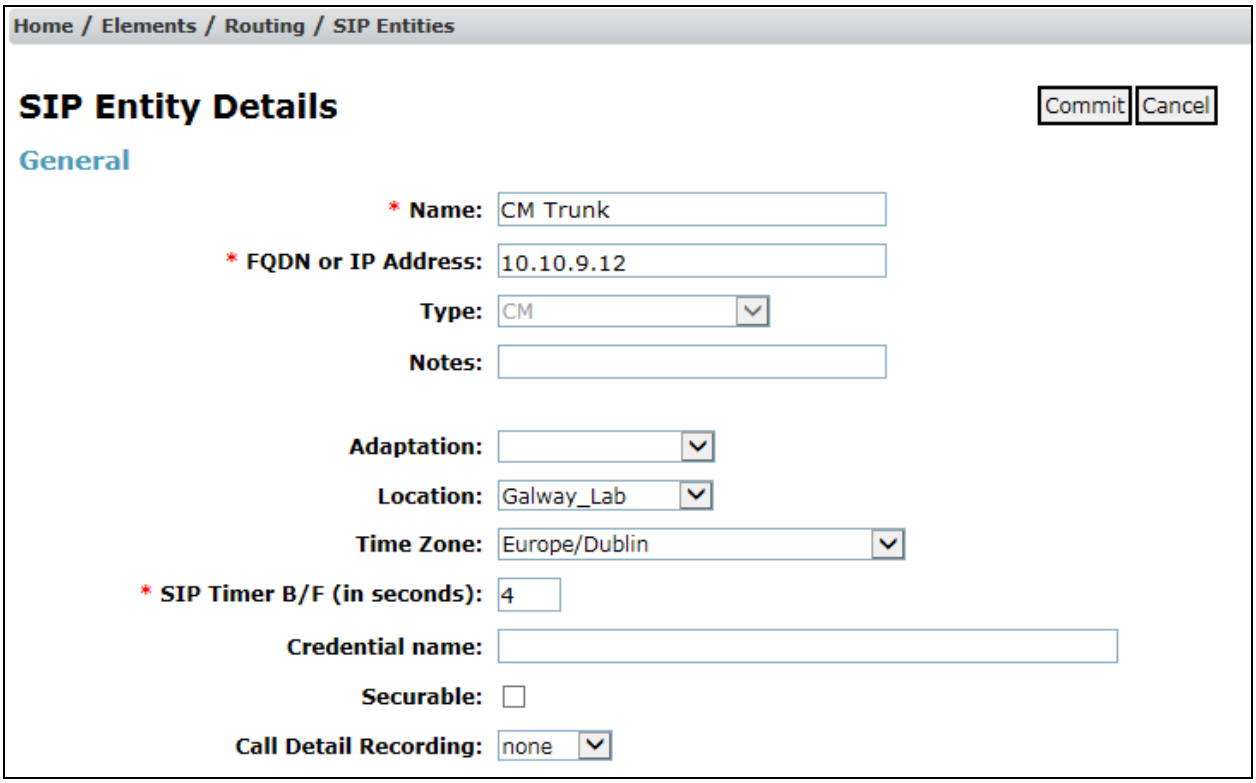
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Listen Ports**, click **Add**, then edit the fields in the resulting new row.

- In the **Listen Ports** 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 the domain added in **Section 6.2** as the default domain.
- Click on **Commit** (not shown).

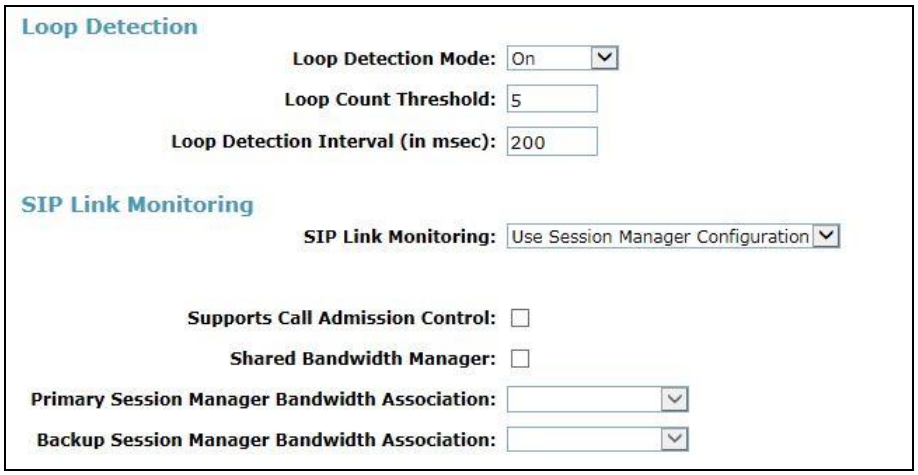


6.5.2. Avaya Aura® Communication Manager SIP Entities

The following screen shows one of the SIP entities for Communication Manager which is configured as an Evolution Server. This SIP Entity is used for the SIP Trunk. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. There was no Adaptation required on the Communication manager SIP Entity during testing. Set the **Location** to that defined in **Section 6.3**.



Other parameters can be set for the SIP Entity as shown in the following screenshot, but for test, these were left at default values.

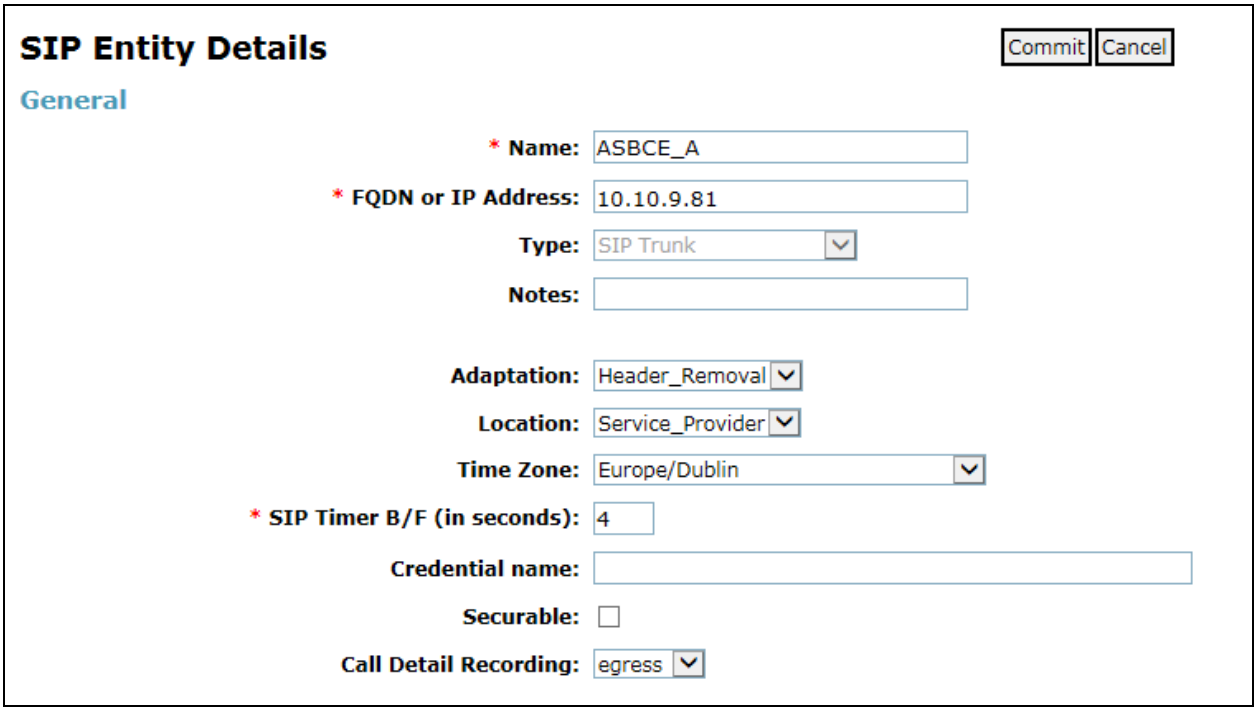


Note: A second SIP Entity for Communication Manager is defined for SIP Endpoints. In the test environment this is named "CM_SIP_Endpoints". The parameters are the same and the two are assigned to different Entity Links, as described in **Section 6.6**, so that different ports can be used. It is these different ports that distinguish between traffic for SIP Endpoints and traffic for the SIP Trunk.

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

There are two SIP Entities required for the Avaya SBCE in this configuration. One is for the Avaya SBCE internal interface that maps to the server flow for the primary Orange SBC, and the other is for the internal interface that maps to the secondary Orange SBC.

The screenshot shows the SIP Entity for the internal interface mapping to the primary Orange SBC. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE internal interface (see **Figure 1**). Set the **Adaptation** to that defined in **Section 6.4**, the **Location** to that defined in **Section 6.3** for the SIP Trunk, and the **Time Zone** to the appropriate time zone.



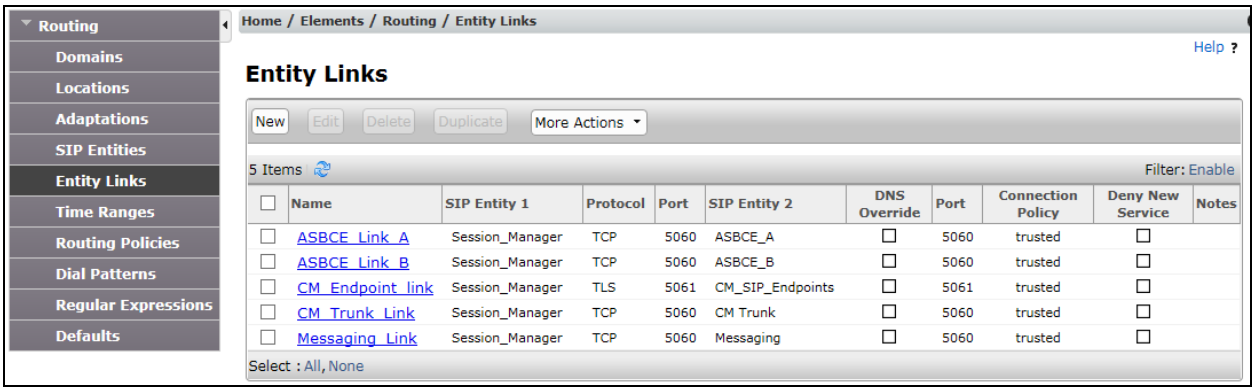
Note: The **Location** selected would allow routing based on origination if required. This is used in Dial Patterns as described in **Section 6.8**. It was not required during testing.

The SIP Entity for the internal interface mapping to the secondary Orange SBC is configured with the same parameters apart from the **Name** and **FQDN or IP Address** fields (not shown). In the test environment, these were **ASBCE_B** and **10.10.9.82** respectively.

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. Fill in the following fields in the new row that is displayed (not shown).

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **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.
- Leave the **Connection Policy** drop down menu at the default value of **trusted** to make the other system trusted.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.
- Click **Commit** (not shown) to save changes. The screenshot shows the Entity Links used in this configuration.



Note: There are two Entity Links for Communication Manager, one for the SIP Endpoints and the other for the SIP Trunk. These are differentiated by **Protocol** and **Port**. The **Messaging_Link** Entity Link is used for the Avaya Aura® Messaging system and is not described in this document.

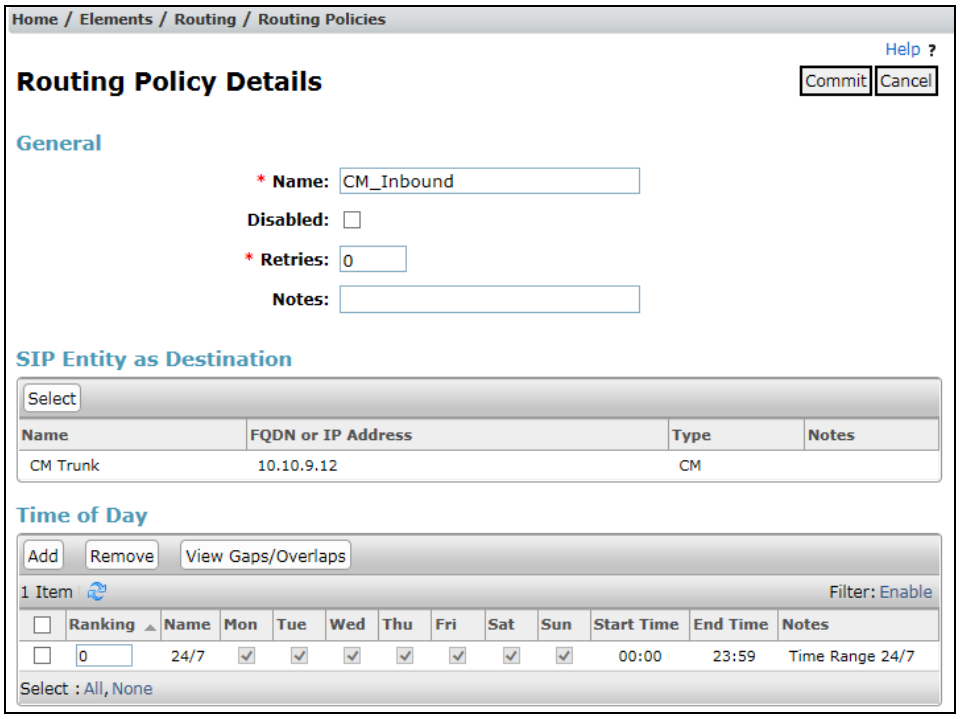
6.7. Administer Routing Policies

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).

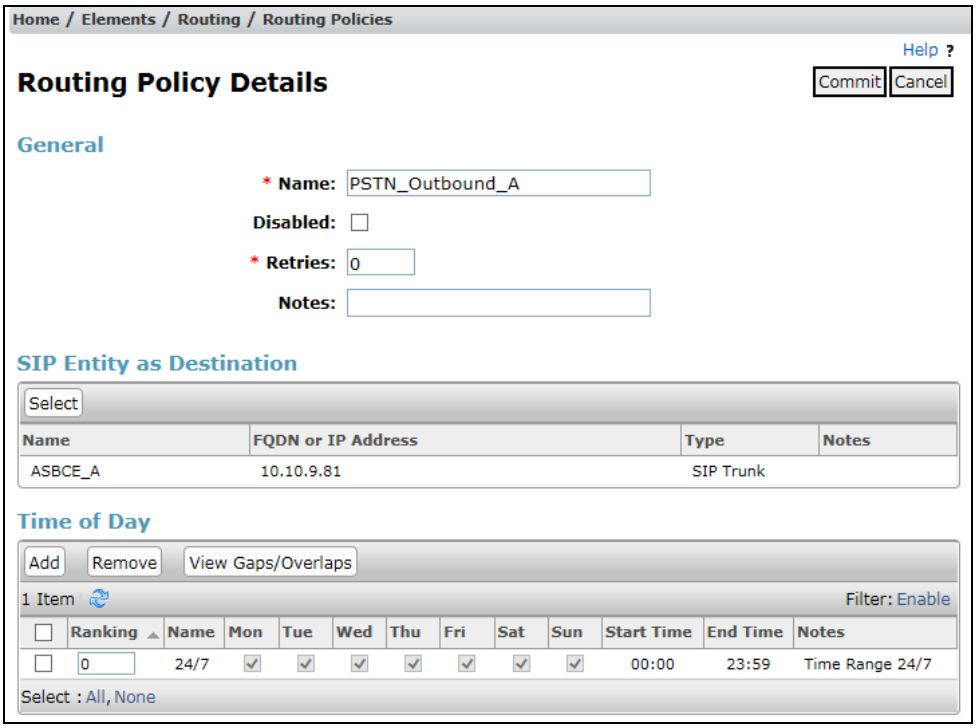
Under **General**:

- Enter an informative name in the **Name** field.
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity, defined in **Section 6.5**, to which this routing policy applies (not shown).
- Under **Time of Day**, click **Add**, and then select the time range. **24/7** is provided as a default.

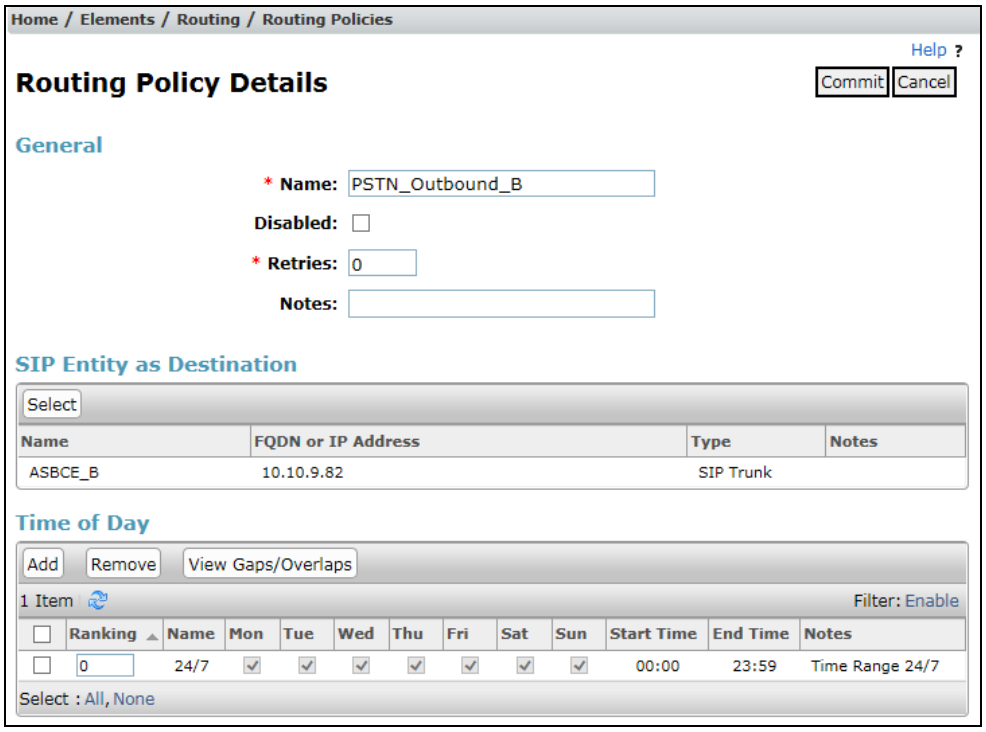
The following screen shows the routing policy for calls inbound from the SIP Trunk to Communication Manager.



The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed to PSTN destinations via the primary Orange SBC.



The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed to PSTN destinations via the secondary Orange SBC.



