Application Notes for Configuring Avaya Aura® Communication Manager R6.2 as an Evolution Server, Avaya Aura® Session Manager R6.1 and Avaya Session Border Controller Advanced for Enterprise to support BT Italia SIP Trunk Service – Issue 1.0

Abstract

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

NOTE: This Application Note focused on the SIP Trunking aspect of the Avaya Session Border Controller Advanced for Enterprise. Advanced enterprise capabilities such as Remote Worker "a.k.a. Remote SIP Endpoints", dual forking, and TLS/SRTP were not tested. As a result, the Avaya Session Border Controller for Enterprise is also considered Compliance Tested for this solution.

NOTE: This Application Note is applicable with Avaya Aura® 6.2 which is currently in Controlled Introduction. Avaya Aura® 6.2 will be Generally Available in Summer 2012.

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between BT Italia SIP Trunk service and an Avaya SIP-enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller Advanced for Enterprise (ASBCAE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with BT Italia SIP Trunk service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the Enterprise 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 Session Border Controller. The enterprise site was configured to use the SIP Trunk service provided by BT Italia.

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN routed to the DDI numbers assigned by BT Italia
- Incoming PSTN calls made to SIP, H.323 and Digital telephones at the enterprise
- Outgoing calls from the enterprise site completed via BT Italia to PSTN destinations
- Outgoing calls from the enterprise to the PSTN made from SIP, H.323 and Analogue telephones
- Calls using the G.711A and G.729A codecs
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Direct IP-to-IP media (also known as "shuffling") with 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 BT Italia requiring Avaya response and sent by Avaya requiring BT Italia response

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the BT Italia SIP Trunk service with the following observations:

- No inbound toll free numbers were tested as none were available from the Service Provider
- No Emergency Services numbers tested as test calls to these numbers should be pre-arranged with the Operator
- Outbound calls to numbers other than test numbers provided were not permitted for regulatory reasons
- BT Italia sends OPTIONS with a Max Forward value of 0 which must be responded to directly by the ASBCAE using a signalling rule
- For inbound calls, the format of the ACK response to the 200OK sent on answer is not handled correctly by the Session Manager and it requires a script on the ASBCAE
- For calls forwarded to the PSTN, the CLI of the forwarding number is required in the P-Asserted-ID and From headers requiring a script on the ASBCAE
- For calls from the PSTN to an EC500 mobile phone, the CLI of the forwarding number is required in the P-Asserted-ID and From headers requiring a script on the ASBCAE
- When an SDP is included in the 183 Session Progress response to the INVITE for PSTN forwarding, no ring back tone is heard requiring removal of the SDP in the ASBCAE Server Interworking
- Incoming multi-page T38 fax transmission is unreliable from Avaya Galway premises, thought to be a local network issue.
- Fax transmission failed when SIP UPDATE messages were used requiring configuration of the Communication Manager to use re-INVITEs

2.3. Support

For technical support on BT Italia products please visit the website at www.btitalia.it or contact an authorized BT Italia representative.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the BT Italia SIP Trunk Service. Located at the Enterprise site is a Session Border Controller, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya 16xx series IP telephones (with SIP firmware) Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone running on a laptop PC configured for H.323.

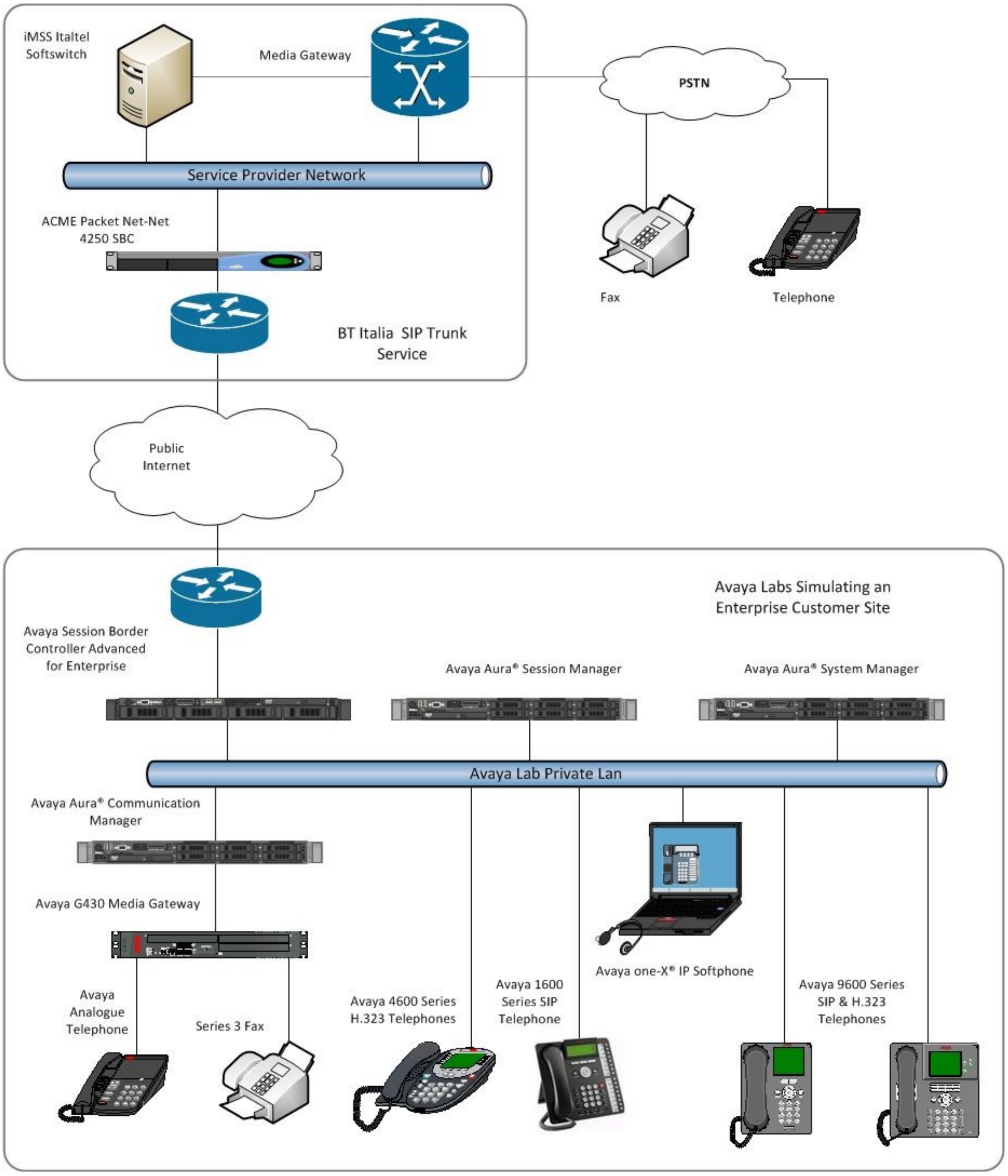

iMSS Italtel Softswitch
Media Gateway
PSTN
Service Provider Network
ACME Packet Net-Net 4250 SBC
Fax
Telephone
BT Italia SIP Trunk Service
Public Internet
Avaya Labs Simulating an Enterprise Customer Site
Avaya Session Border Controller Advanced for Enterprise
Avaya Aura® Session Manager
Avaya Aura® System Manager
Avaya Lab Private Lan
Avaya Aura® Communication Manager
Avaya G430 Media Gateway
Avaya one-X® IP Softphone
Avaya Analogue Telephone
Series 3 Fax
Avaya 4600 Series H.323 Telephones
Avaya 1600 Series SIP Telephone
Avaya 9600 Series SIP & H.323 Telephones

Figure 1: Test Setup BT Italia SIP Trunk to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment	Software
Avaya	
Avaya S8800 Server	Avaya Aura® Communication Manager R6.2 (R016x.02.0.823.0)
Avaya G430 Media Gateway	FW 30.12.1
Avaya S8800 Server	Avaya Aura® Session Manager R6.1 (6.1.5.0.615006)
Avaya S8800 Server	Avaya Aura® System Manager R6.1 (System Platform 6.0.3.1.3, Template 6.1.5.0)
Avaya Session Border Controller Advanced for Enterprise Server	Avaya Session Border Controller Advanced for Enterprise 4.0.5.Q02
Avaya 1616 Phone (H.323)	1.22
Avaya 4621 Phone (H.323)	2.901
Avaya 9670 Phone (H.323)	2.0
Avaya 9601 Phone (SIP)	R6.1 SP3
Avaya one–X® Communicator (H.323) on Lenovo T510 Laptop PC	Avaya one–X® Communicator 6.0.1.16-SP1-25226
Analogue Phone	N/A
BT Italia	
ACME Packet SBC Net-Net4250 SBC	6.1
iMSS Italtel Softswitch	22.30.23

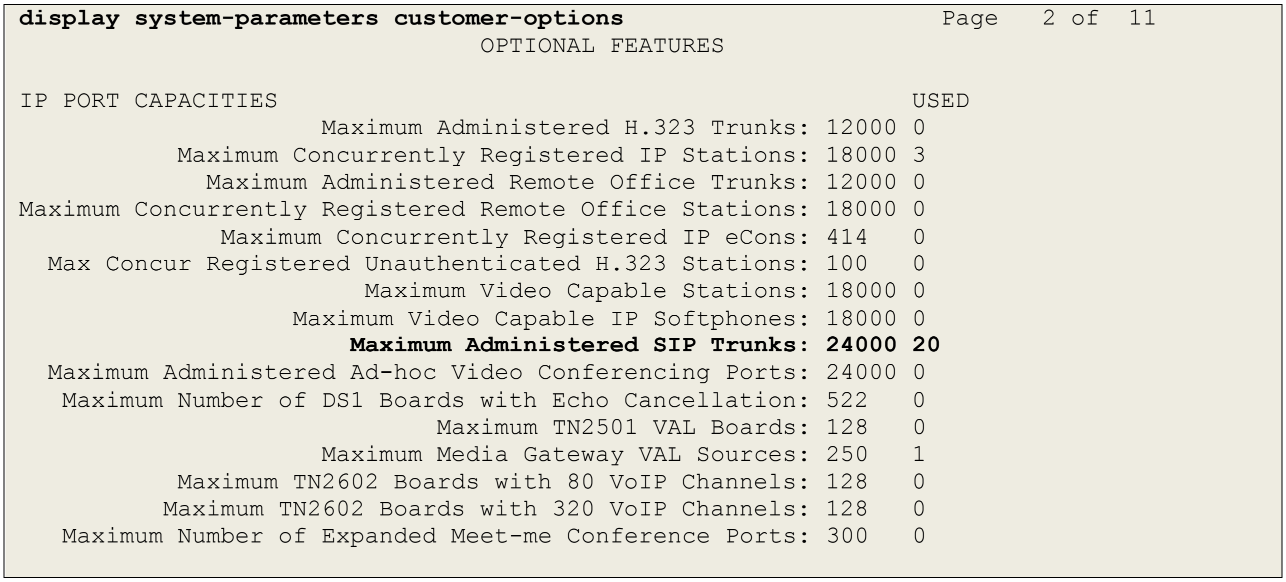
Note: At the time of test, Communication Manager R6.2 was in Control Induction phase prior to being made GA, System Manager R6.2 and Session Manager R6.2 were not in Control Induction phase or GA so testing was done with System Manager and Session Manager at R6.1.

5. Configure Avaya Aura ® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP Signalling associated with the BT Italia SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the Avaya Session Border Controller Advanced for Enterprise and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Session Border Controller at the enterprise site that then sends the SIP messages to the BT Italia network. Communication Manager Configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the Avaya S8800 Servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the BT Italia network, and any other SIP trunks used.



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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 20
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

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

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

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

           IP Attendant Consoles? y
```

5.2. Administer IP Node Names

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

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

5.3. Administer IP Network Region

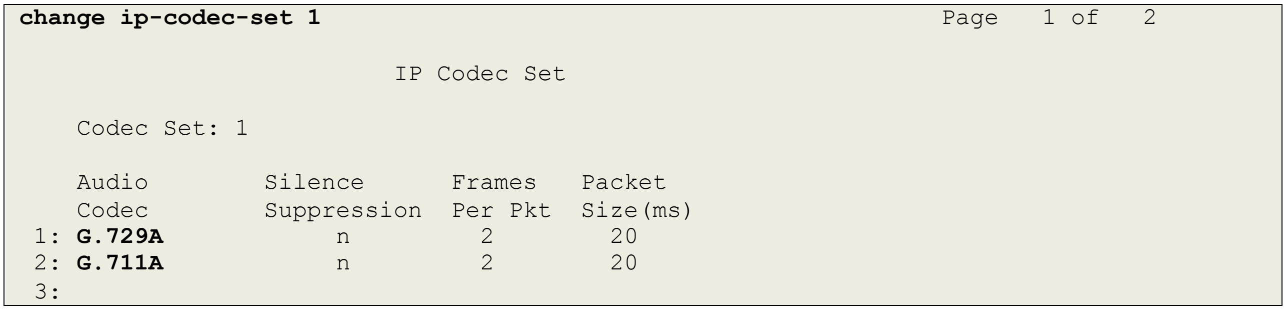
Use the **change ip-network-region 1** command to set the following values:

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

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: default
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

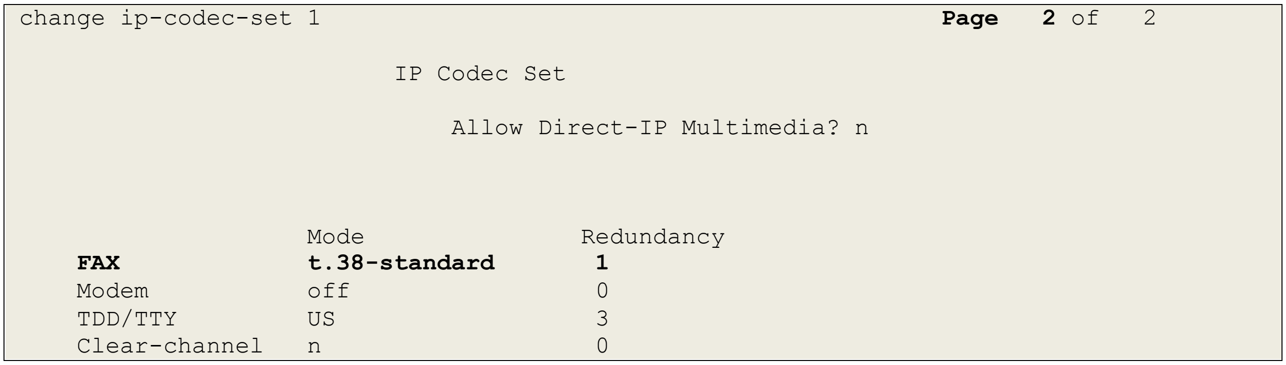
5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form, **Section 5.3.** Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec supported by BT Italia was configured, namely **G.711A** and **G.729A**.



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

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729A            n          2        20
 2: G.711A            n          2        20
 3:
```

The BT Italia SIP Trunk service supports T.38 for transmission of fax. Navigate to **Page 2** to configure T.38 by setting the **Fax Mode** to **t.38-standard** as shown below.



