Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R8.0, Avaya Aura® Session Manager R8.0 and Avaya Session Border Controller for Enterprise R7.2 to support Orange Business Talk SIP Trunking - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Orange Business Talk 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 Talk SIP Trunking provides PSTN access via a SIP Trunk connected to the Orange Business Talk 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 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.

©2019 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Orange Business Talk SIP Trunking (BTIP) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R8.0; Avaya Aura® Session Manager R8.0 and Avaya Session Border Controller for Enterprise R7.2. 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 BTIP 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.

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 Orange BTIP.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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

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

©2019 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using Orange BTIP, calls made to SIP, H.323, Digital and Analogue telephones.
- Outgoing calls from the enterprise site completed via Orange BTIP to PSTN destinations, calls made from SIP, H.323, Digital and Analogue telephones.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator and Avaya Equinox for Windows soft phones.
- Calls using the G.711A, G,722 and G.729A codec's.
- 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 BTIP requiring Avaya response and sent by Avaya requiring Orange BTIP response.

2.2. Test Results

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

- Intermittent outbound calls to the Orange SIP Trunk were rejected with "500 Internal Server Error" due to bandwidth limitations causing them to overflow to the alternative Orange BTIP SBC. This is a characteristic of the test environment and not an interoperability issue.
- Intermittent outbound calls to the Orange SIP Trunk, though successful, would send multiple outbound INVITEs due to a timing issues on the Orange SIP Trunk. This was due to network delays in the test environment and is not considered to be an interoperability issue.
- 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.

©2019 Avaya Inc. All Rights Reserved.

- Both T.38 inbound and outbound fax calls failed to terminate. The SIP signalling and T.38 negotiation process was successful, however no T.38 packets were received from the Orange BTIP network to Avaya. The reason for the failure is still unknown but it may be caused by bandwidth issues experienced on the Orange BTIP SIP trunk, too many hops or that Orange's preferred fax transmission speed is V17 where as the Avaya G430 Media Gateway only negotiates transmission speeds of V27 and V29. As a result of T.38 fax calls failing, T.38 fax transmission is not supported on the Orange BTIP SIP trunk.
- 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 BTIP network is 101. If required, the Payload Type can be changed by adding the following lines in the config.xml file located in the 1xc 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 likely to be a characteristic of the test environment and not an interoperability issue.
- EC500 features such as on-net and off-net calling were not tested as the From, Contact and PAI Header CLIDs containing the EC500 mobility number on inbound calls to Orange BTIP SIP Trunk was automatically changed by Orange to a CLID number recognizable to the Orange network.

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 Orange BTIP, please contact Orange Business Talk at http://www.orange-business.com/en/products/business-talk

©2019 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to Orange BTIP. Located at the enterprise site is an Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 IP telephones (with SIP and H.323 firmware), Avaya 1600 series IP telephone (with H.323 firmware), Avaya digital and analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator and Avaya Equinox™ for Windows soft phones running on laptop PCs.

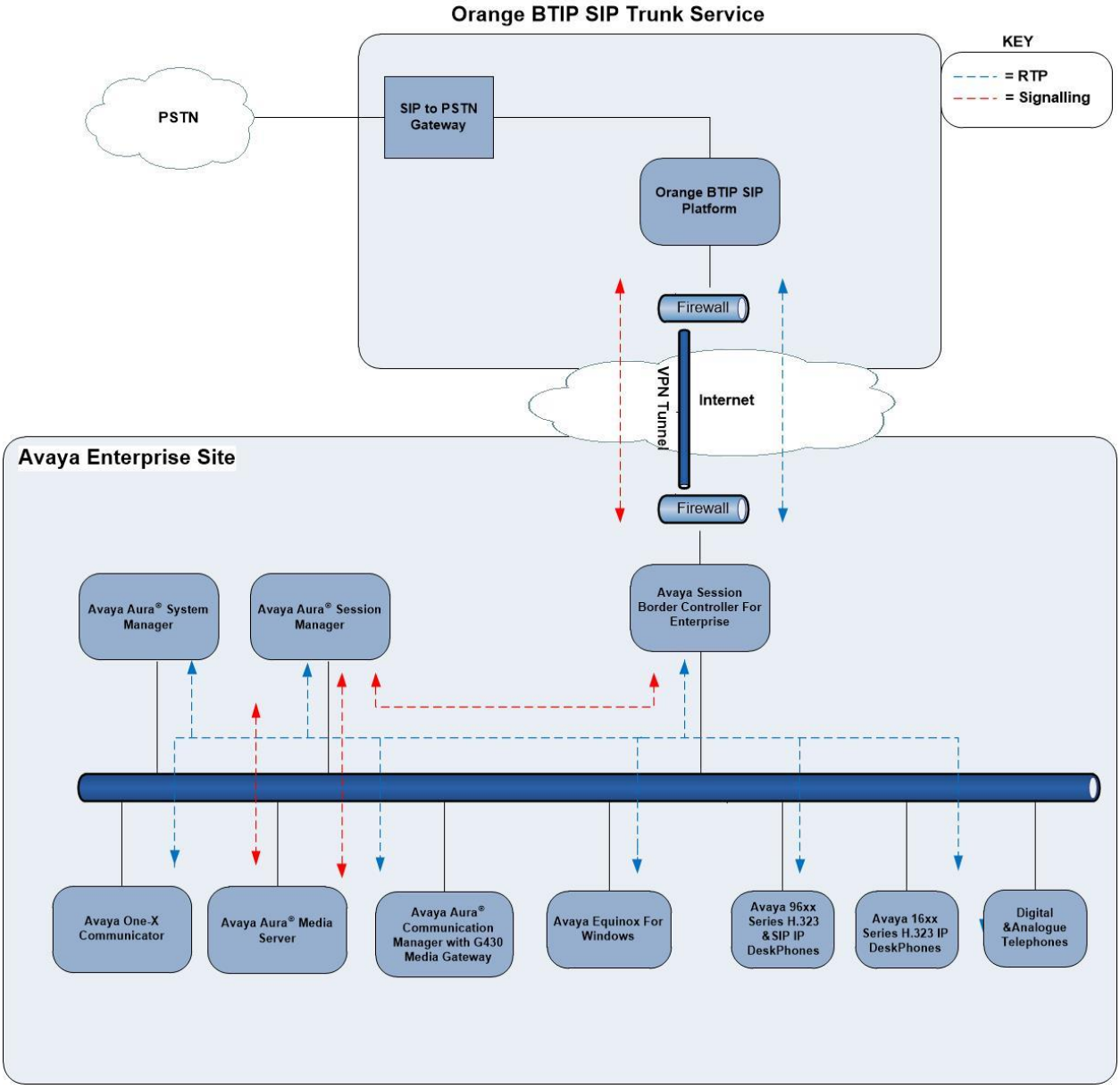


Figure 1: Test Setup Orange BTIP to Avaya Enterprise

©2019 Avaya Inc. All Rights Reserved.

Note: A standard IPSec tunnel was used to connect the Avaya Lab to the Orange BTIP 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® System Manager	8.0.1.0 Build No. – 8.0.0.0.931077 Software Update Revision No: 8.0.1.0.038836 Feature Pack 1
Avaya Aura® Session Manager	8.0.1.0.801007
Avaya Aura® Communication Manager	8.0.1.1.0 – Feature Pack 1
Avaya Session Border Controller for Enterprise	7.2.2.2-04-17187
Avaya Aura® Media Server	v.8.0.0.183
Avaya G430 Media Gateway	40.20.0
Avaya 1600 IP Deskphone (H.323)	1.3.12
Avaya 96x0 IP DeskPhone (H.323)	3.2.4
Avaya 96x1 IP DeskPhone (H.323)	6.8.2
Avaya 9611 IP DeskPhone (SIP)	7.1.5.0
Avaya 9608 IP DeskPhone (SIP)	7.1.5.0
Avaya one–X® Communicator (H.323 & SIP)	6.2.12.23 -SP12-Patch13
Avaya Equinox™ for Windows	3.5.7
Avaya 2400 Series Digital Handsets	N/A
Analogue Handset	N/A
Analogue Fax	N/A
Orange BTIP	
ORACLE Acme Packet SBC 4600	R8.1.0M1P14
French GW Call server: Italtel	release 5.3
International GW Call server: Italtel	release 5.4

©2019 Avaya Inc. All Rights Reserved.

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 BTIP. 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 BTIP 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 BTIP 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
```


©2019 Avaya Inc. All Rights Reserved.

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. In this case, **Session Manager** and **10.10.3.42** 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.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
AMS                 10.10.3.45
Session_Manager     10.10.3.42
default             0.0.0.0
procr               10.10.3.44
procr6              ::
```


©2019 Avaya Inc. All Rights Reserved.

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 BTIP.
- 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.

©2019 Avaya Inc. All Rights Reserved.

5.4. Administer IP Codec Set

Open the IP Codec Set form for the codec set specified in the IP Network Region form in **Section 5.3** by typing **change ip-codec set n w**here **n** is the chosen value of the configuration for the SIP Trunk. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codecs supported by Orange were configured, namely **G.722-64K** and **G.711A**. **Note**: G729 codec is also supported by Orange but not in order of preference in the same codec set with **G.722-64K** and **G.711A** codecs due to bandwidth limitations on the SIP trunk.

```
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.722-64K                     2        20
 1: G.711A              n         2        20
```


©2019 Avaya Inc. All Rights Reserved.

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to Orange BTIP. 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 BTIP 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
```


©2019 Avaya Inc. All Rights Reserved.

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 a value mutually agreed with Orange BTIP to prevent unnecessary SIP messages during call setup. During testing, a value of **600** was used that sets the SIP Min-SE header to 1200.

```
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): 600

Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n

 Caller ID for Service Link Call to H.323 1xC: station-extension
```


©2019 Avaya Inc. All Rights Reserved.

On **Page 3** of this form:

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

 Show ANSWERED BY on Display? y
```

On **Page 4** of this form:

- Set **Mark Users as Phone** to **y** for consistency with the Orange BTIP network.
- Set **Network Call Redirection** to **n** as SIP "302 Moved Temporarily" and REFER are not supported by Orange BTIP.
- Set **Send Diversion Header** to **n** in line with Orange BTIP configuration guidelines.
- Set **Support Request History** to **y** in line with Orange BTIP configuration guidelines.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Orange BTIP (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
          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                  Request URI Contents: may-have-extra-digits
```


©2019 Avaya Inc. All Rights Reserved.

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           Trk       CPN
Len Code          Grp(s)    Prefix          Len
                                                   Total Administered: 6
 4  6             1                          4        Maximum Entries: 240
 4  6102          2         33296xxxx41      11
 4  6010          2         33296xxxx42      11    Note: If an entry applies to
 4  6020          2         33296xxxx43      11    a SIP connection to Avaya
 4  6104          2         33296xxxx44      11    Aura(R) Session Manager,
 4  6100          2         33296xxxx45      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 BTIP 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:
```


©2019 Avaya Inc. All Rights Reserved.

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
```


©2019 Avaya Inc. All Rights Reserved.

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 (not shown), 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 BTIP 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        Del Insert
 Feature        Len      Digits
 public-ntwrk    12 +33296xxxx41     12  6102
 public-ntwrk    12 +33296xxxx42     12  6010
 public-ntwrk    12 +33296xxxx43     12  6020
 public-ntwrk    12 +33296xxxx44     12  6104
 public-ntwrk    12 +33296xxxx45     12  6100
```


©2019 Avaya Inc. All Rights Reserved.

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 6102. 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. **3314094xxxx**).
- 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 6102                    Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                    Selection   Set     Mode
 6102             EC500         -     3314094xxxx      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 BTIP 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**.

©2019 Avaya Inc. All Rights Reserved.

6. Configuring Avaya Aura® Session Manager

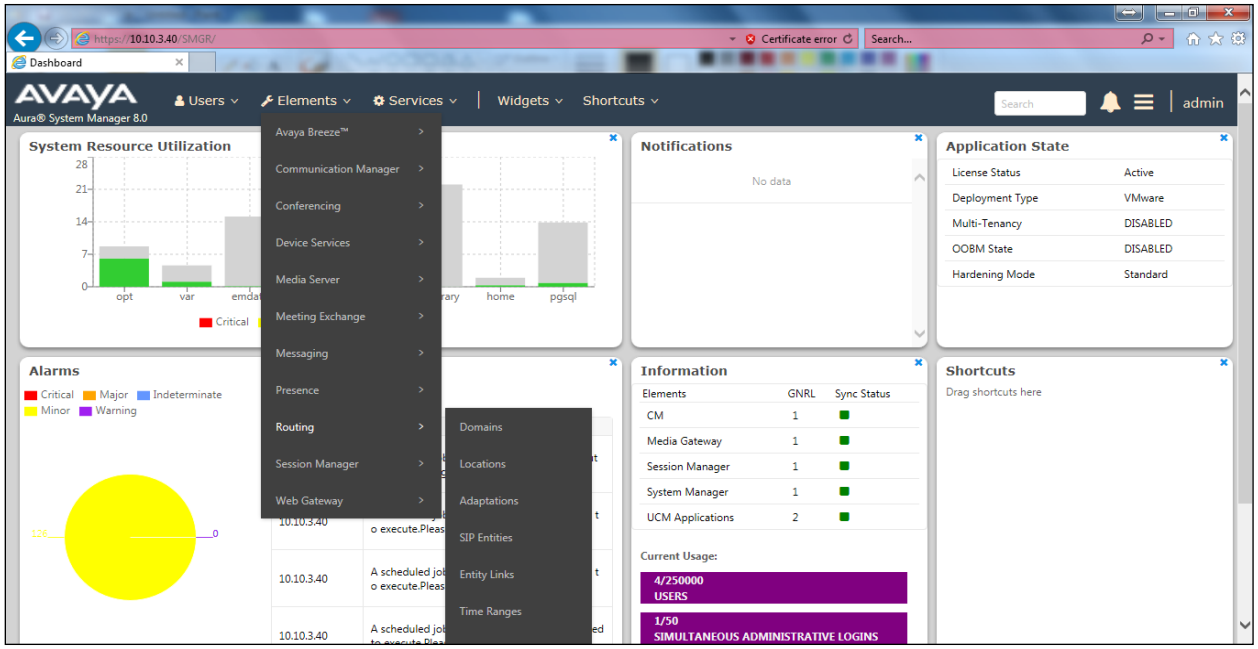
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager.
- Administer SIP Domain.
- Administer SIP Location.
- Administer Adaptations.
- Administer SIP Entities.
- Administer Entity Links.
- Administer Routing Policies.
- Administer Dial Patterns.

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

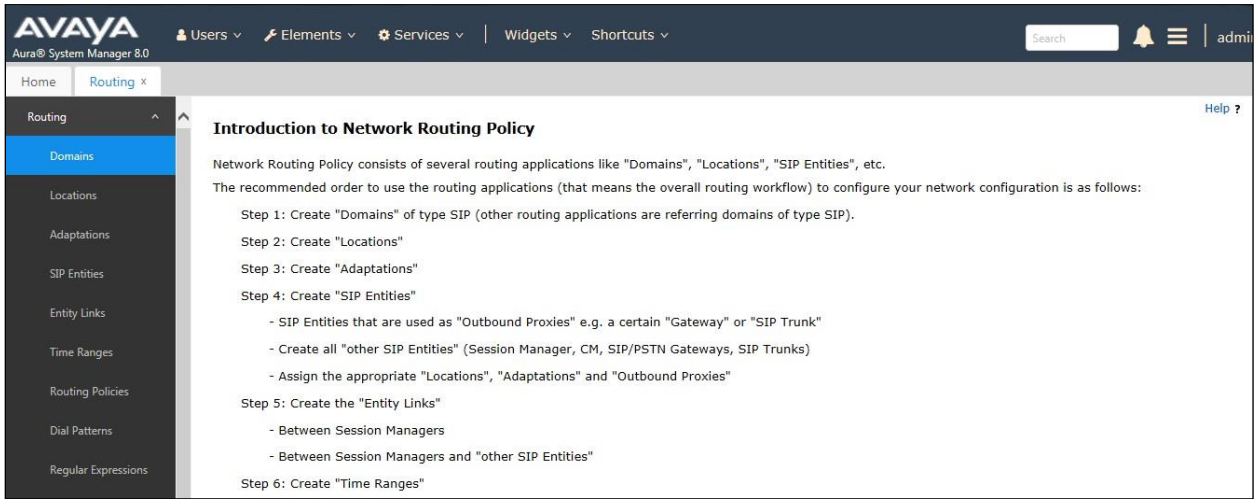
6.1. Log in to Avaya Aura® System Manager

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 Dashboard tab will be presented with menu options shown below.



©2019 Avaya Inc. All Rights Reserved.

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

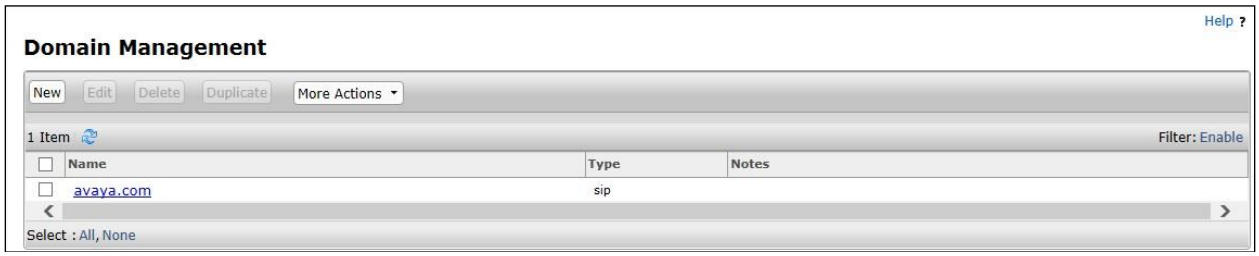


6.2. Administer SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. Expand **Elements → Routing** and select **Domains** from the left navigation menu, click **New** (not shown)**.** Enter the following values and use default values for remaining fields.

- **Name** Enter a Domain Name**.** In the sample configuration, **avaya.com** was used.
- **Type** Verify **SIP** is selected.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.



©2019 Avaya Inc. All Rights Reserved.