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**:

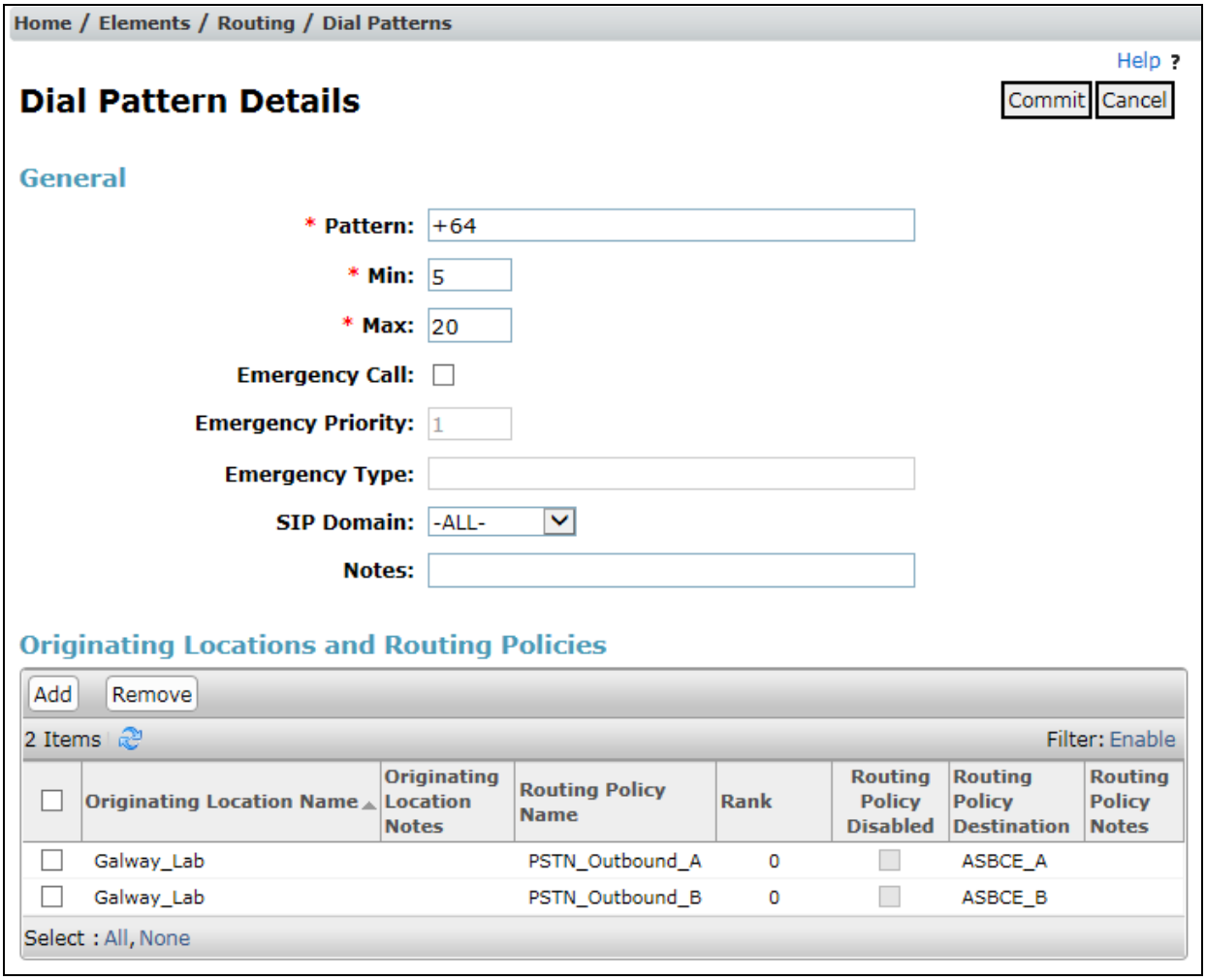
- In the **Pattern** field enter a dialled number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialled number.
- In the **Max** field enter the maximum length of the dialled number.
- In the **SIP Domain** field select **ALL** or alternatively one of those configured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

Under **Originating Locations and Routing Policies**:

- Click **Add**, in the resulting screen (not shown).
- Under **Originating Location**, select one of the locations defined in **Section 6.3** if routing depending on originating location is required. Alternatively, select **ALL**.
- Under **Routing Policies** select one of the routing policies defined in **Section 6.7**.
- Click **Select** button to save.

Note that routing policies can be added if alternative routing is required which was the case in the test environment.

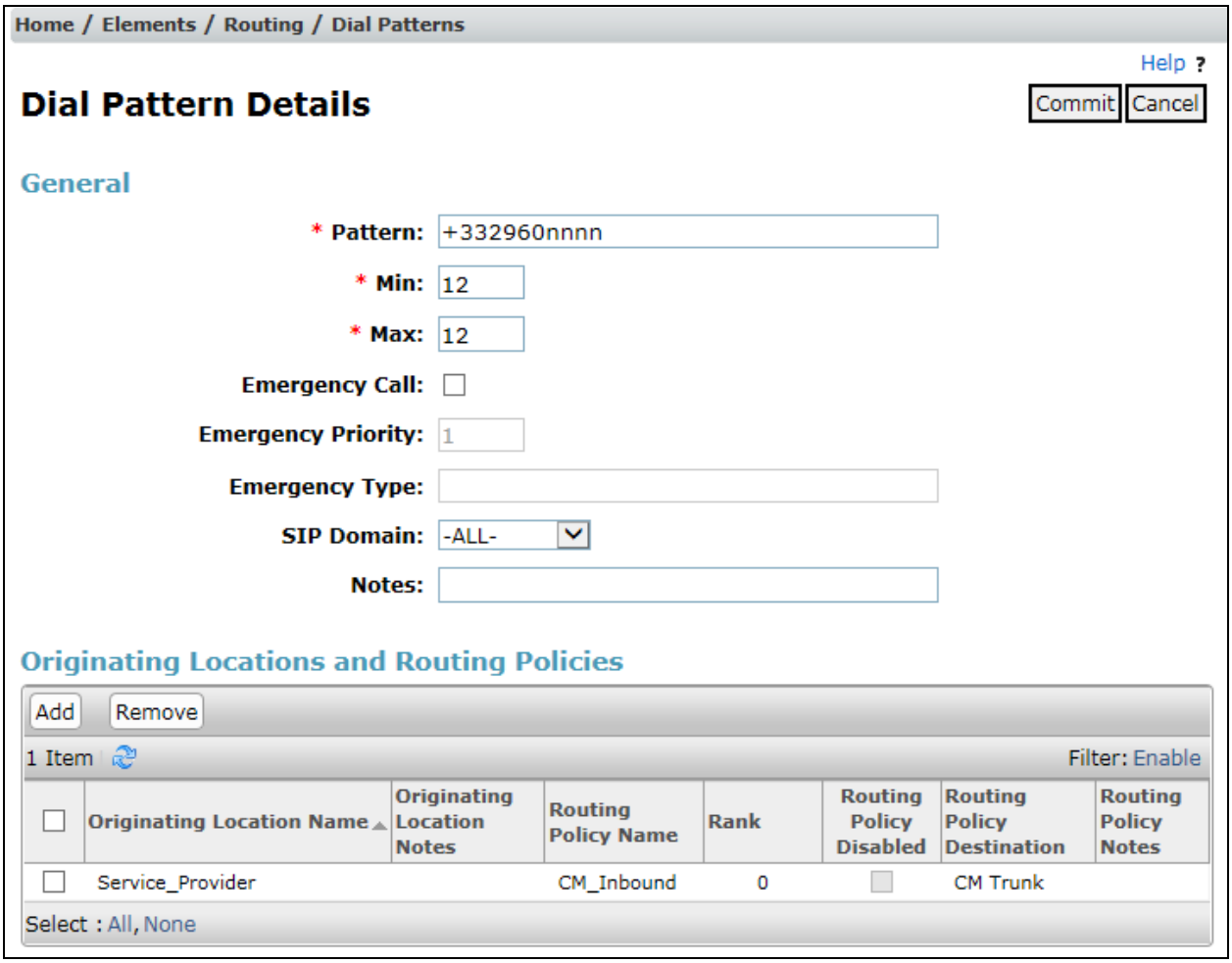
The following screen shows an example dial pattern configured for the Avaya SBCE which will route all calls originating in the enterprise and starting with "+64" to the PSTN via Orange SIP Trunking.



Note: The **Pattern** shown in the example was for a prefix used in the test environment, this will be different in the Live environment.

Two **Routing Policies** are defined for the primary and secondary BTIP SBCs.

The next screenshot shows the test dial pattern configured for Communication Manager. This is used to analyze the DDI numbers assigned to the extensions on Communication Manager. If the **Originating Location** is the SIP Trunk and the digits match the **Pattern**, the calls are routed to Communication Manager. Some of the digits of the pattern to be matched have been obscured.

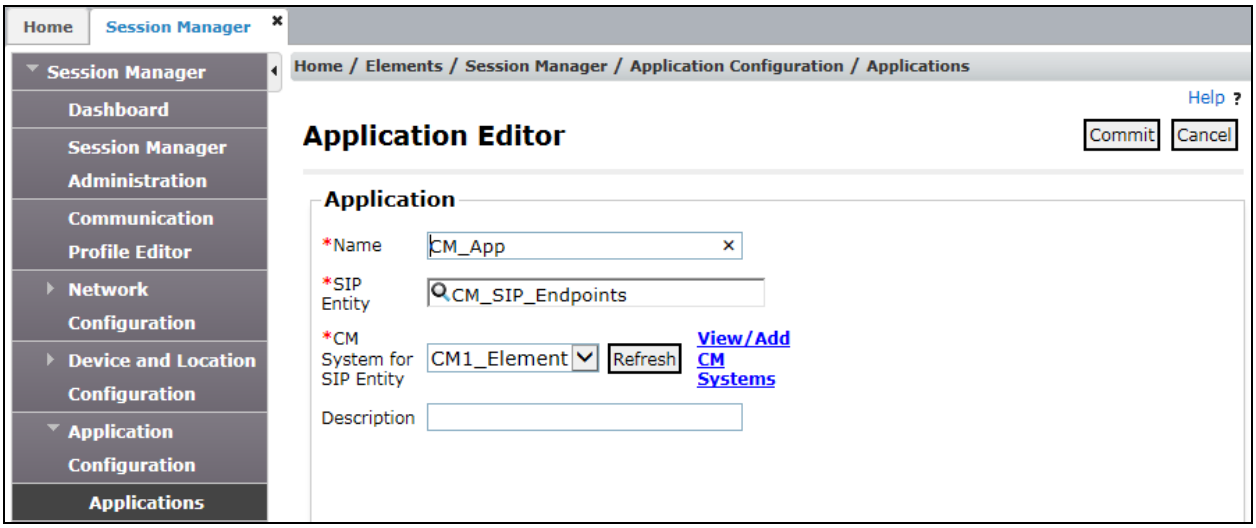


Note: In the test environment, Locations were used so that if the number matched one of the DDI numbers assigned to Communication Manager, it was only routed to Communication Manager if came in from the SIP Trunk. If it originated from Communication Manager, it would be routed out to the SIP Trunk. This was useful to ensure that all test calls were routed via the SIP Trunk.

6.9. Administer Application for Avaya Aura® Communication Manager

From the **Home** screen select **Session Manager** from the Elements menu. In the resulting tab from the left panel menu select **Application Configuration → Applications** and click **New** (not shown).

- In the **Name** field enter a name for the application.
- In the **SIP Entity** field select the SIP Entity for Communication Manager Endpoints described in **Section 6.5**.
- In the **CM System for SIP Entity** field select the appropriate Communication Manager from the System Manager inventory and select **Commit** to save the configuration.

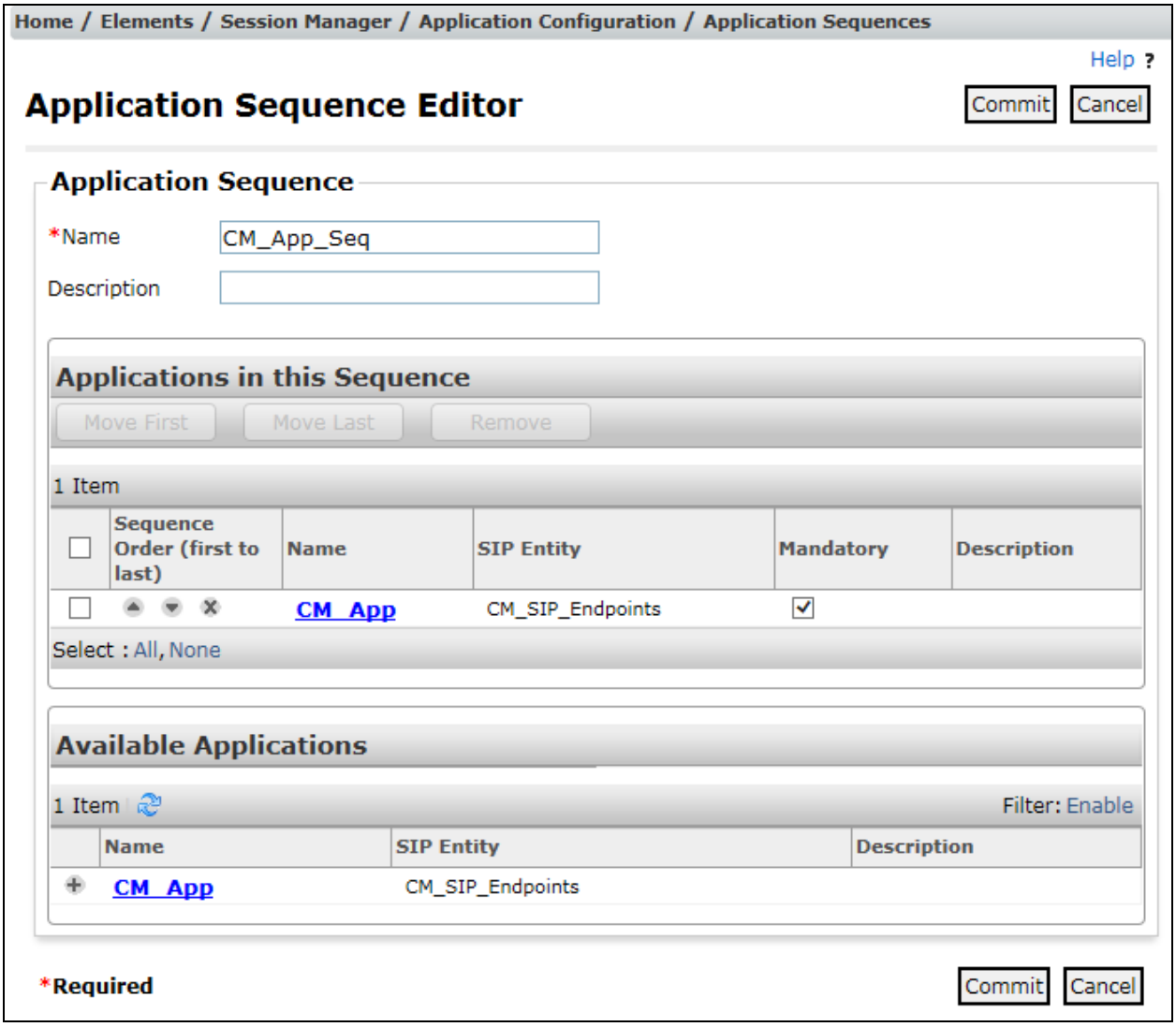


Note: The Application described here and the Application Sequence described in the next section are likely to have been defined during installation. The configuration is shown here for reference. Note also that the Communication Manager SIP Entity selected is that set up specifically for SIP endpoints. In the test environment there is also a Communication Manager SIP Entity that is used specifically for the SIP Trunk and is not to be used in this case.

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** (not shown).

- 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**.

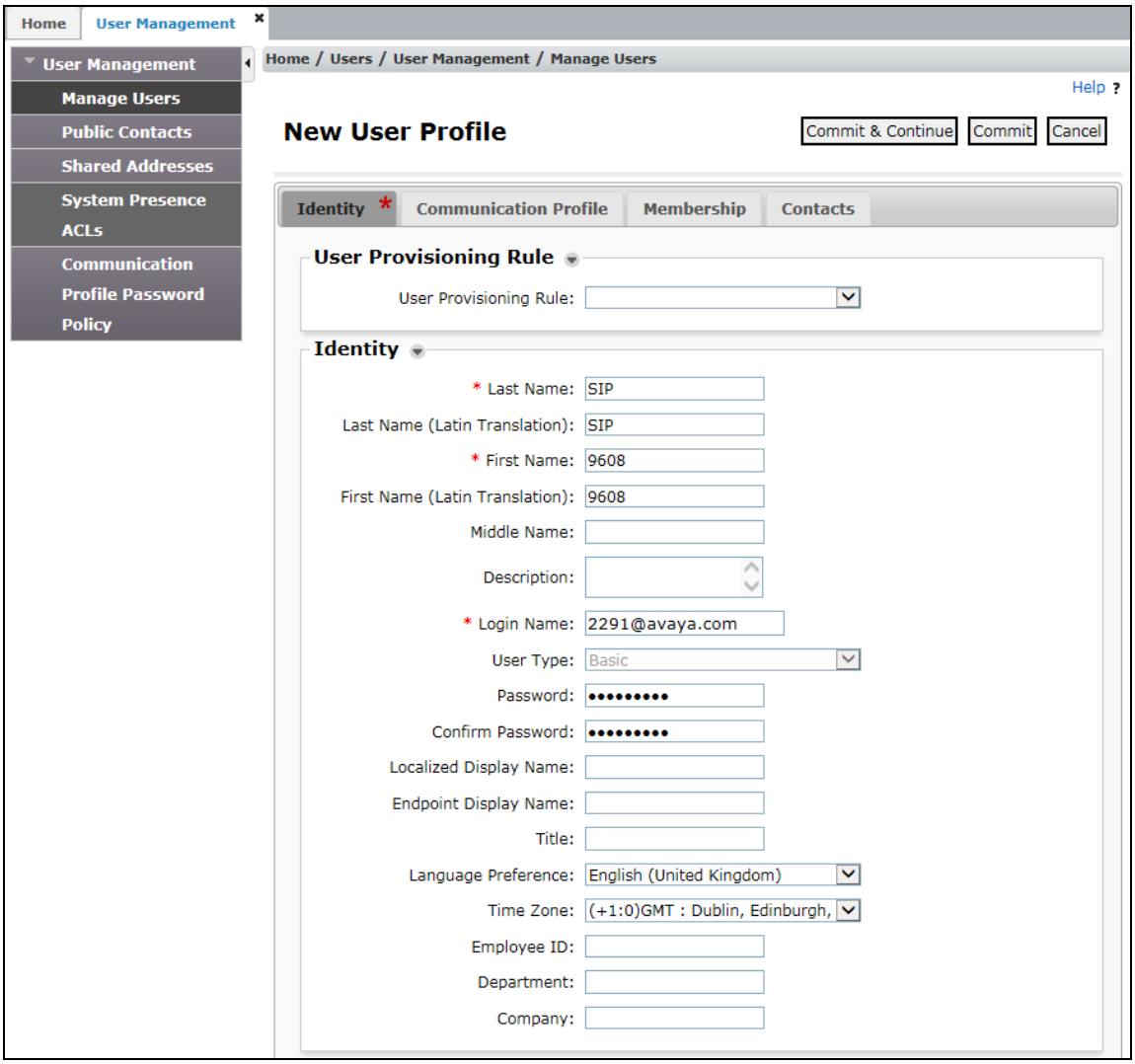


6.11. Administer SIP Extensions

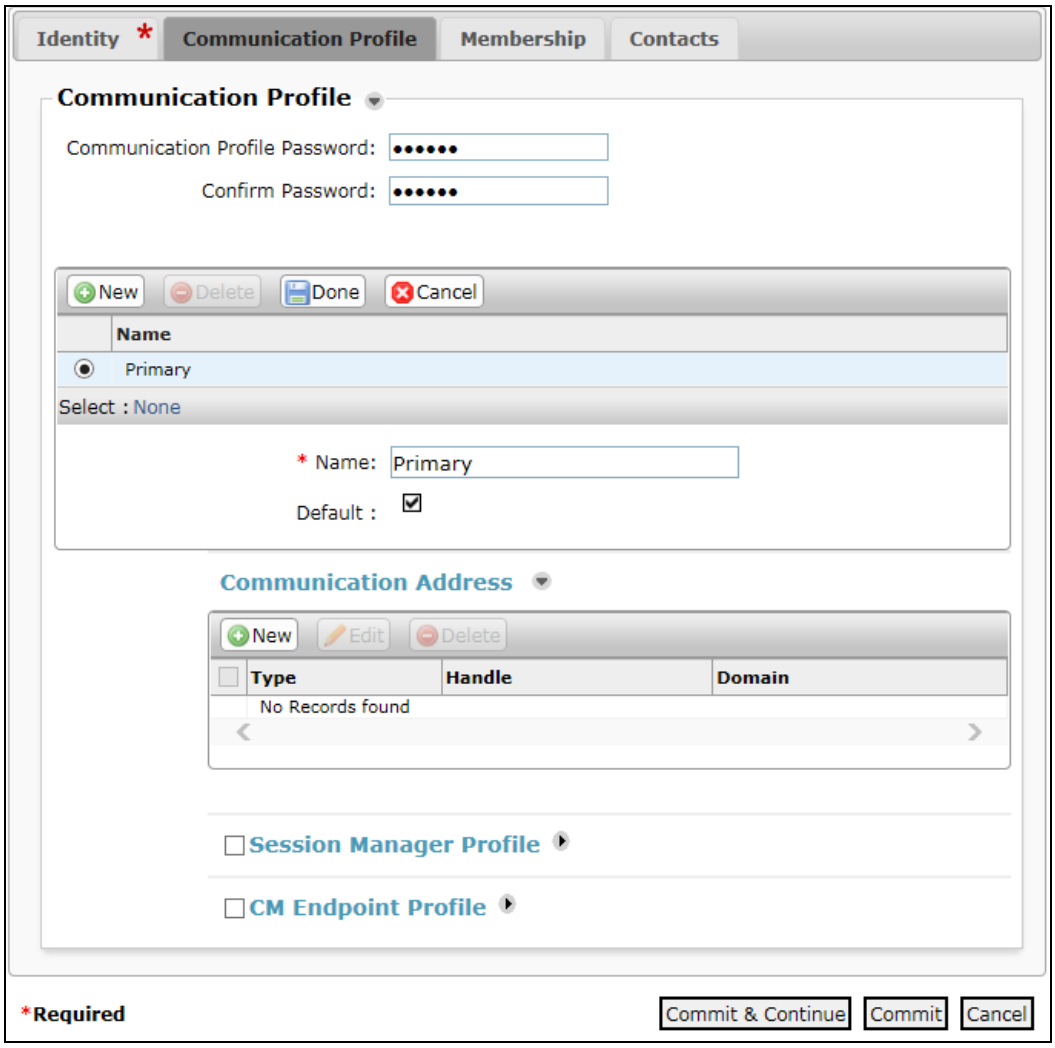
The SIP extensions are likely to have been defined during installation. The configuration shown in this section is for reference. SIP extensions are registered with Session Manager and use Communication Manager for their feature and configuration settings. From the **Home** screen select **User Management** from the **Users** menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

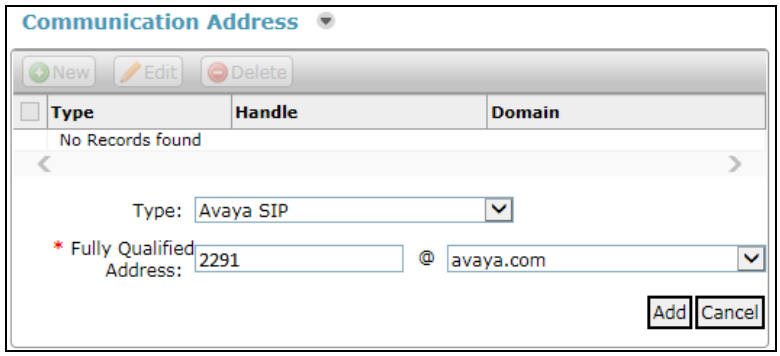
- Enter the user's name in the **Last Name** and **First Name** fields.
- In the **Login Name** field enter a unique system login name in the form of user@domain e.g. **2291@avaya.com** which is used to create the user's primary handle.
- The **Authentication Type** should be **Basic**.
- In the **Password/Confirm Password** fields enter an alphanumeric password.
- Set the **Language Preference** and **Time Zone** as required.