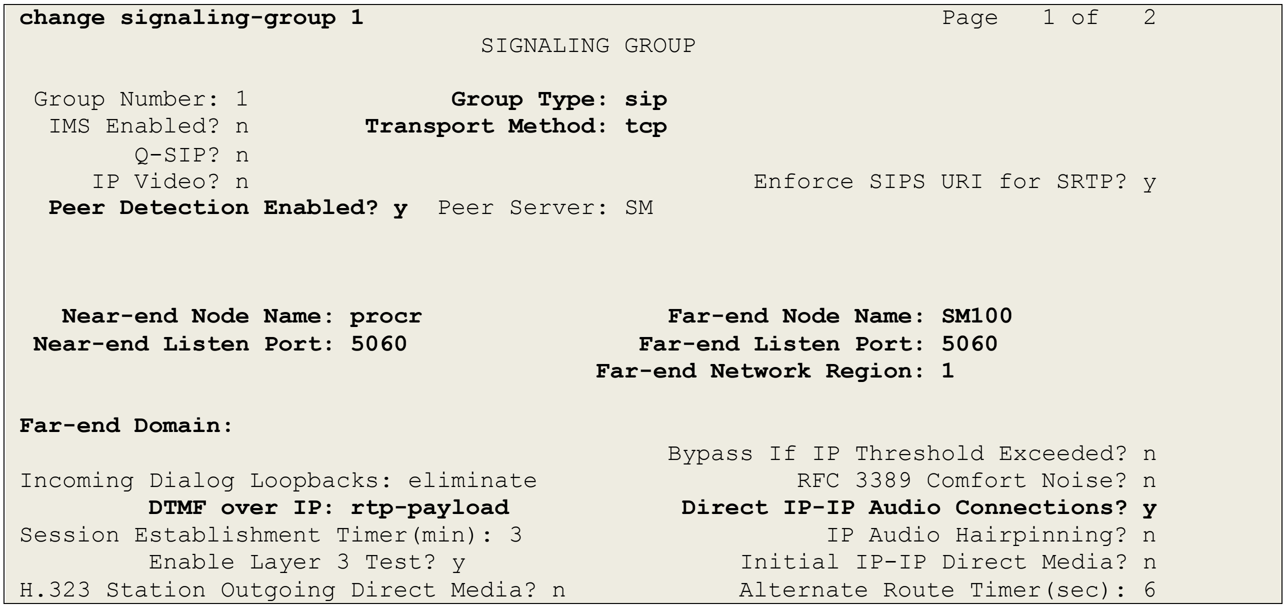
```
change ip-codec-set 1                                          Page   2 of   2

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



                    Mode                 Redundancy
    FAX             t.38-standard         1
    Modem           off                   0
    TDD/TTY         US                    3
    Clear-channel   n                     0
```

5.5. Administer SIP Signaling Groups

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

- Set **Group Type** to **sip**
- Set **Transport Method** to **tcp**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region **1**)
- Leave **Far-end Domain** blank (removes the analysis of the far end domain name and subsequent handling of multiple signalling groups where it is not required)
- Set **Direct IP-IP Audio Connections** to **y**
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.



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

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



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

Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload              Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

5.6. Administer SIP Trunk Group

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

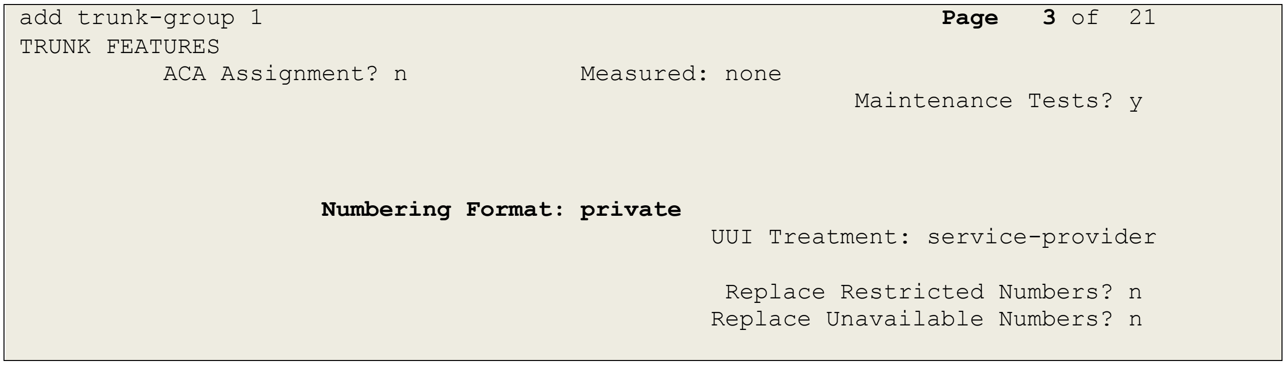
- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **public-netwrk** – required setting when using the Diversion header
- 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 1                                              Page   1 of  21
                                TRUNK GROUP

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

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

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

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

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

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

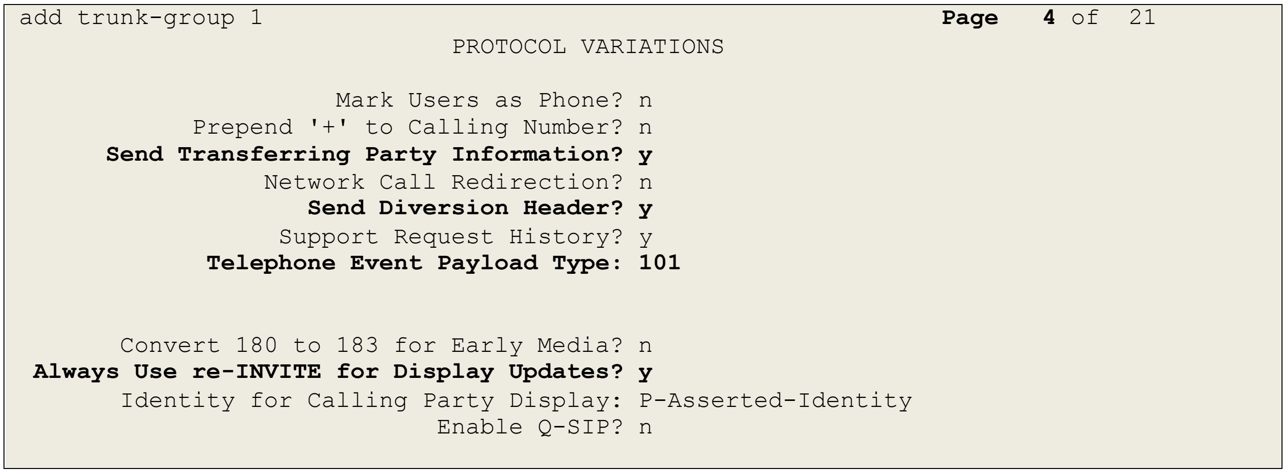
On **Page 3**, set the **Numbering Format** field to **private**. This ensure delivery of CLI in national format with no leading “+” indicating E.164 format



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



                     Numbering Format: private
                                                UUI Treatment: service-provider

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

On **Page 4** of this form:

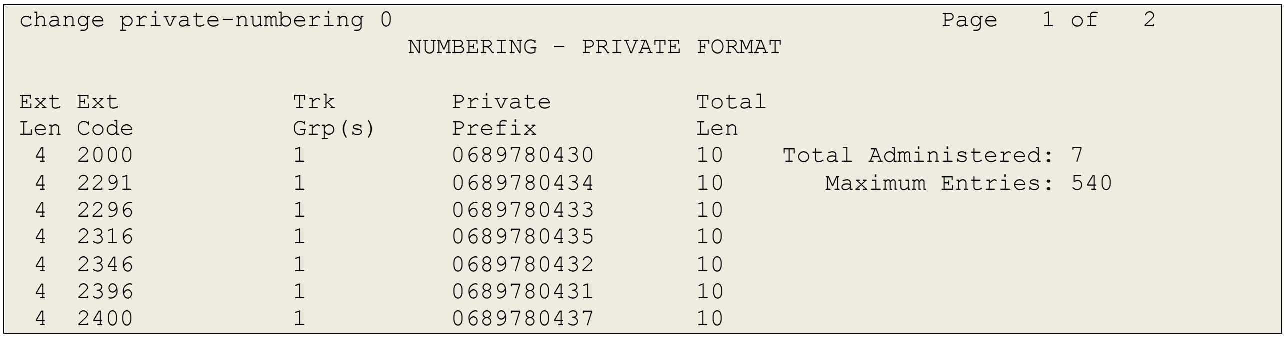
- Set **Send Diversion Header** to **y** so that the header is sent for call forwarding and EC500
- Set **Send Transferring Party Information** to **y**
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by BT Italia
- Set **Always Use re-INVITE for Display Updates** to **y** to allow correct operation of fax



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

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? y
                 Network Call Redirection? n
                    Send Diversion Header? y
                  Support Request History? y
             Telephone Event Payload Type: 101


       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? y
       Identity for Calling Party Display: P-Asserted-Identity
                            Enable Q-SIP? n
```

5.7. Administer Calling Party Number Information

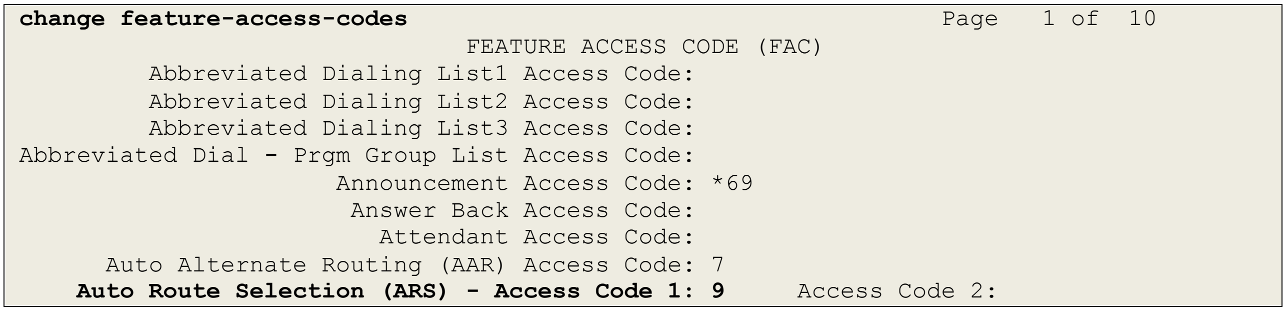
Use the **change private-unknown-numbering** command to configure Communication Manager to send the calling party number. In the test configuration, individual stations were mapped to send numbers allocated from the BT Italia DDI range supplied. This calling party number is sent in the SIP From, Contact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



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

Ext Ext              Trk         Private           Total
Len Code             Grp(s)      Prefix            Len
 4  2000             1           0689780430        10    Total Administered: 7
 4  2291             1           0689780434        10       Maximum Entries: 540
 4  2296             1           0689780433        10
 4  2316             1           0689780435        10
 4  2346             1           0689780432        10
 4  2396             1           0689780431        10
 4  2400             1           0689780437        10
```

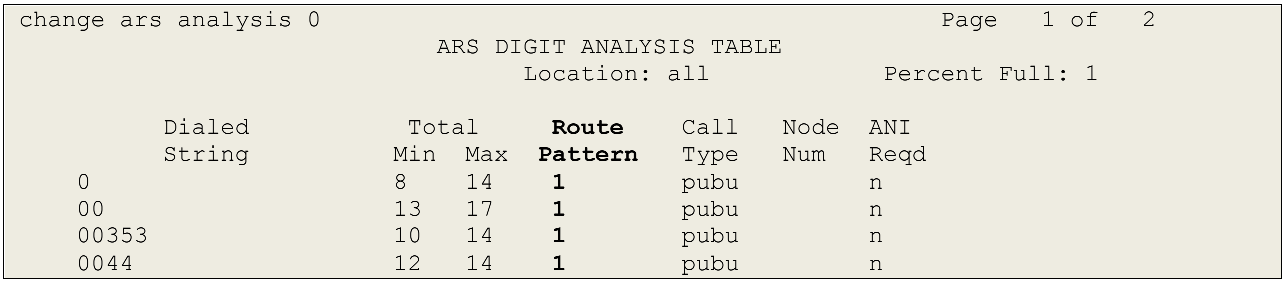
5.8. Administer Route Selection for Outbound Calls

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



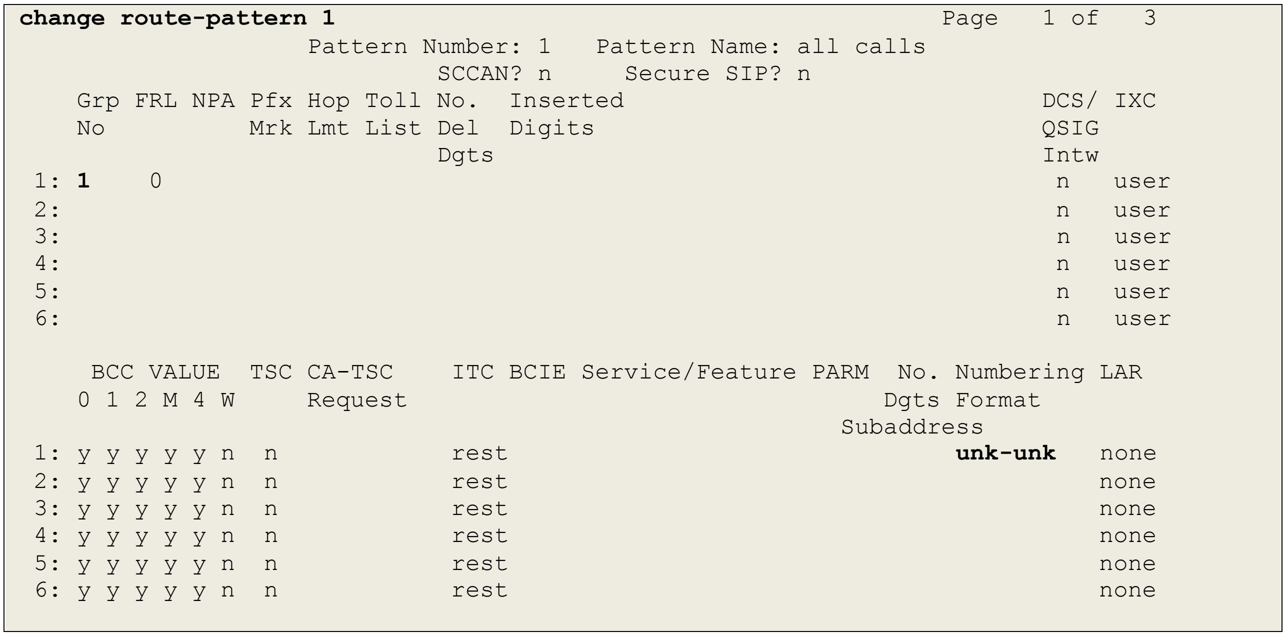
```
change feature-access-codes                                     Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial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

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0 or 00. Note that exact maximum number lengths have been used as it was found during test that a greater value resulted in transmission of a DTMF "#" after establishment of the media stream. Calls are sent to **Route Pattern 1**.



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

          Dialed           Total      Route    Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    0                     8    14     1        pubu         n
    00                    13   17     1        pubu         n
    00353                 10   14     1        pubu         n
    0044                  12   14     1        pubu         n
```

Use the **change route-pattern x** command to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**. Set the **Numbering Format** to **unk-unk**.



```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: all calls
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                                DCS/ IXC
    No          Mrk Lmt List Del  Digits                                  QSIG
                             Dgts                                         Intw
 1: 1    0                                                                 n   user
 2:                                                                        n   user
 3:                                                                        n   user
 4:                                                                        n   user
 5:                                                                        n   user
 6:                                                                        n   user

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

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from BT Italia can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by BT Italia for testing are assigned to the internal extensions of the test equipment configured within the Communication Manager. The **change inc-call-handling-trmt trunk-group x** command is used to translate numbers 068xxxxxx0-068xxxxxx9 to the 4 digit extension by deleting all of the incoming digits and inserting the extension number. Note that the significant digits beyond the city code have been obscured.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 0689780430       all 2000
 public-ntwrk    10 0689780431       all 2396
 public-ntwrk    10 0689780432       all 2346
 public-ntwrk    10 0689780433       all 2296
 public-ntwrk    10 0689780434       all 2291
 public-ntwrk    10 0689780435       all 2316
 public-ntwrk    10 0689780436       all 6101
 public-ntwrk    10 0689780437       all 2400
 public-ntwrk    10 0689780438       all 6103
 public-ntwrk    10 0689780439       all 2501
```