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

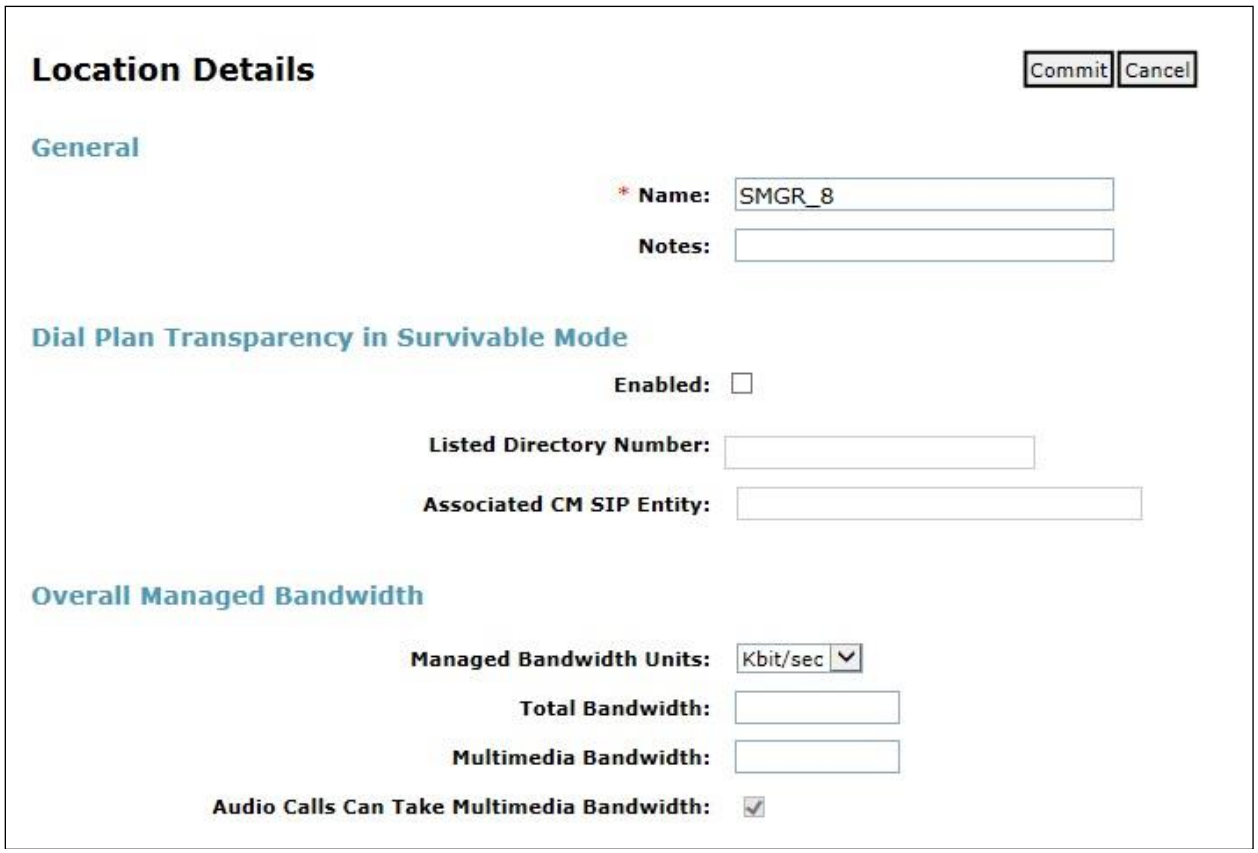
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern, then Session Manager uses the location administered for the SIP Entity.

In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screenshot below shows the Location **SMGR_8** defined for the compliance testing.



©2019 Avaya Inc. All Rights Reserved.

©2019 Avaya Inc. All Rights Reserved.

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**).

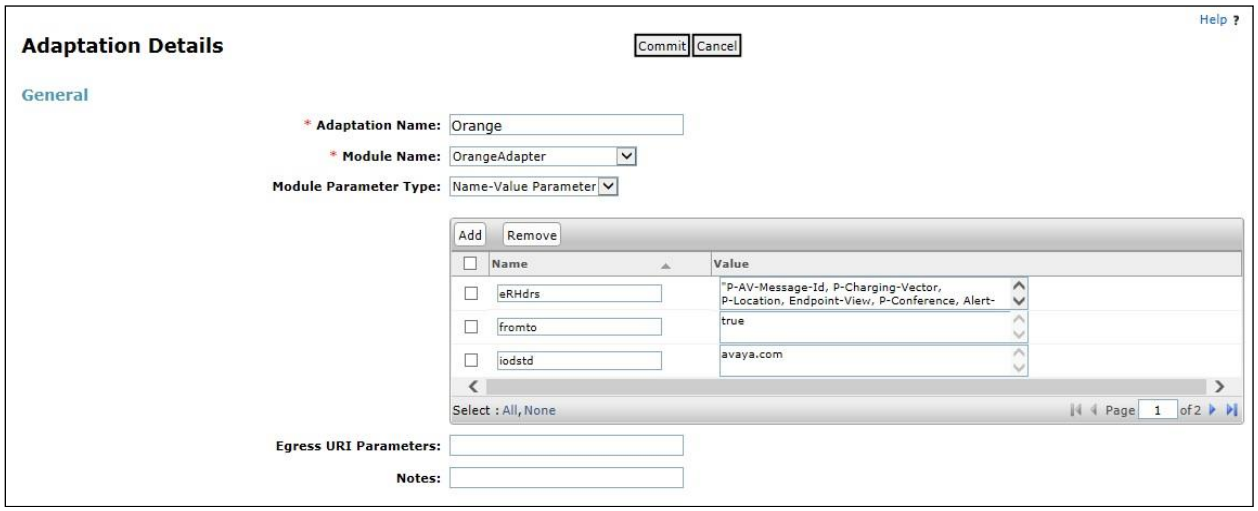
Communication Manager and Session Manager make use of Avaya proprietary SIP headers to facilitate the full suite of Avaya functionality within the enterprise. These are not required on the SIP trunk however, and make the SIP messages unnecessarily large. A Session Manager Adaptation is used to remove proprietary headers.

To add an adaptation, under the **Routing** tab select **Adaptations** on the left-hand menu and then click on the **New** button (not shown). Under **Adaptation Details →General**:

- **Adaption Name**: Enter an appropriate name such as **Orange**.
- **Module Name**: Select **OrangeAdapter**.
- **Modular Parameter Type**: Select **Name-Value Parameter**.

Click **Add** to add the name and value parameters.

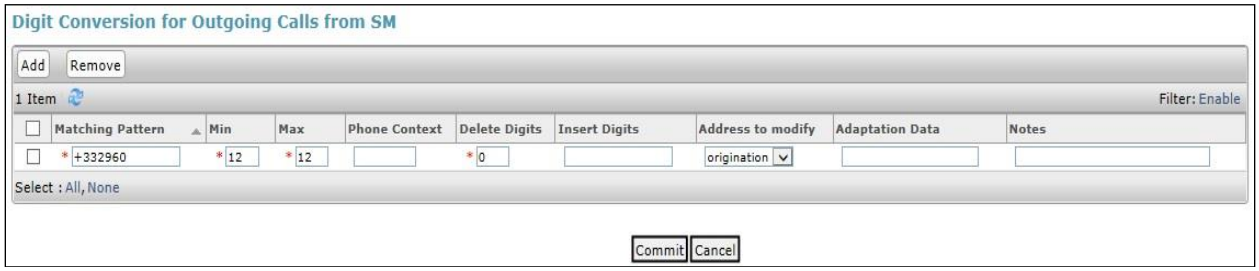
- **Name**: Enter **eRHdrs**. This parameter will remove the specific headers from messages in the egress direction.
- **Value**: Enter **AV-Global-Session-ID**, **AV-Correlation-ID**, **Alert-Info**, **Endpoint-View**, **P-AV-Message-ID**, **P-Charging-Vector**, **P-Location**.
- **Name**: Enter **fromto**. Modifies From and To header of a message.
- **Value**: Enter **true**.
- **Name**: Enter **MIME**. Remove MIME message bodies from Session Manager.
- **Value**: Enter **no**.



©2019 Avaya Inc. All Rights Reserved.

Scroll down the page and under **Digit Conversion for Outgoing Calls from SM**, click the **Add** button and specify the digit manipulation to be performed as follows:

- Enter the leading digits that will be matched in the Matching Pattern field.
- In the **Min** and **Max** fields set the minimum and maximum digits allowed in the digit string to be matched.
- In the **Delete Digits** field enter the number of leading digits to be removed.
- In the **Insert Digits** field specify the digits to be prefixed to the digit string.
- In the **Address to modify** field specify the digits to manipulate by the adaptation.



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**.

©2019 Avaya Inc. All Rights Reserved.

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:

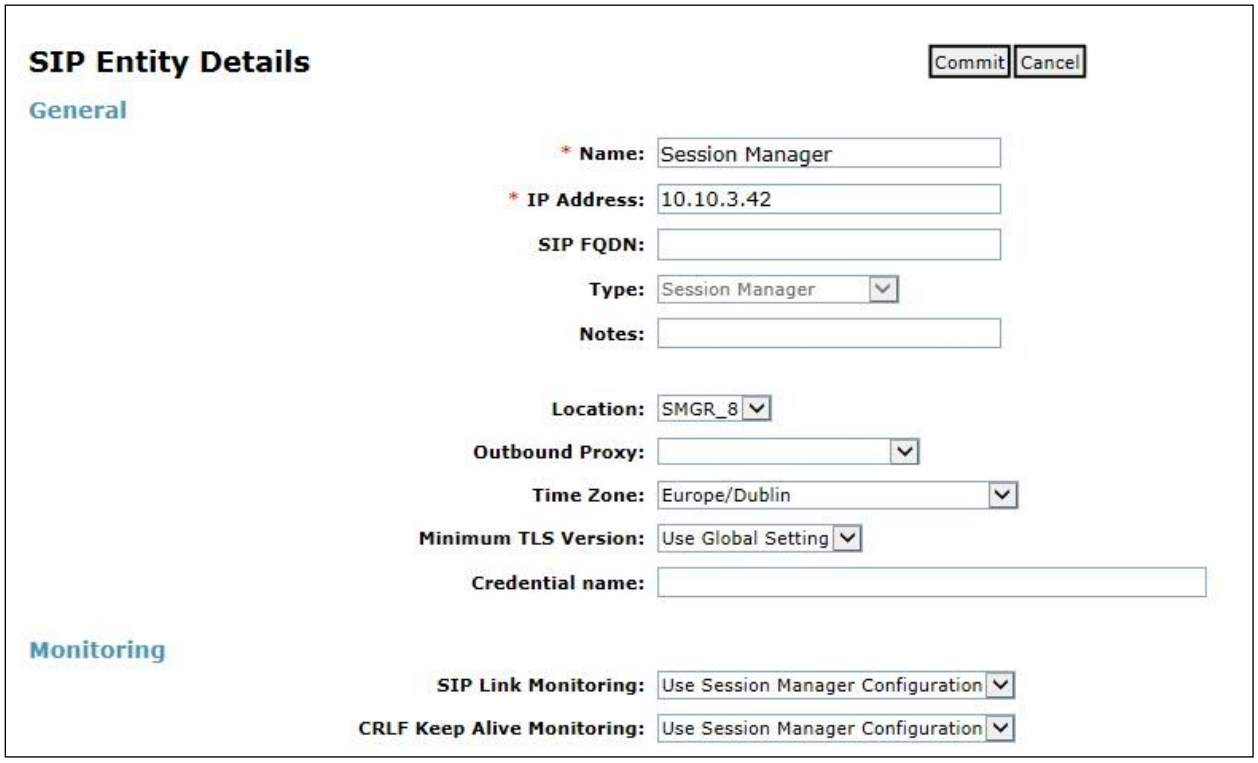
- Avaya Aura® Session Manager SIP Entity.
- Avaya Aura® Communication Manager SIP Entity for the SIP Trunk.
- Avaya Session Border Controller for Enterprise (Avaya SBCE) SIP Entity for PSTN destinations.

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

©2019 Avaya Inc. All Rights Reserved.

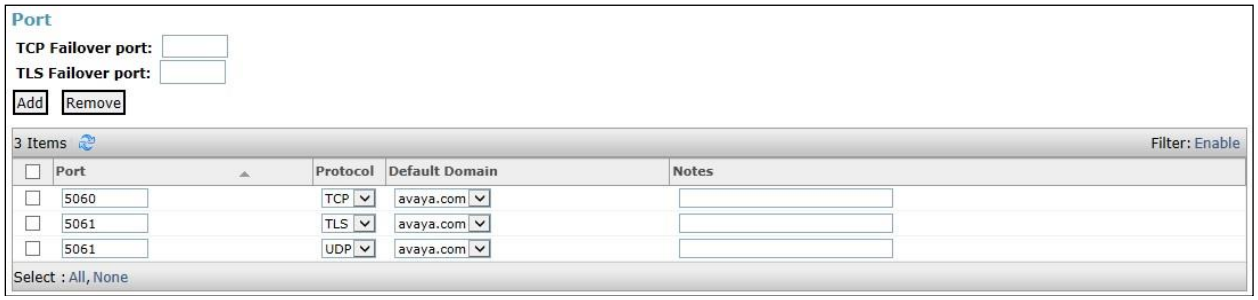
6.5.1. Avaya Aura® Session Manager SIP Entity

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 and **Type** is **Session Manager**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.



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

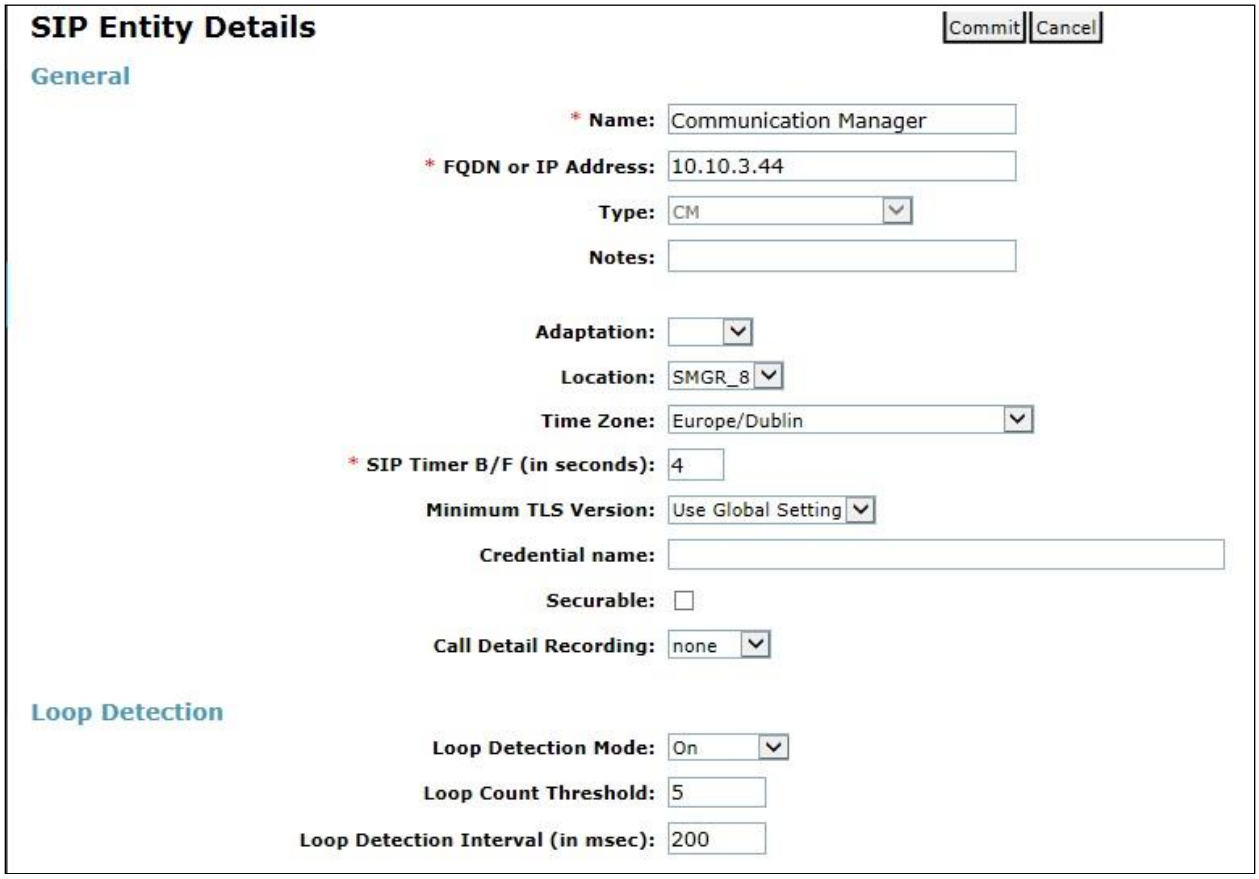
- In the **Port** field enter the port number on which the system listens for SIP requests.
- In the **Protocol** field enter the transport protocol to be used for SIP requests.
- In the **Default Domain** field, from the drop-down menu select the domain added in **Section 6.2** as the default domain.



©2019 Avaya Inc. All Rights Reserved.

6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. 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. Set the **Location** to that defined in **Section 6.3**.