In the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it.

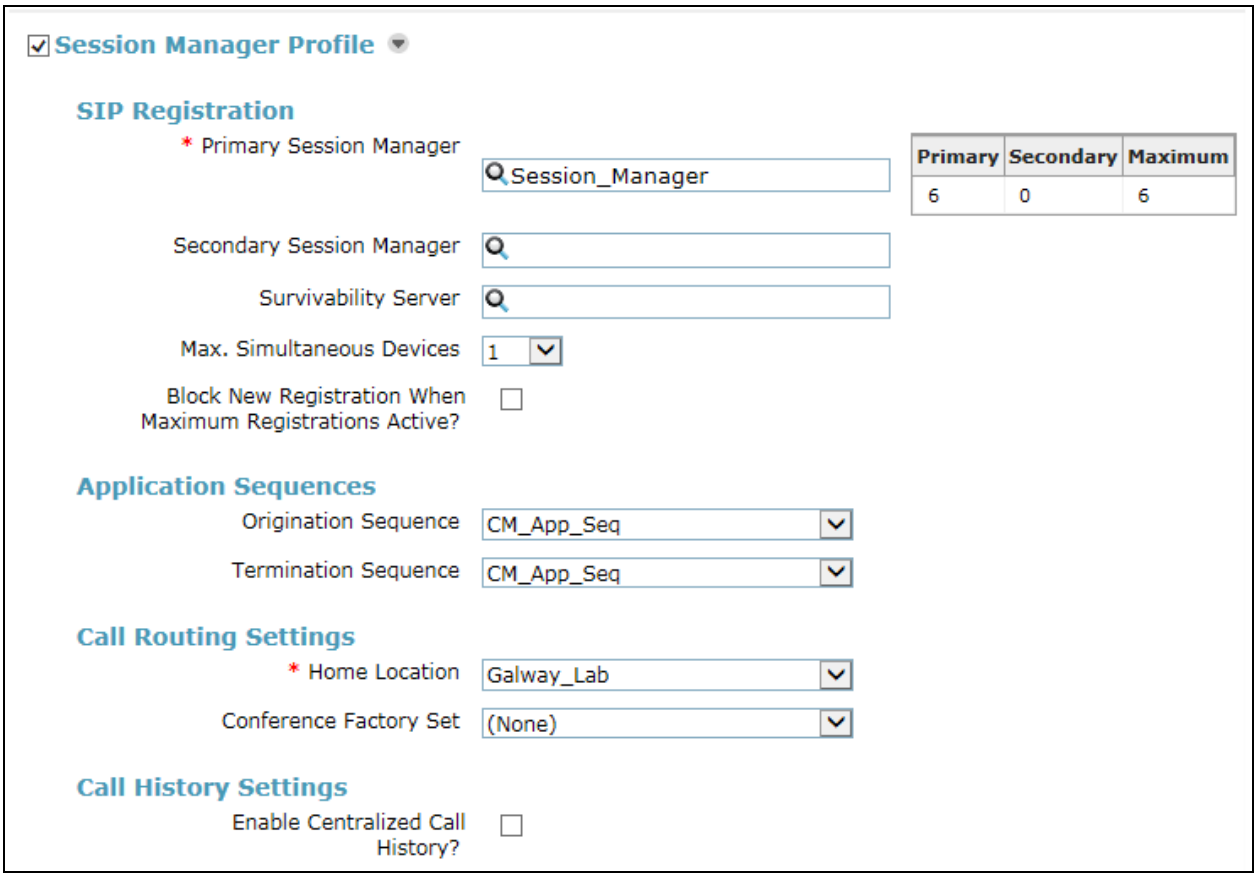


Expand the **Communication Address** section and click **New**. For the **Type** field select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.



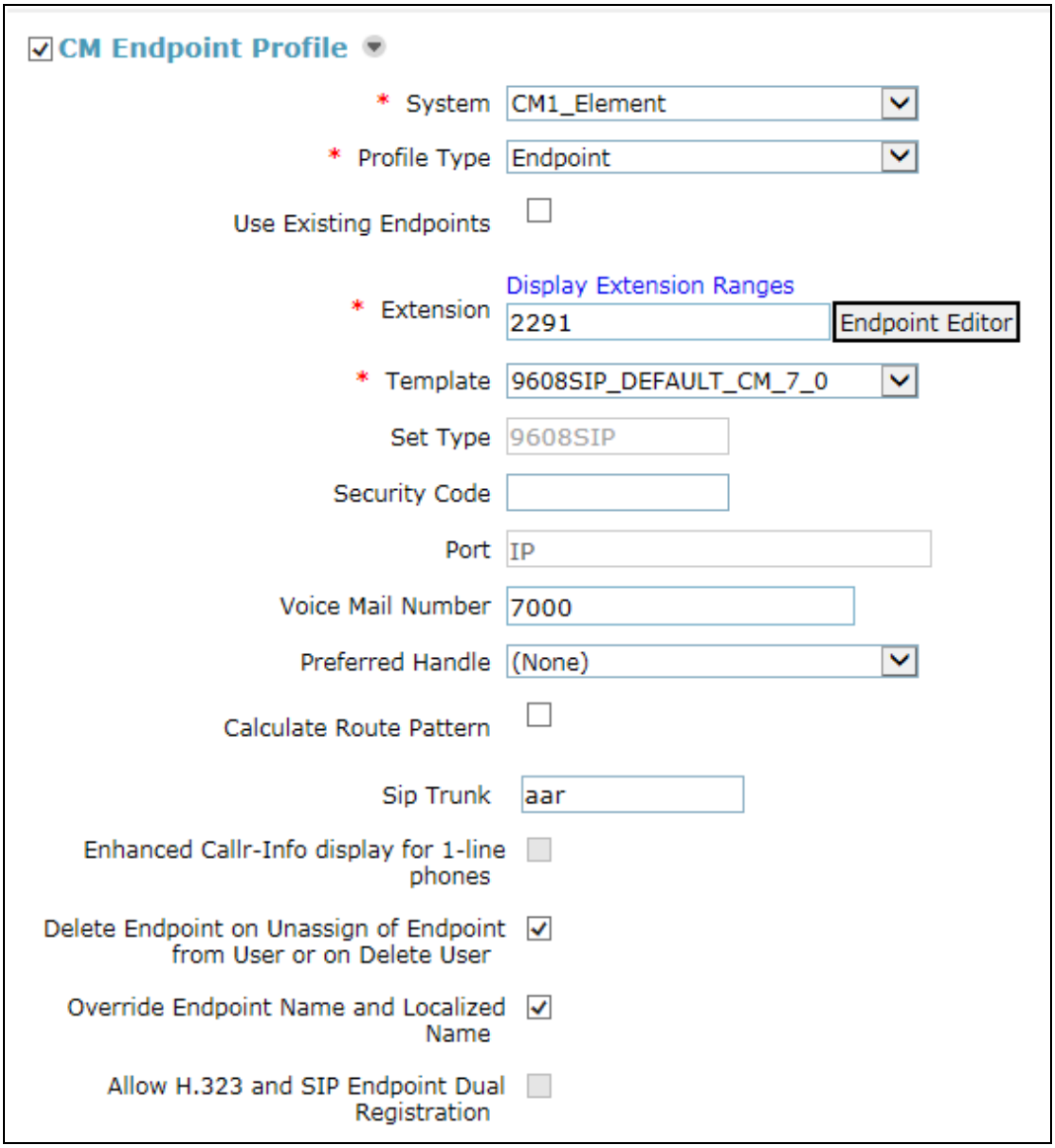
Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** 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 Sequence** field configured in **Section 6.10**.
- Select the appropriate application sequence from the drop-down menu in the **Termination Sequence** field configured in **Section 6.10**.
- Select the appropriate location from the drop-down menu in the **Home Location** field.



Expand the **Endpoint Profile** section.

- Select Communication Manager Element 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.
- In the **Port** field **IP** is automatically inserted.
- Enter a **Voice Mail Number** if required. In the test environment, this was **7000**
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box.



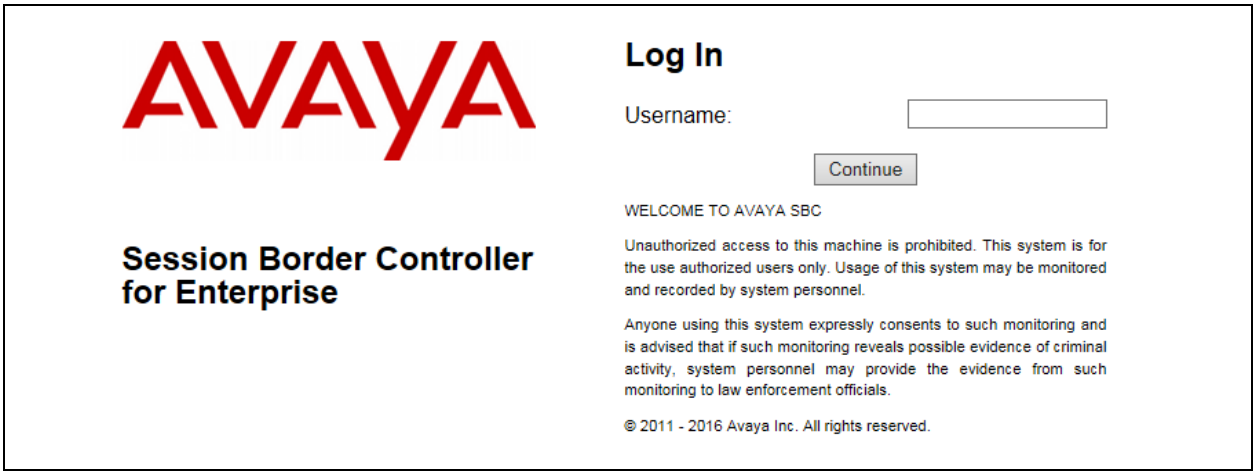
Select **Commit** (Not Shown) to save changes and the System Manager will add Communication Manager user configuration automatically.

7. Configure Avaya Session Border Controller for Enterprise

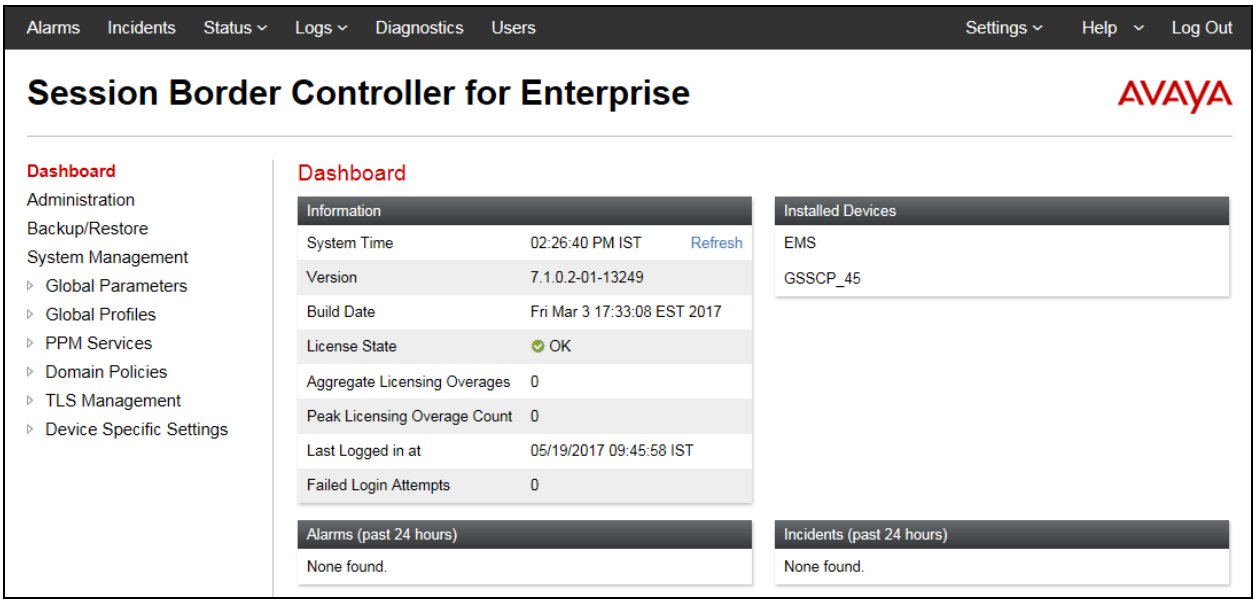
This section describes the configuration of the Avaya Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

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. A log in screen is presented. Log in using the appropriate username and password.



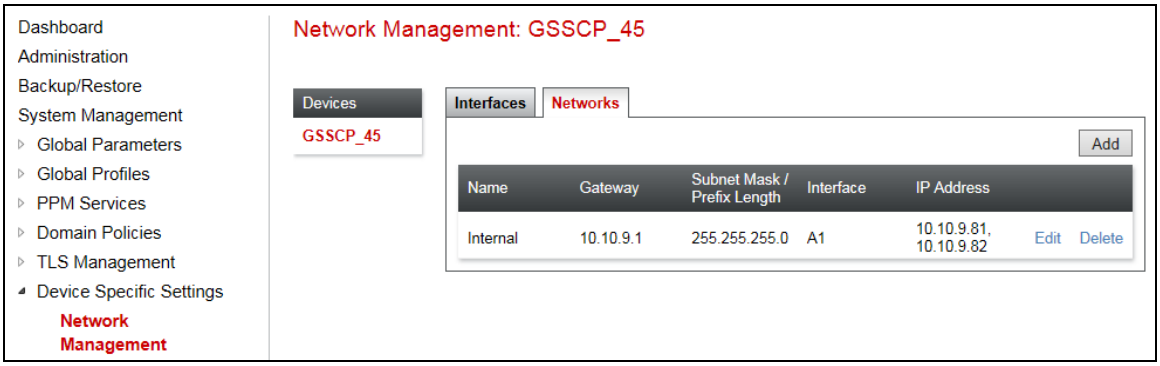
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



7.2. Define Network Management

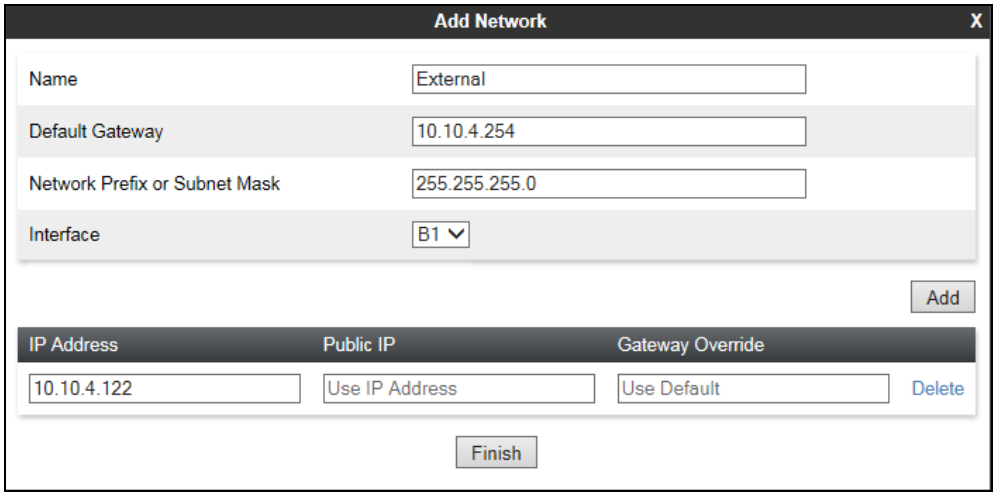
Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that in the test environment only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external.

To define the network information, navigate to **Device Specific Settings → Network Management** in the main menu on the left hand side and click on **Add**.



Enter details for the external interfaces in the dialogue box:

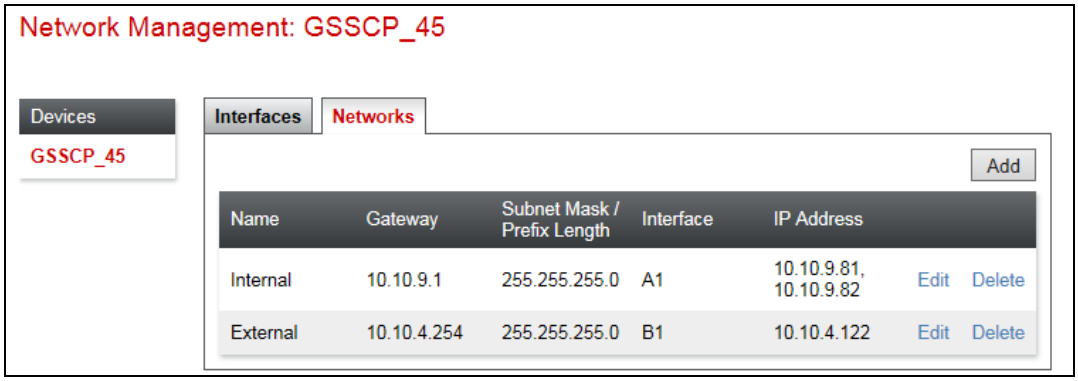
- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the test environment, this was **B1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.



Click on **Add** to define the internal interface if required. Enter details in the dialogue box (not shown):

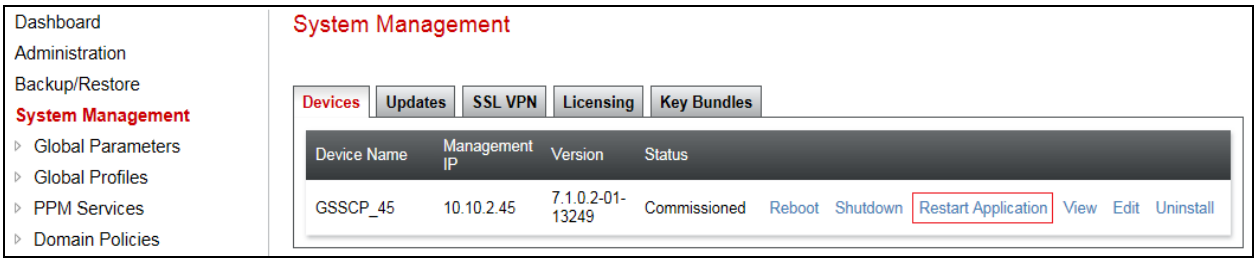
- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the first internal IP address for the Avaya SBCE in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Repeat the previous two steps and enter the second internal IP address for the Avaya SBCE in the **IP Address** field.
- Click on **Finish** to complete the interface definition.