5.10. EC500 Configuration

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

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

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

 Station       Application Dial   CC  Phone Number     Trunk       Config  Dual
 Extension                 Prefix                      Selection   Set     Mode
 2396             EC500         -     00353867818306    1          1
                                -
```

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

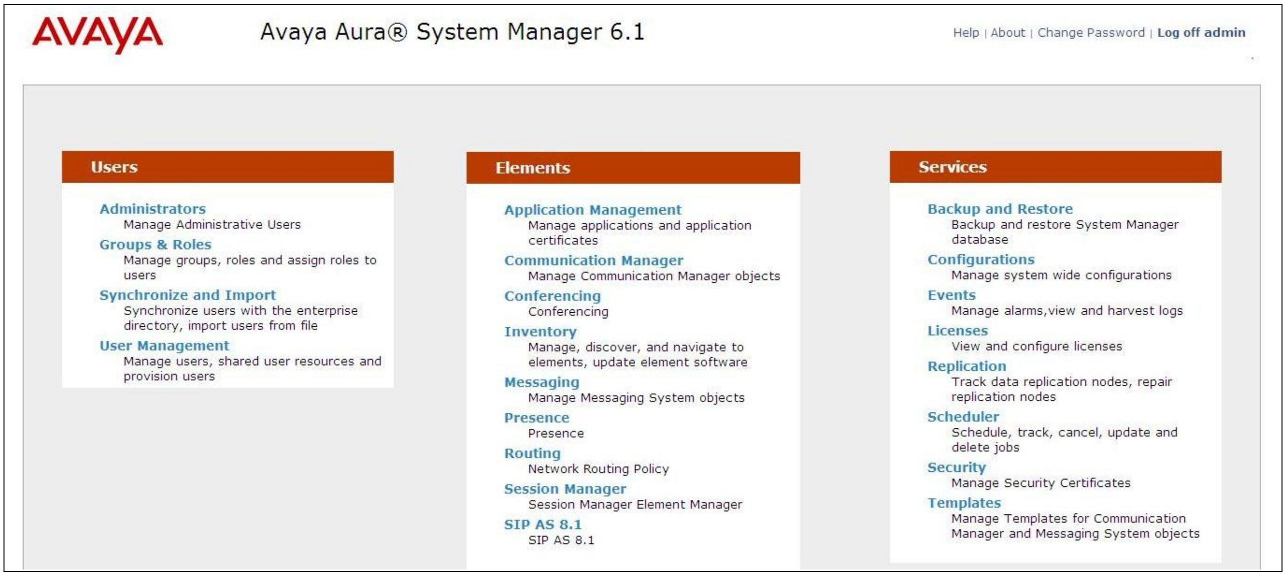
6. Configuring Avaya Aura® Session Manager

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

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

6.1. Log in to Avaya Aura® System Manager

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



AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Users

Administrators
Manage Administrative Users

Groups & Roles
Manage groups, roles and assign roles to users

Synchronize and Import
Synchronize users with the enterprise directory, import users from file

User Management
Manage users, shared user resources and provision users

Elements

Application Management
Manage applications and application certificates

Communication Manager
Manage Communication Manager objects

Conferencing
Conferencing

Inventory
Manage, discover, and navigate to elements, update element software

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

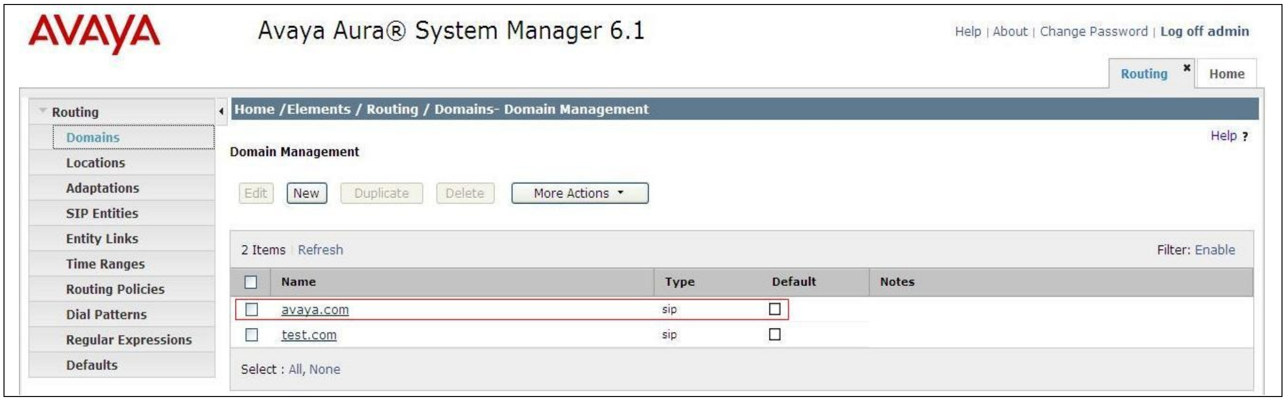
Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager and Messaging System objects

6.2. Administer SIP Domain

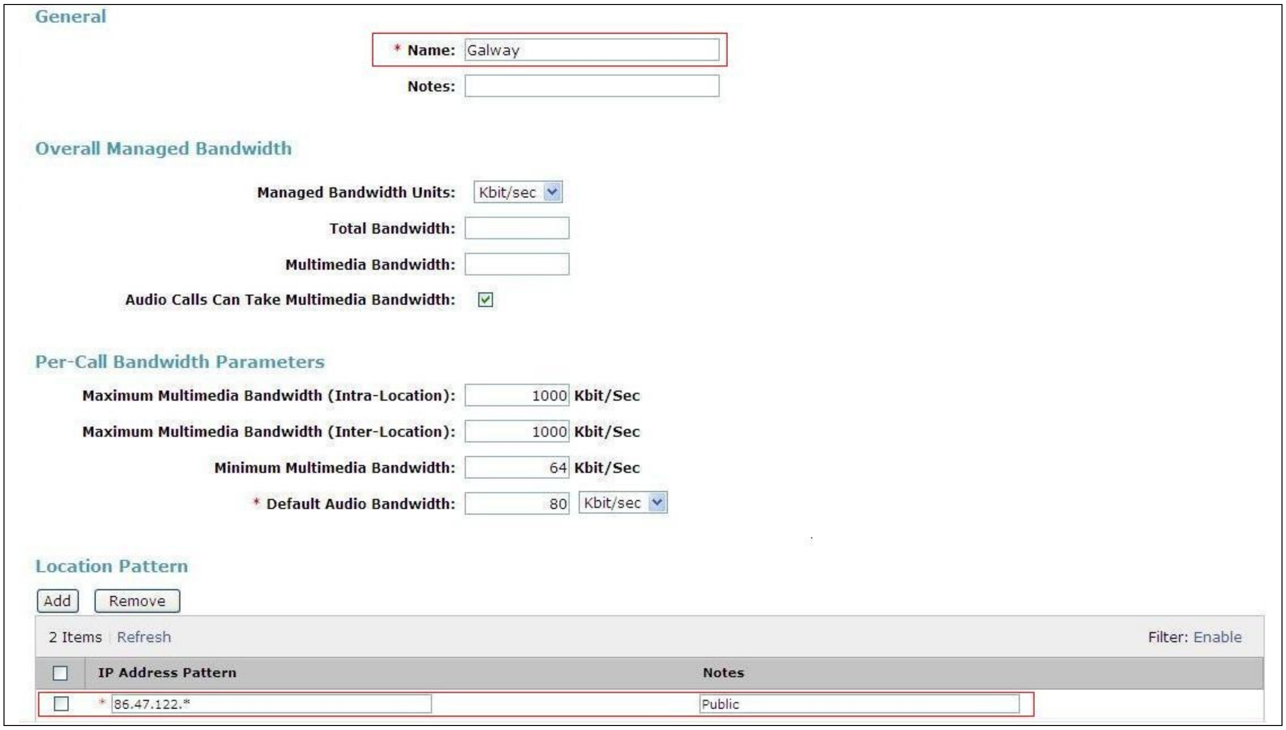
To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **avaya.com**) and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



□	Name	Type	Default	Notes
□	avaya.com	sip	□	
□	test.com	sip	□	

6.3. Administer Locations

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



General

* Name:	Galway
Notes:	

Overall Managed Bandwidth

Managed Bandwidth Units:	Kbit/sec
Total Bandwidth:	
Multimedia Bandwidth:	
Audio Calls Can Take Multimedia Bandwidth:	☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):	1000 Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location):	1000 Kbit/Sec
Minimum Multimedia Bandwidth:	64 Kbit/Sec
* Default Audio Bandwidth:	80 Kbit/sec

Location Pattern

□	IP Address Pattern	Notes
□	* 86.47.122.*	Public

6.4. Administer SIP Entities

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

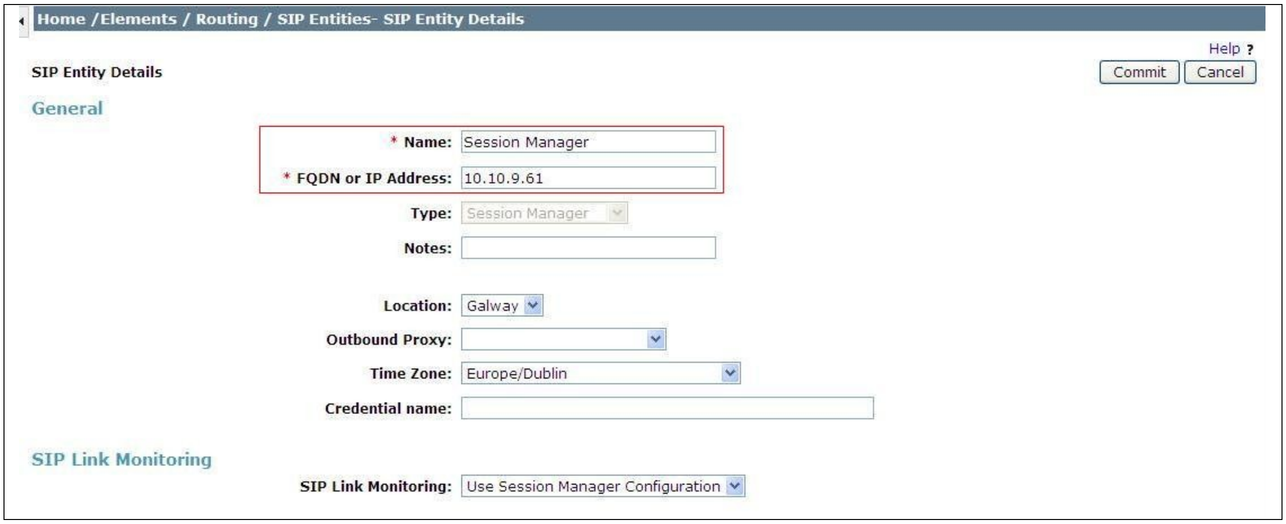
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **Gateway** for the Session Border Controller SIP entity
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities:

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

6.4.1. 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.



SIP Entity Details

General

* Name: Session Manager

* FQDN or IP Address: 10.10.9.61

Type: Session Manager

Notes:

Location: Galway

Outbound Proxy:

Time Zone: Europe/Dublin

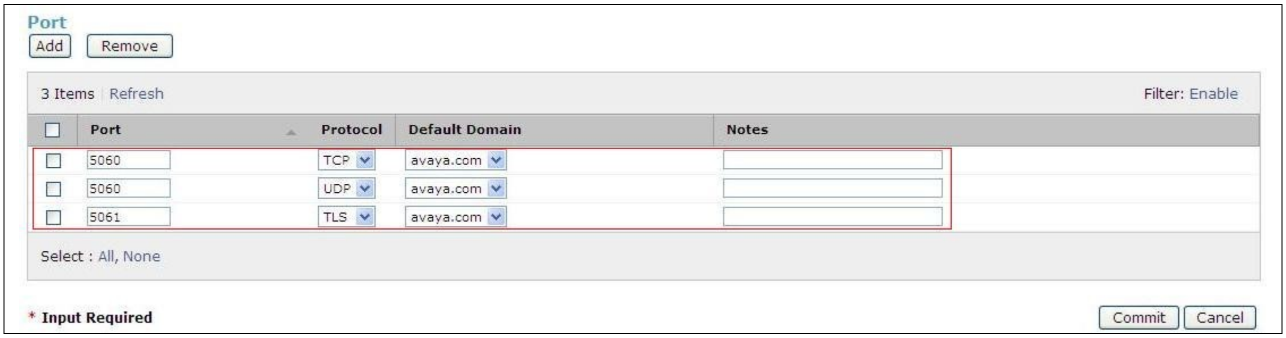
Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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

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



Port

Add | Remove

3 Items | Refresh   Filter: Enable

□	Port	Protocol	Default Domain	Notes
□	5060	TCP	avaya.com	
□	5060	UDP	avaya.com	
□	5061	TLS	avaya.com	

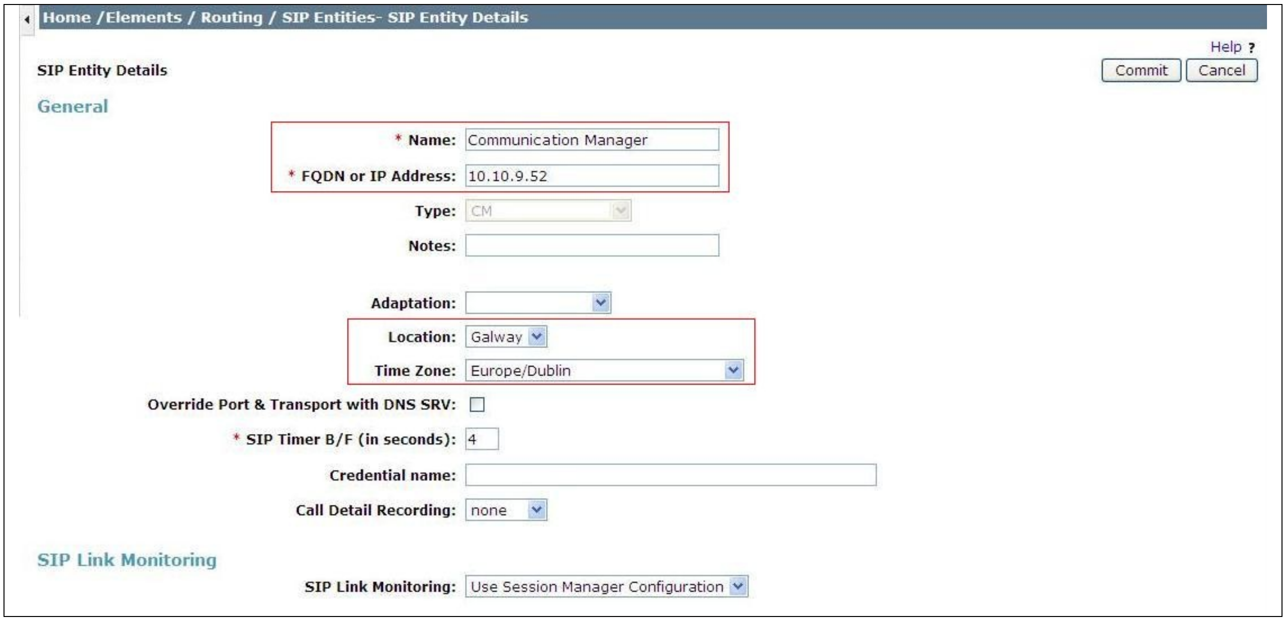
Select : All, None

* Input Required

Commit | Cancel

6.4.2. Avaya Aura® Communication Manager SIP Entity

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



Home /Elements / Routing / SIP Entities- SIP Entity Details

Help ?

SIP Entity Details

Commit | Cancel

General

* Name: Communication Manager

* FQDN or IP Address: 10.10.9.52

Type: CM

Notes:

Adaptation:

Location: Galway

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: □

* SIP Timer B/F (in seconds): 4

Credential name:

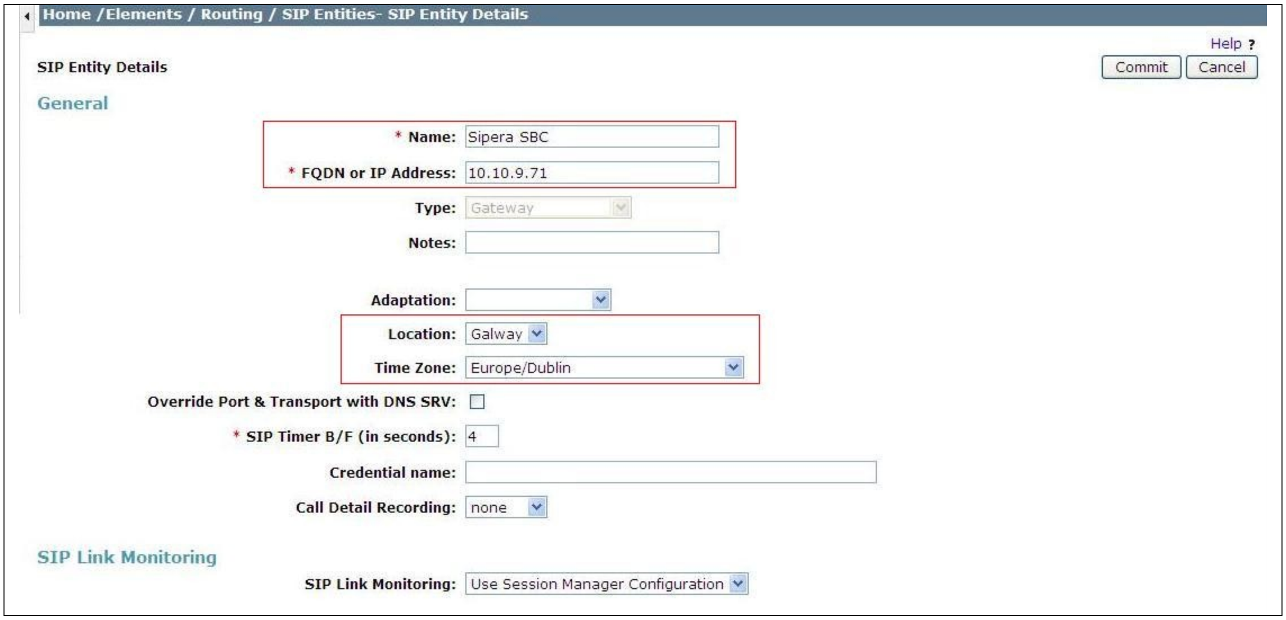
Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.4.3. Avaya Session Border Controller Advanced for Enterprise SIP Entity