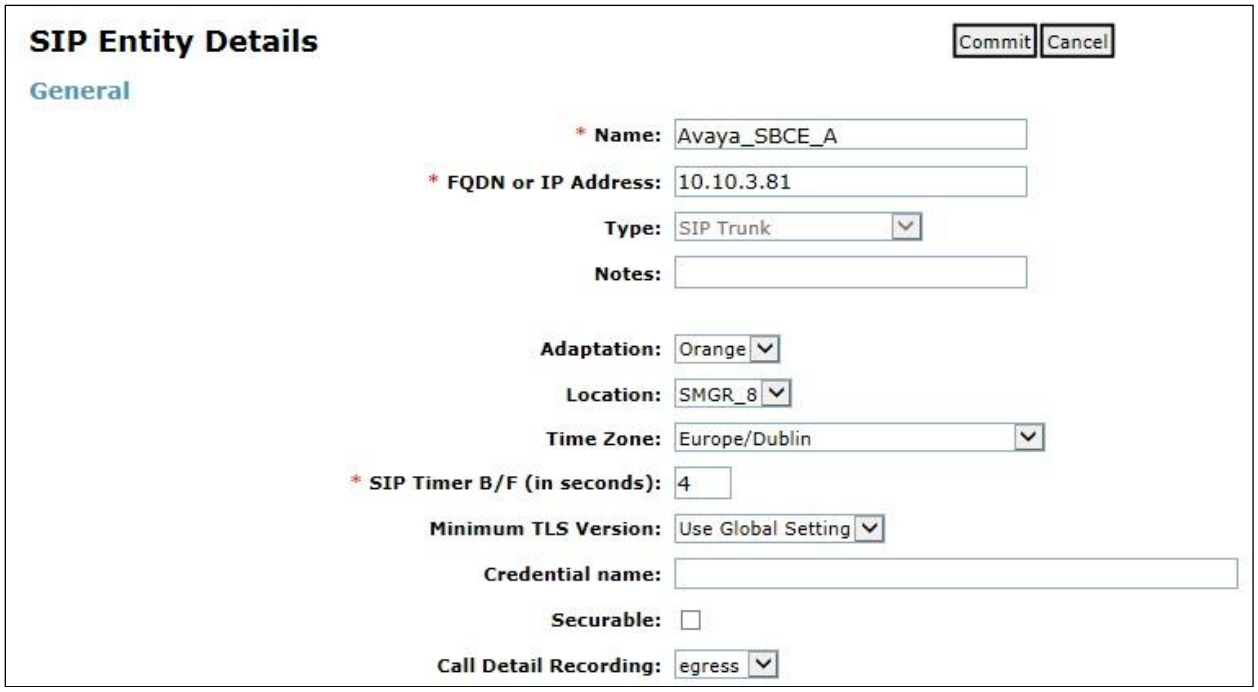
Other parameters can be set for the SIP Entity as shown in the following screenshot, but for test, these were left at default values.

©2019 Avaya Inc. All Rights Reserved.

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

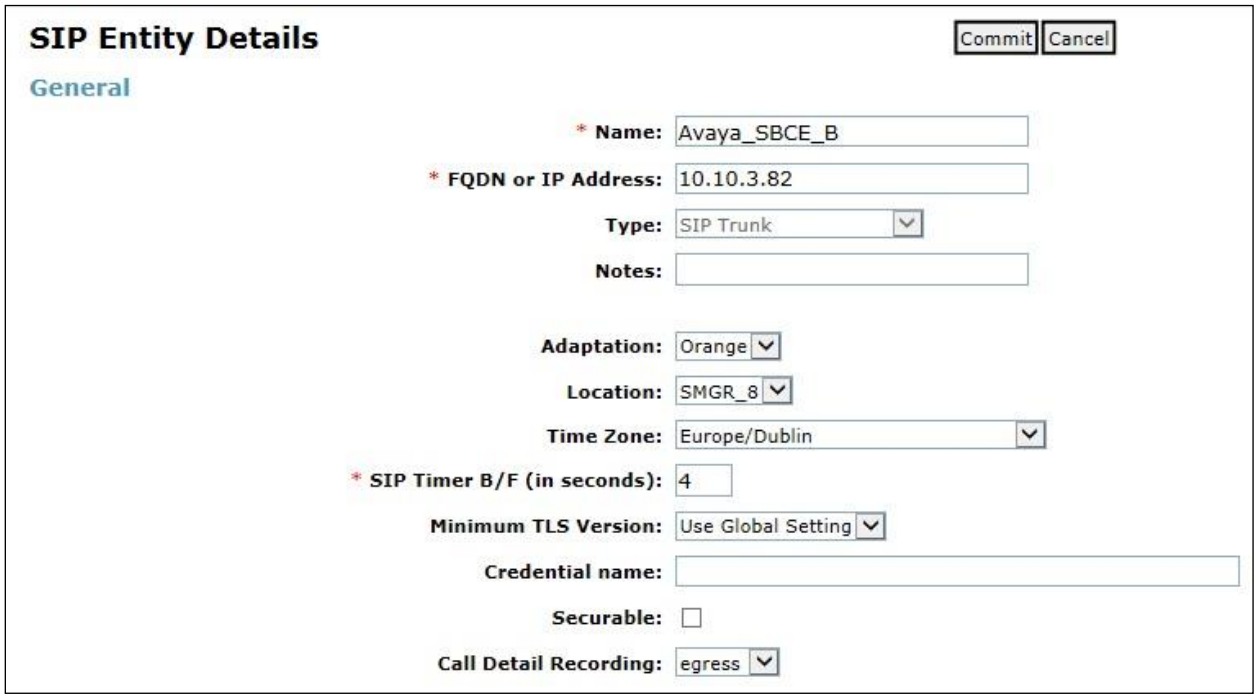
There are two SIP Entities required for the Avaya SBCE in this configuration. One is for the Avaya SBCE internal interface that maps to the server flow for the primary Orange BTIP SBC, and the other is for the internal interface that maps to the secondary Orange BTIP SBC.

The screenshot shows the SIP Entity for the internal interface mapping to the primary Orange BTIP 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.



©2019 Avaya Inc. All Rights Reserved.

The SIP Entity for the internal interface mapping to the secondary Orange BTIP SBC is configured with the same parameters apart from the **Name** and **FQDN or IP Address** fields. In the test environment, these were **Avaya_SBCE_B** and **10.10.3.82** respectively.

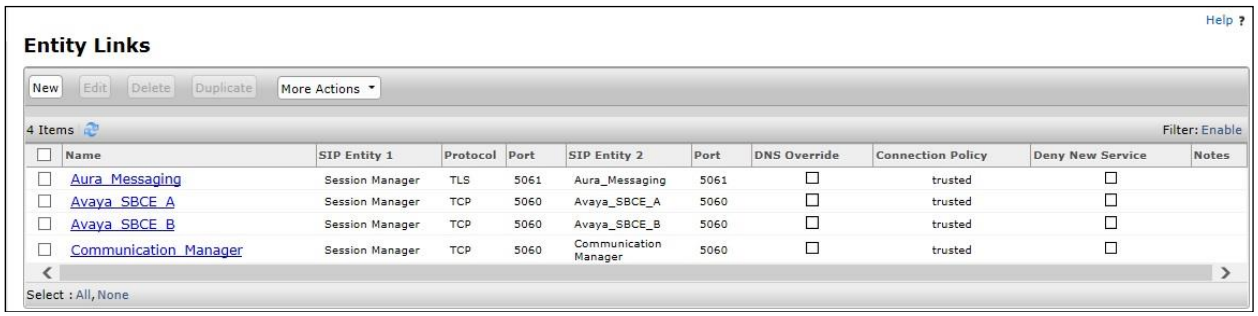


©2019 Avaya Inc. All Rights Reserved.

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.



Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
Aura_Messaging	Session Manager	TLS	5061	Aura_Messaging	5061	☐	trusted	☐	
Avaya_SBCE_A	Session Manager	TCP	5060	Avaya_SBCE_A	5060	☐	trusted	☐	
Avaya_SBCE_B	Session Manager	TCP	5060	Avaya_SBCE_B	5060	☐	trusted	☐	
Communication_Manager	Session Manager	TCP	5060	Communication Manager	5060	☐	trusted	☐	

Note: The **Aura_Messaging** Entity Link is used for the Avaya Aura® Messaging system and is not described in this document.

6.7. Administer Routing Policies

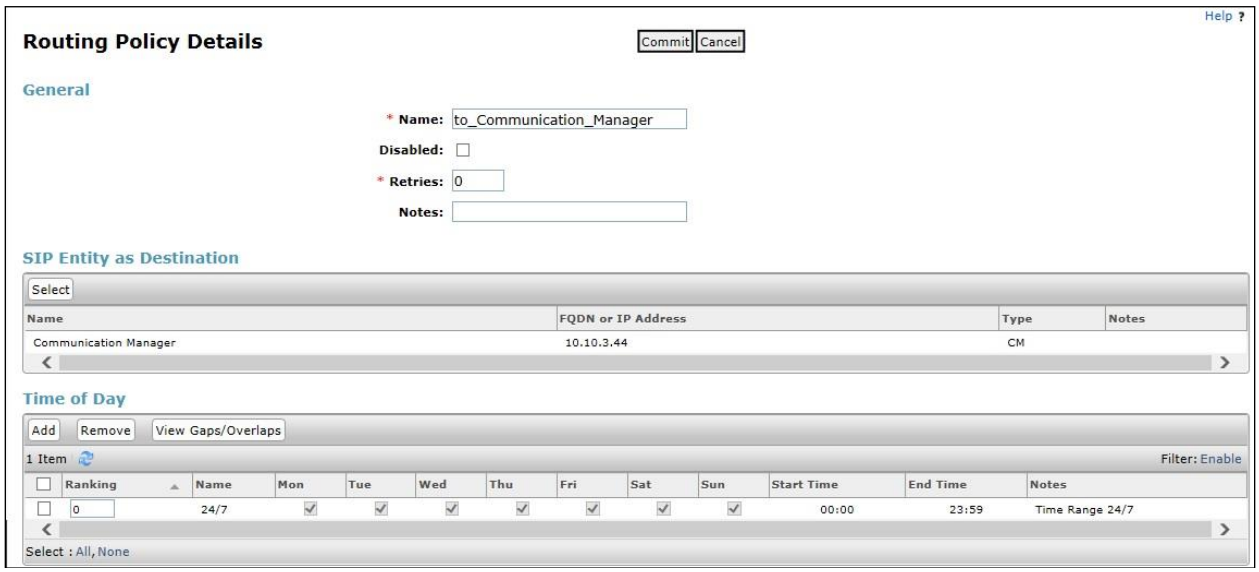
Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

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.

©2019 Avaya Inc. All Rights Reserved.

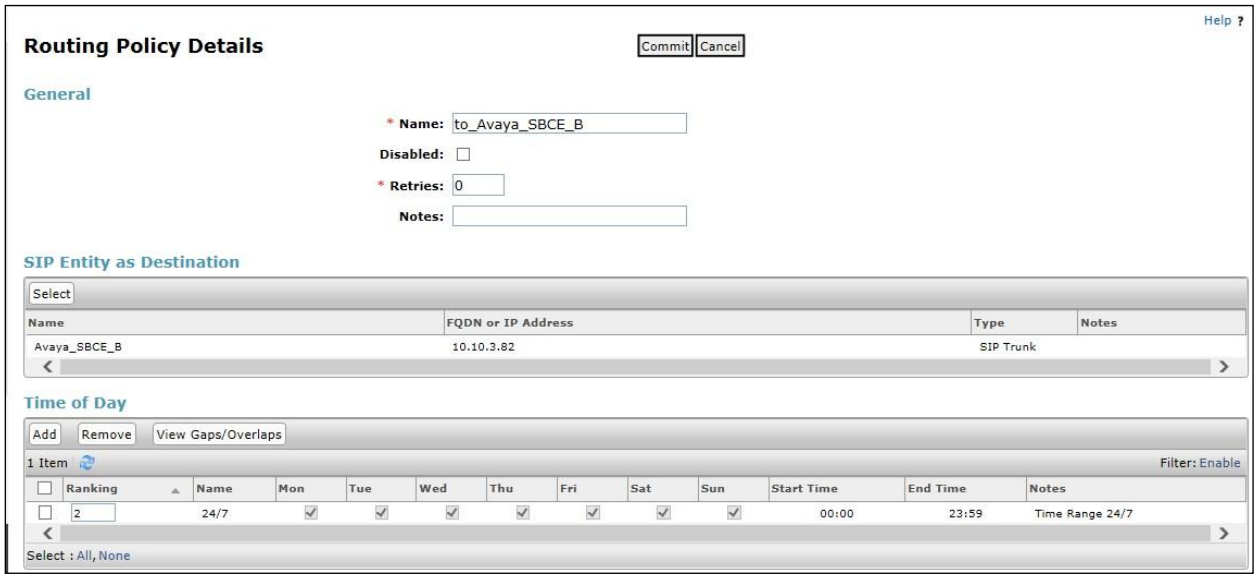
The following screen shows the routing policy for calls inbound from the SIP Trunk to Communication Manager.



The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed to PSTN destinations via the primary SBC in Orange BTIP. Ensure **Ranking** is set to **1** for **to_Avaya_SBCE_A** Routing Policy.

©2019 Avaya Inc. All Rights Reserved.

The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed to PSTN destinations via the secondary SBC in Orange BTIP. Ensure **Ranking** is set to **2** for **to_Avaya_SBCE_B** Routing Policy



Note: Ranking value has been set to **1** for the primary Orange BTIP SBC and set to **2** for the secondary Orange BTIP SBC. Lower ranking values indicate higher priority for call routing so all calls will route to the primary Orange BTIP SBC. Should the primary Orange BTIP SBC encounter routing difficulties, then all call routing will automatically failover to the secondary Orange BTIP SBC.

©2019 Avaya Inc. All Rights Reserved.

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**:

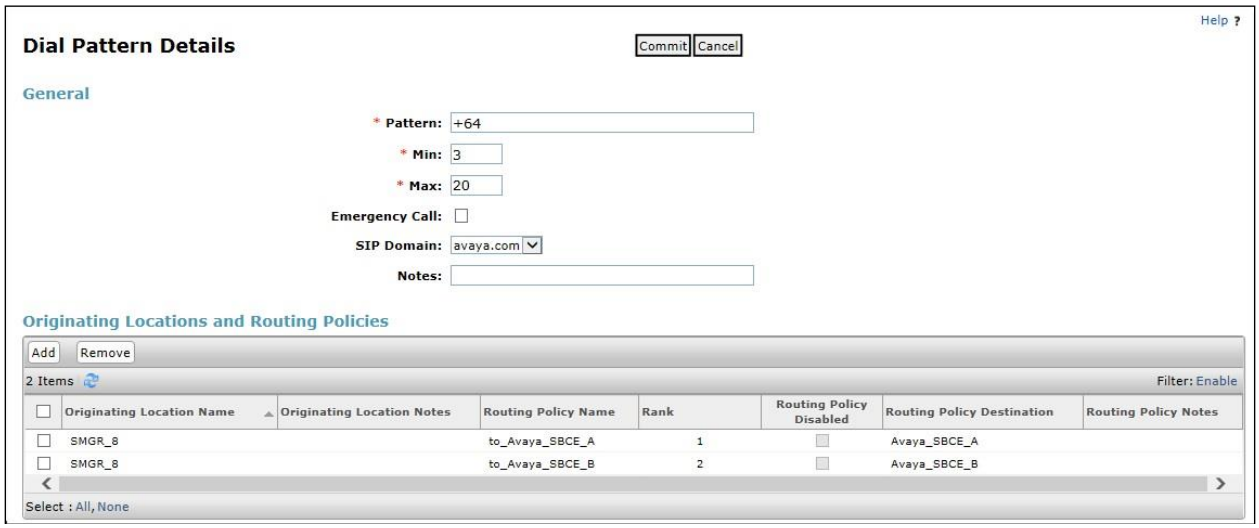
- In the **Pattern** field enter a dialled number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialled number.
- In the **Max** field enter the maximum length of the dialled number.
- In the **SIP Domain** field select **ALL** or alternatively one of those configured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

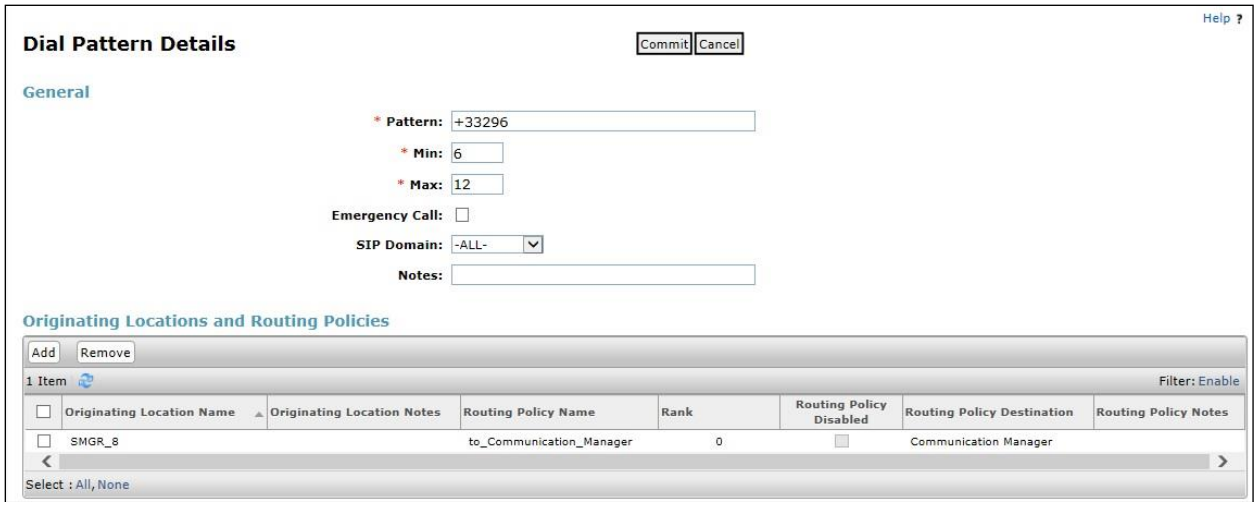
The following screen shows an example dial pattern configured for the Avaya SBCE which will route all calls originating in the enterprise and starting with "+64" to the PSTN via Orange BTIP.



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.

©2019 Avaya Inc. All Rights Reserved.

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.



©2019 Avaya Inc. All Rights Reserved.