The following screenshot shows the completed Network Management configuration:



Select the **Interface Configuration** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.

Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted. Click on **System Management** in the main menu and select **Restart Application**.



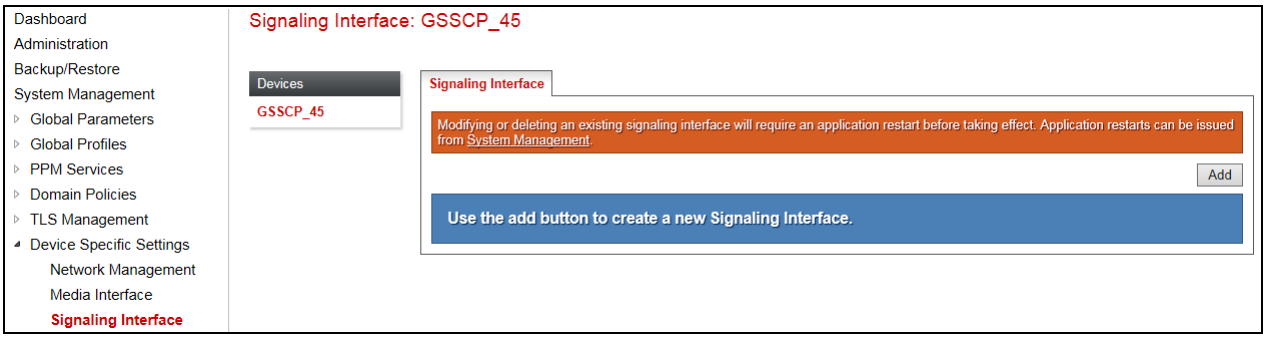
7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces. Testing was carried out with TCP used for transport of signalling between Session Manager and the Avaya SBCE, and UDP for transport of signalling between the Avaya SBCE and Orange SIP Trunking.

Signalling and media interfaces were required on both the internal and external sides of the Avaya SBCE, with two internal interfaces defined to facilitate separate server flows for the primary and secondary BTIP SBCs (see **Section 7.8**). This document shows the configuration for TCP and UDP, if additional security is required, it's recommended to use TLS and port 5061.

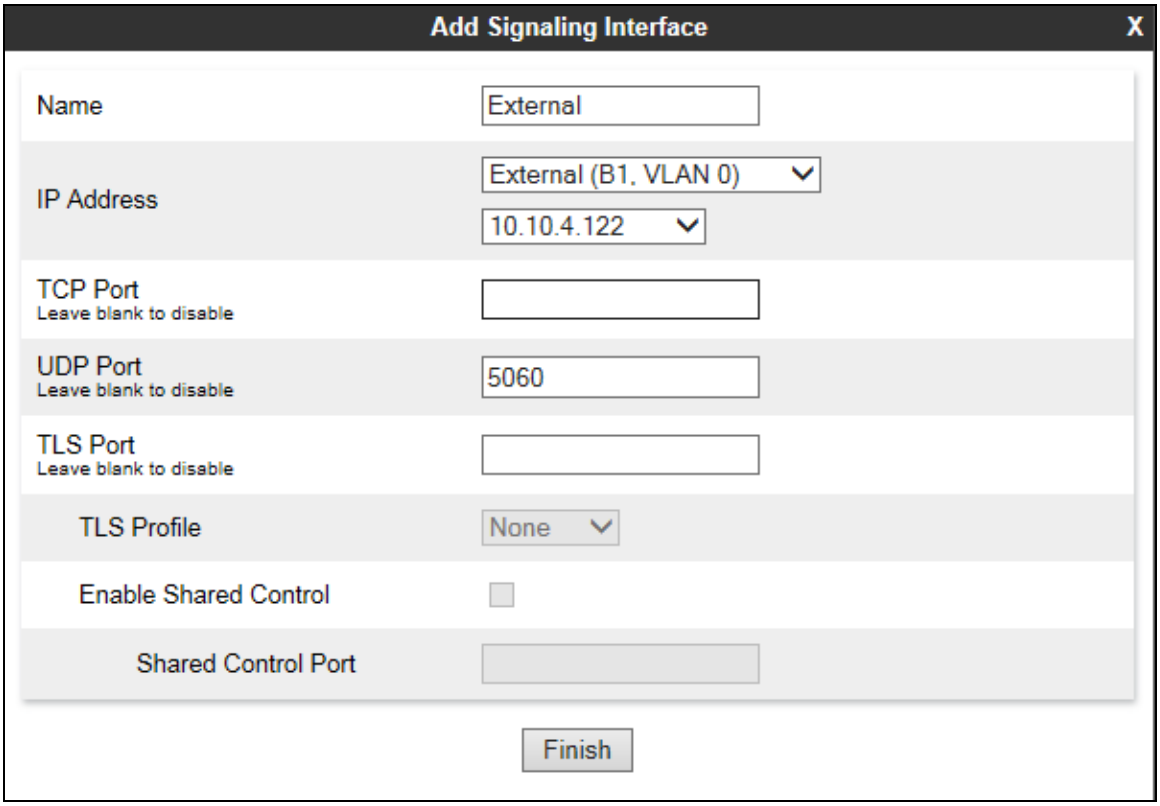
7.3.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Signaling Interface** in the main menu on the left hand side. Click on **Add**.



Details of transport protocol and ports for the external and internal SIP signalling are entered in the dialogue box.

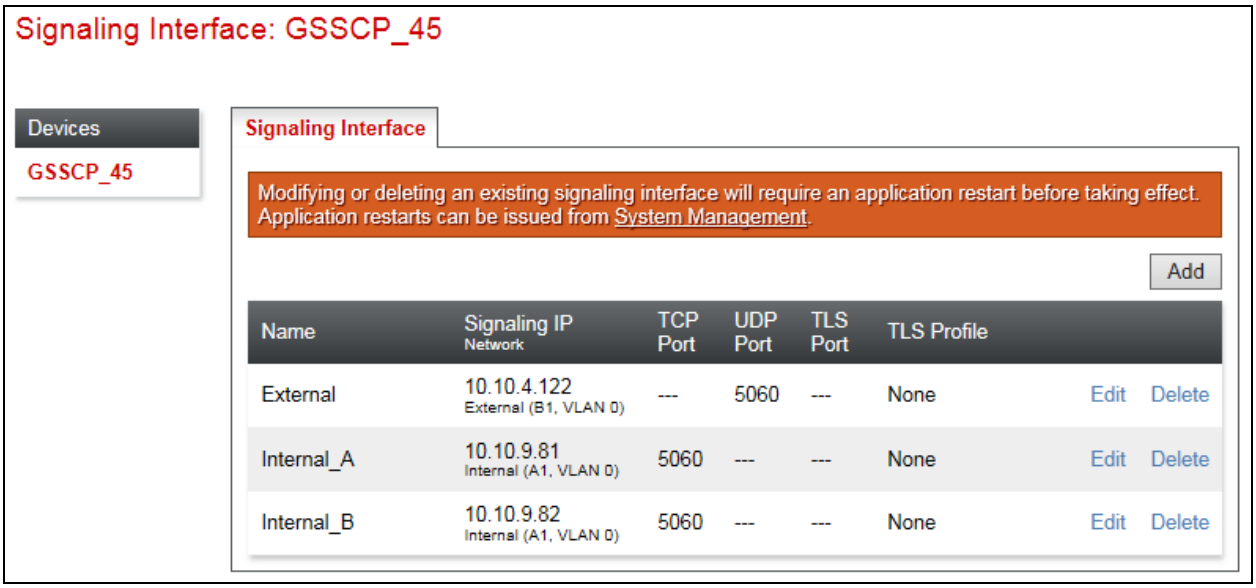
- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP address **10.10.4.122** for the Avaya SBCE interface on the SIP Trunk.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for Orange SIP Trunking.
- Click on **Finish**.



The internal signalling interfaces are defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the first internal signalling interface.
- In the **IP Address** drop down menus, select the internal network interface and the first internal IP address.
- Select **TCP** port number, **5060** is used for Session Manager.
- Repeat the process for the second internal IP address.

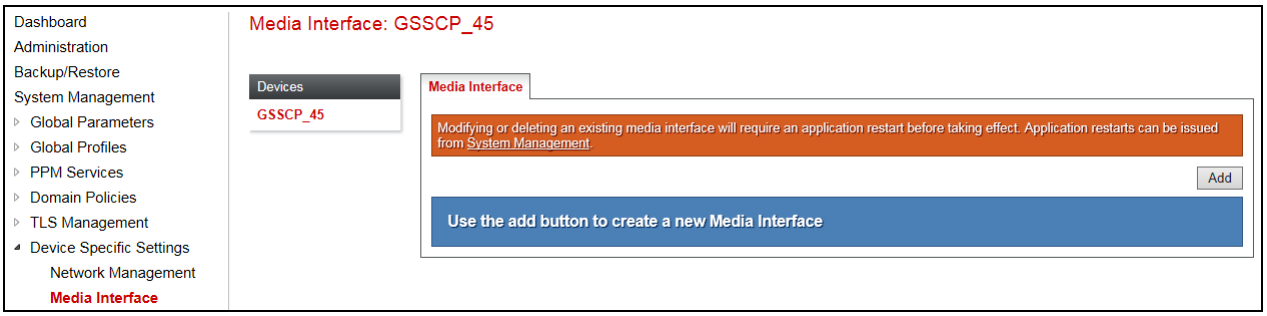
The following screenshot shows details of the signalling interfaces:



Note: In the test environment, the internal IP addresses were **10.10.9.81** and **10.10.9.82**. Two interfaces are required so that separate server flows can be implemented for the two BTIP network SBC's.

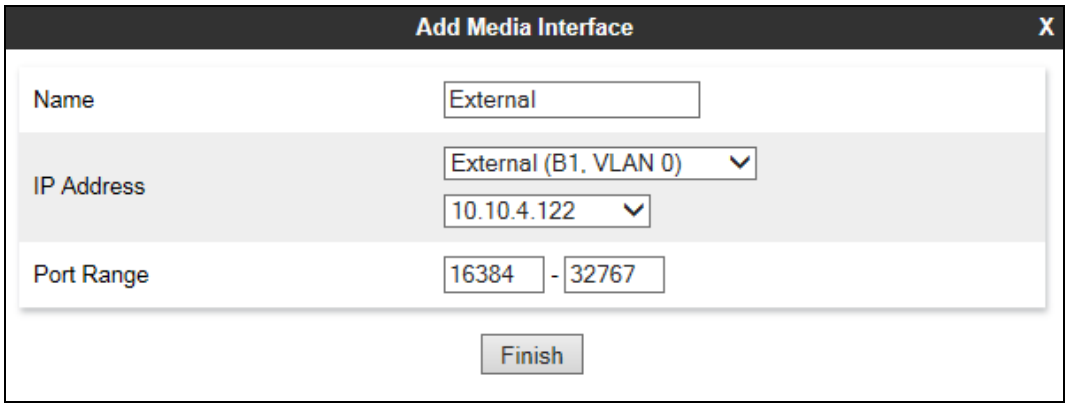
7.3.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Media Interface** in the main menu on the left hand side. Click on **Add**.



Details of the RTP port ranges for the internal and external media streams are entered in the dialogue box. The IP addresses for media can be the same as those used for signalling.

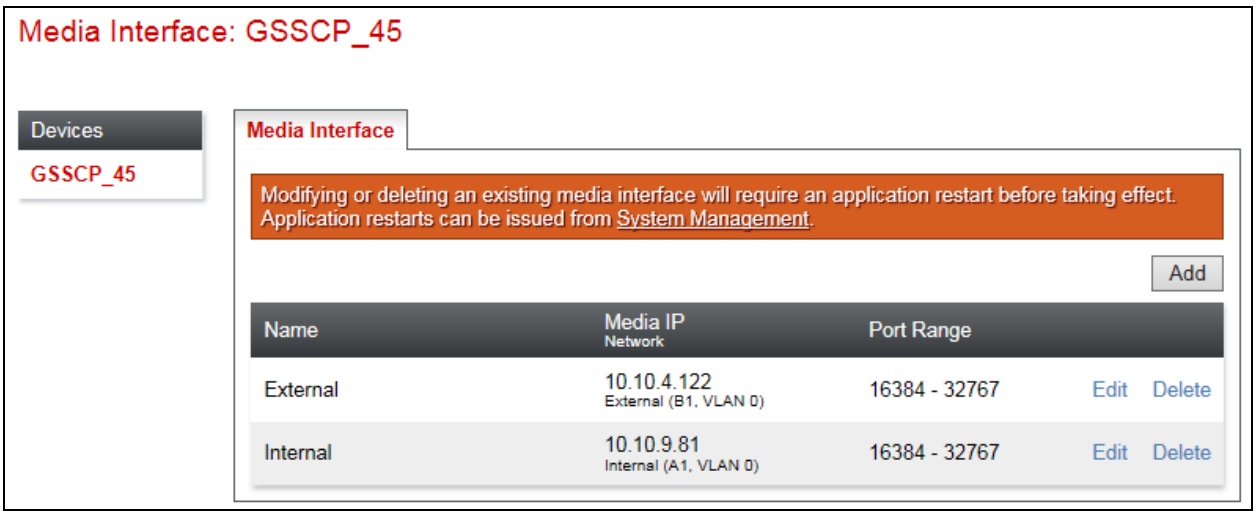
- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP address **10.10.4.122**.
- Define the RTP **Port Range** for the media path with Orange SIP Trunking, during testing this was **16384 - 32767**.



The internal media interfaces are defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.

The following screenshot shows details of the media interfaces:

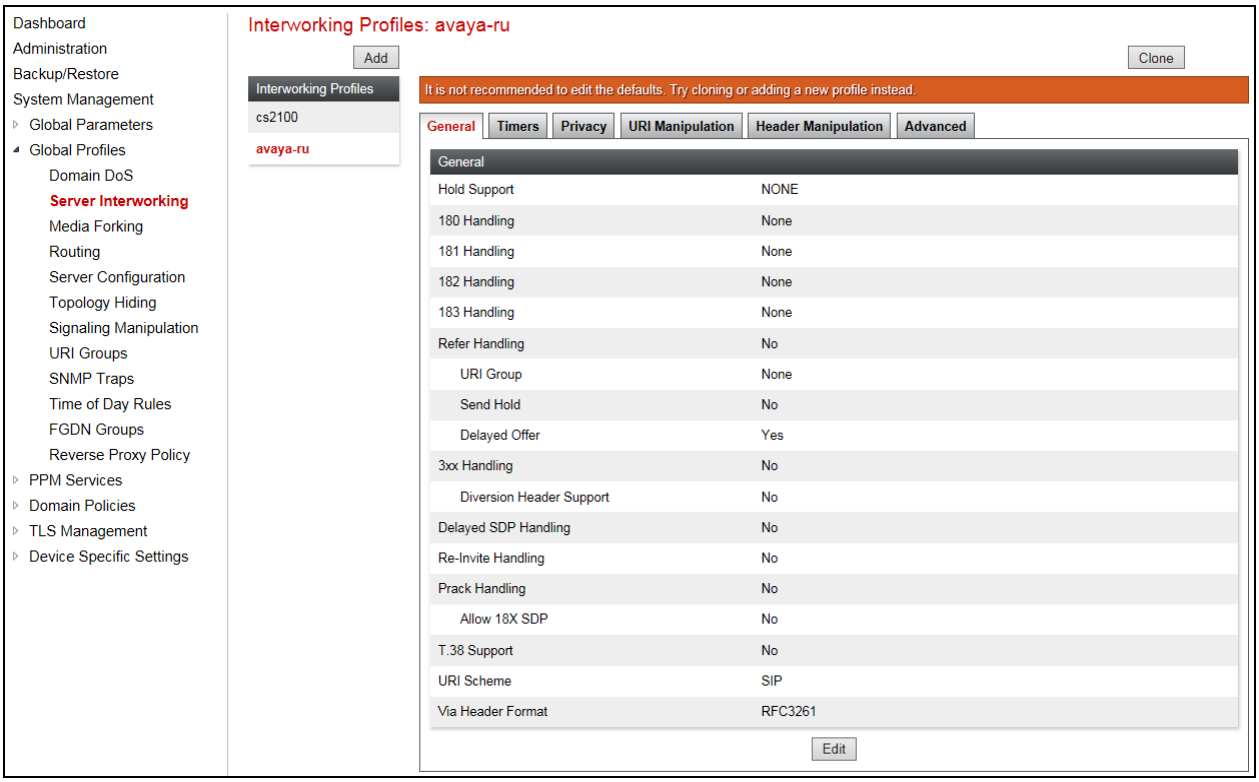


Note: In the test environment, the internal IP address was **10.10.9.81** and the port range was left at default values.

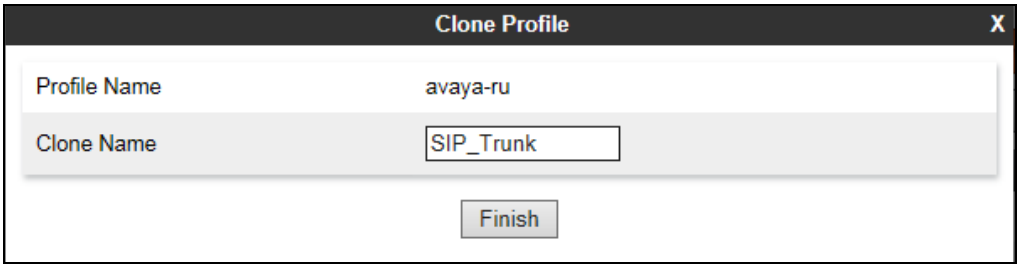
7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, Orange SIP Trunking is connected as the Trunk Server and the Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

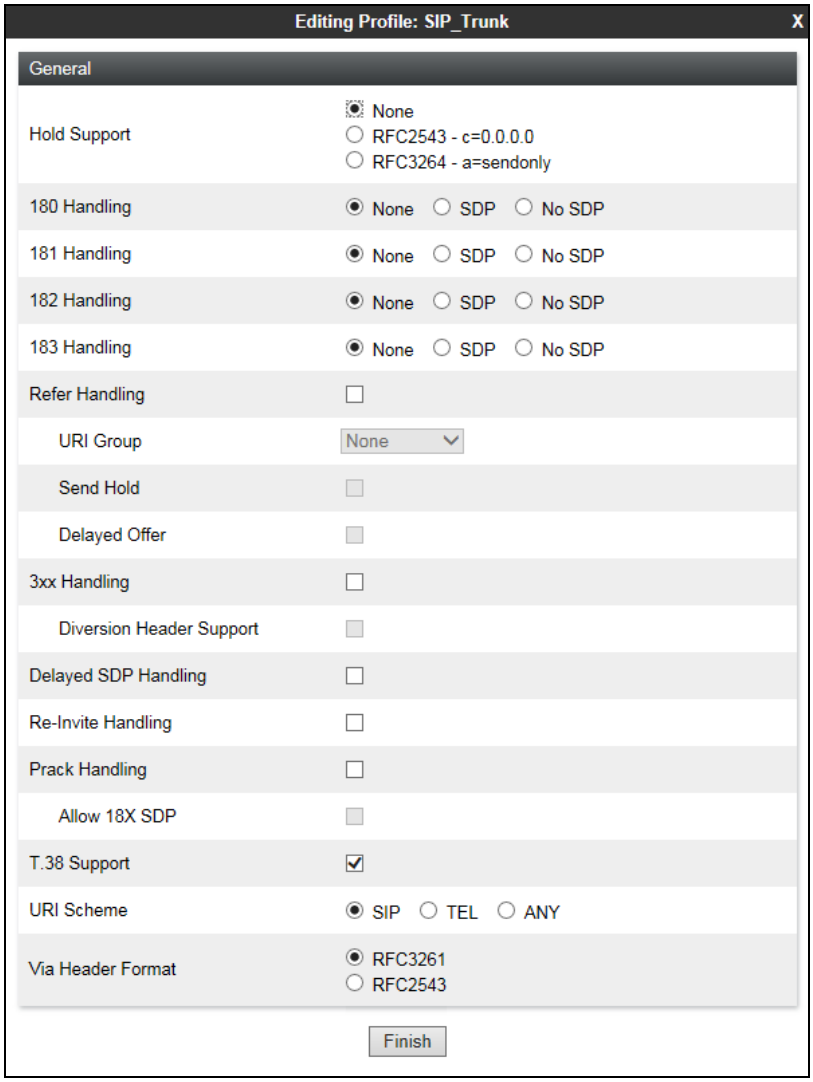
To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. To define Server Interworking for Orange SIP Trunking, highlight the **avaya-ru** profile and click on **Clone**.