The following screen shows the SIP Entity for the Session Border Controller. The **FQDN or IP Address** field is set to the IP address of the Session Border Controller private network interface (see **Figure 1**).



SIP Entity Details

General

* Name:	Sipera SBC
* FQDN or IP Address:	10.10.9.71
Type:	Gateway
Notes:	
Adaptation:	
Location:	Galway
Time Zone:	Europe/Dublin
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

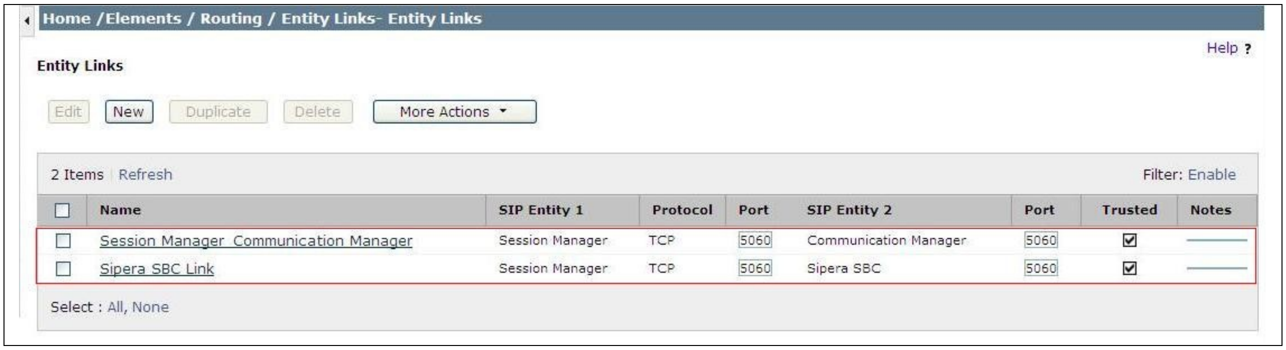
SIP Link Monitoring: Use Session Manager Configuration

6.5. Administer Entity Links

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

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select **Session Manager** 1
- 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 6.4**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- Select the **Trusted** tick box to make the other system trusted
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

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



☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
☐	Session Manager_Communication Manager	Session Manager	TCP	5060	Communication Manager	5060	☑	
☐	Sipera SBC Link	Session Manager	TCP	5060	Sipera SBC	5060	☑	

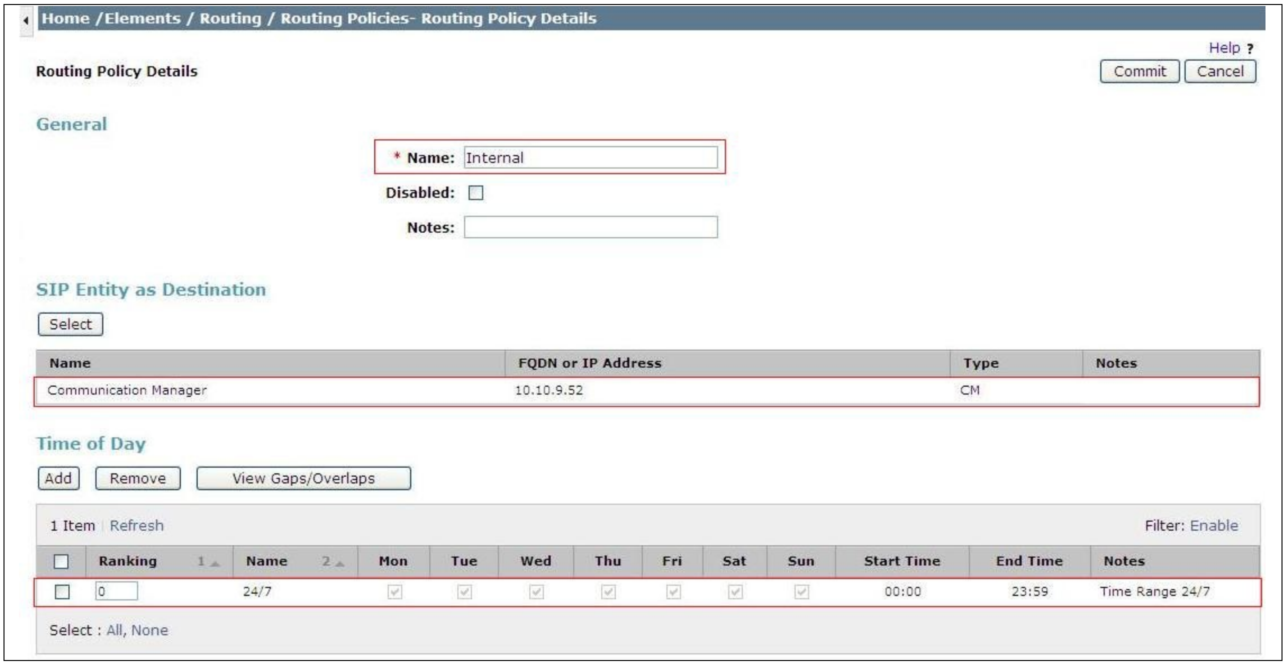
6.6. Administer Routing Policies

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

Under **General**:

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

The following screen shows the routing policy for Communication Manager



Routing Policy Details

General

* Name: Internal

Disabled: □

Notes:

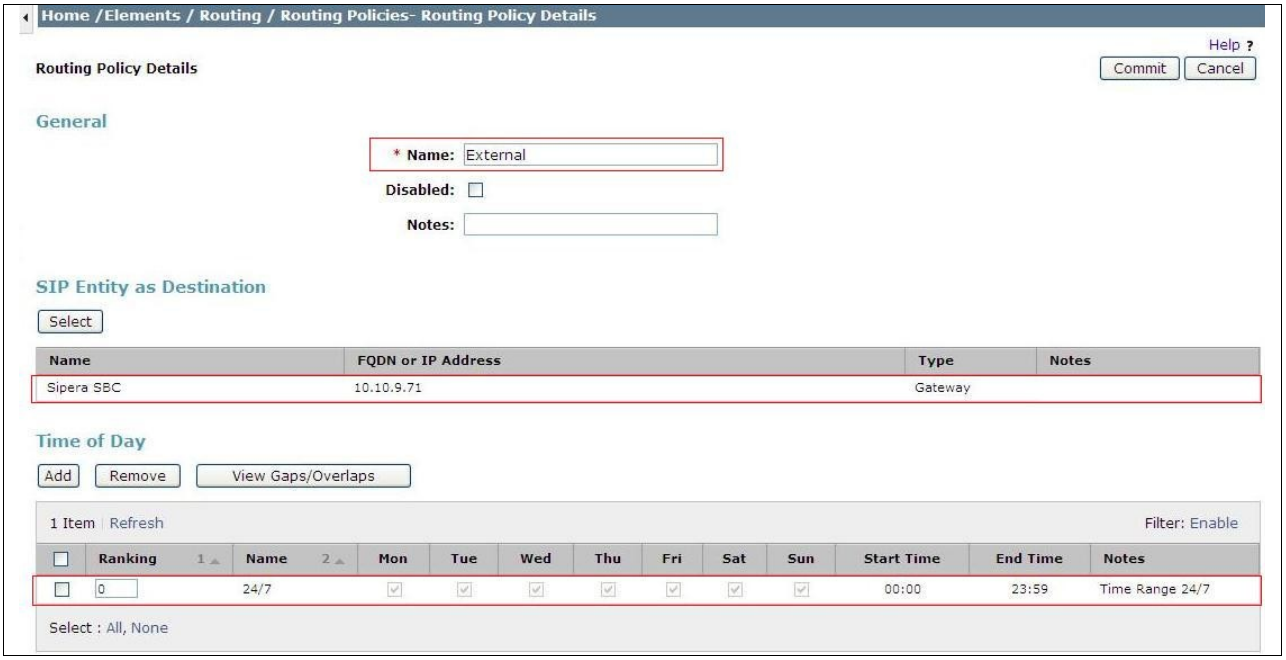
SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Communication Manager	10.10.9.52	CM	

Time of Day

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

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



Home /Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details

General

* Name: External

Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Sipera SBC	10.10.9.71	Gateway	

Time of Day

1 Item | Refresh Filter: Enable

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

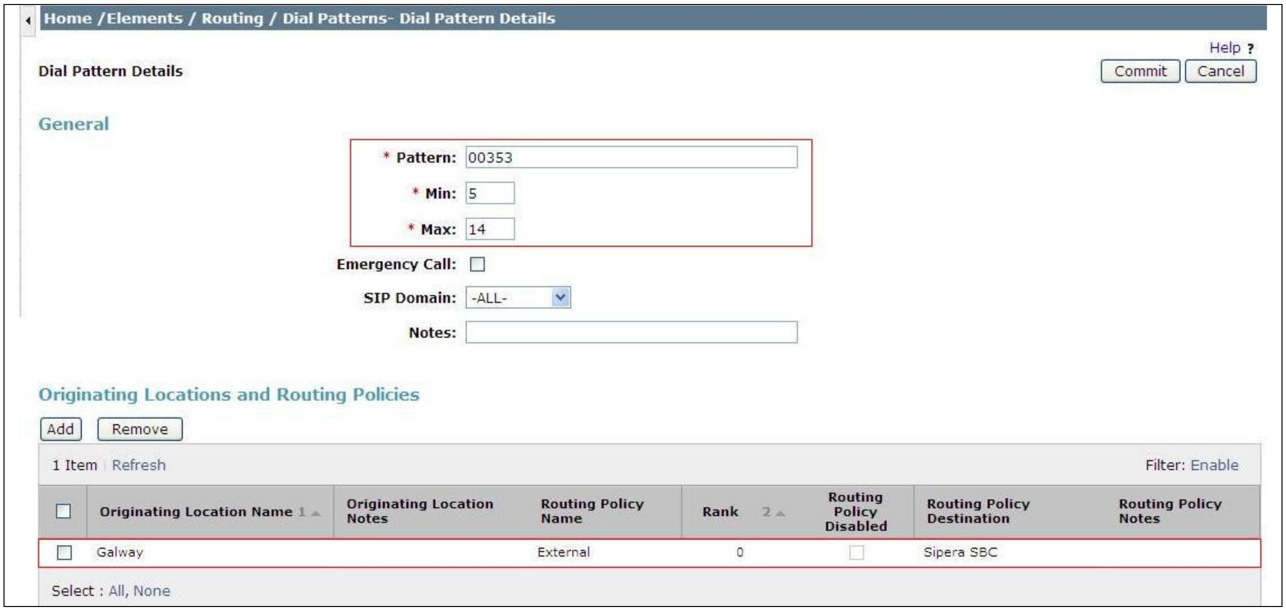
6.7. Administer Dial Patterns

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

Under **General**:

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

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown), under **Originating Location** select **ALL** and under **Routing Policies** select one of the routing policies defined in **Section 6.6**, click **Select** button to save. The following screen shows an example dial pattern configured for the Session Border Controller which will route the calls out to the BT Italia SIP Trunk service.


Home /Elements / Routing / Dial Patterns- Dial Pattern Details
Help ?
Commit
Cancel
Add
Remove
1 Item | Refresh
Filter: Enable

Dial Pattern Details

General

* Pattern: 00353

* Min: 5

* Max: 14

Emergency Call: □

SIP Domain: -ALL-

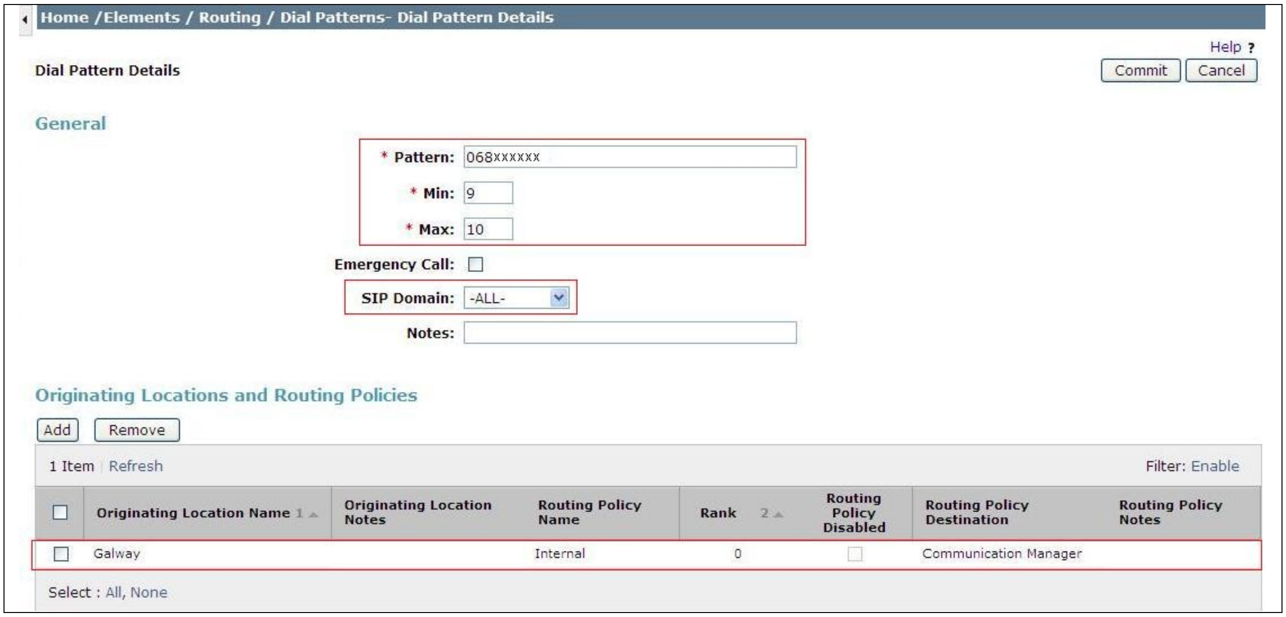
Notes:

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Galway		External	0	□	Sipera SBC	

Select : All, None

The following screen shows the test dial pattern configured for Communication Manager. Note that the last four digits are not shown.



Home /Elements / Routing / Dial Patterns- Dial Pattern Details
Help ?
Commit
Cancel

Dial Pattern Details

General

* Pattern:	068xxxxxx
* Min:	9
* Max:	10
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

1 Item | Refresh   Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Galway		Internal	0	□	Communication Manager	

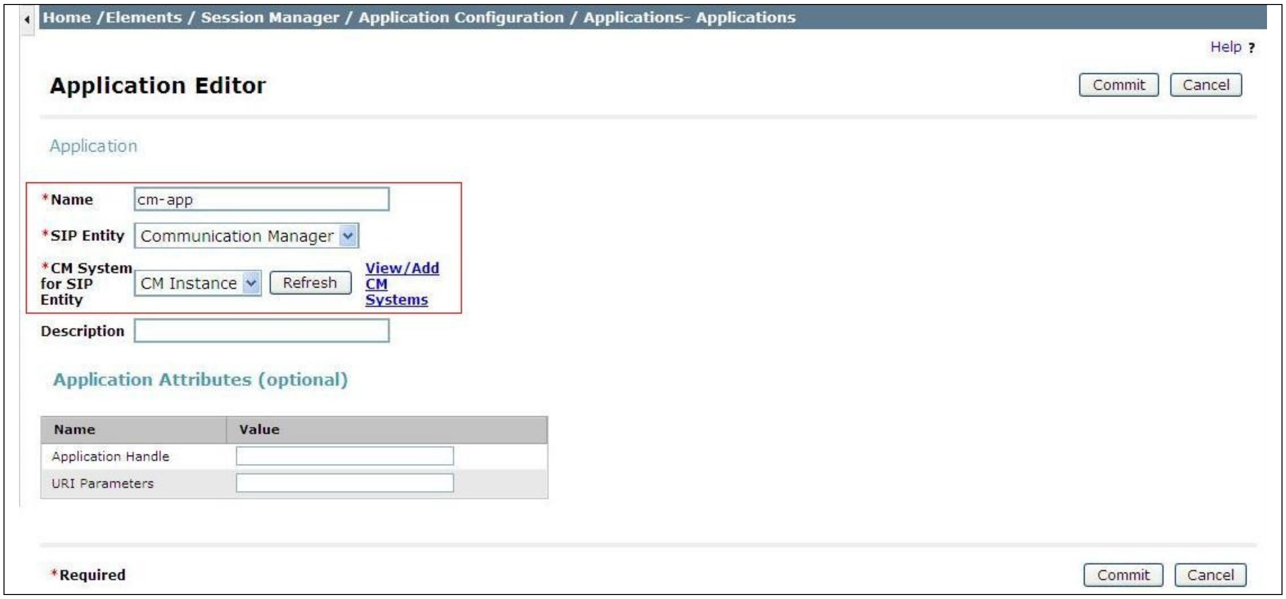
Select : All, None

6.8. Administer Application for Avaya Aura® Communication Manager

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

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

Select **Commit** to save the configuration.


Home /Elements / Session Manager / Application Configuration / Applications- Applications
Help ?
Application Editor
Commit
Cancel
Application

*Name: cm-app

*SIP Entity: Communication Manager

*CM System for SIP Entity: CM Instance

Refresh
View/Add CM Systems
Description
Application Attributes (optional)