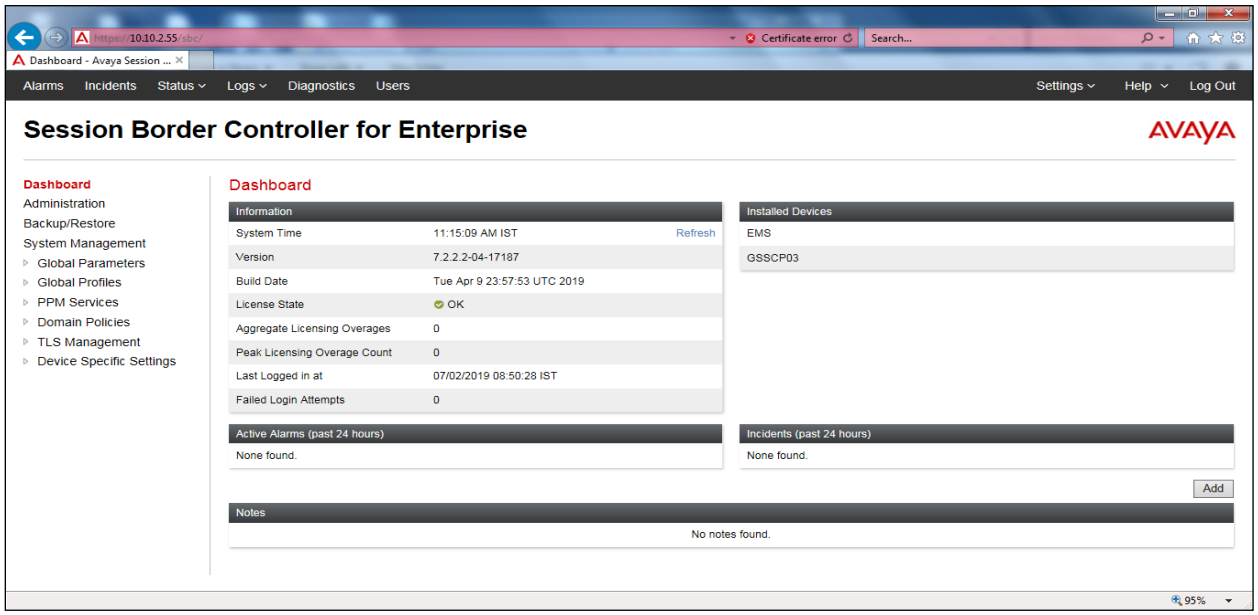
7. Configure Avaya Session Border Controller for Enterprise

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.

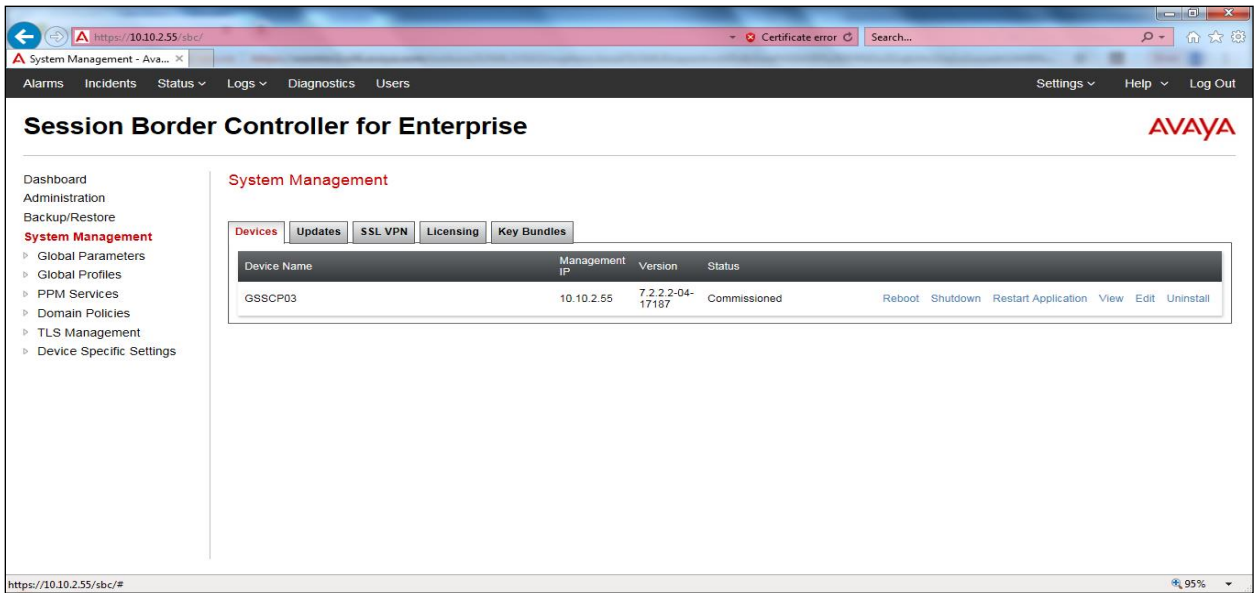
7.1. Access Avaya Session Border Controller for Enterprise

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.

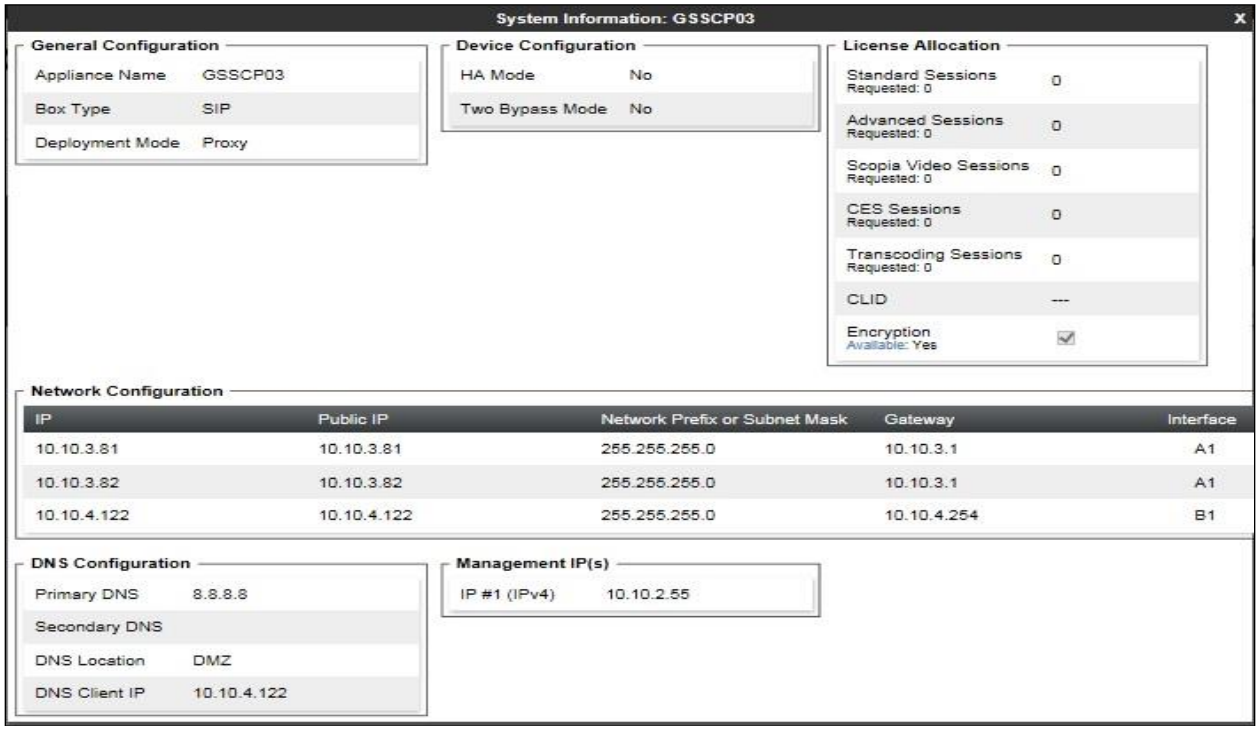
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP03** is shown. To view the configuration of this device, click **View** (the third option from the right).



The **System Information** screen shows the **General Configuration**, **Device Configuration**, **License Allocation**, **Network Configuration**, **DNS Configuration** and **Management IP** information.



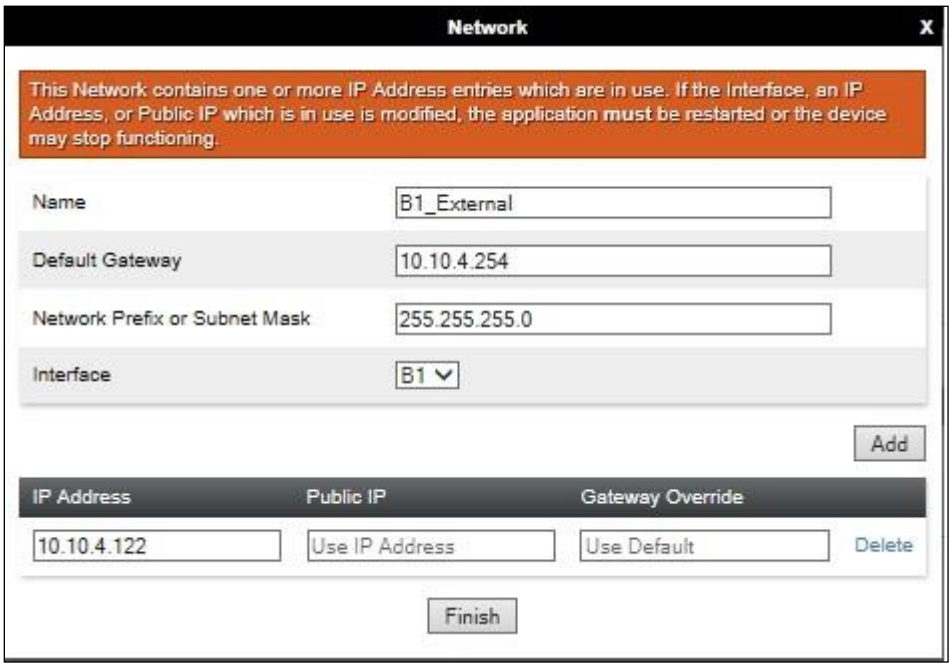
©2019 Avaya Inc. All Rights Reserved.

7.2. Define Network Management

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

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:

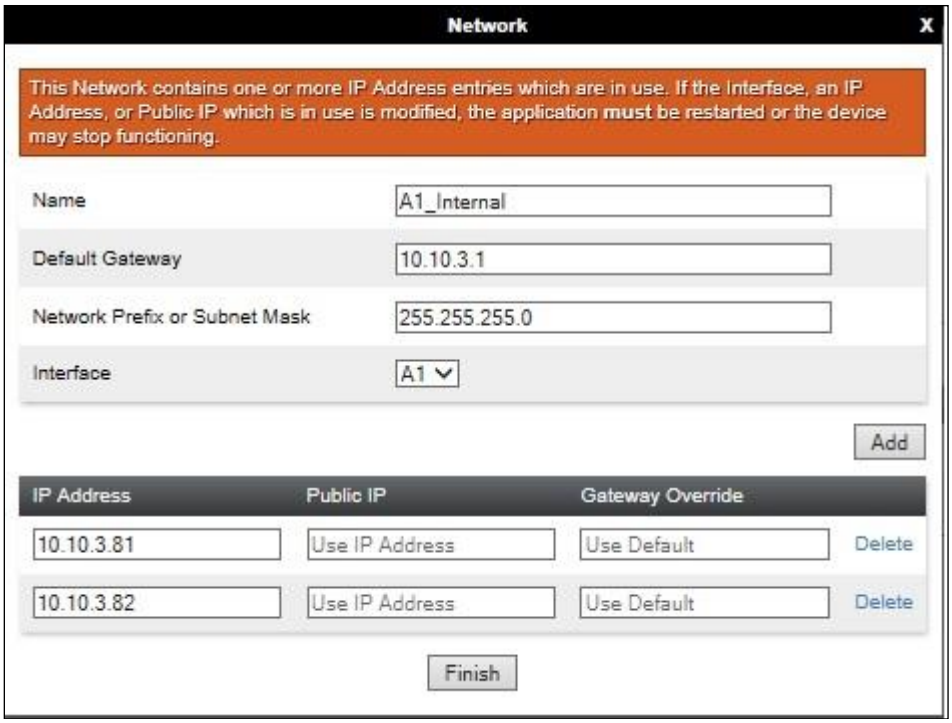
- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the 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.



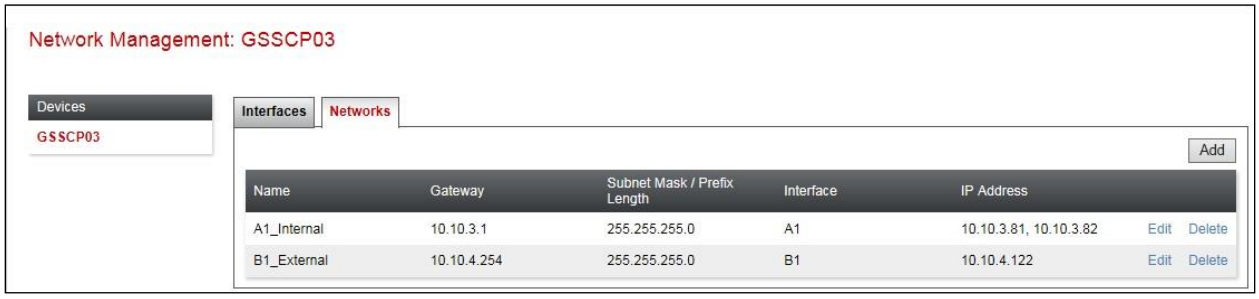
©2019 Avaya Inc. All Rights Reserved.

Click on **Add** to define the internal interfaces or Edit if it was defined during installation of the Avaya SBCE. Enter details in the dialogue box:

- 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 internal 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.
- 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:



©2019 Avaya Inc. All Rights Reserved.

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 (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box will appear that will indicate when the restart is complete.

©2019 Avaya Inc. All Rights Reserved.

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 BTIP.

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**.

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

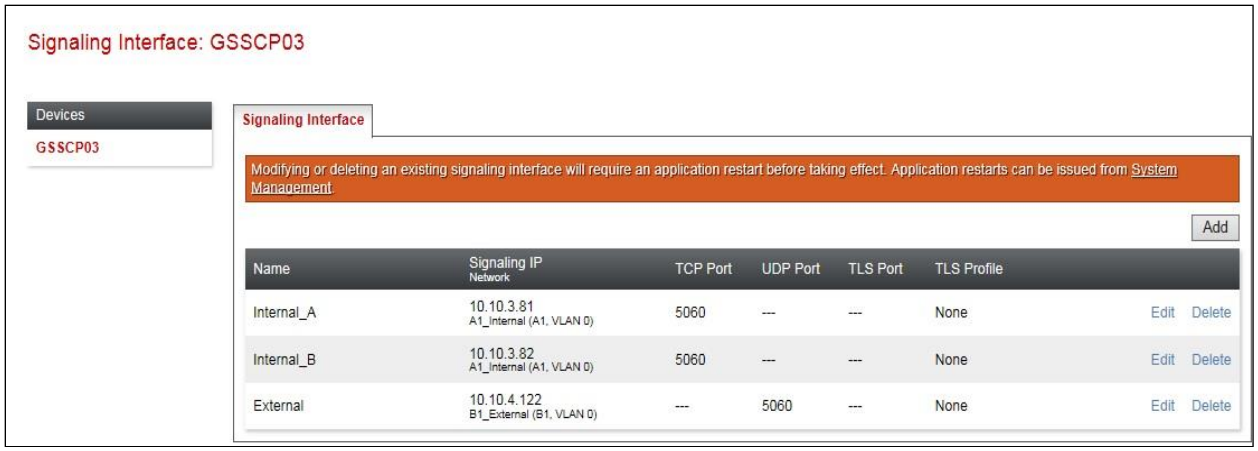
To enter details of transport protocol and ports for the SIP signalling on the internal interface:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **IP Address**, select the **Internal_A** signalling interface IP addresses defined in **Section 7.2**.
- Select **TCP** port number, **5060** is used for Session Manager.
- Repeat the process for the second **Internal_B** internal IP address
- Click **Finish**.

To enter details of transport protocol and ports for the SIP signalling on the external interface:

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **IP Address**, select the **External** signalling interface IP address defined in **Section 7.2**.
- Select **UDP** port number, **5060** is used for the Orange BTIP SIP Trunk.
- Click **Finish**.

©2019 Avaya Inc. All Rights Reserved.



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.

©2019 Avaya Inc. All Rights Reserved.

7.3.2. Media Interfaces

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

To enter details of the media IP and RTP port range for the internal interfaces to be used in the server flow:

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **IP Address**, select the **Internal_A** media interface IP address defined in **Section 7.2**.
- For **Port Range**, enter **16384-32767**.
- Click **Finish**.

Repeat the process for the second **Internal_B** internal media interface.

To enter details of the media IP and RTP port range on the external interface to be used in the server flow.

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **IP Address**, select the **External** media interface IP address defined in **Section 7.2**.
- Select **Port Range**, enter **16384-32767**.
- Click **Finish**.

The following screenshot shows details of the media interfaces:

©2019 Avaya Inc. All Rights Reserved.

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, Orange BTIP 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.

7.4.1. Server Interworking Avaya

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles → Server Interworking** and click on **Add**.