A pop-up menu is generated. In the **Name** field enter a descriptive name for the Orange SIP Trunking network and click **Finish**.

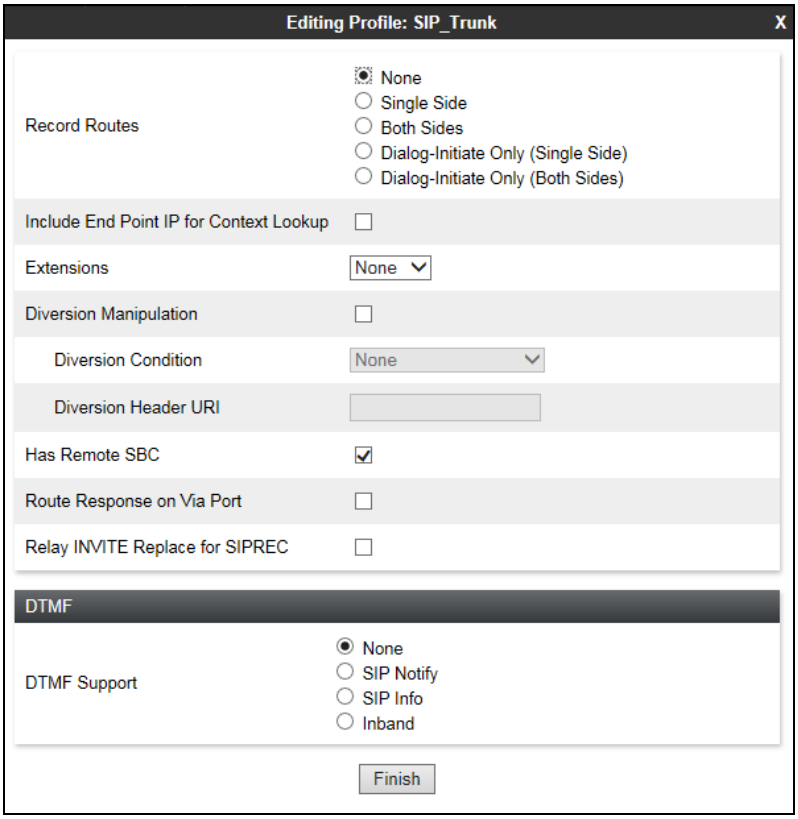


Select the General tab of the resulting Interworking Profile and click on Edit (not shown). The screenshot shows the cloned profile. Check the **T.38 Support** box and leave the rest of the parameters at their original settings. Click on **Finish**.



Select the **Advanced** tab (not shown) and click on **Edit**.

Set **Record Routes** to **None** as this header is not used by the network and select **None** in the **Extensions** drop down menu. Ensure that the **Has Remote SBC** box is checked. Click on **Finish**.



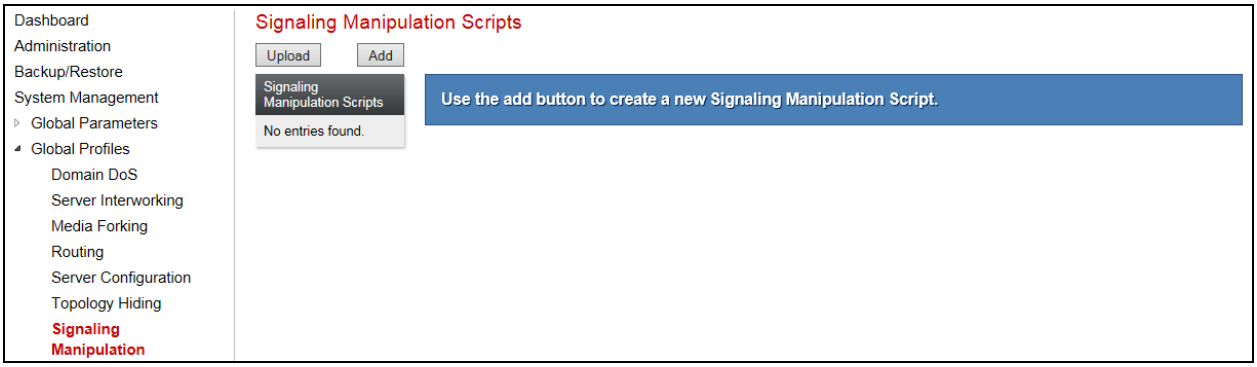
Repeat the process to define Server Interworking for Session Manager. In the Advanced tab (not shown), leave the settings at the original values cloned from the avaya-ru profile. **Record Routes** is set to **Both Sides** as the Session Manager uses the Record-Route header and **Avaya** is selected in the **Extensions** drop down menu.

7.5. Define Signalling Manipulation

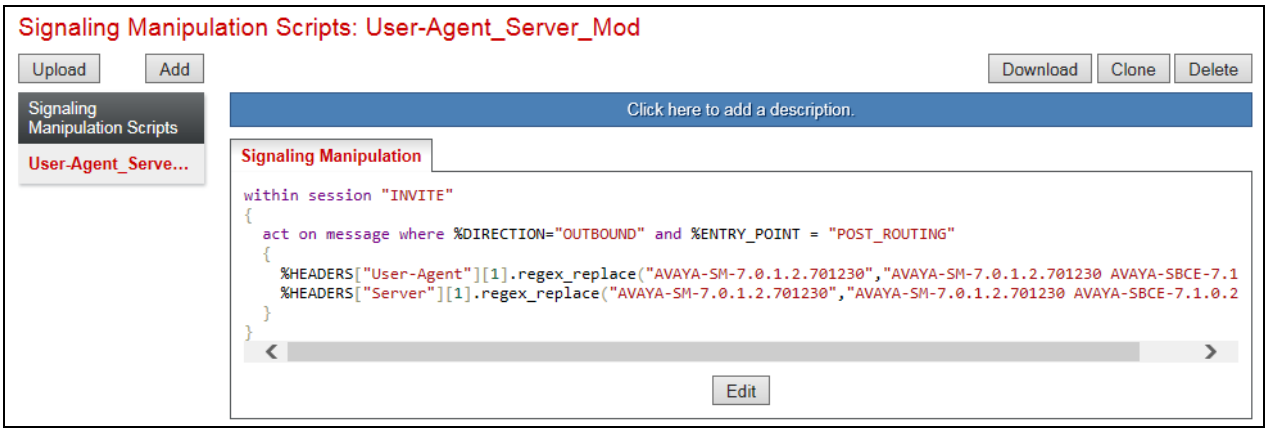
Signalling manipulation is required in cases where changes in signalling are needed between the Call Server and Trunk Server that can't be done by the Server Interworking described in the previous section. Orange requested that the User-Agent and Server parameters in the request and response messages from the Avaya solution include the Avaya SBCE information in addition to Communication Manager and Session Manager.

By default, the User-Agent and Server parameters in the request and response messages from the Avaya solution include the Communication Manager and Session Manager build levels. Typically, it would look something like this: "Avaya CM/R017x.00.0.441.0 AVAYA-SM-7.0.1.2.701230". During testing, a simple script was written to replace the Session Manager portion with both the Session Manager and Avaya SBCE build levels.

To define the signalling manipulation to add the Avaya SBCE build level, navigate to **Global Profiles → Signaling Manipulation** in the main menu on the left hand side. Click on **Add** which will open a script editor (not shown). Enter a title and the script.



Click on **Save** (not shown). The following screenshot shows the completed script used for the SIP compliance testing:



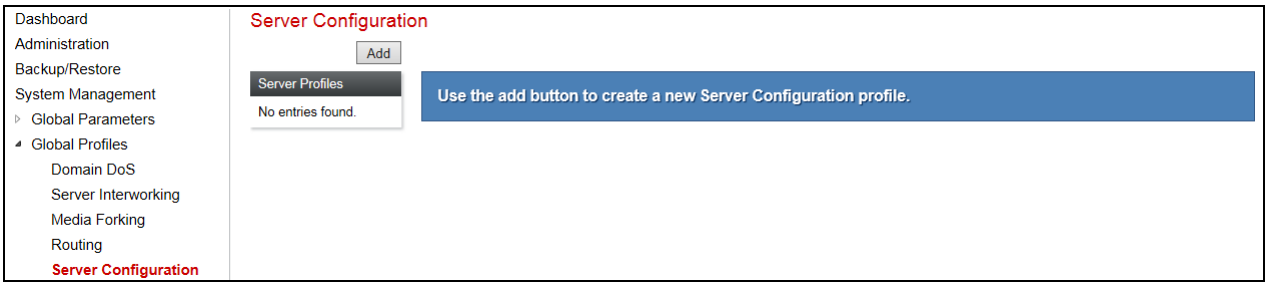
The name given to the script used in the test environment was **User-Agent_Server_Mod**. The script text is shown for reference:

```
within session "INVITE"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT = "POST_ROUTING"
  {
    %HEADERS["User-Agent"][1].regex_replace("AVAYA-SM-7.0.1.2.701230","AVAYA-SM-
7.0.1.2.701230 AVAYA-SBCE-7.1.0.2");
    %HEADERS["Server"][1].regex_replace("AVAYA-SM-7.0.1.2.701230","AVAYA-SM-
7.0.1.2.701230 AVAYA-SBCE-7.1.0.2");
  }
}
```

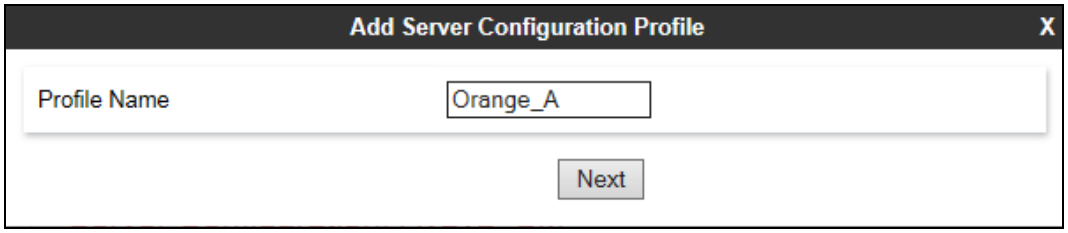
Note: The above script is only useful in an environment where it is kept updated when the Session Manager and/or the Avaya SBCE are updated.

7.6. Define Servers

A server definition is required for each server connected to the Avaya SBCE. Orange SIP Trunking is connected as two Trunk Servers, one for each SBC. Session Manager is connected as a Call Server. To define the Orange SIP Trunking Servers, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add**.

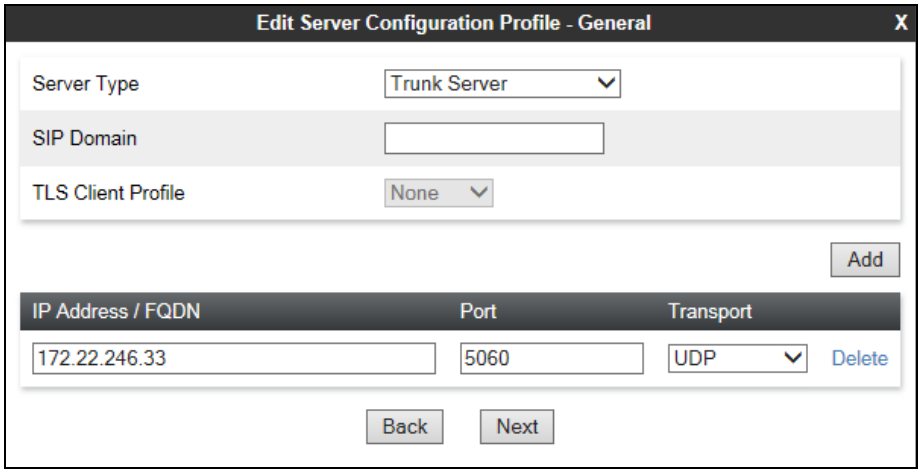


Enter an appropriate name for the primary SBC in the pop-up menu and click on **Next**.

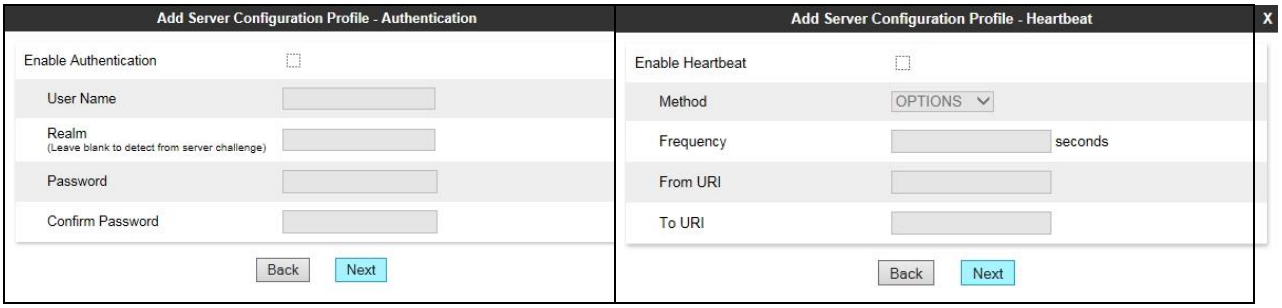


Enter details in the dialogue box.

- In the **Server Type** drop down menu, select **Trunk Server**.
- Click on **Add** to enter an IP address.
- In the **IP Addresses / FQDN** box, type the IP address of the primary SBC.
- In the **Port** box, enter the port to be used for the SIP Trunk.
- In the **Transport** drop down menu, select **UDP**.
- Click on **Next**.

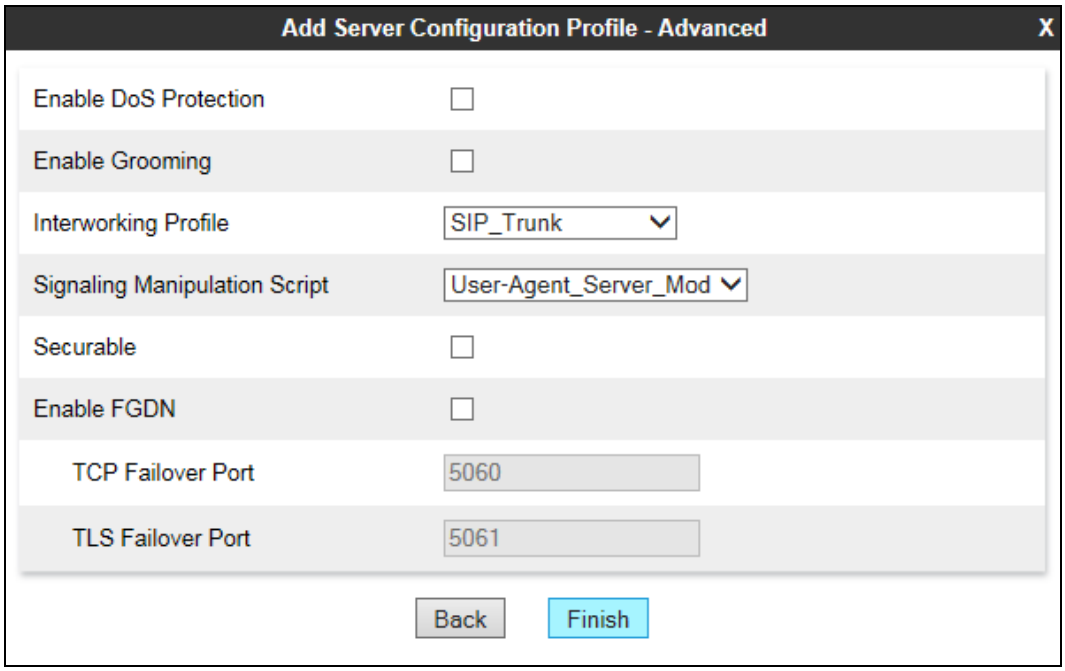


Click on **Next** and **Next** again. Leave the fields in the dialogue boxes at default values.



Click on **Next** again to get to the final dialogue box. This contains the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for Orange SIP Trunking defined in **Section 7.4**.
- In the **Signalling Manipulation Script** drop down menu, select the Sigma Script defined in **Section 7.5** if required.
- Leave the other fields at default settings.
- Click **Finish**.

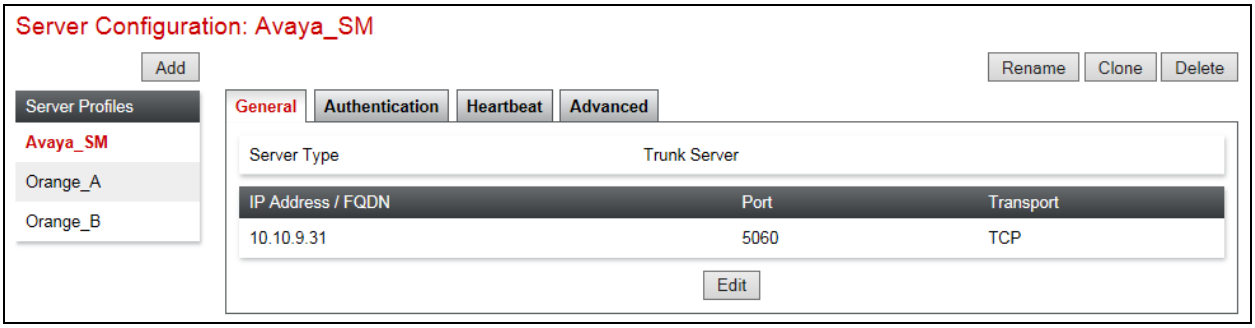


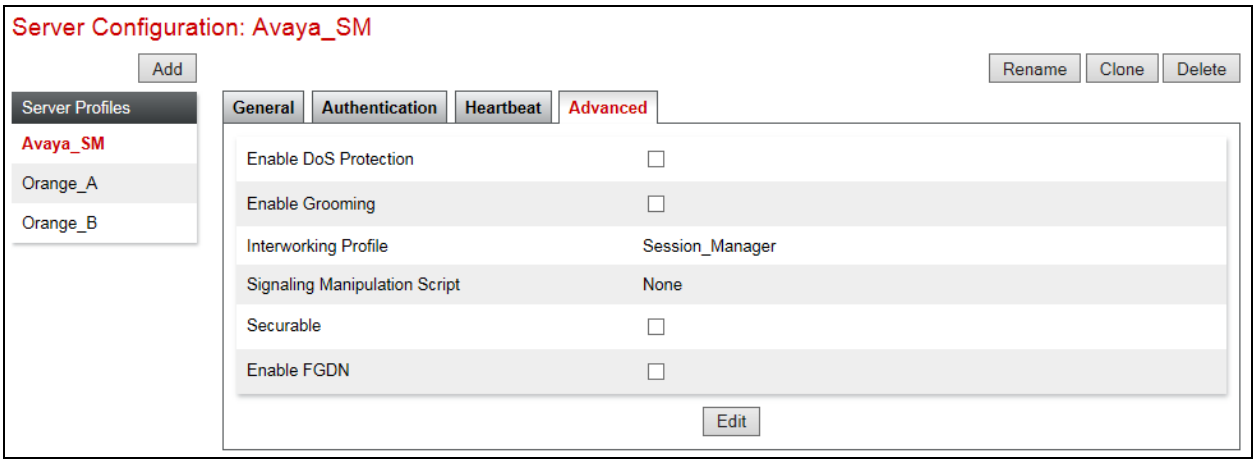
Repeat the above process to define the Trunk Server configuration (not shown) for the alternative Orange SBC. This is identical apart from the name and IP address which were **Orange_B** and **172.22.246.73** respectively.

Use the process described to define the Call Server configuration for Session Manager if not already defined. Leave the Authentication and Heartbeat settings at default values.

- Ensure that **Call Server** is selected in the **Server Type** drop down menu in the **General** dialogue box (not shown).
- Ensure that the Interworking Profile defined for Session Manager in **Section 7.4** is selected in the **Interworking Profile** drop down menu in the **Advanced** dialogue box (not shown).