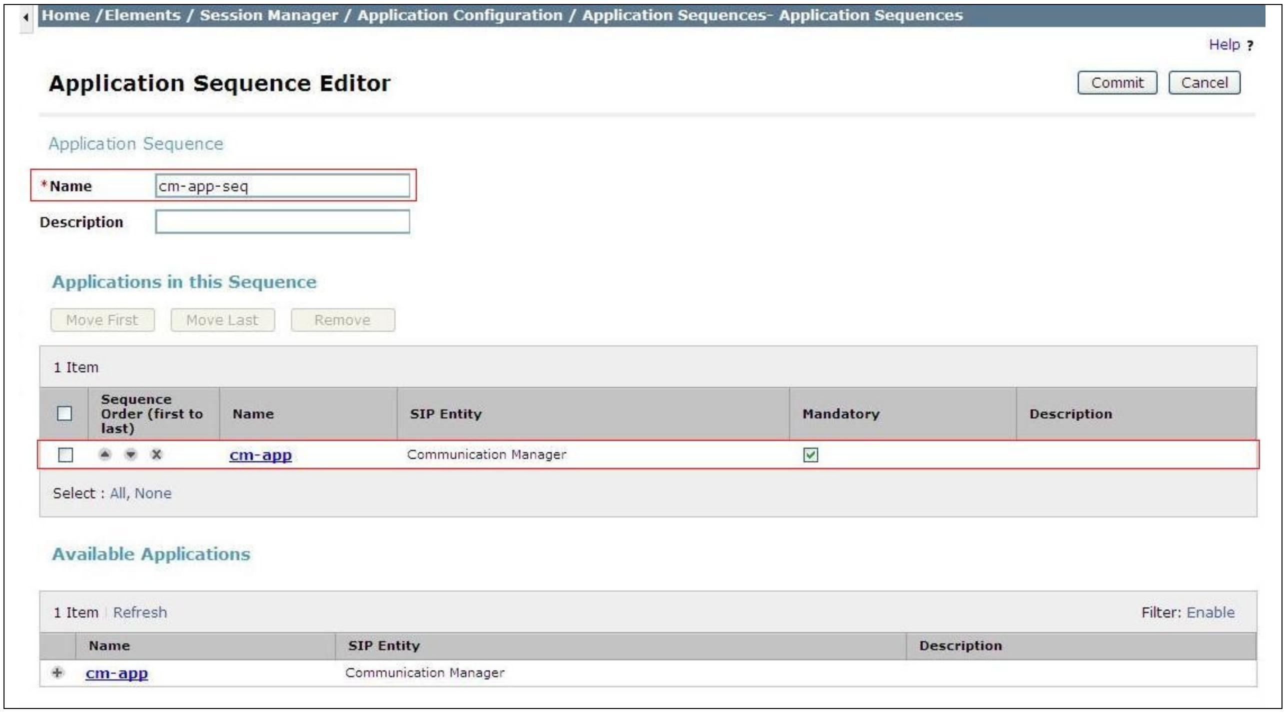
Name	Value
Application Handle	
URI Parameters	

6.9. Administer Application Sequence for Avaya Aura® Communication Manager

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

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

Select **Commit**.


Home /Elements / Session Manager / Application Configuration / Application Sequences- Application Sequences
Help ?
Application Sequence Editor
Commit
Cancel
Application Sequence
Applications in this Sequence
Move First
Move Last
Remove
Available Applications
Filter: Enable

*Name: cm-app-seq

Description:

1 Item

□	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
□	▲ ▼ ✕	cm-app	Communication Manager	☑	

Select : All, None

1 Item | Refresh

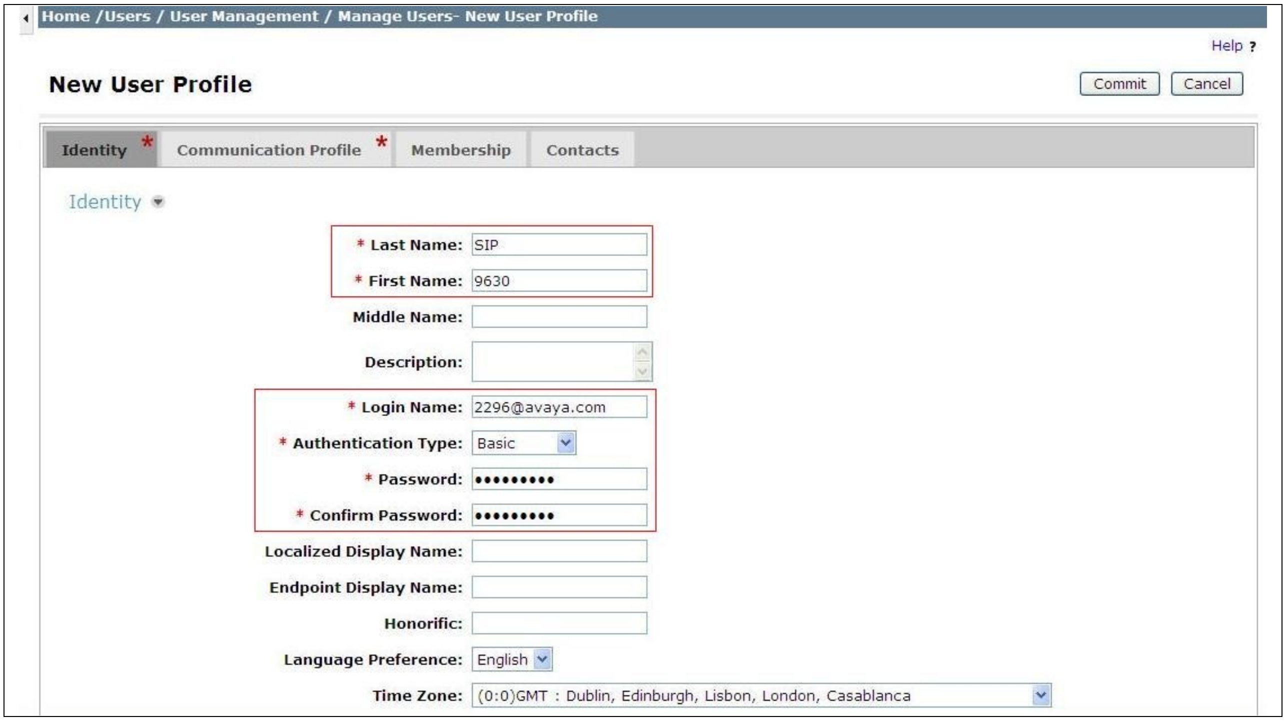
	Name	SIP Entity	Description
+	cm-app	Communication Manager	

6.10. Administer SIP Extensions

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

On the **Identity** tab:

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

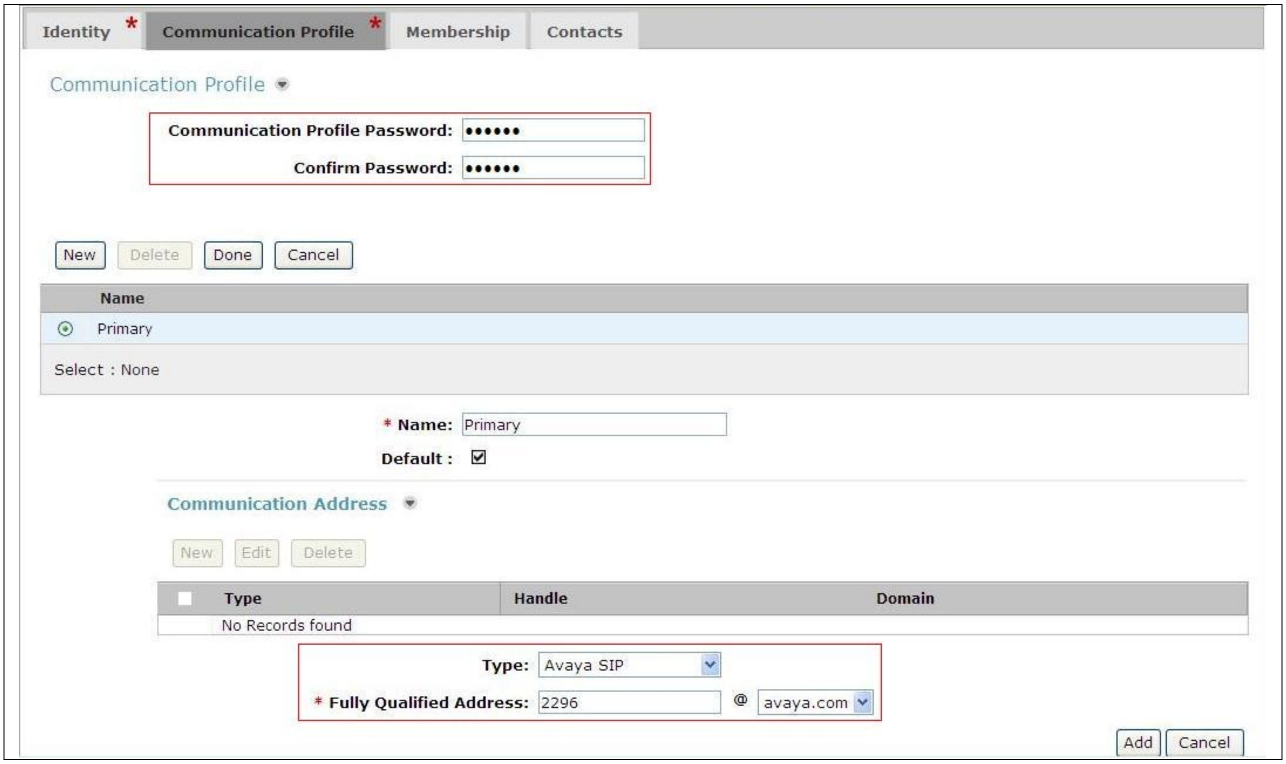


New User Profile

Identity

* Last Name:	SIP
* First Name:	9630
Middle Name:	
Description:	
* Login Name:	2296@avaya.com
* Authentication Type:	Basic
* Password:	•••••••••
* Confirm Password:	•••••••••
Localized Display Name:	
Endpoint Display Name:	
Honorific:	
Language Preference:	English
Time Zone:	(0:0)GMT : Dublin, Edinburgh, Lisbon, London, Casablanca

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



Communication Profile Password: ••••••

Confirm Password: ••••••

Name
● Primary

Select : None

* Name: Primary

Default : ☑

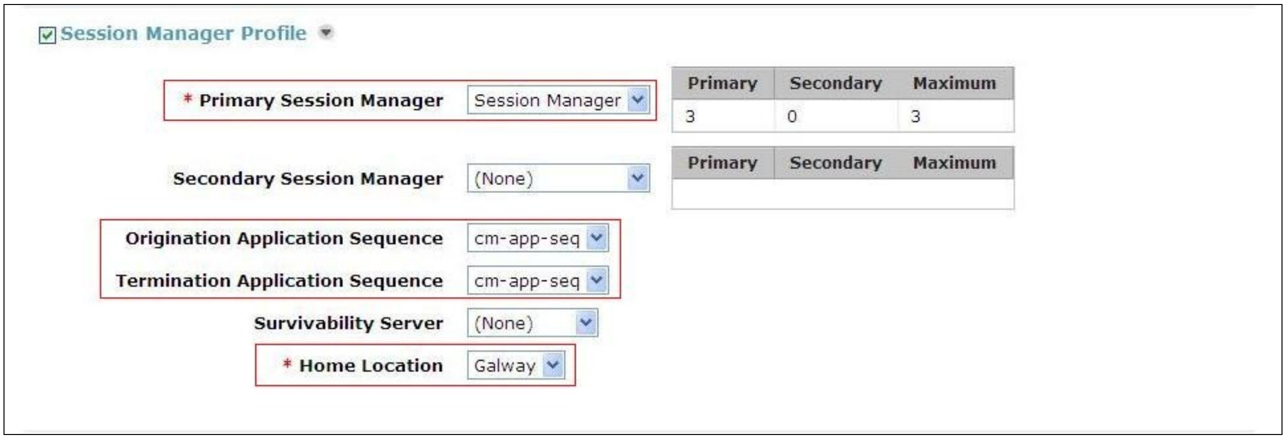
□	Type	Handle	Domain
	No Records found		

Type: Avaya SIP

* Fully Qualified Address: 2296 @ avaya.com

Expand the **Session Manager Profile** section.

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



☑ Session Manager Profile

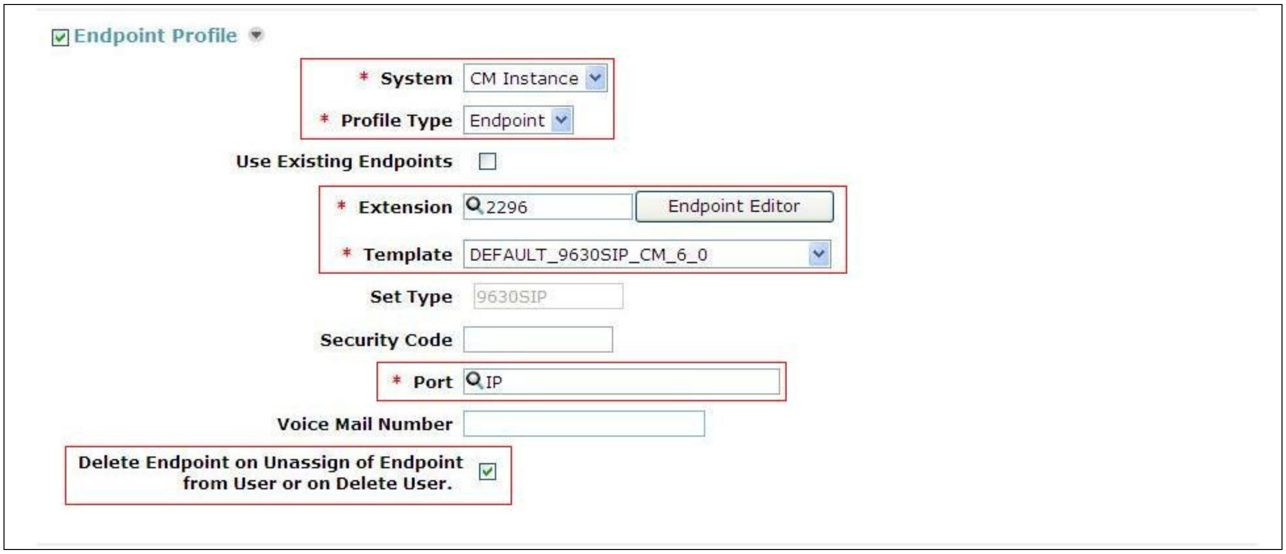
* Primary Session Manager	Session Manager
Secondary Session Manager	(None)
Origination Application Sequence	cm-app-seq
Termination Application Sequence	cm-app-seq
Survivability Server	(None)
* Home Location	Galway

Primary	Secondary	Maximum
3	0	3

Primary	Secondary	Maximum

Expand the **Endpoint Profile** section.

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



☑ Endpoint Profile

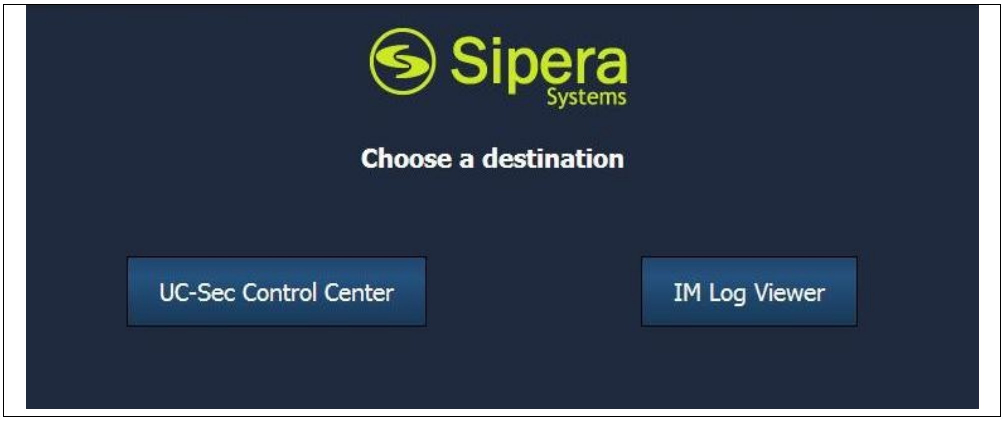
* System	CM Instance
* Profile Type	Endpoint
Use Existing Endpoints	□
* Extension	2296
* Template	DEFAULT_9630SIP_CM_6_0
Set Type	9630SIP
Security Code	
* Port	IP
Voice Mail Number	
Delete Endpoint on Unassign of Endpoint from User or on Delete User.	☑

7. Configure Avaya Session Border Controller Advanced for Enterprise

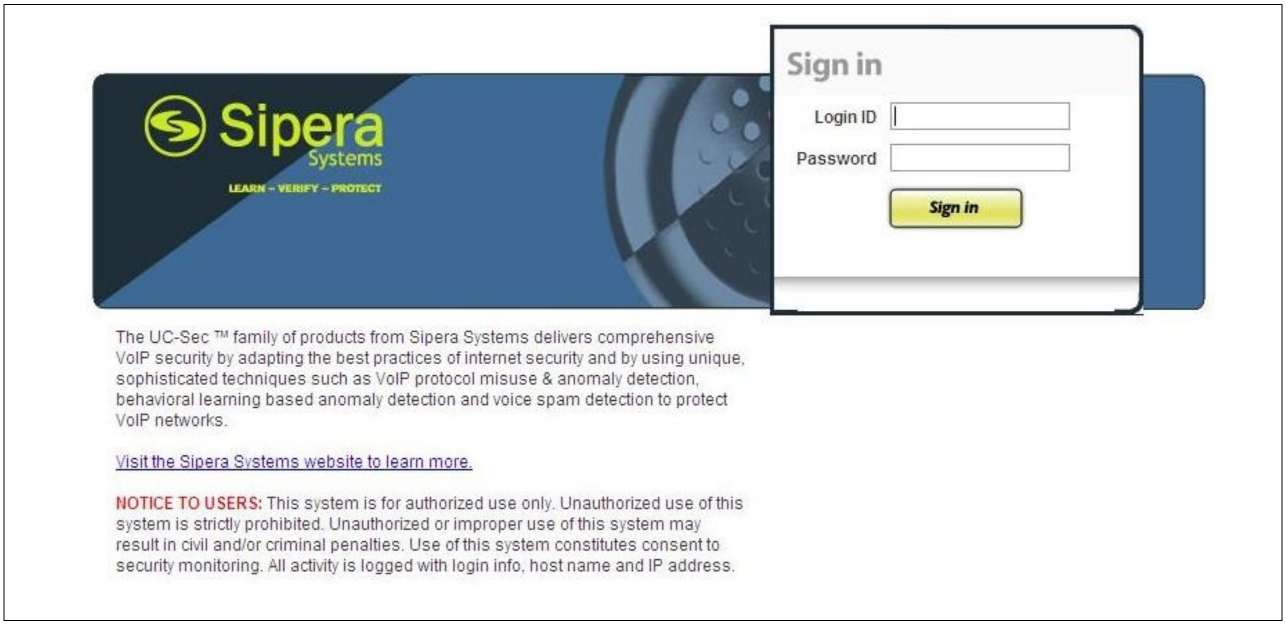
This section describes the configuration of the Session Border Controller. At the time of writing the Avaya Session Border Controller Advanced for Enterprise was badged as the Sipera E-SBC (Enterprise Session Border Controller) developed for Unified Communications Security (UC-Sec). The Avaya Session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

7.1. Access Avaya Session Border Controller Advanced for Enterprise

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



Log in with the appropriate credentials.



The UC-Sec ™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

Visit the Sipera Systems website to learn more.

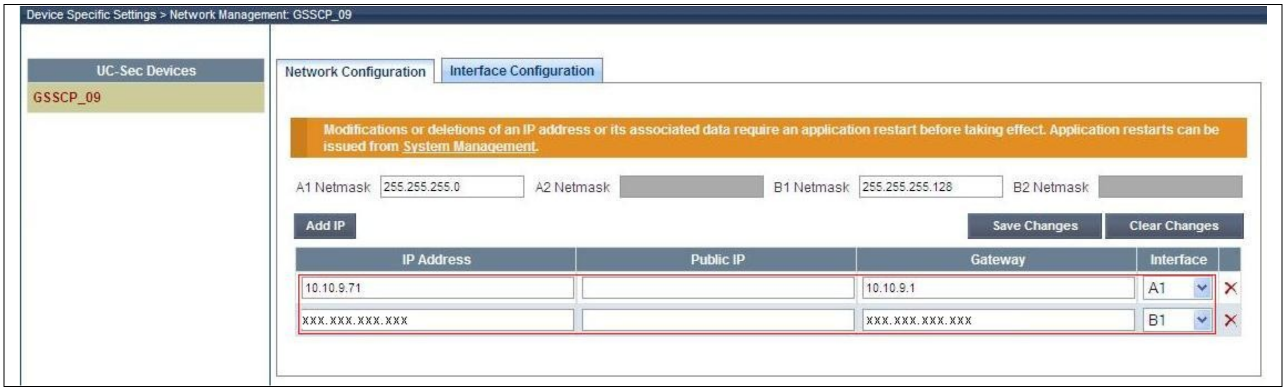
NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

7.2. Define Network Information

Network information is required on the ASBCAE 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 ASBCAE can have only one interface assigned.

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

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



Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask 255.255.255.0 A2 Netmask B1 Netmask 255.255.255.128 B2 Netmask

IP Address	Public IP	Gateway	Interface
10.10.9.71		10.10.9.1	A1
xxx.xxx.xxx.xxx		xxx.xxx.xxx.xxx	B1

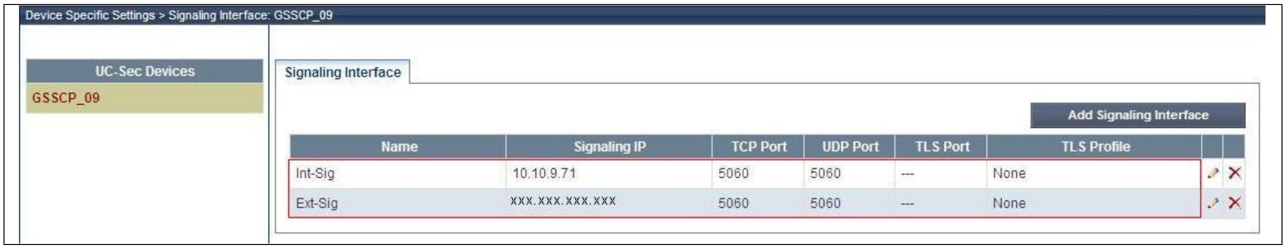
7.3. Define Interfaces

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

7.3.1. Signalling Interfaces