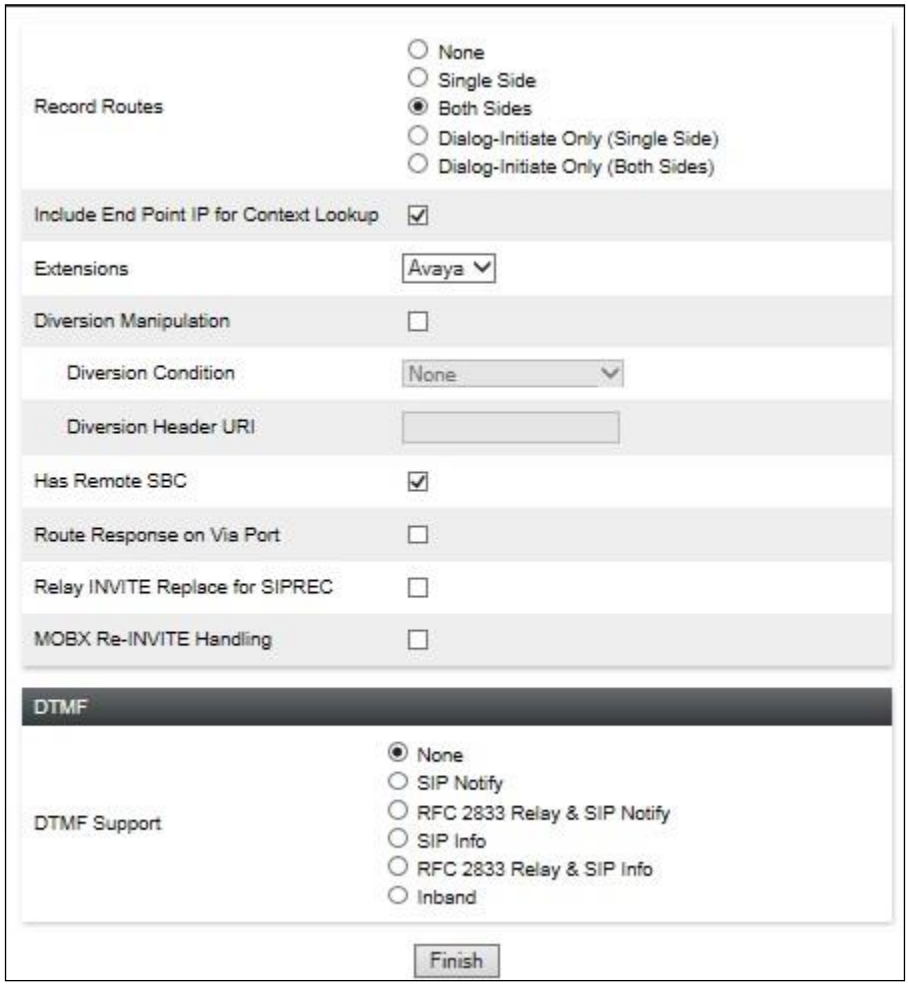
- Enter profile name such as **Avaya** and click **Next** (Not Shown).
- Check **Hold Support = None**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

©2019 Avaya Inc. All Rights Reserved.

On the **Advanced** Tab:

- Check **Record Routes** = **Both Sides**.
- Ensure **Extensions** = **Avaya**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

7.4.2. Server Interworking – Orange

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles → Server Interworking** and click on **Add**.

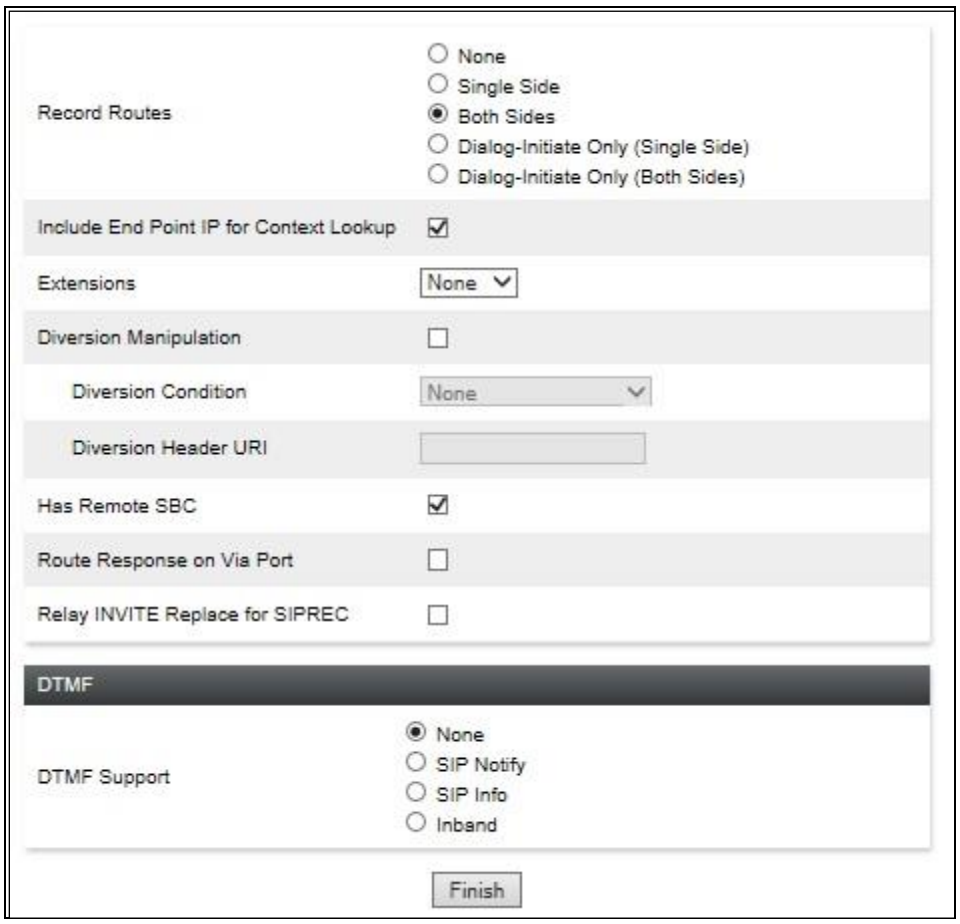
- Enter profile name such as **Orange** and click **Next** (Not Shown).
- Check **Hold Support = None**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

©2019 Avaya Inc. All Rights Reserved.

On the **Advanced** Tab:

- Check **Record Routes** = **Both Sides**.
- Ensure **Extensions** = **None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

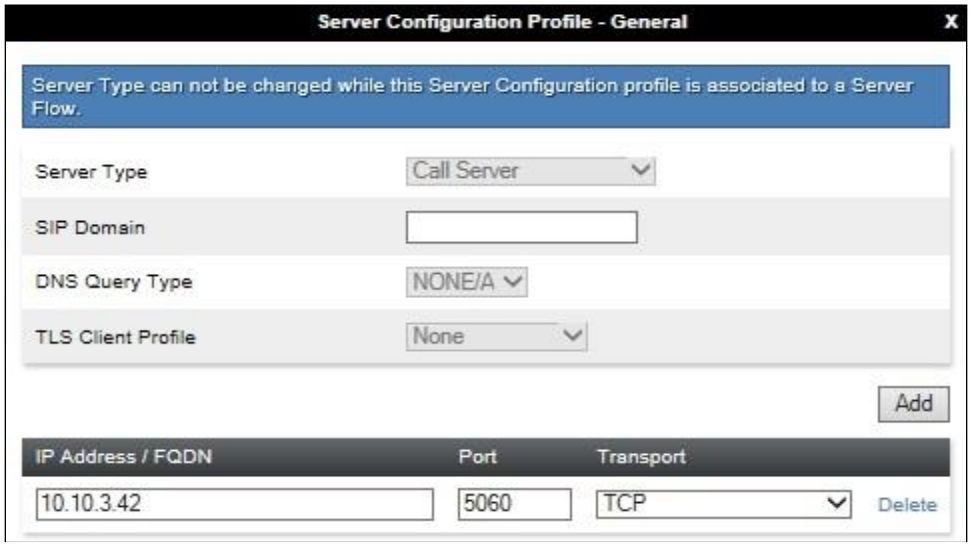
7.5. Define Servers

A server definition is required for each server connected to the Avaya SBCE. Orange BTIP is connected as two Trunk Servers, one for each SBC. Session Manager is connected as a Call Server. To define the Orange BTIP Servers.

7.5.1. Server Configuration – Avaya

From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

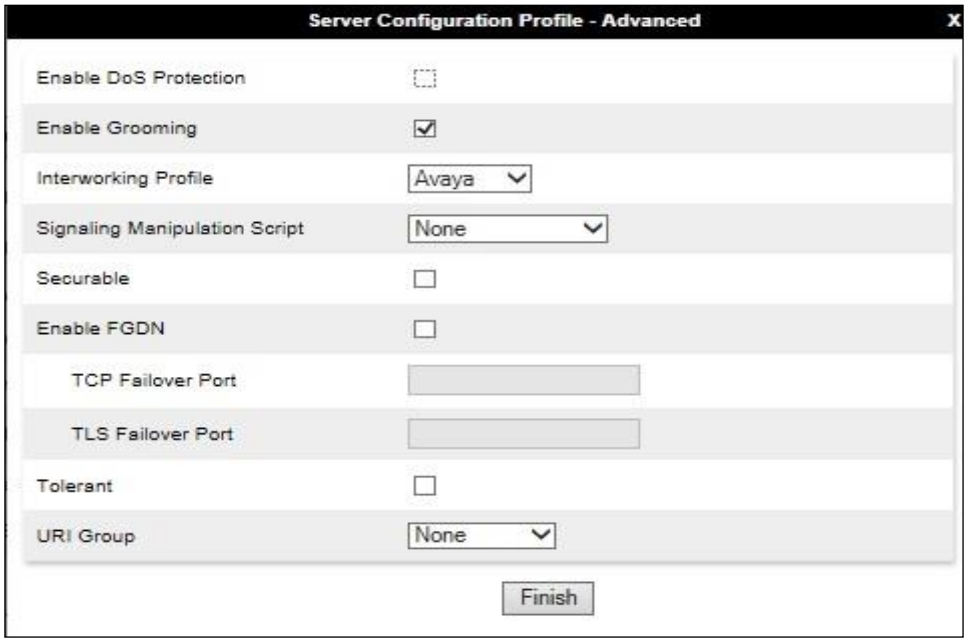
- Select **Server Type** to be **Call Server**.
- Enter **IP Address / FQDN** to **10.10.3.42** (Session Manager IP Address).
- For **Port**, enter **5060**.
- For **Transport,** select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



On the **Advanced** tab:

- Check **Enable Grooming**.
- Select **Avaya** for **Interworking Profile**.
- Click **Finish**.

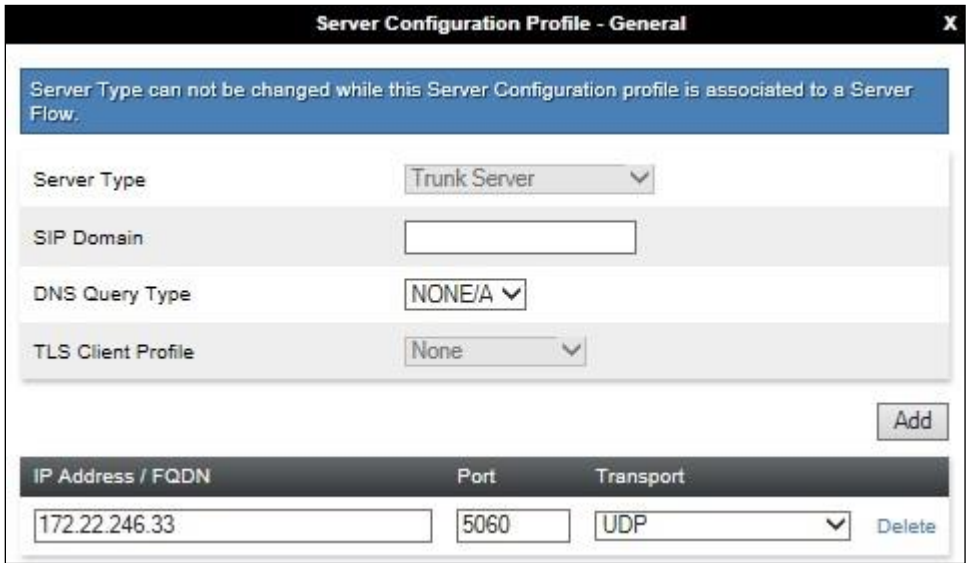
©2019 Avaya Inc. All Rights Reserved.



7.5.2. Server Configuration – Orange BTIP

To define the Orange BTIP primary Trunk Server, navigate to **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

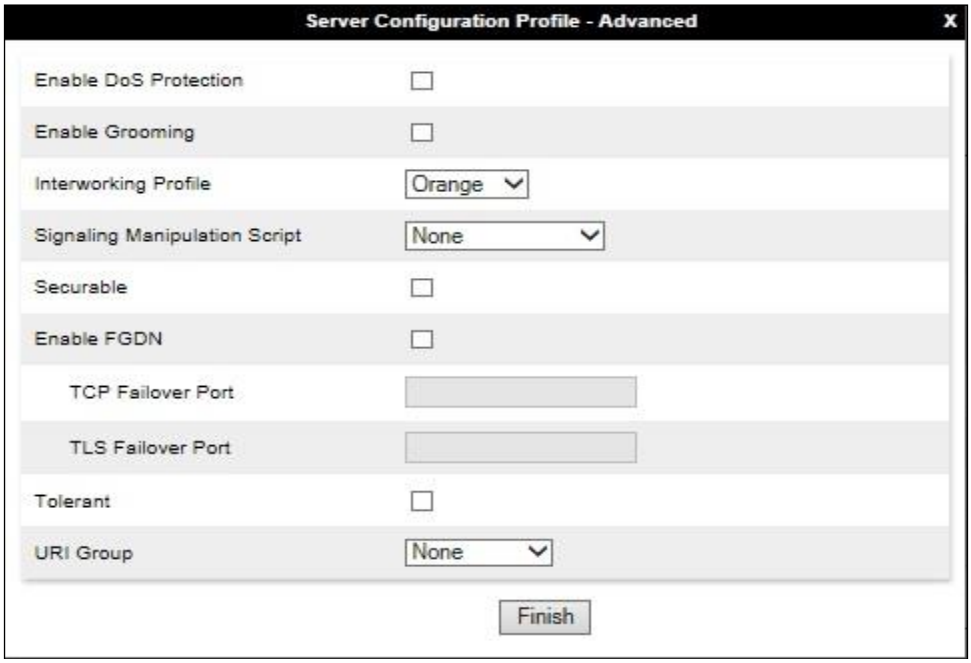
- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **172.22.246.33** (Orange BTIP primary SBC).
- For **Port**, enter **5060**.
- For **Transport,** select **UDP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



©2019 Avaya Inc. All Rights Reserved.

On the Advanced tab:

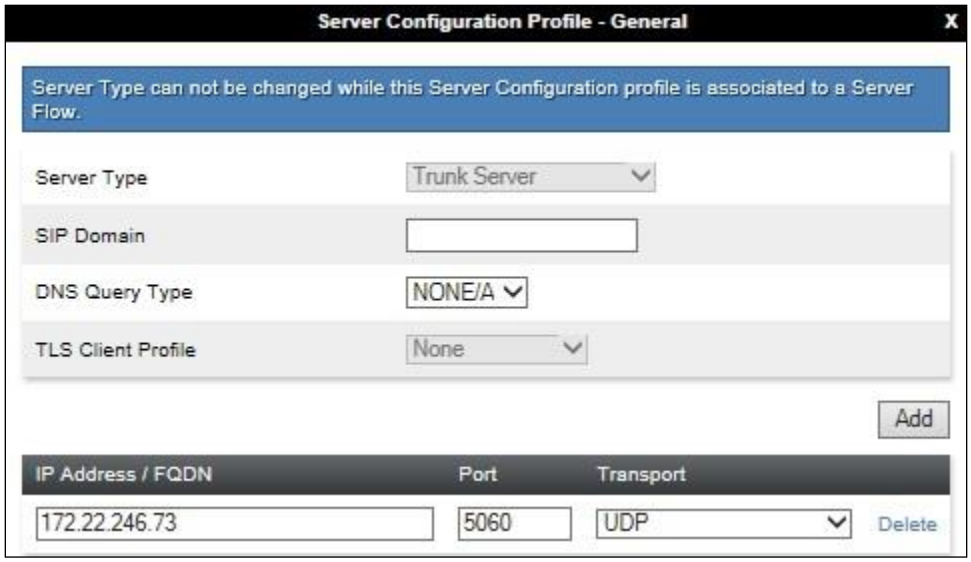
- Select **Orange** for Interworking Profile.
- Click **Finish**.



To define the Orange BTIP secondary Trunk Server, navigate to **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

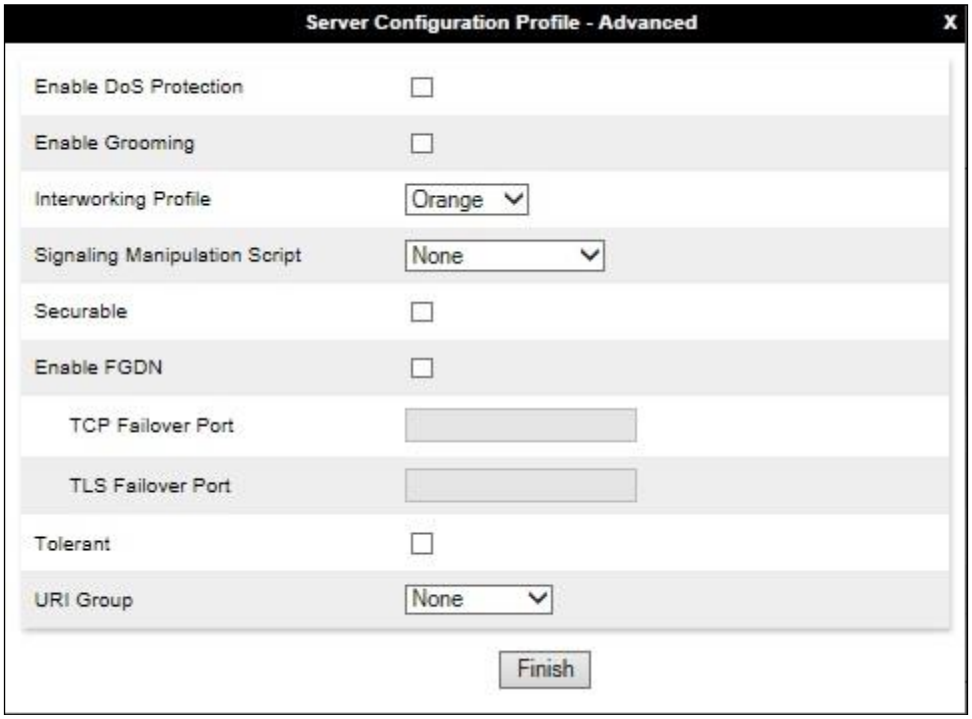
- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **172.22.246.73** (Orange BTIP secondary SBC).
- For **Port**, enter **5060**.
- For **Transport,** select **UDP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

©2019 Avaya Inc. All Rights Reserved.