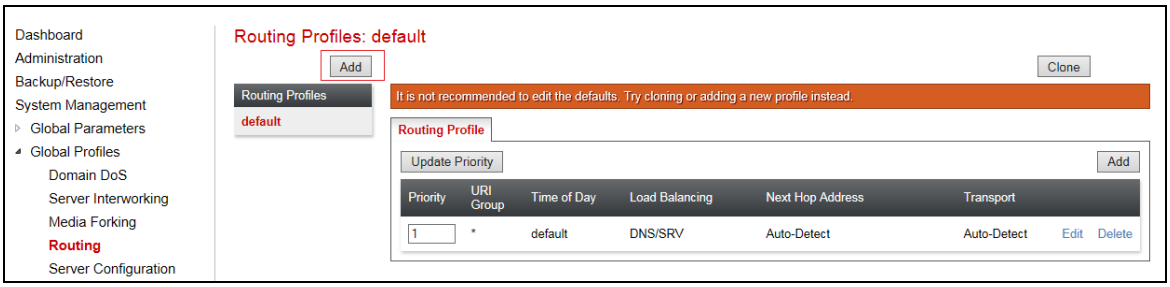
The following screenshots show the **General** and **Advanced** tabs of the Server Configuration:



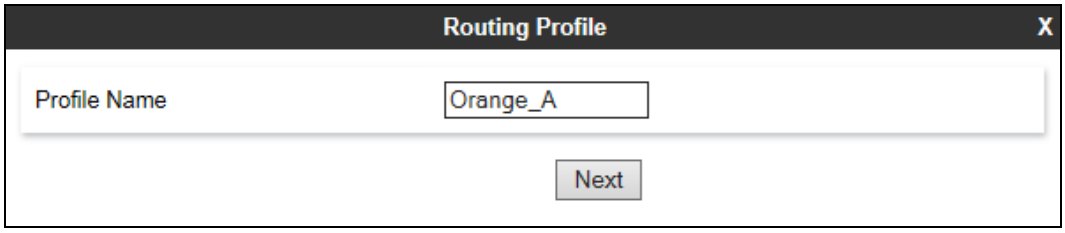


7.7. Define Routing

Routing information is required for routing to Orange SIP Trunking on the external side and Session Manager on the internal side. The IP addresses and ports defined here will be used as the destination addresses for signalling. To define routing to the Orange primary SBC, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add**.

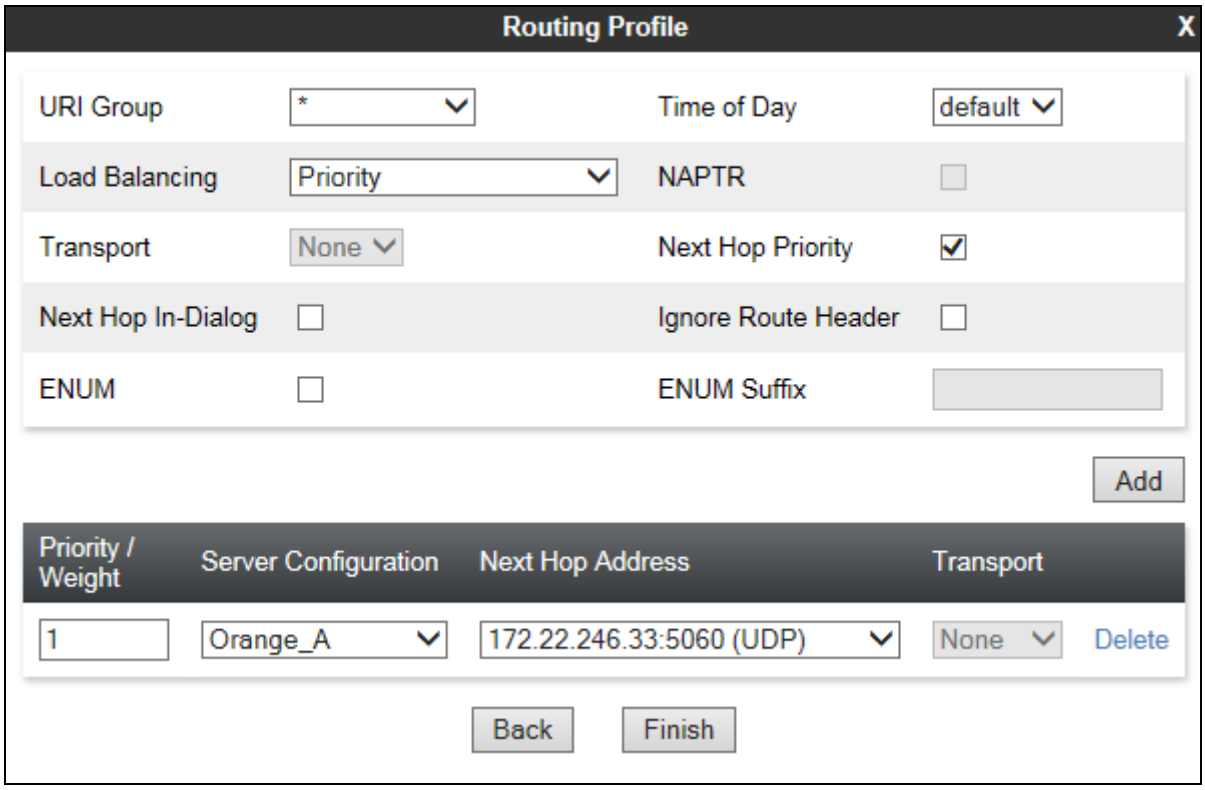


Enter an appropriate name in the dialogue box. And click on **Next**.



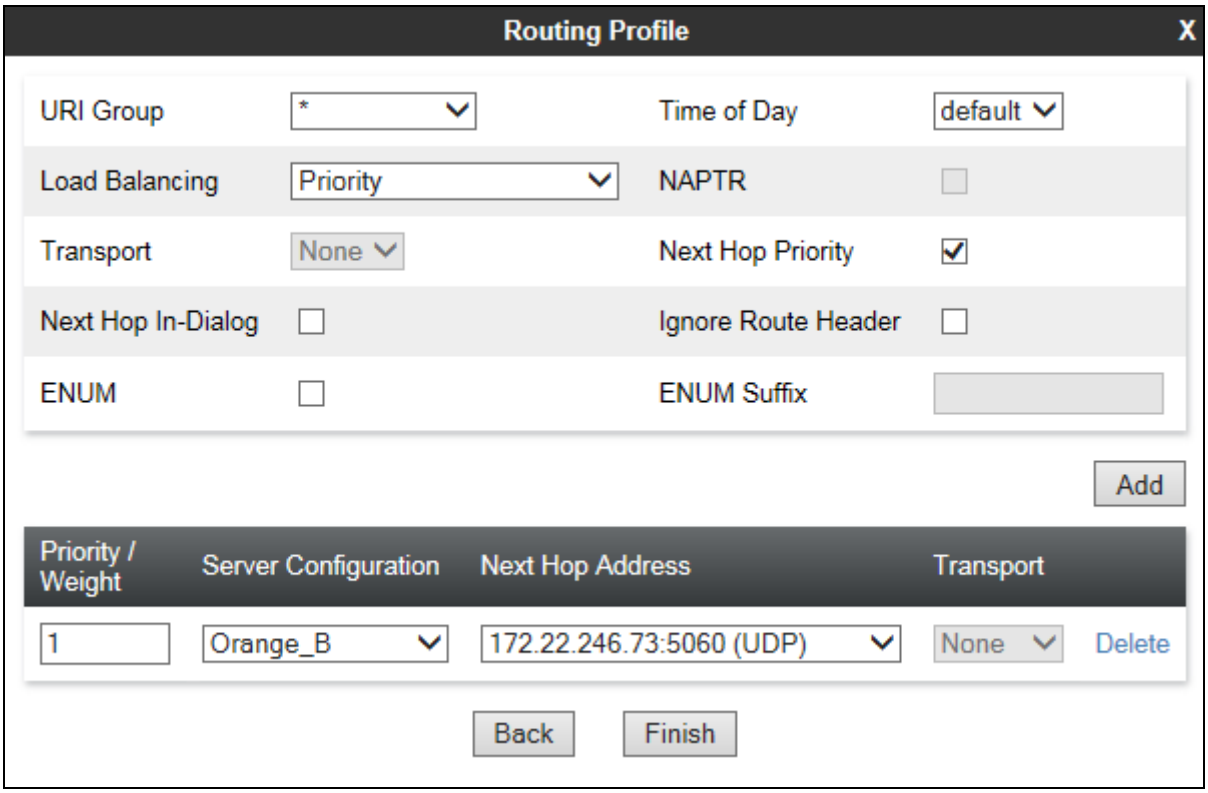
Enter details for the Routing Profile for the SIP Trunk:

- During testing, **Load Balancing** was not required and was left at the default value of **Priority**.
- Click on **Add** to specify an address for the SIP Trunk.
- Assign a priority in the **Priority / Weight** field, during testing **1** was used.
- Select the Server Configuration for the Orange primary SBC defined in **Section 7.6** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field.
- Click **Finish**.

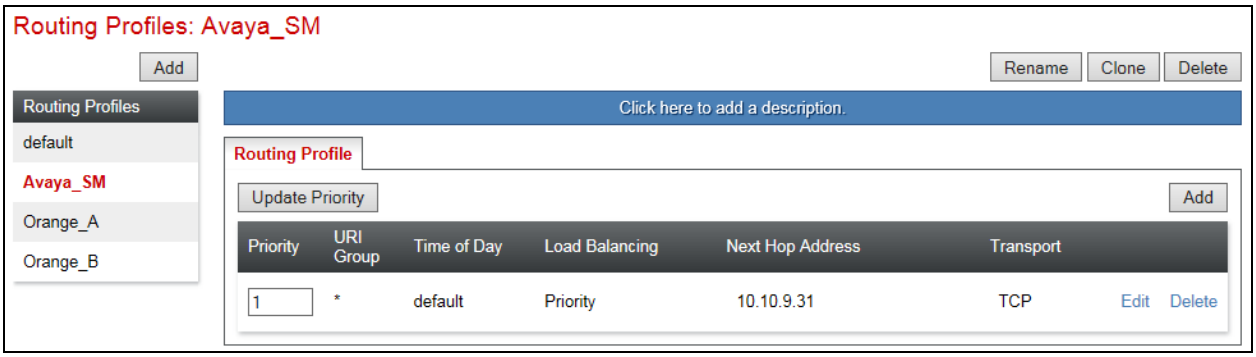


Repeat the above process to define a Routing Profile for the Orange secondary SBC.

The screenshot shows the configuration used for the Orange secondary SBC in the test environment:



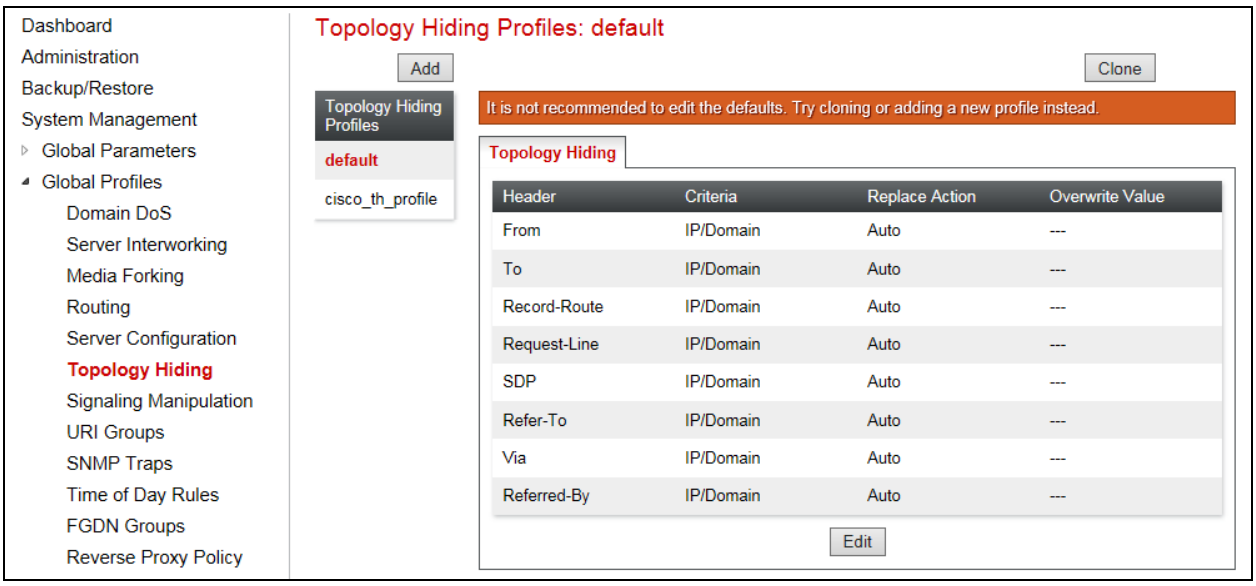
Repeat the process for the Routing Profile for Session Manager. The following screenshot shows the completed configuration:



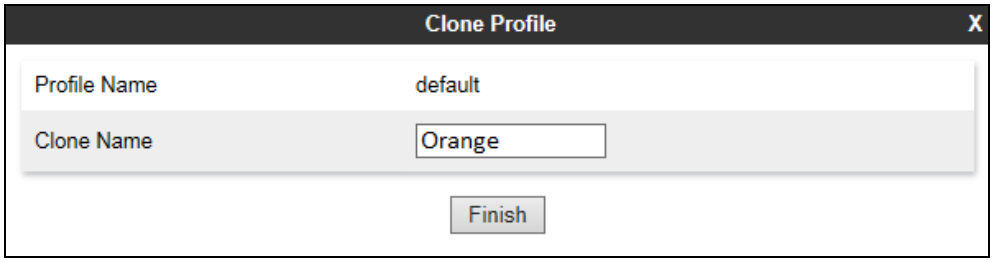
7.8. Topology Hiding

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 for termination information and the external interfaces for origination information.

To define Topology Hiding for Orange SIP Trunking, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side. Select the default profile and click on **Clone**.



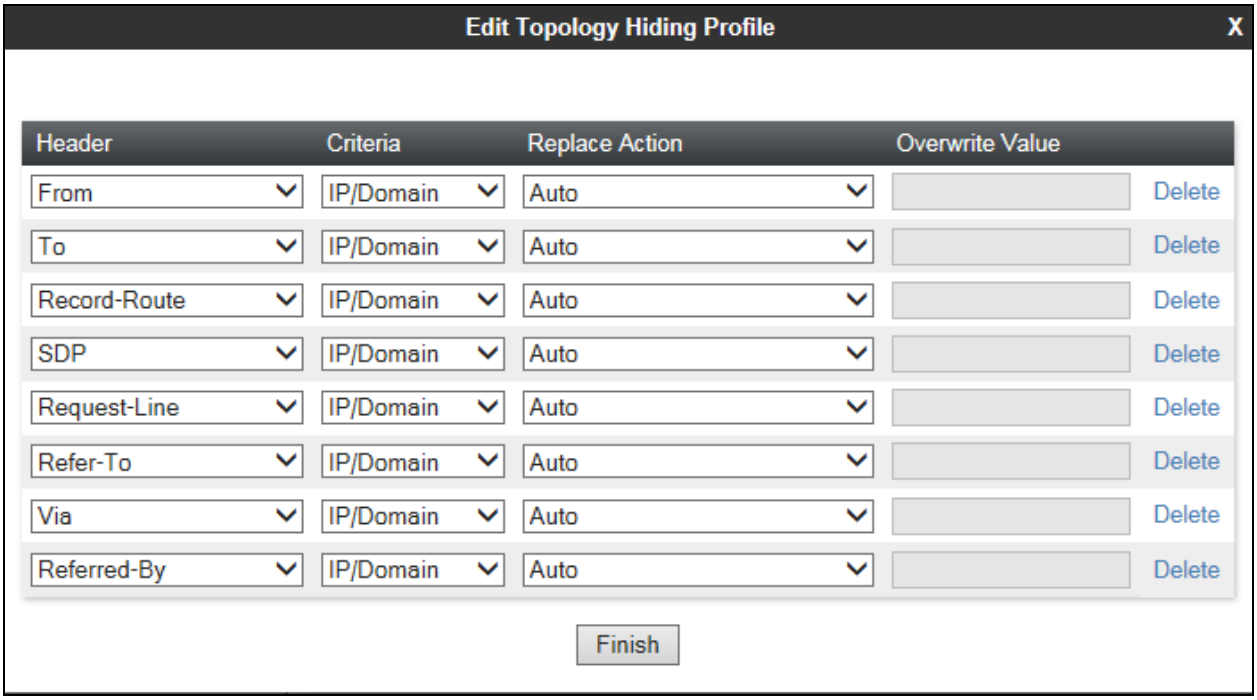
Assign an appropriate name in the dialogue box and click on **Finish**:



Highlight the new Topology Hiding profile (not shown) and click on **Edit**. Make changes if required.

During testing, fields were left at default values. If changes are required:

- Select **IP** or **IP/Domain** from the **Criteria** drop down menu. The default setting **IP/Domain** hides both domain names and IP addresses.
- Default action **Auto** in the **Replace Action** drop down menu replaces internal IP addresses or domain names with external IP addresses.
- If **Overwrite** is selected as the action, define the required domain name in the **Overwrite Value** field. This was not used during testing.
- Click on **Finish**.



To define Topology Hiding for Session Manager, follow the same process. During testing, the default profile was used so an additional profile was not required.

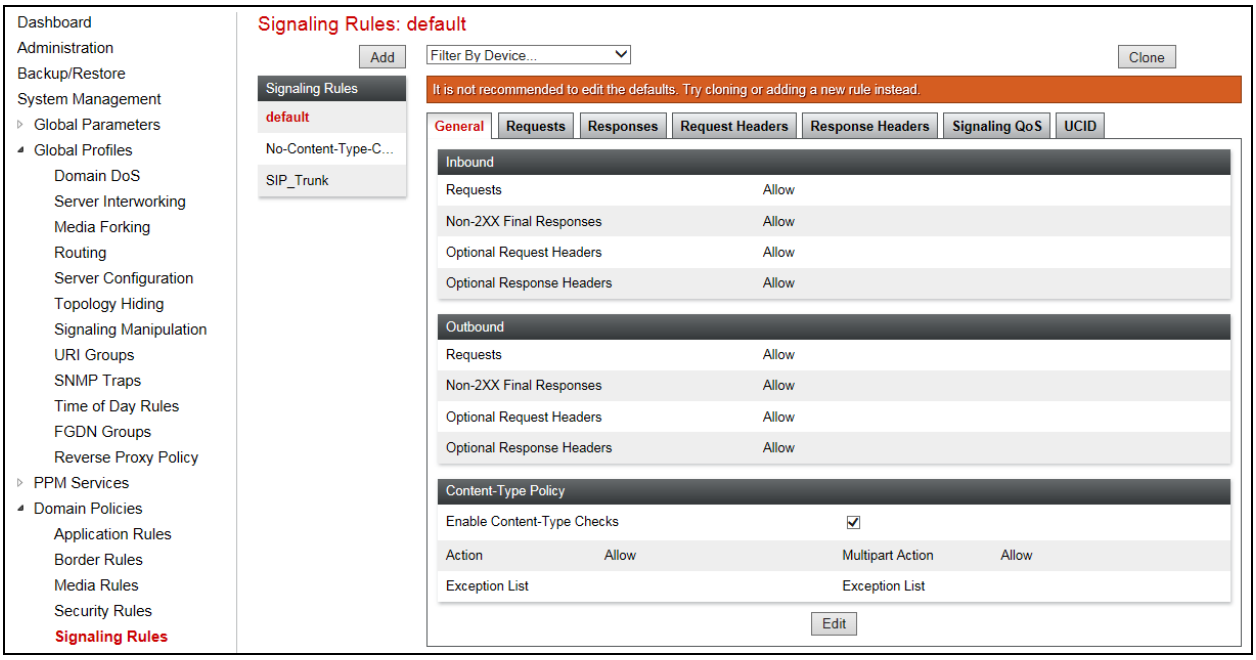
7.9. End Point Policy Groups

End Point Policy Groups are used to bring together a number of different rules for use in a server flow described in **Section 7.10**. Orange SIP Trunking was tested with a signalling rule to remove unnecessary and Avaya proprietary SIP headers that couldn't be removed with a Session Manager Adaptation (see **Section 6.4**). This was not necessary for the effective functioning of the SIP Trunk but was used to reduce the SIP message size.