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

- Select **Add Signalling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal signalling interface
- Select an **internal** interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is used for BT Italia
- Select **Add Signalling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external signalling interface
- Select an **external** interface IP address (not shown) defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is used for BT Italia

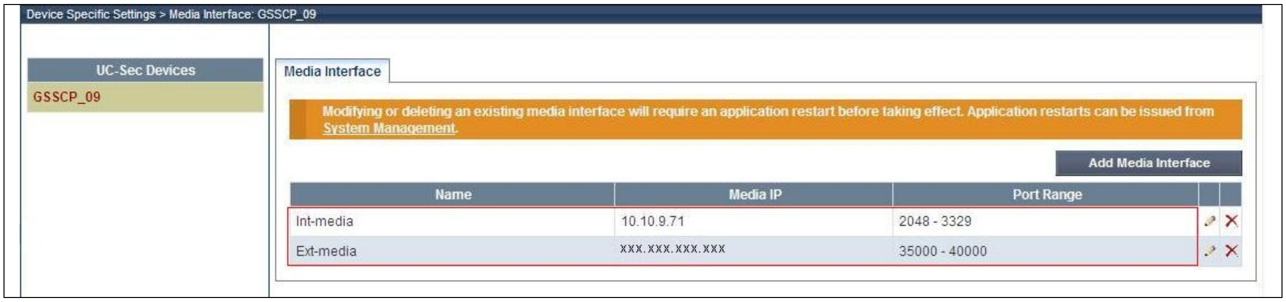


Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
Int-Sig	10.10.9.71	5060	5060	---	None
Ext-Sig	xxx.xxx.xxx.xxx	5060	5060	---	None

7.3.2. Media Interfaces

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

- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface
- Select an **internal** interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external media interface
- Select an **external** interface IP address (not shown) defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the BT Italia SBC



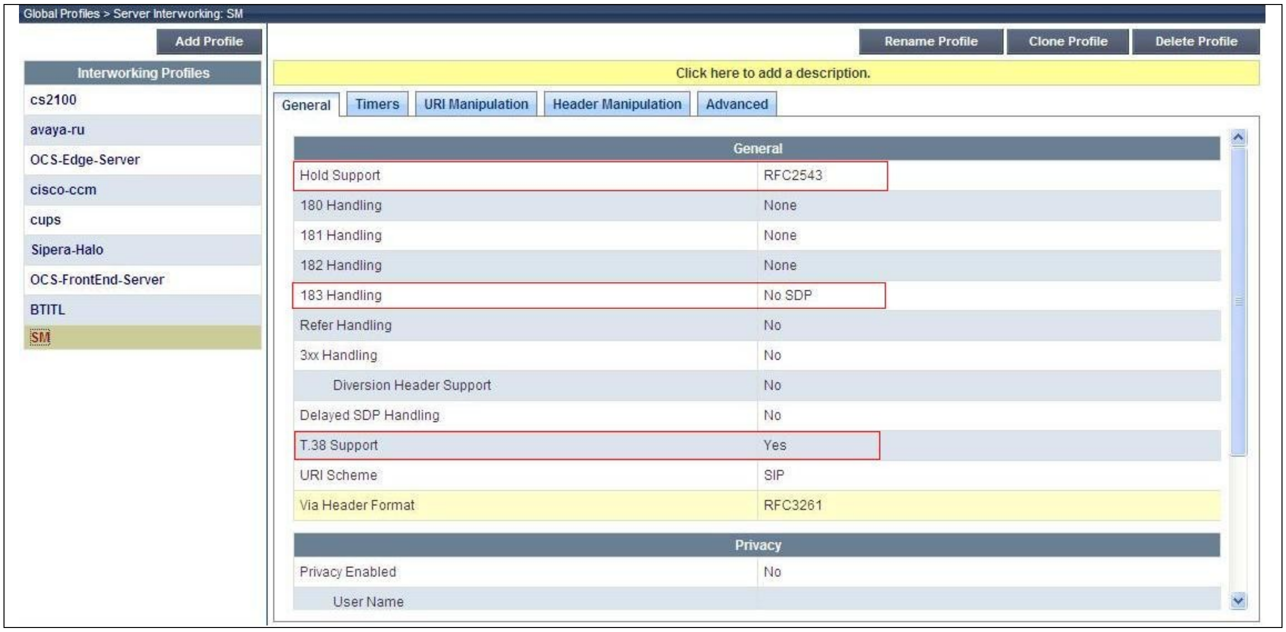
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Media IP	Port Range
Int-media	10.10.9.71	2048 - 3329
Ext-media	xxx.xxx.xxx.xxx	35000 - 40000

7.4. Define Server Interworking

Server interworking is defined for each server connected to the ASBCAE. In this case, the BT Italia SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define server interworking on the ASBCAE, navigate to **Global Profiles → Server interworking** in the **UC-Sec Control Center** menu on the left hand side. To define Server Interworking for the Session Manager, highlight the **avaya-ru** profile which is a factory setting appropriate for Avaya equipment and select **Clone Profile**. A pop-up menu is generated headed "**Clone Profile**"

- In the **Clone Name** field enter a descriptive name for the Session Manager and click **Finish**
- Select **Edit** and enter details in the pop-up menu.
- Check the **T.38** box
- Check the **No SDP** box in the **183 Handling** field
- Change the **Hold Support** RFC to **RFC2543** then click **Next** and **Finish**



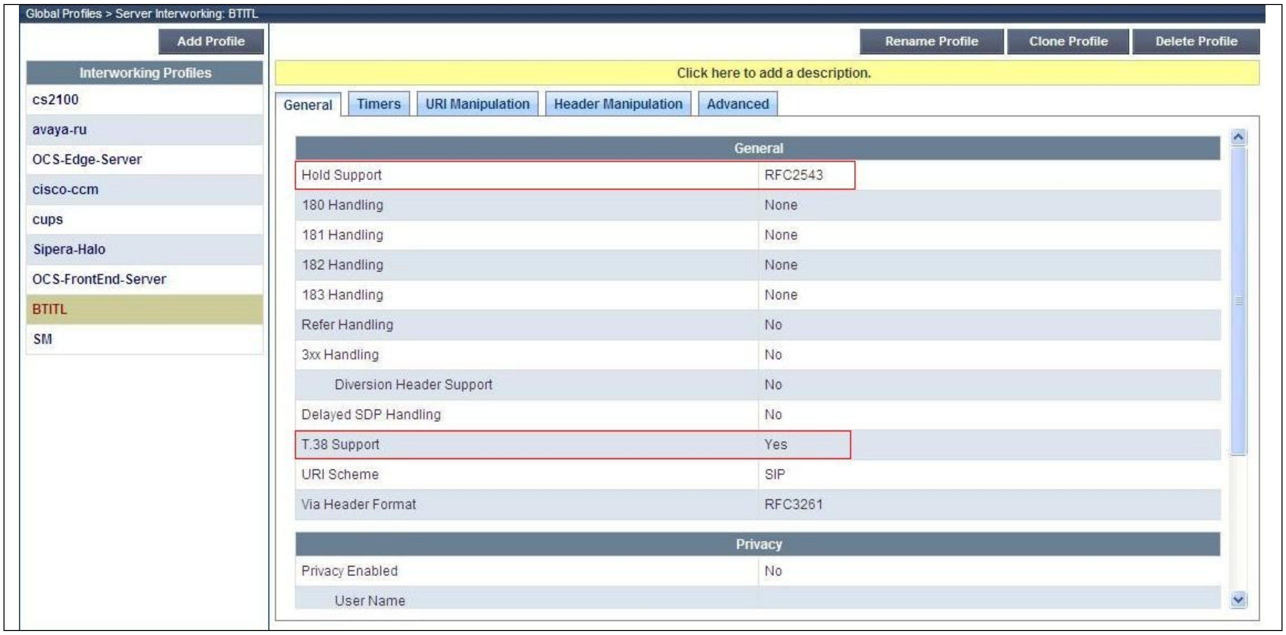
General	
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	No SDP
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No
User Name	

Note: Selection of **No SDP** for **183 Handling** results in removal of the SDP from the 183 Session Progress received from BT Italia as it is transmitted to the Session Manager. This resolves a problem where the Communication Manager was not sending a 180 Ringing on leg 1 of a forwarded or EC500 call despite having received a 180 Ringing in leg 2. The lack of the 180 Ringing on leg 1 meant the caller did not hear ring tone.

When the SDP was removed from the 183 Session Progress, the Communication Manager sent the 180 ringing to leg 1 at the appropriate time and ring tone was heard by the caller.

To define Server Interworking for the BT Italia SBC, highlight the previously defined profile for the Session Manager and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile**

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



General	
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No
User Name	

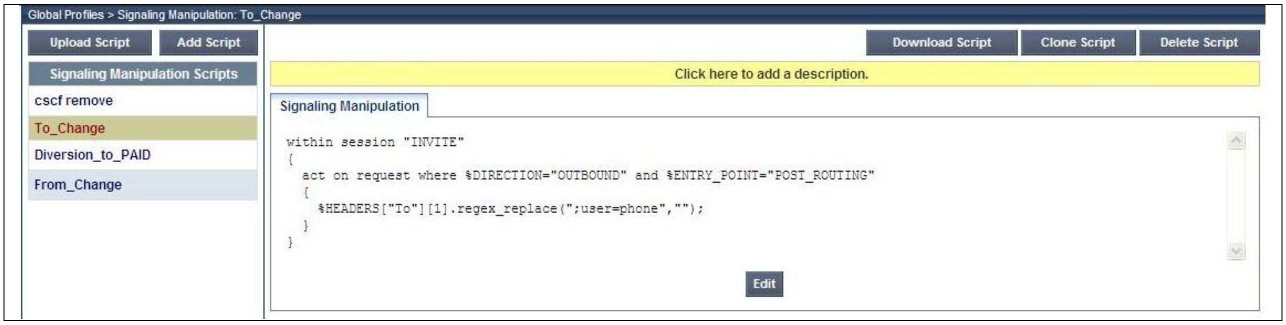
7.5. Define Signalling Manipulation

Signalling manipulation is required in some cases to ensure effective interworking. During test, some issues were found in the interworking between the BT Italia SIP Trunking service and the enterprise. Two of these issues could not be resolved by other methods such as **Server Interworking** and **Signaling Rules.** The first issue is that the SIP ACK message sent in response to the 200 OK when the call was answered was not handled correctly by the Session Manager when additional information was present in the To header. The second issue is that call forwarding to a PSTN number and EC500 could only be routed correctly when the CLI of the forwarding number was present in the P-Asserted-ID and From headers.

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