On the Advanced tab:

- Select **Orange** for Interworking Profile.
- Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

7.6. Define Routing

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

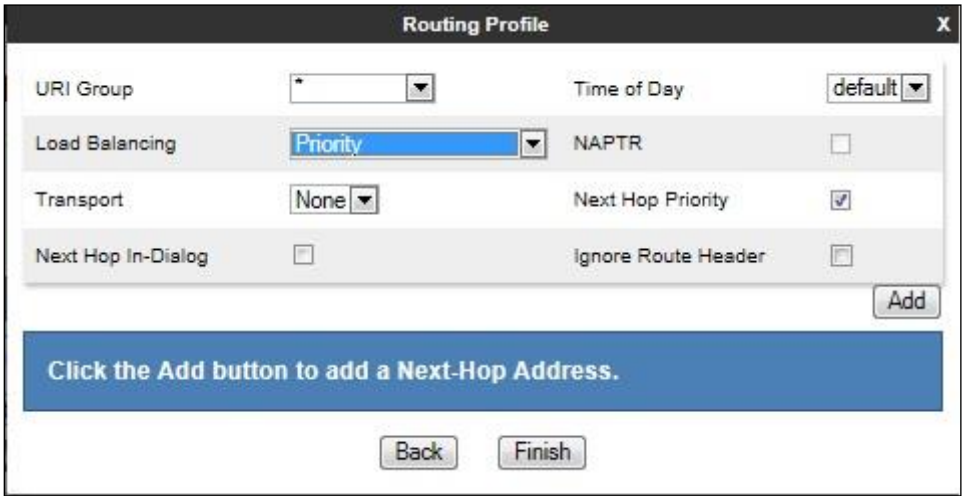
Session Manager on the internal side and Orange addresses on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

7.6.1. Routing – Avaya

Create a Routing Profile for Session Manager.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

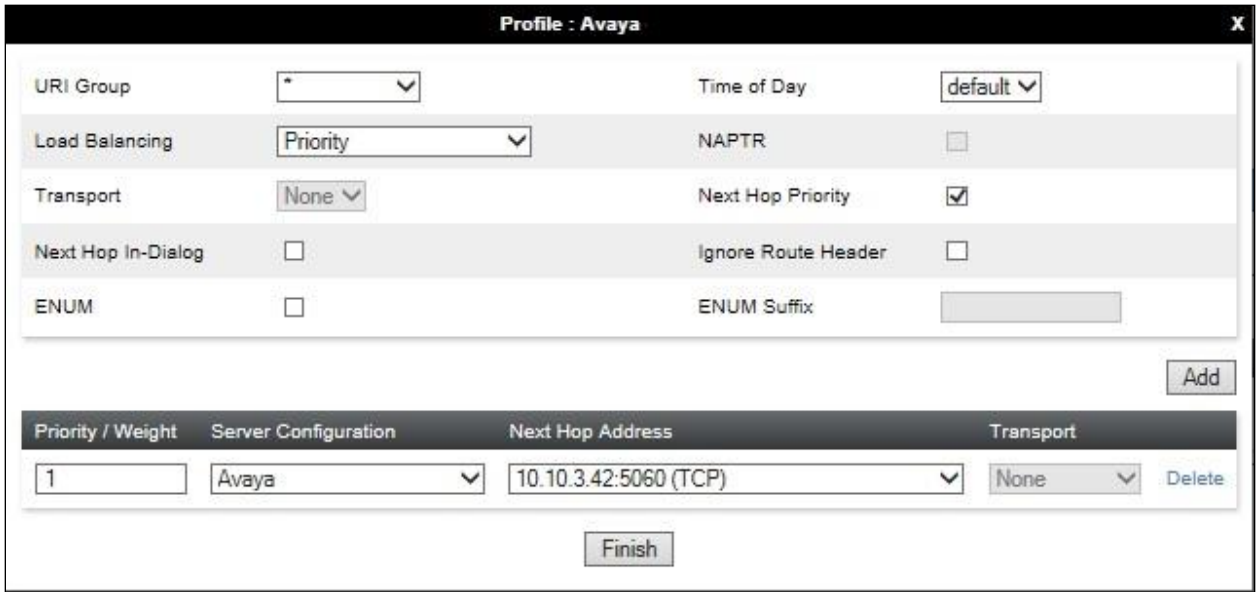
The Routing Profile window will open. Use the default values displayed and click **Add**.



©2019 Avaya Inc. All Rights Reserved.

On the **Next Hop Address** window, set the following:

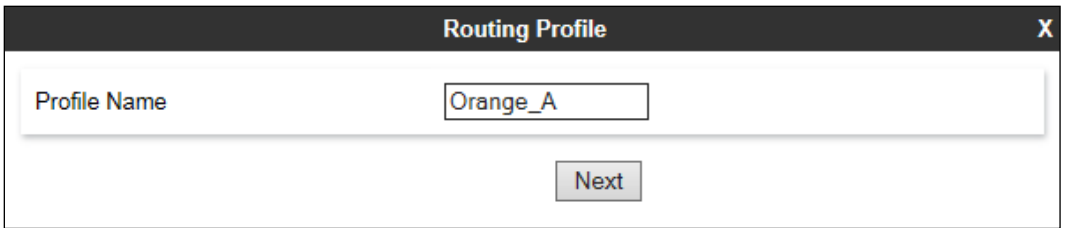
- **Priority/Weight** = **1**.
- **Server Configuration** = **Avaya** (**Section 7.5.1**) from drop down menu.
- **Next Hop Address** = Select **10.10.3.42:5060(TCP)** from drop down menu.
- Click **Finish**.



7.6.2. Routing – Orange

Create a Routing Profile for Orange BTIP primary SBC.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

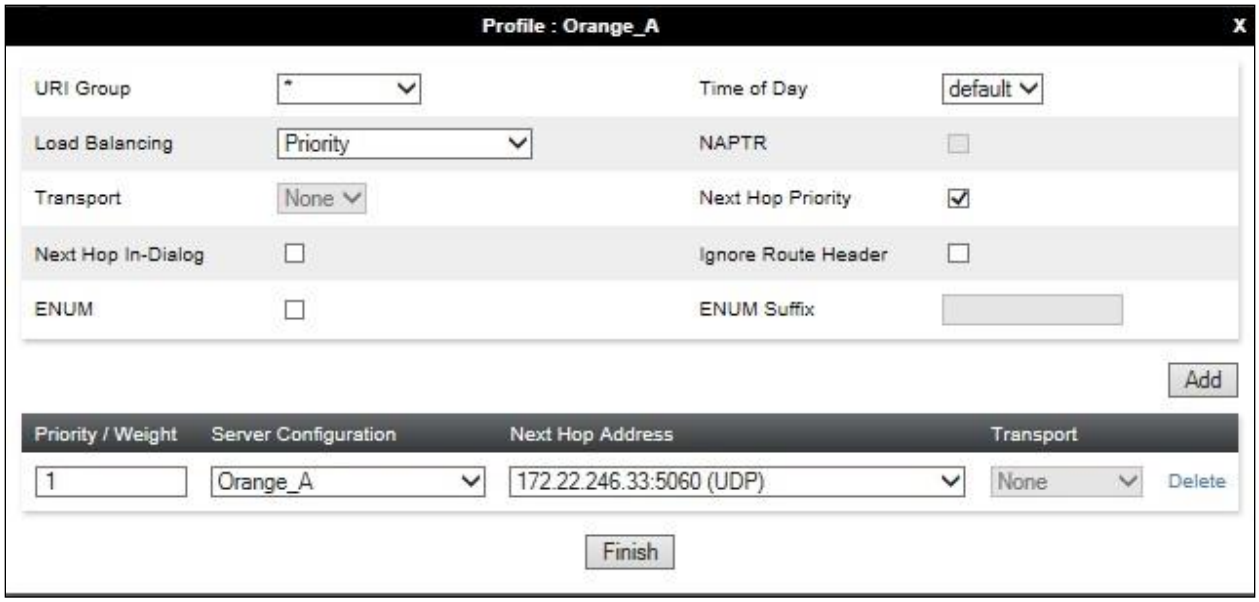


©2019 Avaya Inc. All Rights Reserved.

The Routing Profile window will open. Use the default values displayed and click **Add**.

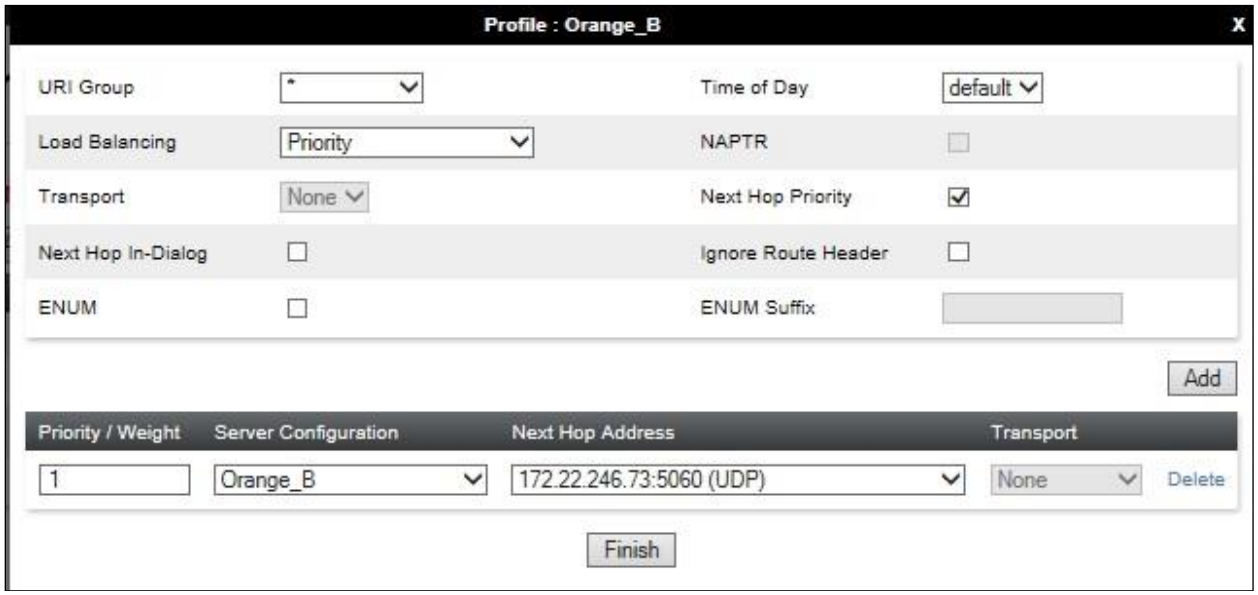
On the **Next Hop Address** window, set the following:

- **Priority/Weight** = **1**.
- **Server Configuration** = **Orange_A** (**Section 7.5.2**) from drop down menu.
- **Next Hop Address** = Select **172.22.246.33 (UDP)** from drop down menu.
- Click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

Repeat the above process to define a Routing Profile for the Orange BTIP secondary SBC. This screenshot shows the configuration used for the Orange BTIP secondary SBC in the test environment:



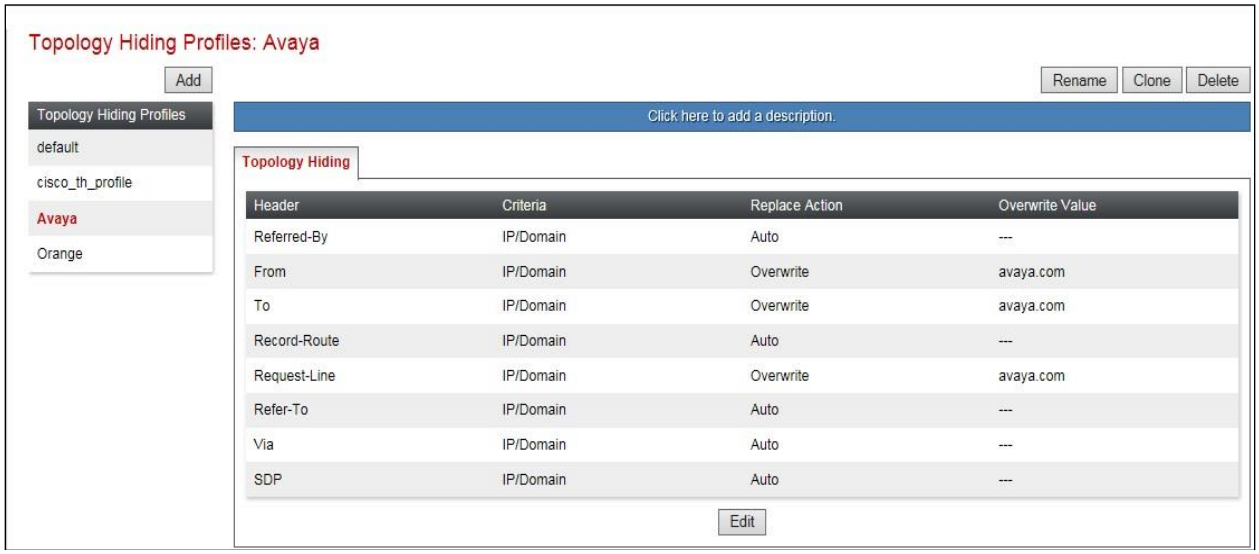
©2019 Avaya Inc. All Rights Reserved.

7.7. Topology Hiding

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

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

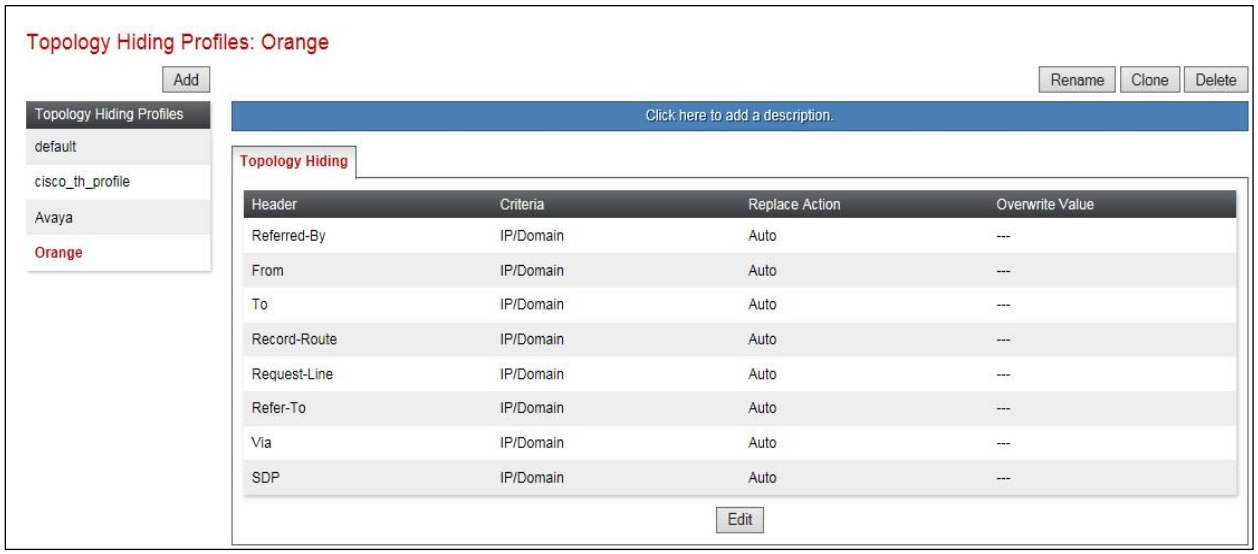
- Enter a descriptive Profile Name such as **Avaya**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **avaya.com**.
- Click **Finish** (not shown).



©2019 Avaya Inc. All Rights Reserved.

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

- In the **Profile Name** field enter a descriptive name for Orange and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Auto** under **Replace Action**.
- Click **Finish** (not shown).



©2019 Avaya Inc. All Rights Reserved.

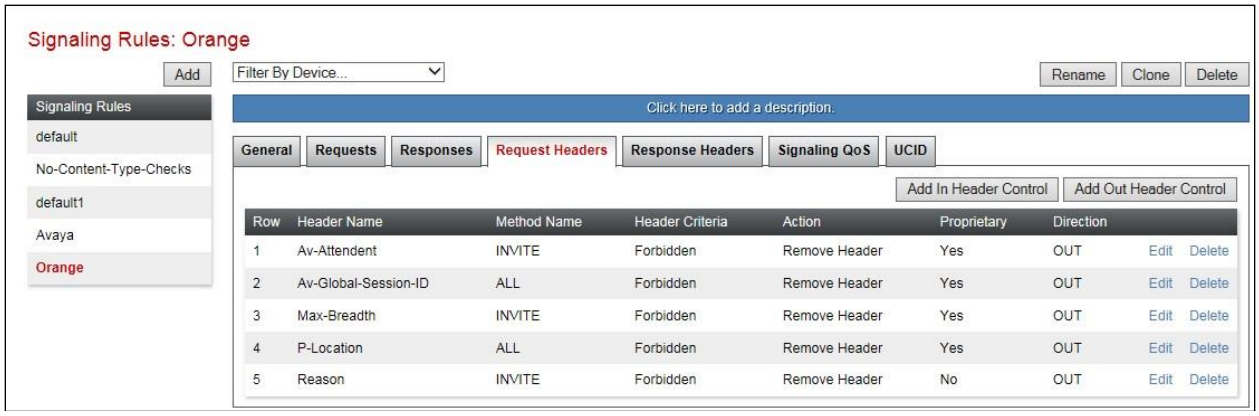
7.8. End Point Policy Groups

End Point Policy Groups are used to bring together a number of different rules for use in a server flow described in **Section 7.9**. Orange BTIP 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.

7.8.1. 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. Signalling rules were created for both Session Manager and Orange BTIP to remove unwanted Avaya proprietary Headers. The Orange BTIP signalling rule was named **Orange** and the Session manager signalling rule was named **Avaya**.

To define the Orange BTIP 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**.