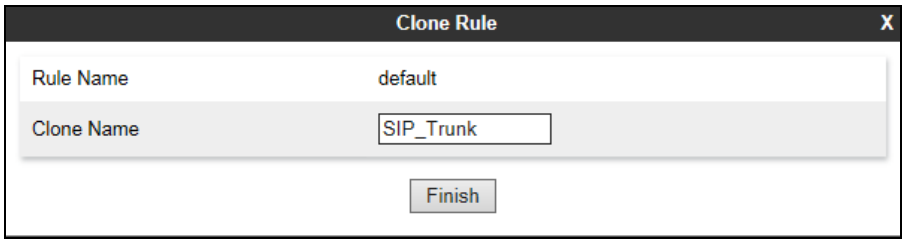
7.9.1. Signalling Rules

Signalling rules are used to handle any non-standard signalling that may be encountered on a SIP Trunk, in this case the transmission of Avaya proprietary and unnecessary SIP message headers from the Avaya equipment.

To define the signalling rule, navigate to **Domain Policies →Signaling Rules** in the main menu on the left hand side. Highlight the default signalling rule and click on **Clone**.



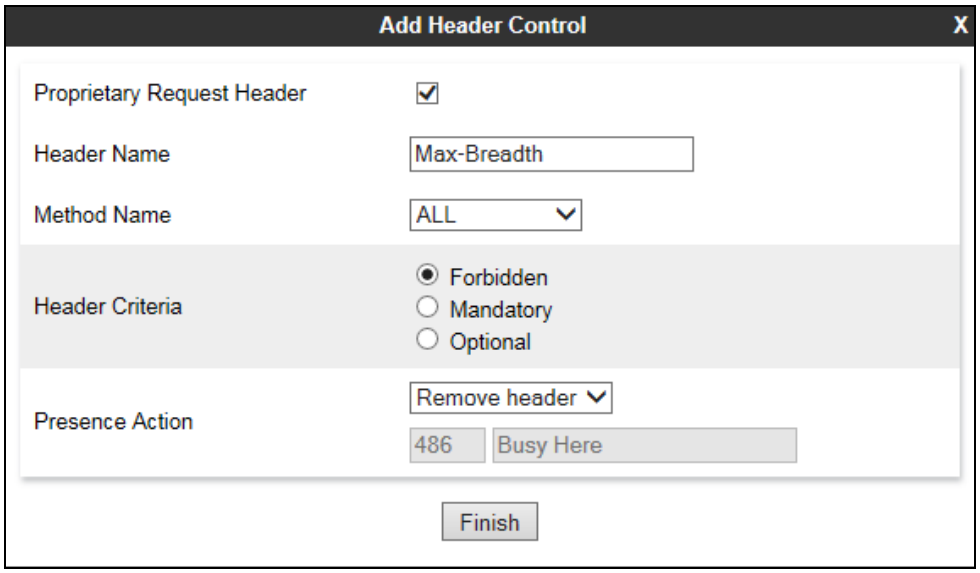
Enter a **Rule Name** in the **Clone Rule** dialogue box and click on **Finish**.



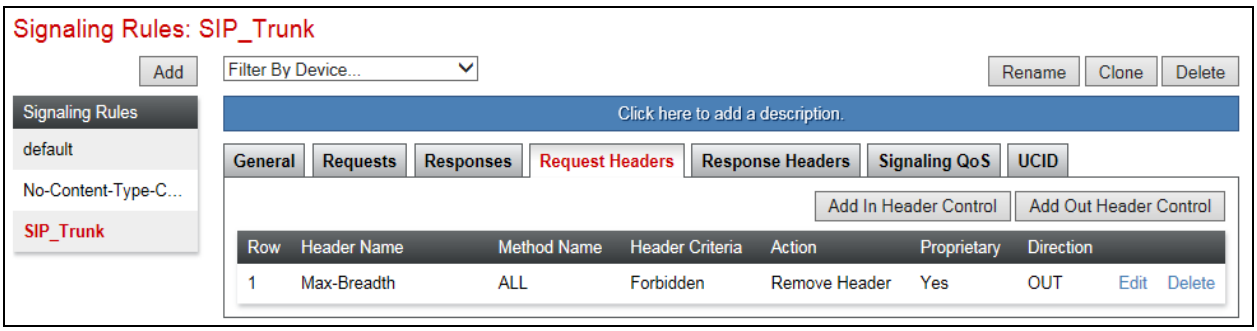
In the test environment, the Max-Breadth parameter was removed from the SIP INVITE message from Communication Manager. This parameter is the only one of the identified unnecessary parameters that could not be removed using the Session Manager Adaptation described in **Section 6.4**. Max-Breadth is used for media forking and is not required in the Orange SIP Trunking service.

To remove the Max-Breadth parameter, highlight the recently created Signalling Rule click on the **Request Headers** tab and click on **Add Out Header Control** (not shown).

- Check the **Proprietary Request Header** box.
- Type **Max-Breadth** in the **Header Name** field.
- Leave **Method Name** at the default value of **ALL**.
- Check the **Forbidden** radio button in the **Header Criteria field**.
- Leave the **Presence Action** at the default value of **Remove Header**.
- Click on **Finish**.



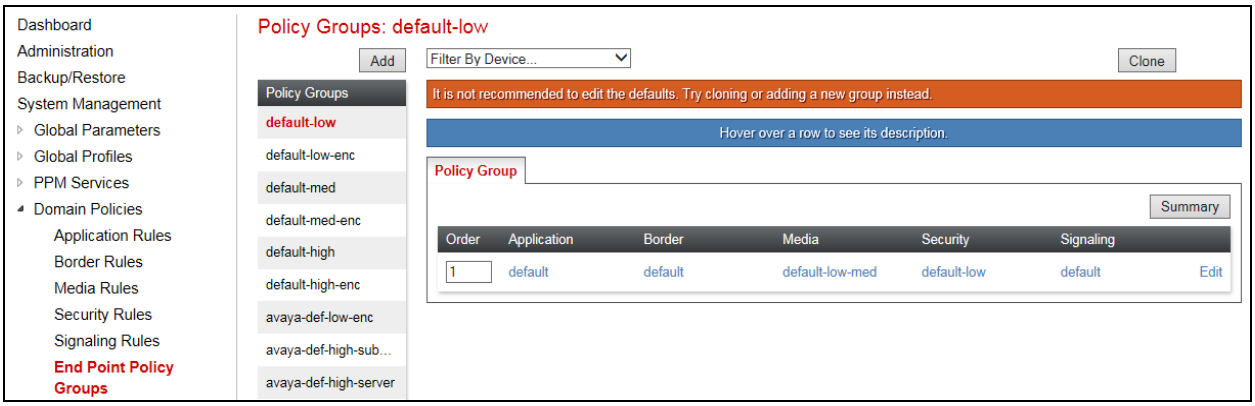
The following screenshot shows the applied Request Header removal:



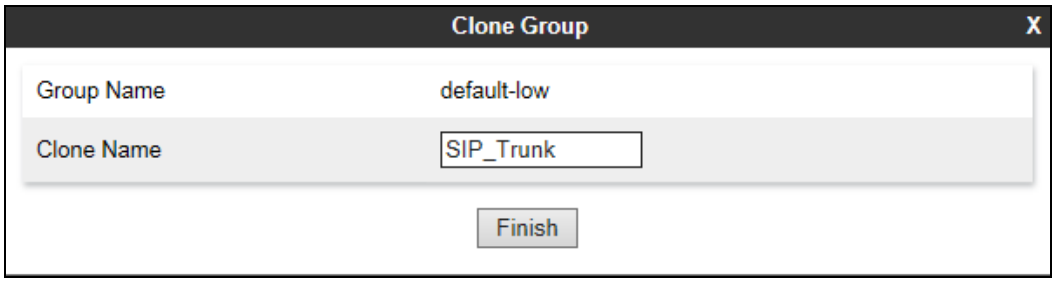
7.9.2. End Point Policy Group

An End Point Policy Group is required to implement the signalling rule. To define one for use in the Session Manager server flow, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left hand side.

Select an appropriate pre-defined Policy Group, in the test environment this was **default-low**, and click on **Clone**.

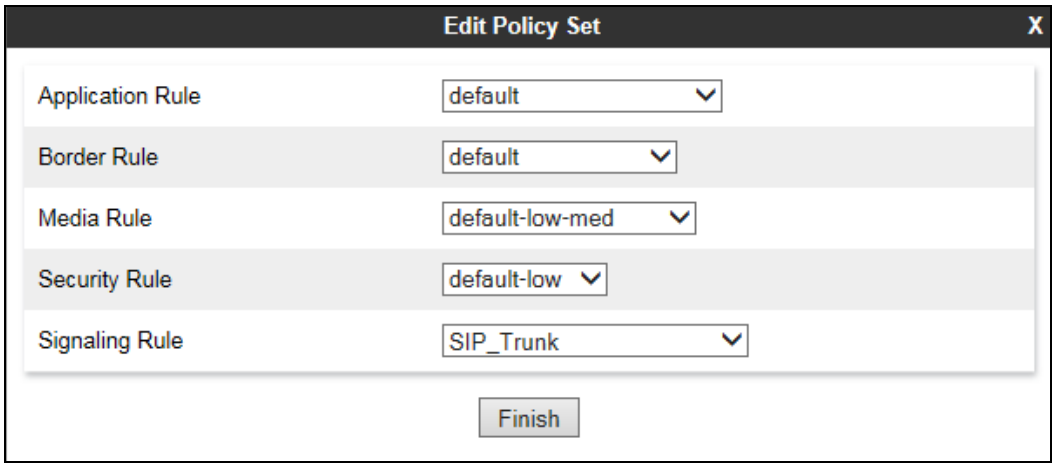


Enter an appropriate name in the pop-up box.

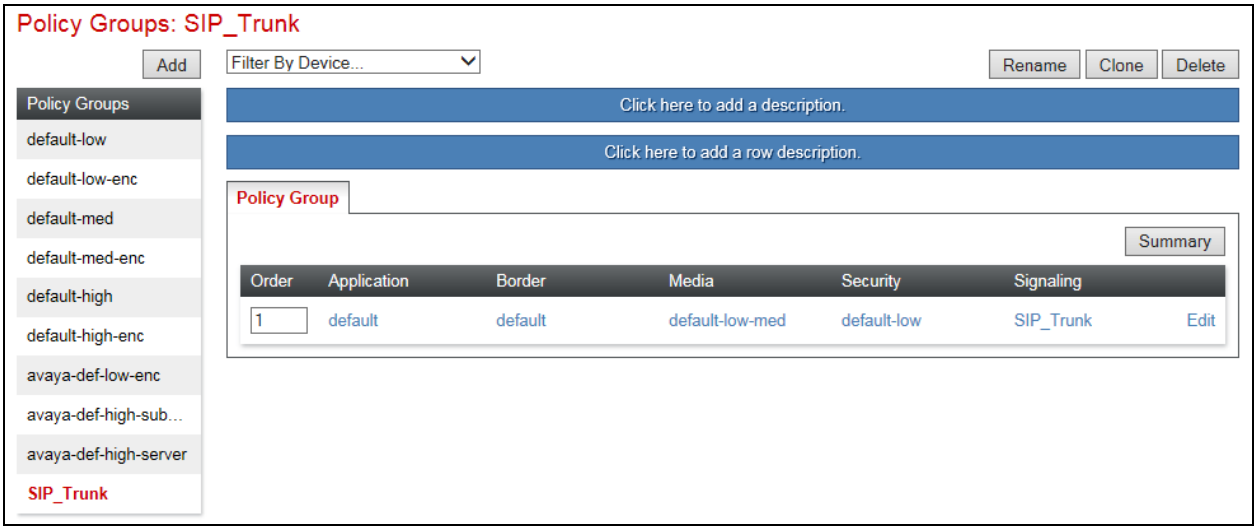


Highlight the resulting Policy Group and click on **Edit**. Enter details as follows:

- Leave the **Application Rule**, **Border Rule**, **Media Rule** and **Security Rule** at their default values.
- Select the **Signaling Rule** created in the previous section in the drop down menu.
- Click on **Finish**.



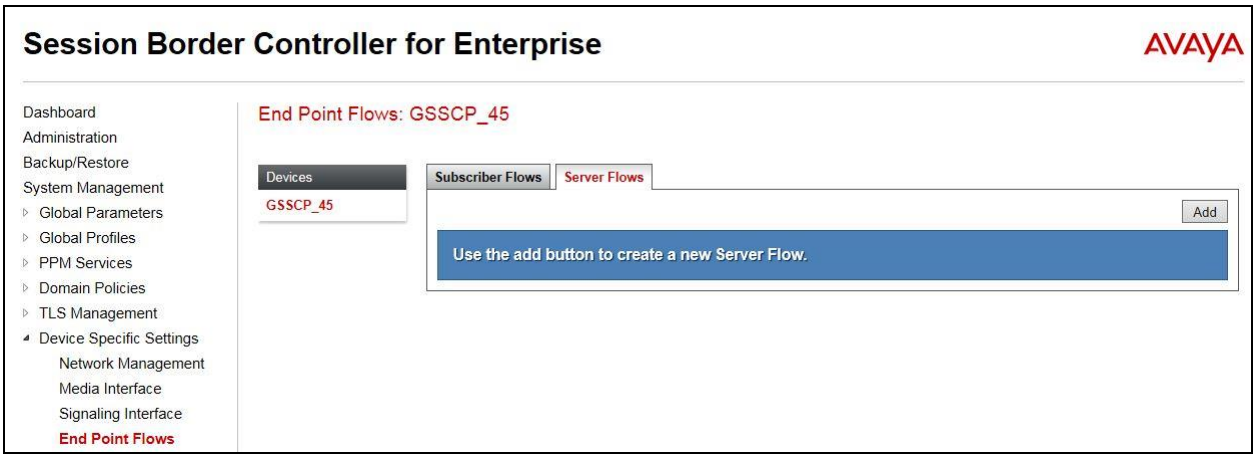
The completed Policy Group is shown in the following screenshot:



7.10. Server Flows

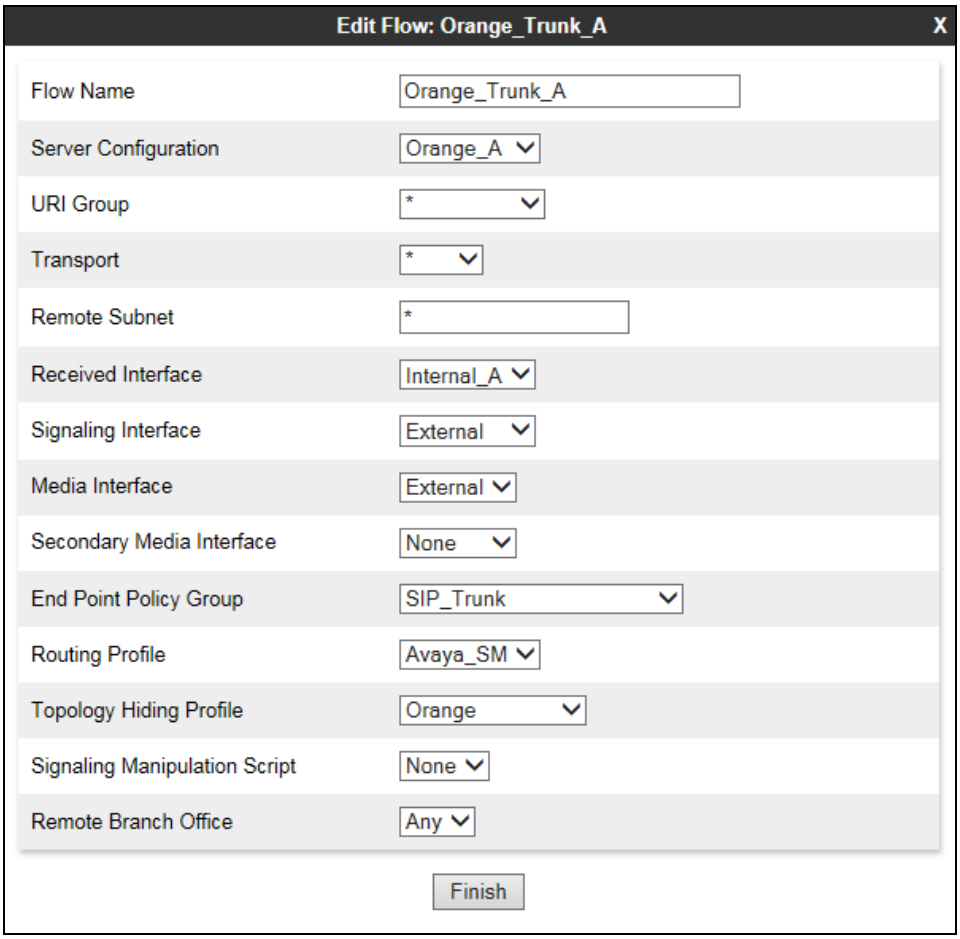
Server Flows combine the previously defined profiles into four End Point Server Flows, two for the Session Manager and two for Orange SIP Trunking. This configuration ties all the previously entered information together so that calls can be routed from Session Manager to the Orange primary and secondary SBC's and vice versa.

To define a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click on **Add**.



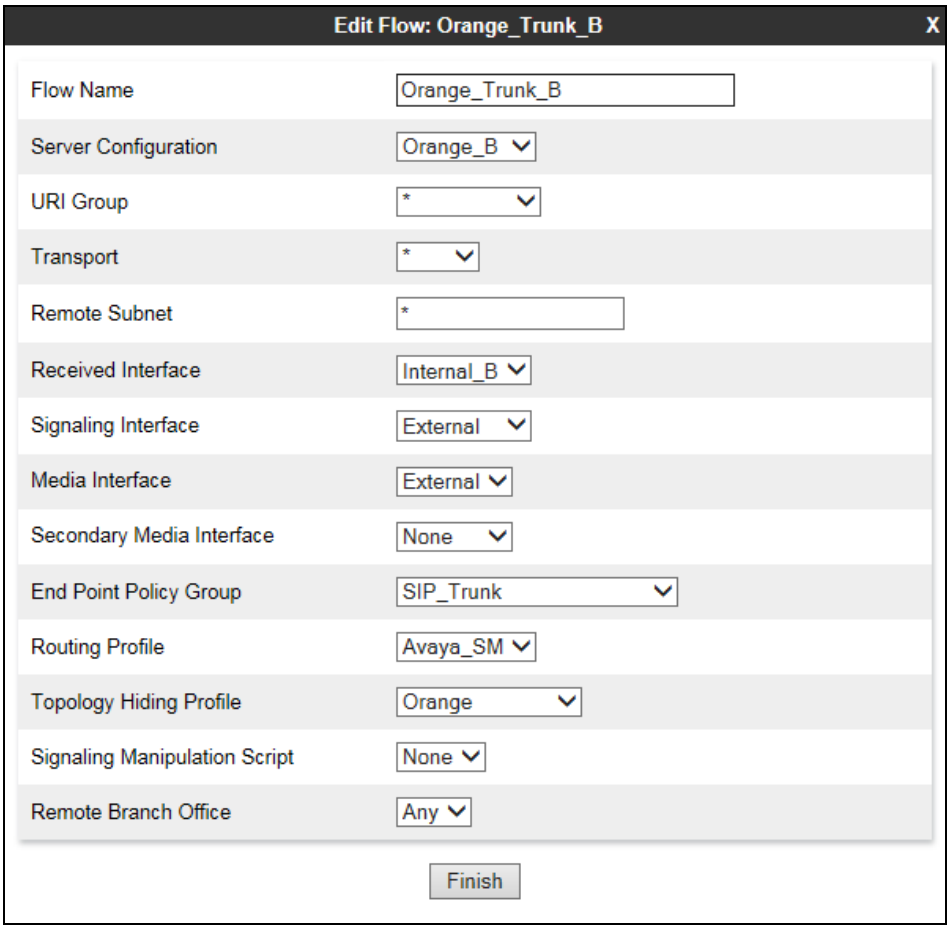
Define the Server flow for the Orange primary SBC as follows:

- In the **Flow Name** field enter a descriptive name for the server flow for the Orange primary SBC, in the test environment **Orange_Trunk_A** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the primary SBC defined in **Section 7.6**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the primary SBC is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the network SBC's (both primary and secondary) is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for the network SBC's is sent on.
- In the **End Point Policy Group** drop-down menu, select the Policy Group for the SIP Trunk defined in **Section 7.9**.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Orange SIP Trunking defined in **Section 7.8** and click **Finish**.