```
within session "INVITE"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["To"][1].regex_replace(";user=phone","");
  }
}
```

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

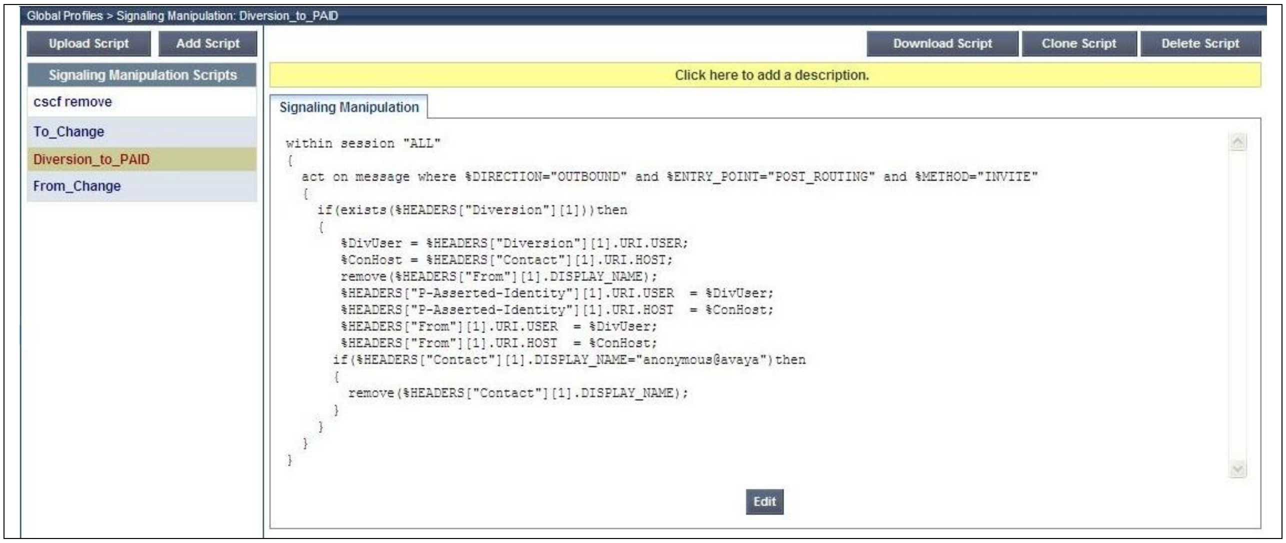