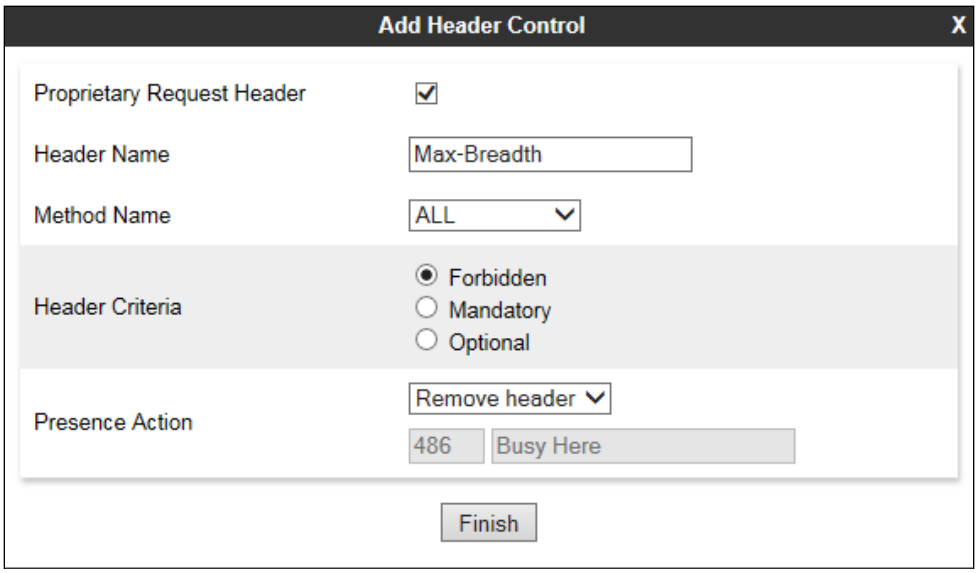
Enter a **Rule Name** in the **Clone Rule** dialogue box and click on **Finish**.

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 Orange BTIP.

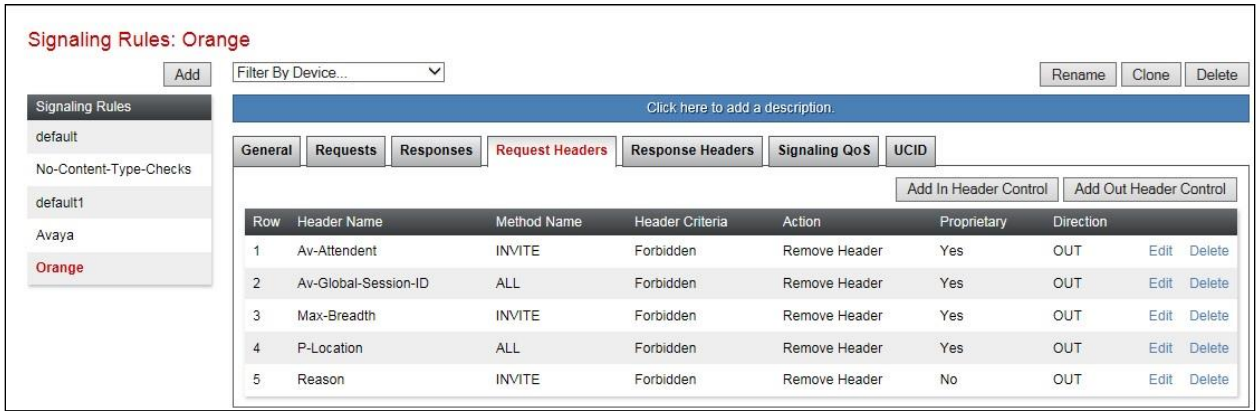
©2019 Avaya Inc. All Rights Reserved.

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**.

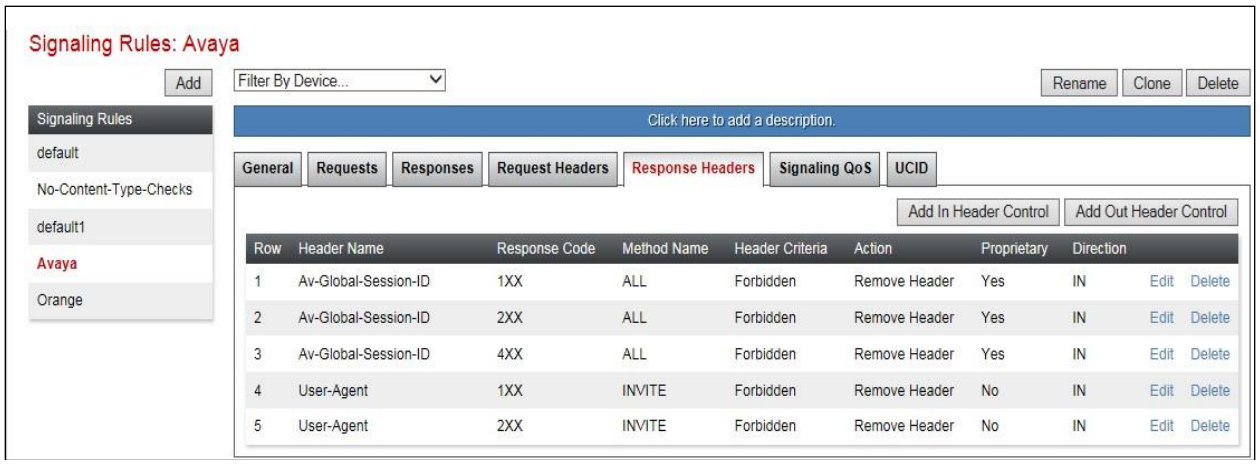


Note: The above is an example of removal of Max-Breadth proprietary header. During test, the same was also done for Av-Attendant, Av-Global-Session-ID, P-Location and Reason Headers. When finished, all the Request Headers defined will be shown under the Request Headers tab as shown in the screenshot below.



©2019 Avaya Inc. All Rights Reserved.

Repeat the process for the Session Manager Signalling rule. **Note:** For the Session Manager signalling rule, Av-Global-Session-ID and User-Agent were the Avaya proprietary headers removed from the **Response Headers** tab. When finished, all the Response Headers defined will be shown under the Response Headers tab as shown in the screenshot below.



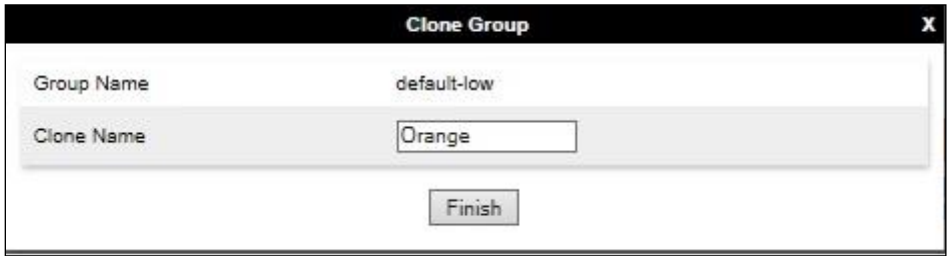
7.8.2. End Point Policy Group

An End Point Policy Group is required to implement the signalling rule. To define one for use in the Session Manager and Orange BTIP server flows, 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**.

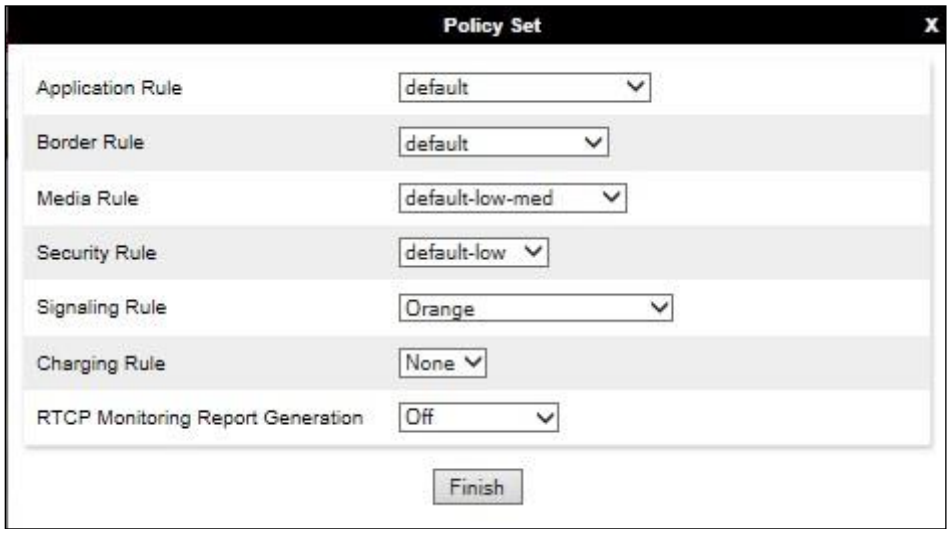
©2019 Avaya Inc. All Rights Reserved.

Enter an appropriate name in the pop-up box.



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

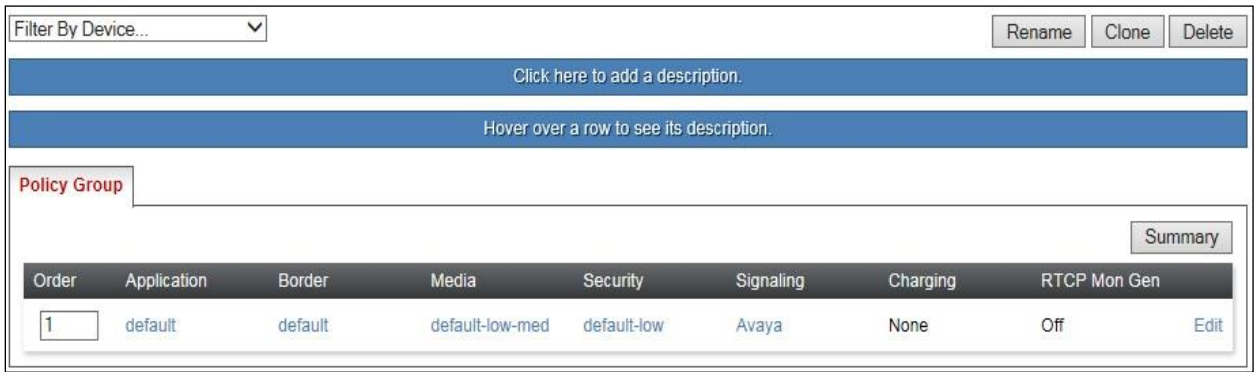
- Leave the **Application Rule**, **Border Rule**, **Media Rule**, **Security Rule**, **Charging Rule** and **RTCP Monitoring Report Generation** at their default values.
- Select the **Signaling Rule** created in the previous section in the drop down menu.
- Click on **Finish**.



©2019 Avaya Inc. All Rights Reserved.

The completed Orange BTIP Policy Group is shown in the screenshot below:

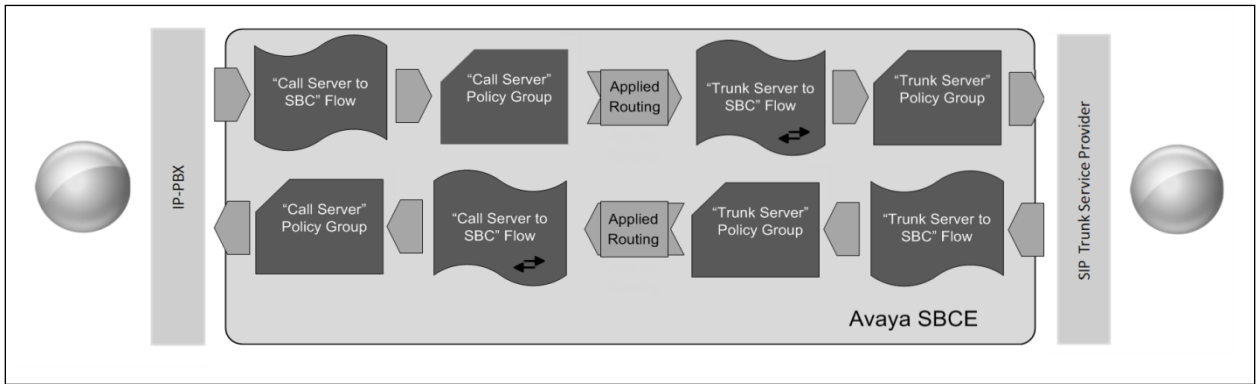
Repeat the process for the Session Manager End Point Policy Group. The completed Session Manager Policy Group is shown in the screenshot below:



©2019 Avaya Inc. All Rights Reserved.

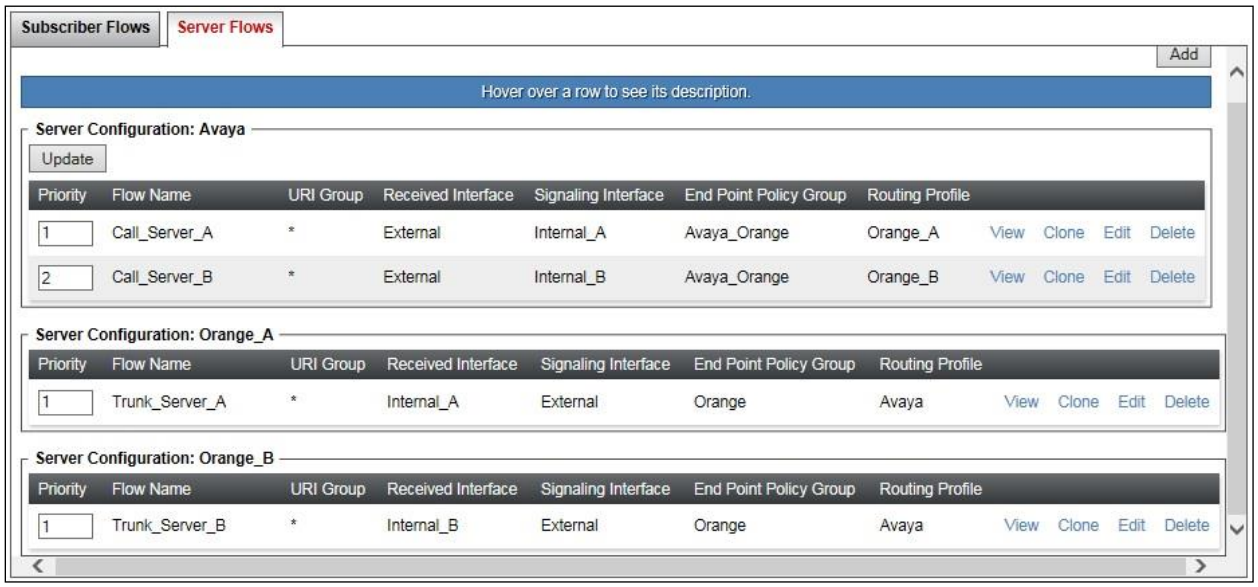
7.9. Server Flows

Server Flows combine the previously defined profiles into four End Point Server Flows, two for the Session Manager and two for Orange BTIP. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



Two server flows are required for outgoing traffic and two are required for incoming. This is so that traffic can be routed to both the primary and secondary Orange SBC's and can also be received from both primary and secondary Orange SBC's . This configuration ties all the previously entered information together so that calls can be routed from Session Manager to the Orange BTIP primary and secondary SBC's and vice versa .

The following screenshot shows all configured flows.



Subscriber Flows | Server Flows

Add

Hover over a row to see its description.

Server Configuration: Avaya

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Call_Server_A	*	External	Internal_A	Avaya_Orange	Orange_A	View	Clone	Edit	Delete
2	Call_Server_B	*	External	Internal_B	Avaya_Orange	Orange_B	View	Clone	Edit	Delete

Server Configuration: Orange_A

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Trunk_Server_A	*	Internal_A	External	Orange	Avaya	View	Clone	Edit	Delete

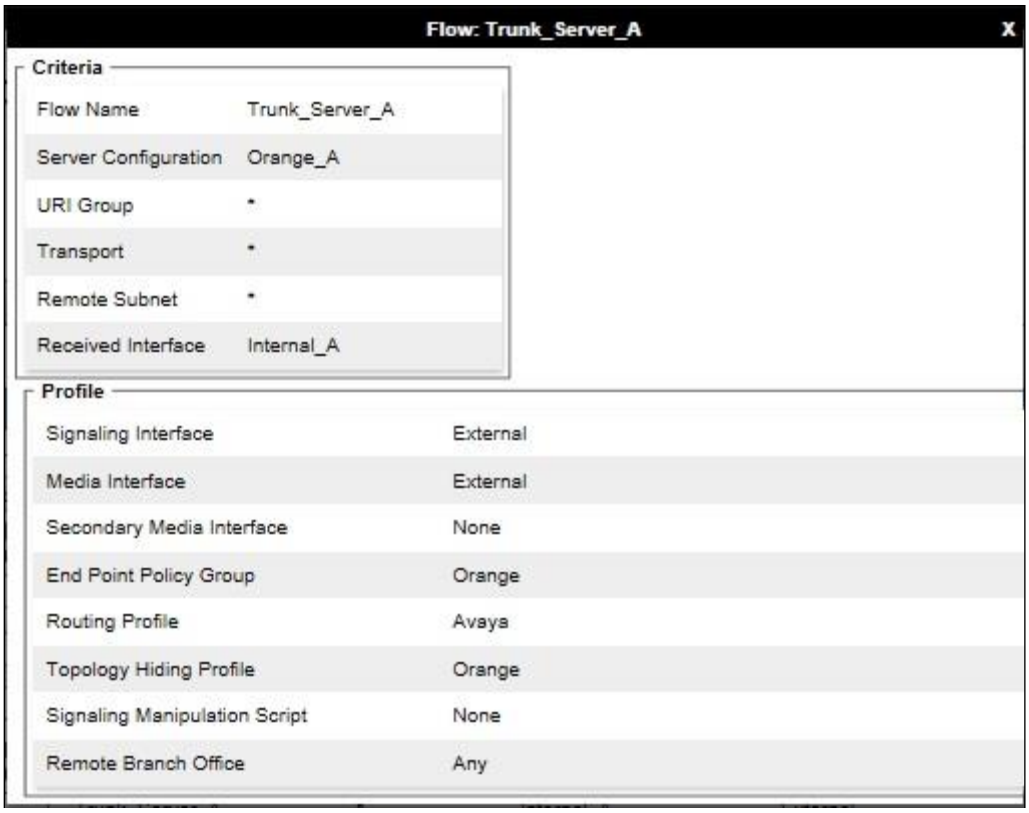
Server Configuration: Orange_B

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Trunk_Server_B	*	Internal_B	External	Orange	Avaya	View	Clone	Edit	Delete

©2019 Avaya Inc. All Rights Reserved.