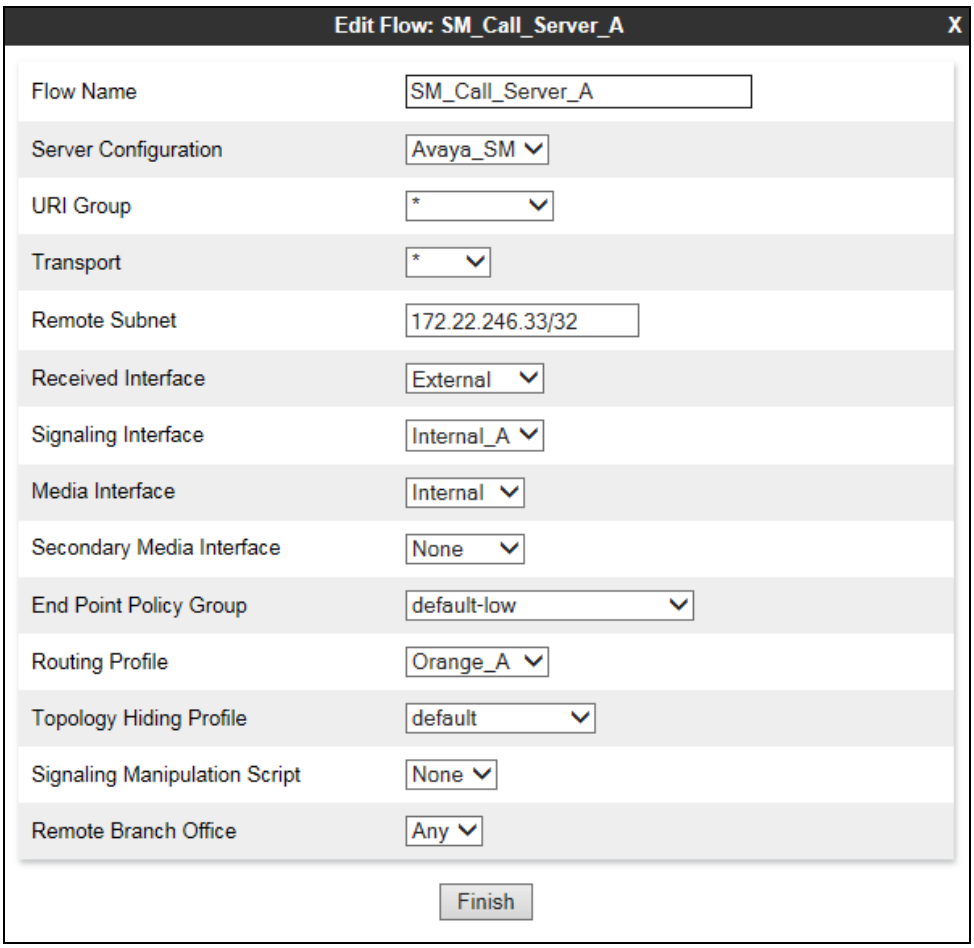
Define the Server flow for the Orange secondary SBC as follows:

- In the **Flow Name** field enter a descriptive name for the server flow for the Orange secondary SBC, in the test environment **Orange_Trunk_B** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the secondary SBC defined in **Section 7.6**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the secondary SBC is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the network SBC's (both primary and secondary) is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for the network SBC's is sent on.
- In the **End Point Policy Group** drop-down menu, select the Policy Group for the SIP Trunk defined in **Section 7.9**.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Orange SIP Trunking defined in **Section 7.8** and click **Finish**.



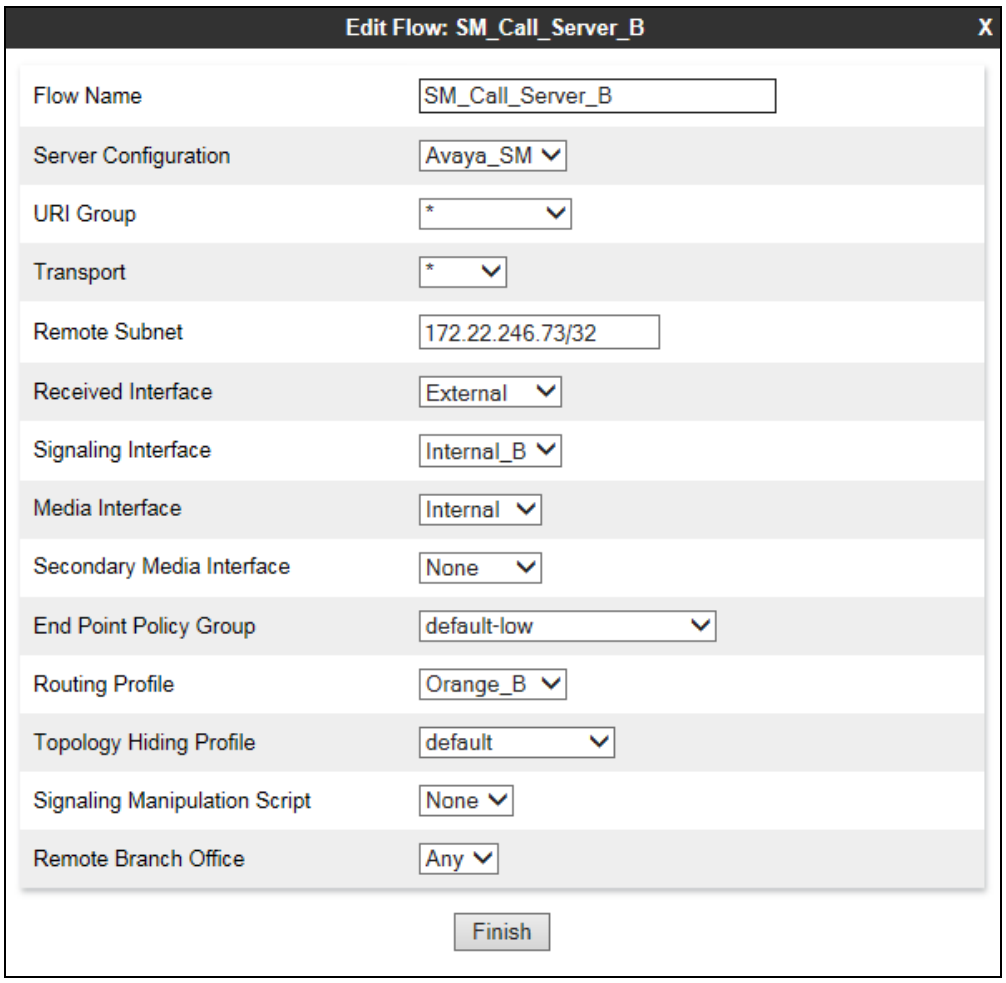
Define a Session Manager Server Flow for signalling between Session Manager and the Orange primary SBC as follows:

- In the **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **SM_Call_Server_A** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.5**.
- In the **Remote Subnet** field, type the IP address of the primary SBC with a 32 bit mask.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling from the primary SBC bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Orange primary SBC defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select **default** and click **Finish**.

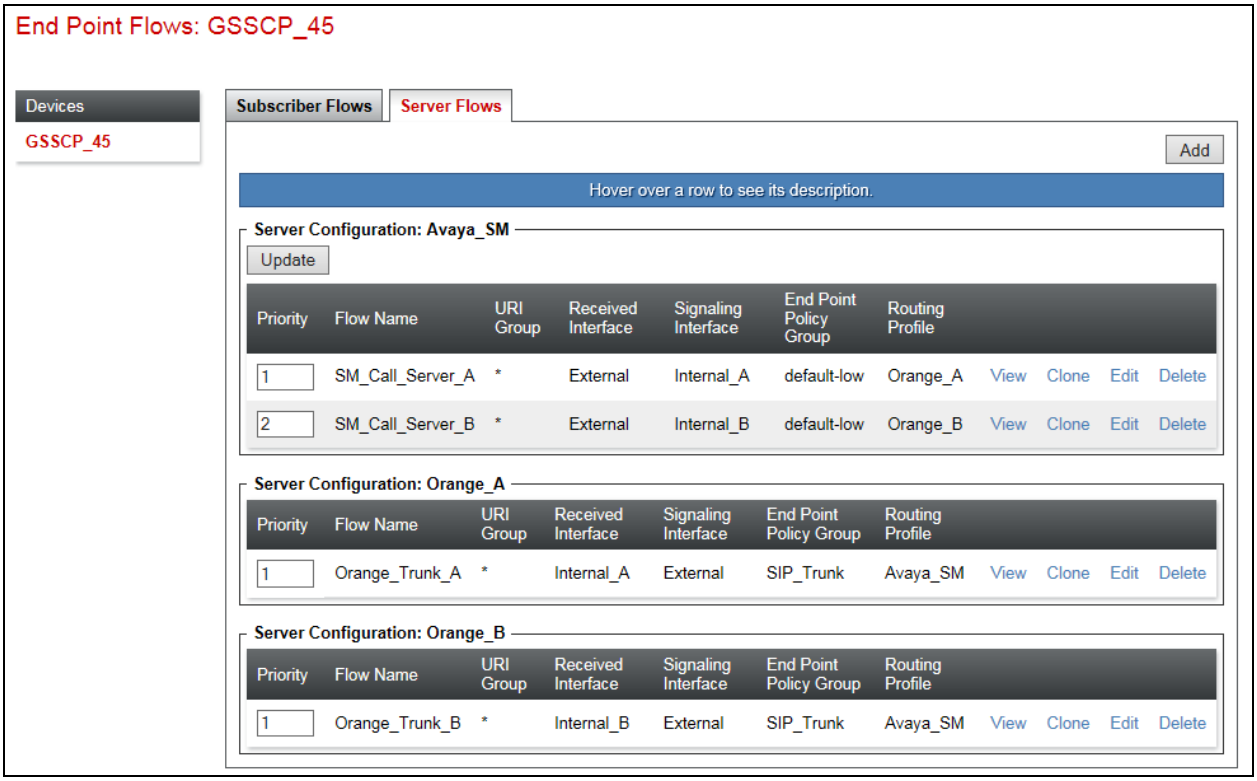


Define a Session Manager Server Flow for signalling between Session Manager and the Orange secondary SBC as follows:

- In the **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **SM_Call_Server_B** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.5**.
- In the **Remote Subnet** field, type the IP address of the primary SBC with a 32 bit mask.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling from the secondary SBC bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Orange secondary SBC defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select **default** and click **Finish**.



The information for all Server Flows is shown on a single screen on the Avaya SBCE.



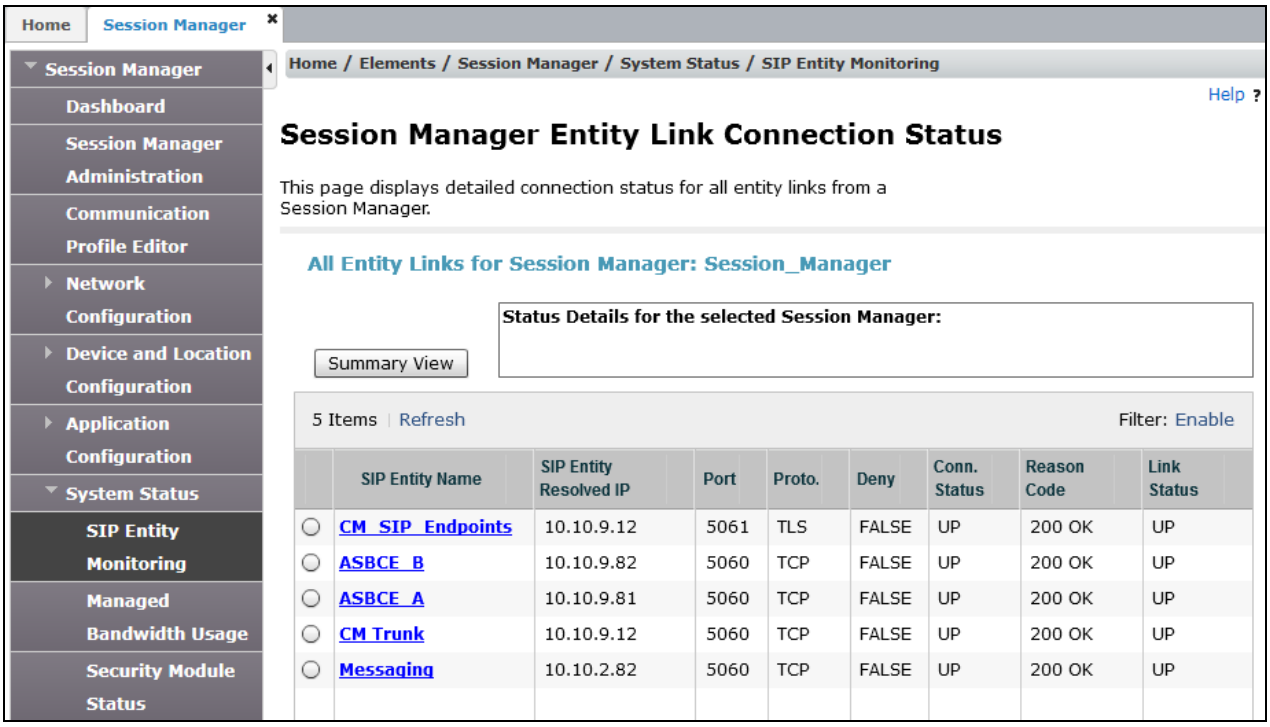
8. Configure the Orange SIP Trunking Equipment

The configuration of the Orange SIP Trunking equipment used to support the SIP Trunk is outside the scope of these Application Notes and will not be covered. To obtain further information on Orange SIP Trunking equipment and system configuration please contact an authorized Orange 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** screen click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entities from the list and observe if the **Conn Status** and **Link Status** are showing as **UP**.



SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
CM_SIP_Endpoints	10.10.9.12	5061	TLS	FALSE	UP	200 OK	UP
ASBCE_B	10.10.9.82	5060	TCP	FALSE	UP	200 OK	UP
ASBCE_A	10.10.9.81	5060	TCP	FALSE	UP	200 OK	UP
CM Trunk	10.10.9.12	5060	TCP	FALSE	UP	200 OK	UP
Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP

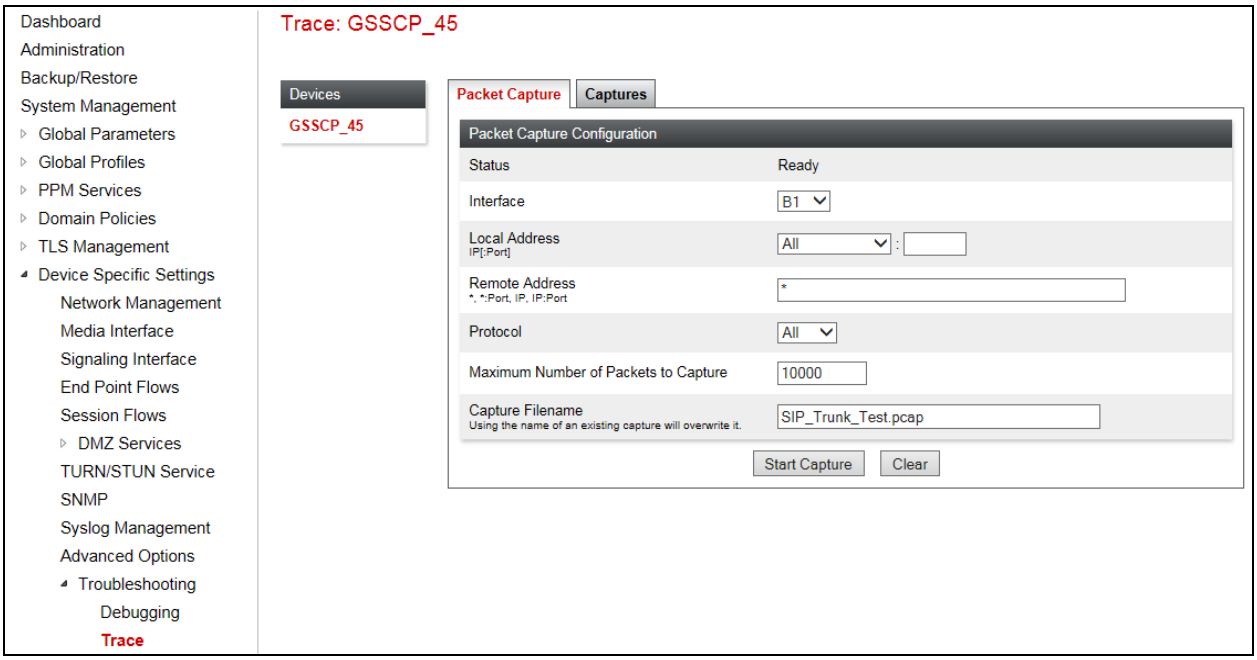
2. From Communication Manager SAT interface run the command **status trunk n** where **n** is the previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/active** or **in-service/idle**.

```
status trunk 2

                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0002/001 T00011   in-service/active  no   S00002
0002/002 T00012   in-service/idle    no
0002/003 T00013   in-service/idle    no
0002/004 T00014   in-service/idle    no
0002/005 T00015   in-service/idle    no
0002/006 T00016   in-service/idle    no
0002/007 T00017   in-service/idle    no
0002/008 T00018   in-service/idle    no
0002/009 T00019   in-service/idle    no
0002/010 T00020   in-service/idle    no
```

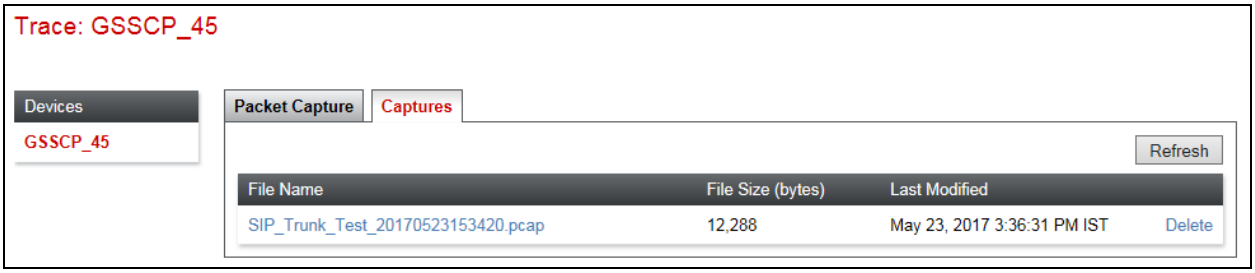
3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
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, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from Session Manager via the Avaya SBCE to the network SBCs are receiving a response.

   To define a trace on the Avaya SBCE, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main 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 or **All** from the **Local Address** drop down menu.
   - Enter the IP address of the network 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 response to OPTIONS in the form of a 200 OK will be seen from the Orange SIP Trunking network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R7.0.1, Avaya Aura® Session Manager R7.0.1 and Avaya Session Border Controller for Enterprise R7.1 to Orange SIP Trunking. The Orange SIP Trunking service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

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

[1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 7.0.1, Aug 2016.

[2] *Upgrading and Migrating Avaya Aura® applications to 7.0.1 from System Manager*, Release 7.0.1, Mar 2017.

[3] *Deploying Avaya Aura® applications from System Manager*, Release 7.0, Aug 2016

[4] *Deploying Avaya Aura® Communication Manager*, Oct 2016

[5] *Administering Avaya Aura® Communication Manager*, Release 7.0.1, May 2016.

[6] *Deploying Avaya Aura® System Manager*, Release 7.0.1 Aug 2016

[7] *Upgrading Avaya Aura® Communication Manager*, Release 7.0.1, Oct 2016

[8] *Upgrading Avaya Aura® System Manager to Release 7.0.1*, Aug 2016.

[9] *Administering Avaya Aura® System Manager for Release 7.0.1*, Nov 2016

[10] *Deploying Avaya Aura® Session Manager*, Release 7.0.1 Nov 2016

[11] *Upgrading Avaya Aura® Session Manager* Release 7.0.1, Mar 2017

[12] *Administering Avaya Aura® Session Manager* Release 7.0.1, May 2016,

[13] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.1, Nov 2016

[14] *Upgrading Avaya Session Border Controller for Enterprise*, Release 7.1, Aug 2016

[15] *Administering Avaya Session Border Controller for Enterprise*, Release 7.1, Jun 2016

[16] *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.