```
within session "INVITE"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["To"][1].regex_replace(";user=phone","");
  }
}
```

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

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

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



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

Note: This script has additional functions to simply taking the forwarding number from the Diversion header and inserting it into the P-Asserted-ID and From headers. It takes the forwarding number from the user portion, and in addition it takes the host portion from the Contact header. It also removes the display name from the Contact header if it is "anonymous" as this was found to cause problems.

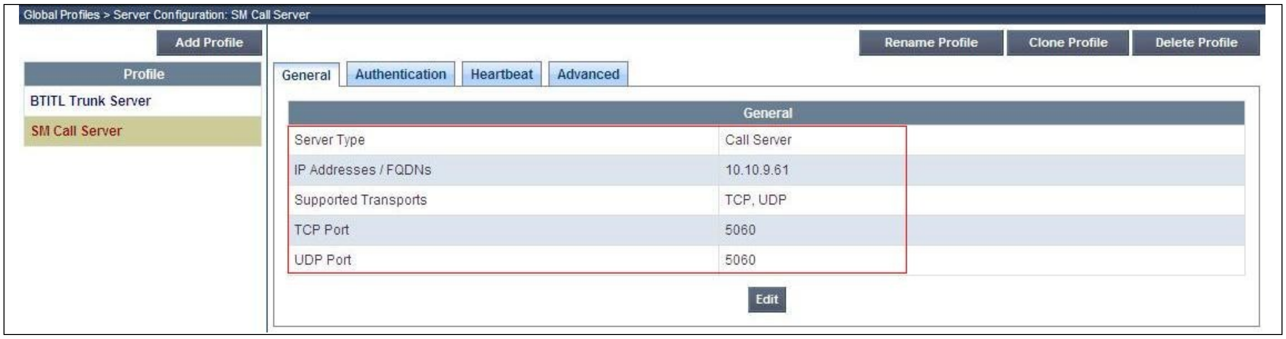
Note also that this script relies on the existence of the Diversion header. This is included for the forwarded and EC 500 calls by configuration of the Communication Manager as described in **Section 5.6**

7.6. Define Servers

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

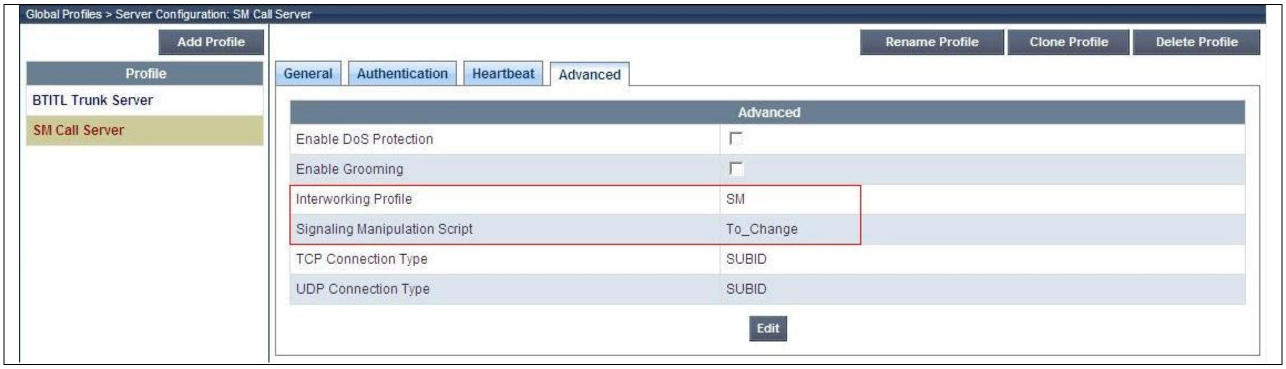
- In the **Profile Name** field enter a descriptive name for the Communication Manager and click **Next**
- In the **Server Type** drop down menu, select **Call Server**
- In the **IP Addresses / Supported FQDNs** box, type the Session Manager SIP interface address which is the same as that defined on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

The **General** tab on the resultant screen shows the **IP addresses**, **TCP Port** and **UDP Port** entered.



General	
Server Type	Call Server
IP Addresses / FQDNs	10.10.9.61
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060

The **Advanced** tab on the resultant screen shows the **Interworking Profile** for the call server defined in **Section 7.4.**

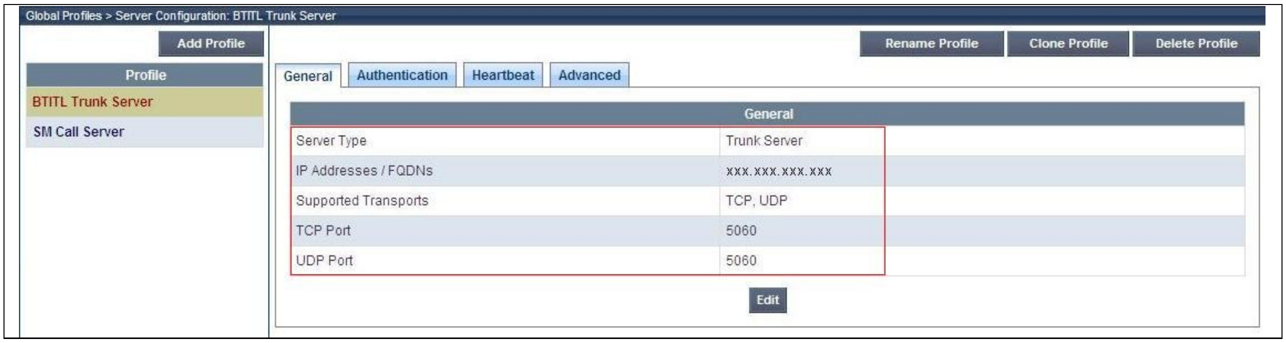


Advanced	
Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	SM
Signaling Manipulation Script	To_Change
TCP Connection Type	SUBID
UDP Connection Type	SUBID

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

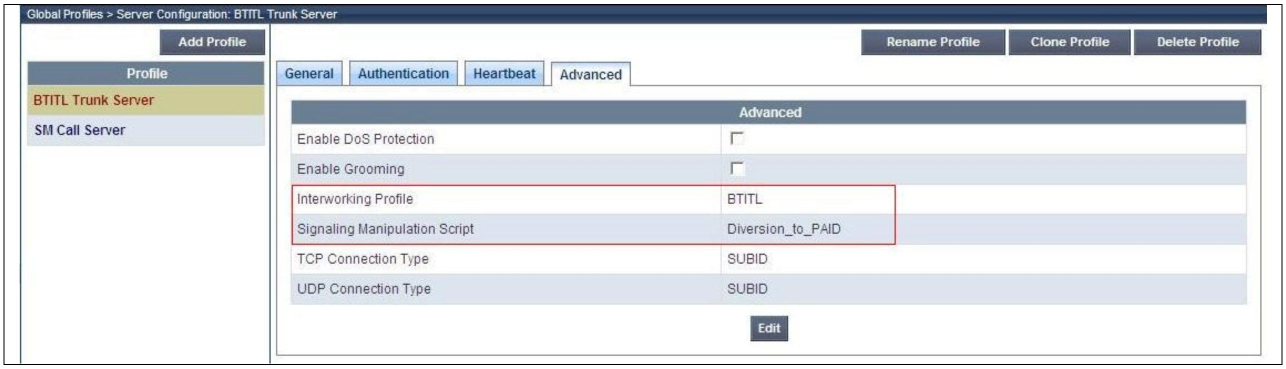
- In the **Profile Name** field enter a descriptive name for the BT Italia SBC and click Next
- In the **Server Type** drop down menu, select **Trunk Server**
- In the **IP Addresses / Supported FQDNs** box, type the IP address of the BT Italia SBC (not shown)
- Check **TCP** and **UDP** in **Supported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

The **General** tab on the resultant screen shows the **IP addresses**, **TCP Port** and **UDP Port** entered.



General	
Server Type	Trunk Server
IP Addresses / FQDNs	xxx.xxx.xxx.xxx
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060

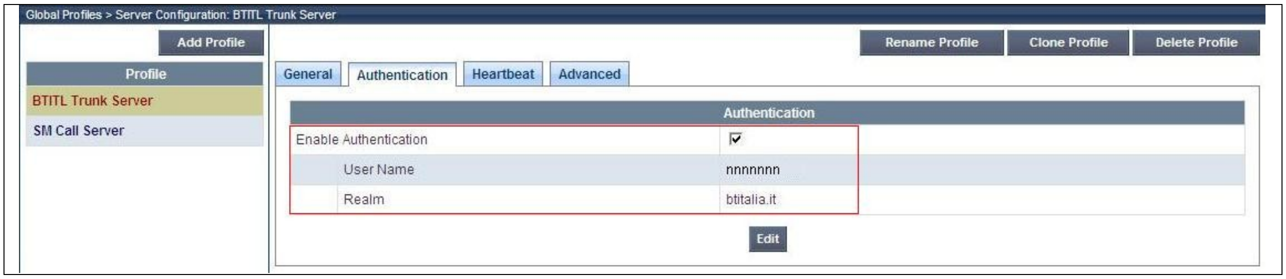
The **Advanced** tab on the resultant screen shows the **Interworking Profile** for the trunk server defined in **Section 7.4.**



Advanced	
Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	BTITL
Signaling Manipulation Script	Diversion_to_PAID
TCP Connection Type	SUBID
UDP Connection Type	SUBID

If authentication is required to BT Italia, it is configured in the server settings. To define authentication, select on the **Authentication** tab in the BT Italia Trunk Server profile and click on **Edit**

- Check the **Enable Authentication** box
- Enter the user name in the **User Name** field (not shown)
- Enter the realm in the **Realm** field, in test this was the domain name of BT Italia
- Enter the password in the **Password** field
- Enter the password again in the **Confirm Password** field
- Click **Finish**



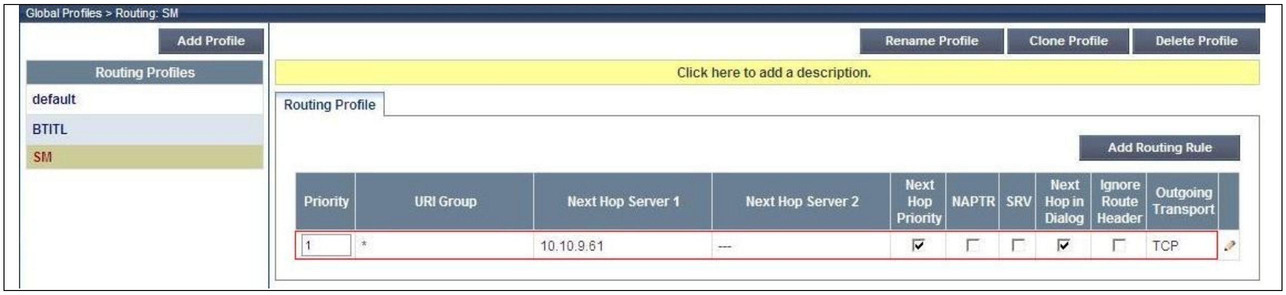
Authentication	
Enable Authentication	☑
User Name	nnnnnnn
Realm	btitalia.it

7.7. Define Routing

Routing information is required for routing to the Session Manager on the internal side and the BT Italia SBC on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used. To define routing to the Communication Manager, navigate to **Global Profiles → Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu.

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

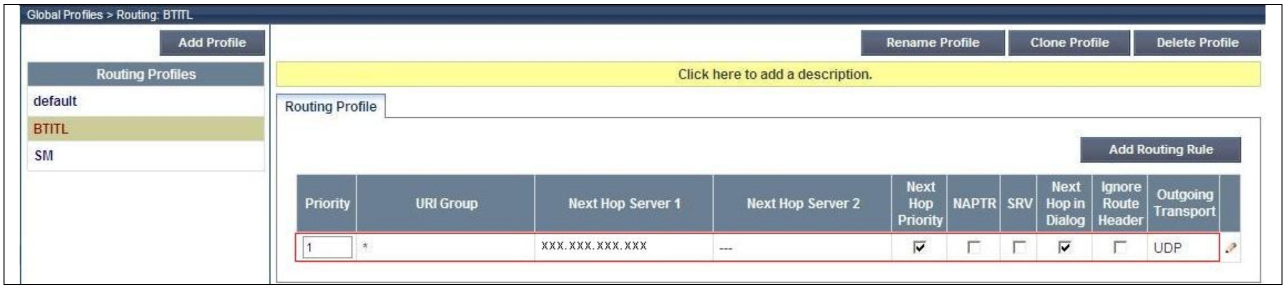
Note: Unless default port 5060 is used, this must be included in the next hop IP address.



Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.10.9.61	---	☑	□	□	☑	□	TCP

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

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



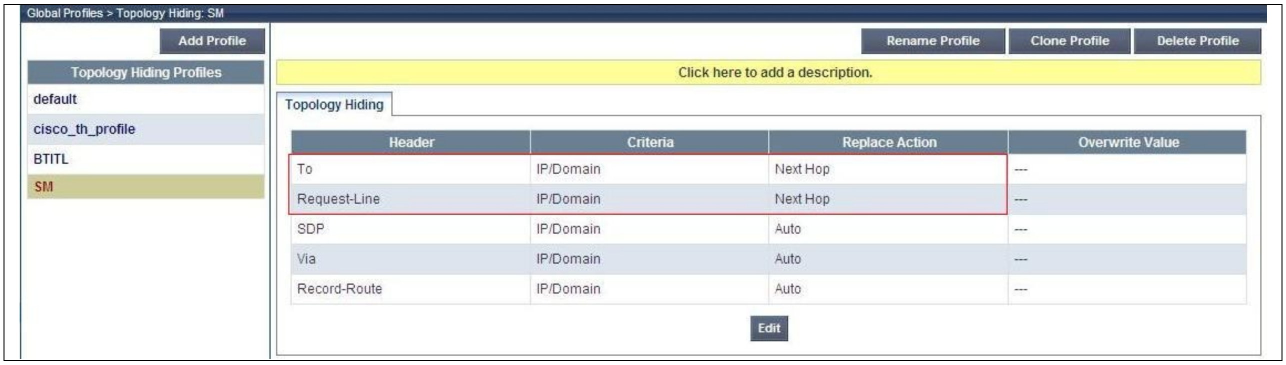
Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	xxx.xxx.xxx.xxx	---	☑	□	□	☑	□	UDP

7.8. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten or next hop IP addresses can be used. To define Topology Hiding for the Communication Manager, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **To** as the required header from the **Header** drop down menu
- Select the required action from the **Required Action** drop down menu, **Next Hop** was used for test
- Repeat for the **Request-Line** header

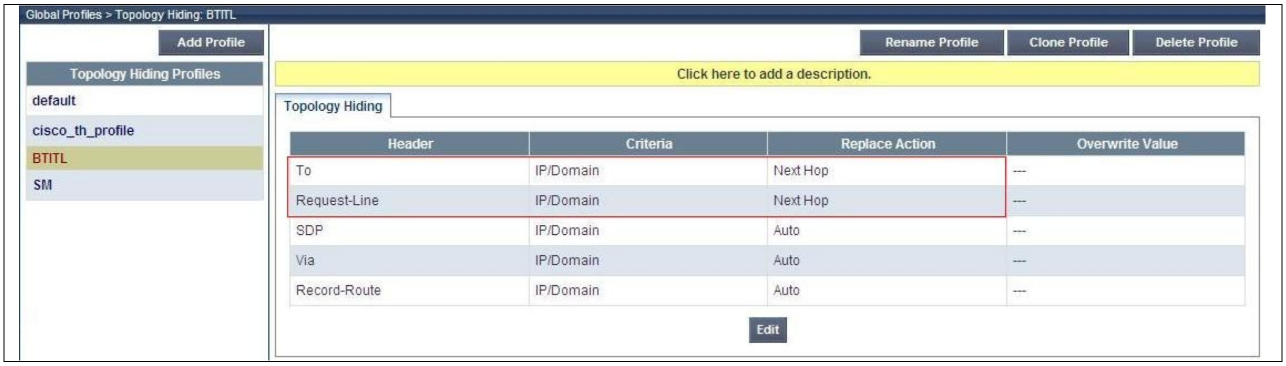
Note: The use of **Next Hop** results in the IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used for the **From**, **To** and **Request-Line** headers with the required domain names entered in the **Overwrite Value** field. Different domain names could be used for the enterprise and the BT Italia network.



Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Next Hop	---
Request-Line	IP/Domain	Next Hop	---
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

To define Topology Hiding for the BT Italia SBC, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the BT Italia SBC and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **To** as the required header from the **Header** drop down menu
- Select the required action from the **Required Action** drop down menu, **Next Hop** was used for test
- Repeat for the **Request-Line** header



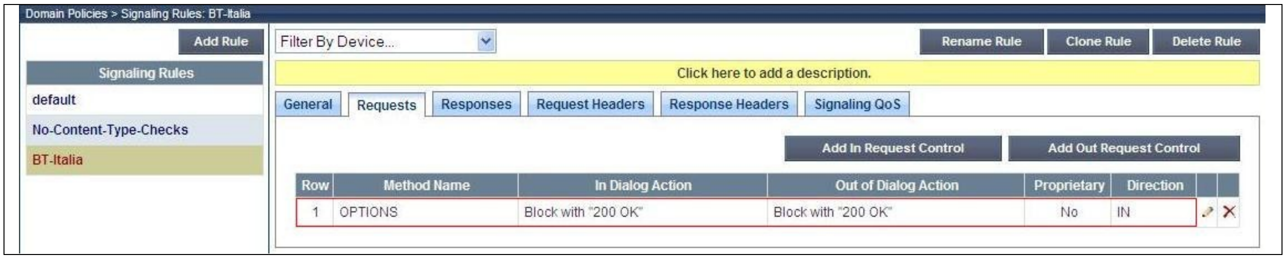
Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Next Hop	---
Request-Line	IP/Domain	Next Hop	---
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

7.9. Signalling Rules

Signalling rules are a mechanism on the Avaya Session Border Controller Advanced for Enterprise to handle any unusual signalling scenarios that may be encountered for a particular Service Provider. In the case of BT Italia, as mentioned in Section 2.2 the network is sending OPTIONS messages with a Max Forward value of 0 which must be responded to directly. The normal behavior of the Avaya Session Border Controller for Enterprise is to pass OPTIONS received from the Trunk Server on to the Call Server.

A signalling rule must be defined for BT Italia to respond directly to OPTIONS from the network with a 200 "OK". To define the signalling rule, navigate to **Domain Policies → Signalling Rules** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Rule** and enter details in the **Signaling Rule** pop-up box.

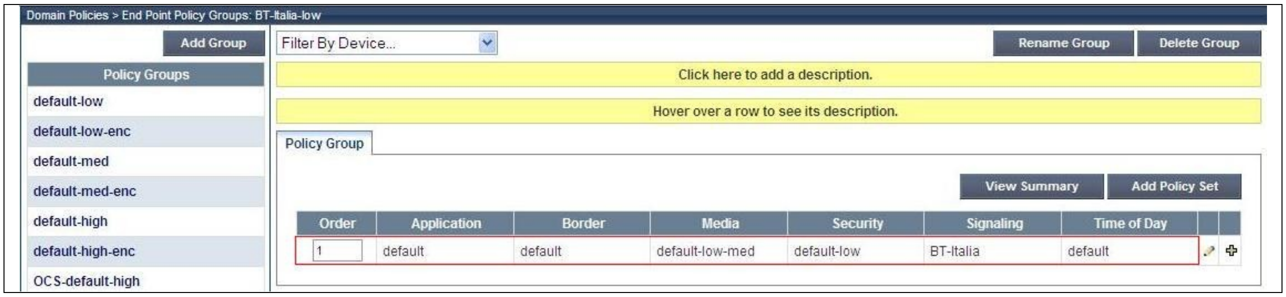
- In the **Rule Name** field enter a descriptive name for the BT Italia signalling rule and click **Next** and **Next** again, then **Finish**
- Click on the **Requests** tab
- Click on the **Add in Request Control**
- Select **OPTIONS** from the **Method Name** drop down menu
- Select **Block** in the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



Row	Method Name	In Dialog Action	Out of Dialog Action	Proprietary	Direction
1	OPTIONS	Block with "200 OK"	Block with "200 OK"	No	IN

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

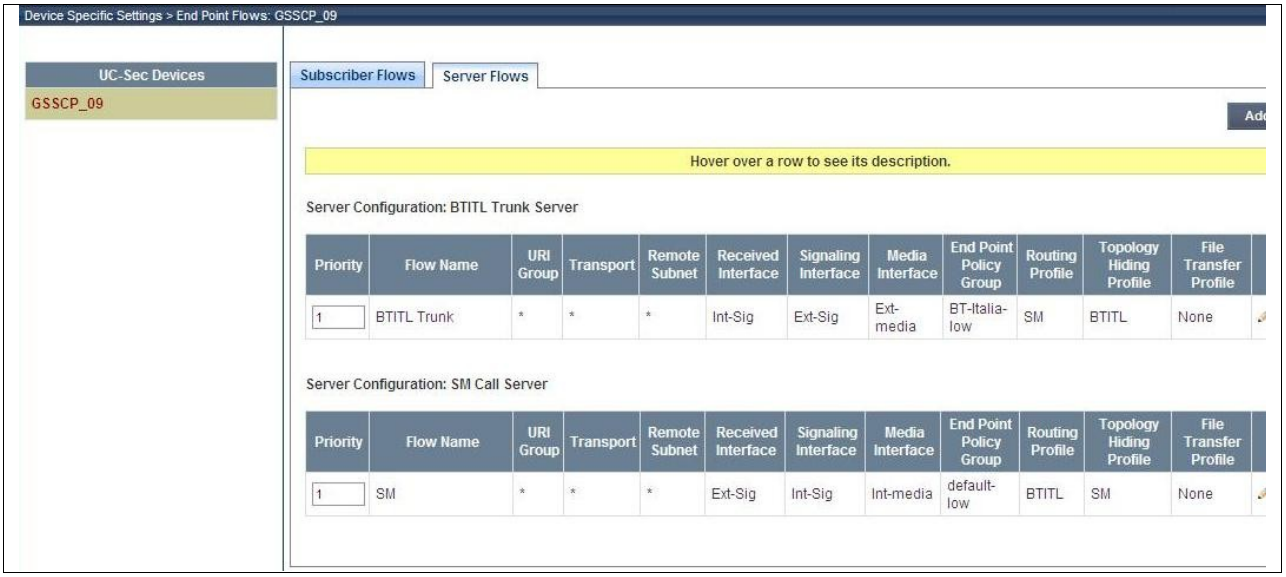
- In the **Group Name** field enter a descriptive name for the BT Italia Policy Group and click **Next**
- In the **Application** drop down menu, select **default**
- In the **Border** drop down menu, select **default**
- In the **Media** drop down menu, select **default-low-med**
- In the **Security** drop down menu, select **default-low**
- In the **Signaling** drop down menu, select the recently added signalling rule for BT Italia (**BT-Italia**)
- In the **Time of Day** drop down menu, select **default**



Order	Application	Border	Media	Security	Signaling	Time of Day
1	default	default	default-low-med	default-low	BT-Italia	default

7.10. Server Flows

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


Device Specific Settings > End Point Flows: GSSCP_09
UC-Sec Devices
GSSCP_09
Subscriber Flows
Server Flows
Ad
Hover over a row to see its description.

Server Configuration: BTITL Trunk Server

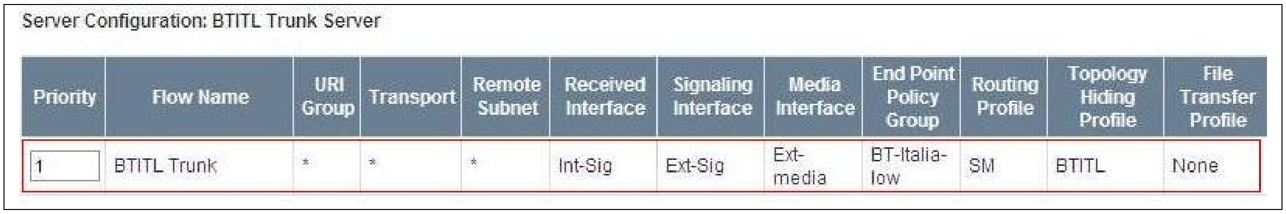
Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile
1	BTITL Trunk	*	*	*	Int-Sig	Ext-Sig	Ext-media	BT-Italia-low	SM	BTITL	None

Server Configuration: SM Call Server

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile
1	SM	*	*	*	Ext-Sig	Int-Sig	Int-media	default-low	BTITL	SM	None

To define an outgoing Server Flow, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the outgoing server flow to the BT Italia SBC
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**
- In the **Signalling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**
- In the **End Point Policy Group** drop-down menu, select the End Point Policy Group for BT Italia defined in **Section 7.9**
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.7**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the BT Italia SBC defined in **Section 7.8** and click **Finish**

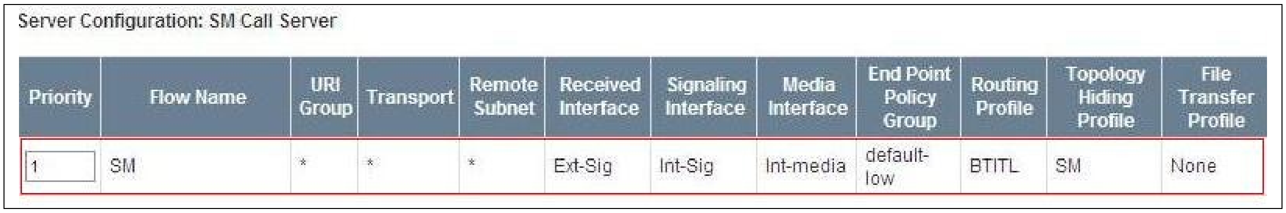


Server Configuration: BTITL Trunk Server

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile
1	BTITL Trunk	*	*	*	Int-Sig	Ext-Sig	Ext-media	BT-Italia-low	SM	BTITL	None

An incoming Server Flow is defined as a reversal of the outgoing Server Flow

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the incoming server flow to the Session Manager
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**
- In the **Signalling Interface** drop-down menu, select the internal SIP signalling defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**
- In the **Routing Profile** drop-down menu, select the routing profile of the BT Italia SBC defined in **Section 7.7**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.8** and click **Finish**



Server Configuration: SM Call Server

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile
1	SM	*	*	*	Ext-Sig	Int-Sig	Int-media	default-low	BTITL	SM	None

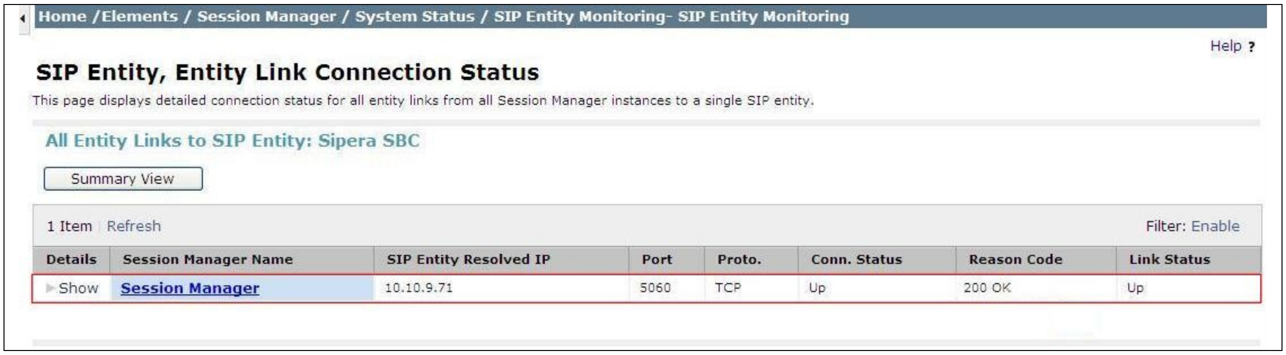
8. Service Provider Configuration

The configuration of the BT Italia equipment used to support the BT Italia SIP Trunking service is outside of the scope of these Application Notes and will not be covered. To obtain further information on BT Italia equipment and system configuration please contact an authorised BT Italia representative.

9. Verification Steps

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

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



Home /Elements / Session Manager / System Status / SIP Entity Monitoring- SIP Entity Monitoring
Help ?

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: Sipera SBC

Summary View
1 Item | Refresh
Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶Show	Session Manager	10.10.9.71	5060	TCP	Up	200 OK	Up

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

```
status trunk 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
0002/007 T00017   in-service/idle    no
0002/008 T00018   in-service/idle    no
0002/009 T00019   in-service/idle    no
0002/010 T00020   in-service/idle    no
```

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller Advanced for Enterprise to BT Italia SIP Trunking Service. The service was successfully tested with a number of observations listed in **Section 2.2**. In a number of cases, configuration of the Avaya Session Border Controller Advanced for Enterprise is required to ensure effective interworking between the enterprise equipment and the network.

11. References

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

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.0.3, February 2011.

[2] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.

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

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

[5] *Installing and Upgrading Avaya Aura® System Manager* Release 6.1, November 2010.

[6] *Installing and Configuring Avaya Aura® Session Manager*, April 2011, Document Number 03-603473

[7] *Administering Avaya Aura® Session Manager*, October 2011, Document Number 03-603324.

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

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

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.