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

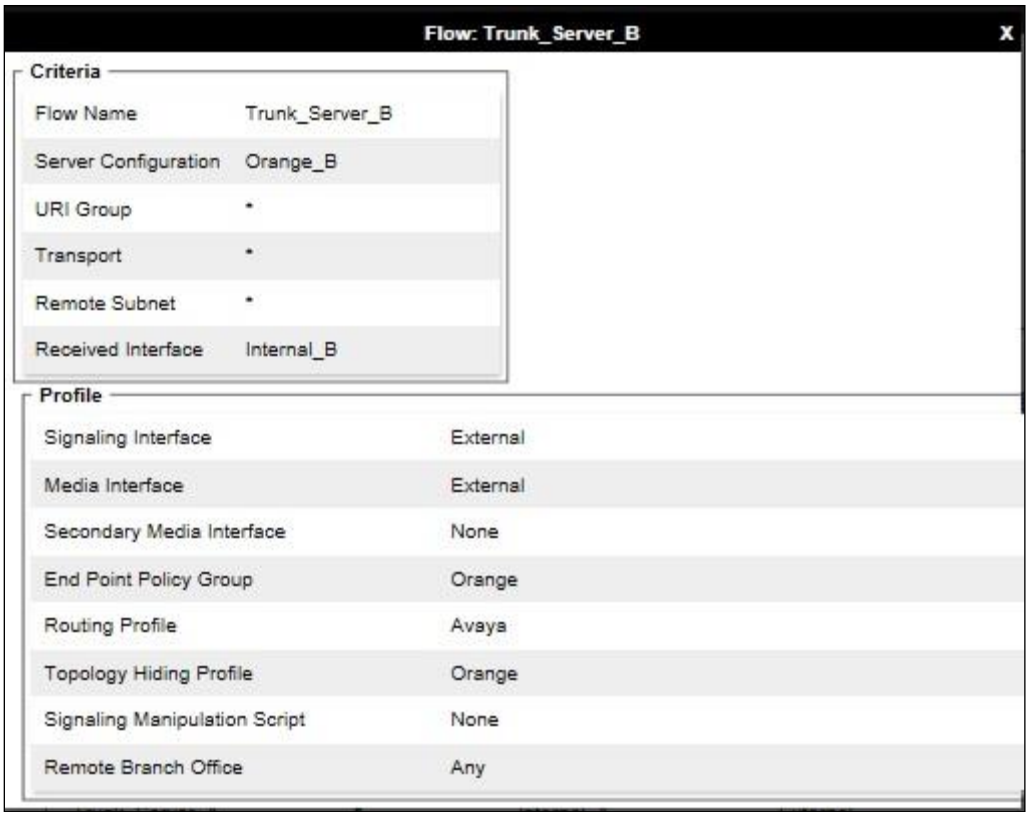
- In the **Flow Name** field enter a descriptive name for the server flow for the Orange BTIP primary SBC, in the test environment **Trunk_Server_A** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the primary SBC defined in **Section 7.5.2**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3.1**. 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 7.3.1**. 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 7.3.2**. 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 Orange BTIP SIP Trunk defined in **Section 7.8.2**.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.6.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Orange BTIP defined in **Section 7.7** and click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

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

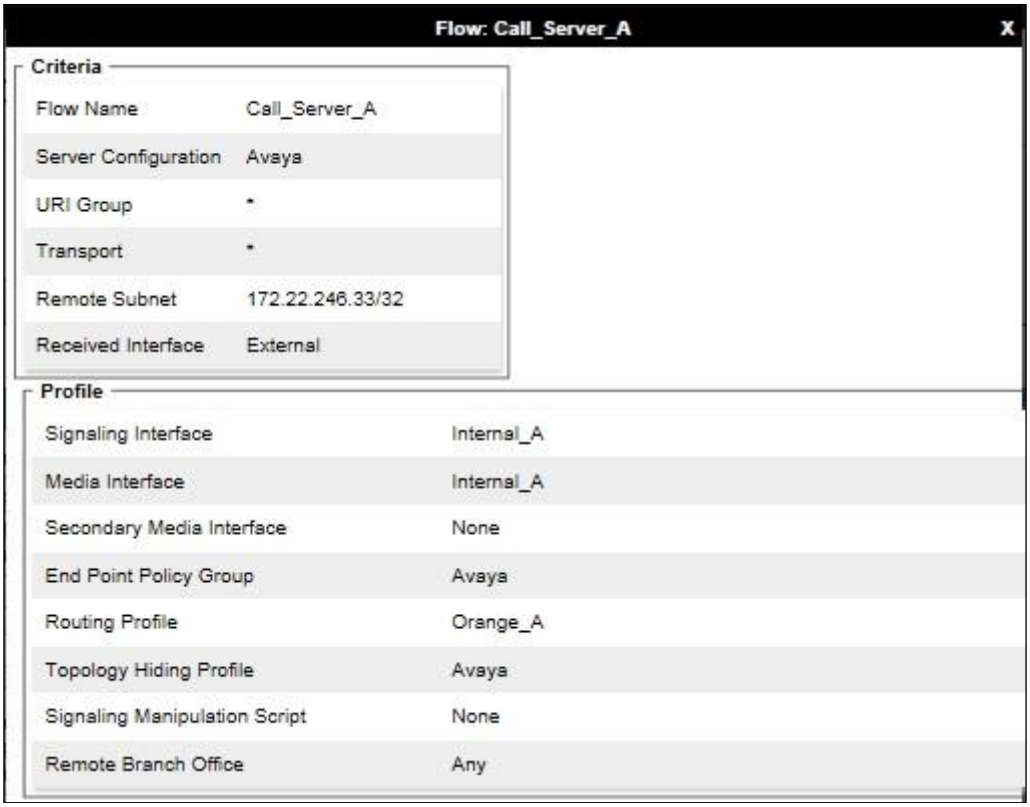
- In the **Flow Name** field enter a descriptive name for the server flow for the Orange BTIP secondary SBC, in the test environment **Trunk_Server_B** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the primary SBC defined in **Section 7.5.2**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3.1**. 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 7.3.1**. 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 7.3.2**. 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 Orange BTIP SIP Trunk defined in **Section 7.8.2**.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.6.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Orange BTIP defined in **Section 7.7** and click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

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

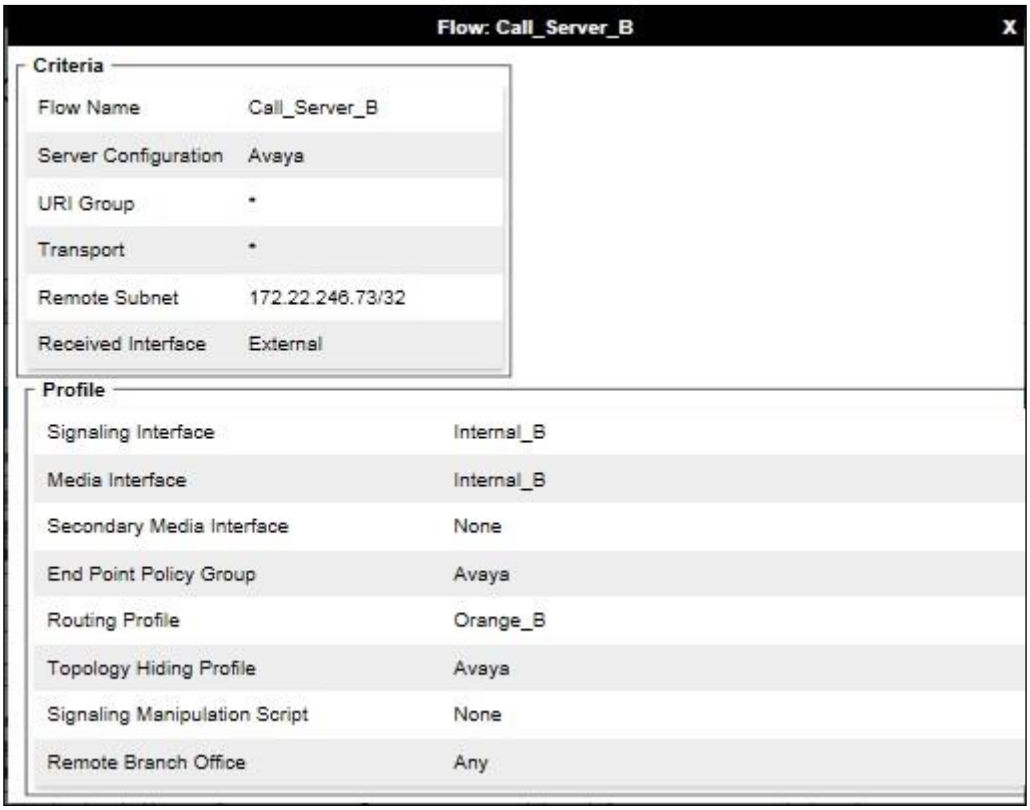
- In the **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **Call_Server_A** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.5.1**.
- In the **Remote Subnet** 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 7.3.1**. 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 7.3.1**. 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 7.3.2**. This is the interface that media bound for Session Manager is sent on.
- In the **End Point Policy Group** drop-down menu, select the Policy Group for Session Manager defined in **Section 7.8.2**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Orange BTIP primary SBC defined in **Section 7.6.2**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.7** and click **Finish**.
- .



©2019 Avaya Inc. All Rights Reserved.

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

- In the **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **Call_Server_B** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.5.1**.
- 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 7.3.1**. 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 7.3.1**. 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 7.3.2**. This is the interface that media bound for Session Manager is sent on.
- In the **End Point Policy Group** drop-down menu, select the Policy Group for Session Manager defined in **Section 7.8.2**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Orange BTIP primary SBC defined in **Section 7.6.2**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.7** and click **Finish**.



©2019 Avaya Inc. All Rights Reserved.

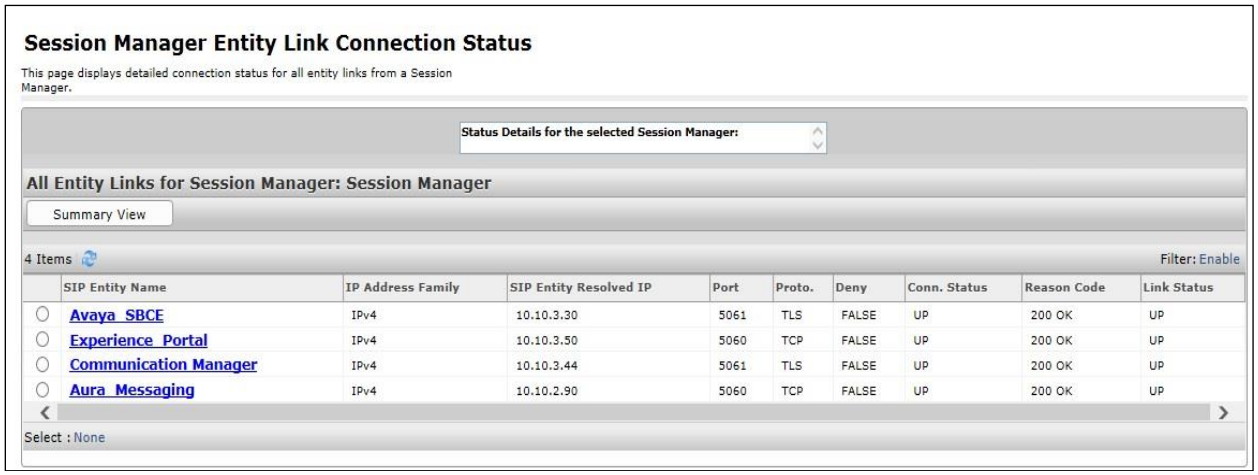
8. Configure Orange BTIP Equipment

The configuration of the Orange BTIP 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 BTIP 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** tab 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	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
Avaya_SBCE	IPv4	10.10.3.30	5061	TLS	FALSE	UP	200 OK	UP
Experience_Portal	IPv4	10.10.3.50	5060	TCP	FALSE	UP	200 OK	UP
Communication Manager	IPv4	10.10.3.44	5061	TLS	FALSE	UP	200 OK	UP
Aura_Messaging	IPv4	10.10.2.90	5060	TCP	FALSE	UP	200 OK	UP

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

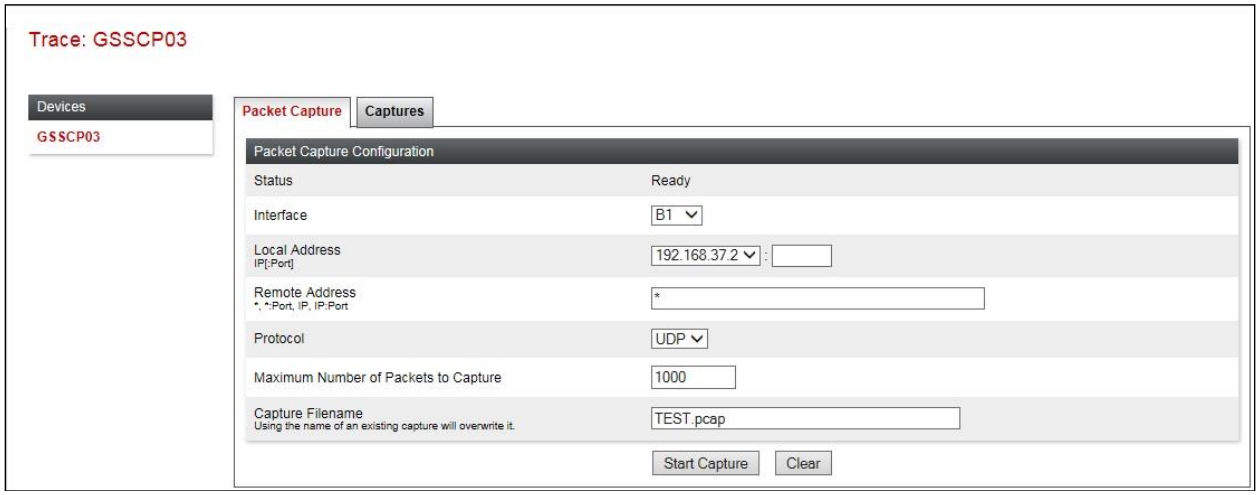
```
status trunk 2

                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0002/001 T00011   in-service/idle    no
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
```


©2019 Avaya Inc. All Rights Reserved.

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.

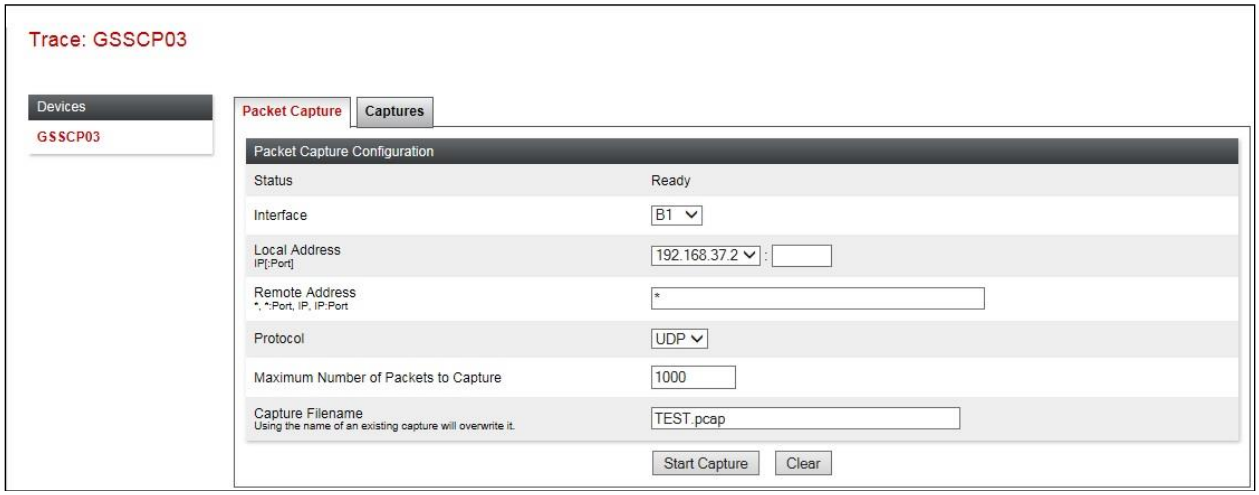
To define the trace, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main menu on the left-hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select the signalling interface IP address or 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**, **1000** is shown as an example.
- Specify the filename of the resultant pcap file in the **Capture Filename** field.
- Click on **Start Capture**.



©2019 Avaya Inc. All Rights Reserved.

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 BTIP network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R8.0, Avaya Aura® Session Manager R8.0 and Avaya Session Border Controller for Enterprise R7.2 to Orange BTIP. Orange BTIP 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**.

©2019 Avaya Inc. All Rights Reserved.

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 8.0, Feb 2019.

[2] *Upgrading and Migrating Avaya Aura® applications to Release 8.0 from System Manager*, Dec 2018.

[3] *Deploying Avaya Aura® applications from System Manager*, Release 8.0, Dec 2018

[4] *Deploying Avaya Aura® Communication Manager*, Release 8.0, Feb 2019

[5] *Administering Avaya Aura® Communication Manager*, Release 8.0, Dec 2018

[6] *Upgrading Avaya Aura® Communication Manager*, Release 8.0, Dec 2018

[7] *Deploying Avaya Aura® System Manager Release 8.0*, Feb 2019

[8] *Upgrading Avaya Aura® System Manager to Release 8.0*, Jan 2019.

[9] *Administering Avaya Aura® System Manager for Release 8.0*, Jan 2019

[10] *Deploying Avaya Aura® Session Manager*, Release 8.0 Mar 2019

[11] *Upgrading Avaya Aura® Session Manager* Release 8.0, Mar 2019

[12] *Administering Avaya Aura® Session Manager* Release 8.0, Mar 2019

[13] *Deploying Avaya Session Border Controller for Enterprise Release 7.2.2*, Apr 2019

[14] *Upgrading Avaya Session Border Controller for Enterprise Release 7.2.2*, Oct 2018

[15] *Administering Avaya Session Border Controller for Enterprise Release 7.2.2*, Apr 2018

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

©2019 Avaya Inc. All Rights Reserved.

©2019 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.