Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager 6.0.1 as an Evolution Server, Avaya Aura® Session Manager 6.1 and Avaya Aura® Session Border Controller to support British Telecom SIP Trunk Service 2.1.0.8 - Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the British Telecom SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Border Controller, Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. British Telecom is a member of the DevConnect Service Provider program.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between British Telecom (BT) SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Border Controller (AASBC), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with BT 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.

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 AASBC. The enterprise site was configured to use the SIP Trunk Service provided by BT.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by BT. Incoming PSTN calls terminated on SIP, H.323 and Digital telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via BT to PSTN destinations.
- Outgoing calls from the enterprise to the PSTN were made from SIP, H.323 and Digital telephones.
- Calls to Emergency Services numbers such as 999 and 112 were made from the enterprise site via the SIP Trunk to BT.
- Calls were made using G.729, and G.711A codecs.
- Fax calls to/from a Group 3 fax machine to a PSTN connected fax machine using the T.38 mode.
- 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 requiring Avaya response and sent by Avaya requiring BT response.

2.2. Test Results

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

- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- G.729 annex b (silence suppression) is not supported by BT SIP Trunk Service and thus was not tested.
- G.711mu is not supported by BT SIP Trunk Service and thus was not tested.
- One-X Communicator was not tested using Telecommuter mode. All one-X Communicator test cases were completed using Road warrior mode.
- For fax calls to be successful a t requested a Min-SE value of 1800 to be set on the Communication Manager (1800 is doubled to make 3600). For incoming calls BT is attempting to use a lower value causing a negotiation of the Min-SE to occur. This increases the number of SIP messages during an inbound call setup.
- It is observed that T.38 Fax calls set up using G.729 were not consistently successful. Thus it is recommended that Fax calls are set up using G.711a.

2.3. Support

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

For technical support on BT products please contact an authorized BT representative.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the BT SIP Trunk Service. Located at the enterprise site is an AASBC, Session Manager and Communication Manager. Endpoints are Avaya 96xx series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya Digital telephones and an analogue fax machine. Also included in the test configuration was an Avaya Desktop Video Device incorporating the Avaya Flare experience. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes. Instead, public IP addresses have been replaced with private addresses and all phone numbers have been replaced with arbitrary numbers that bear no relevance to the test configuration

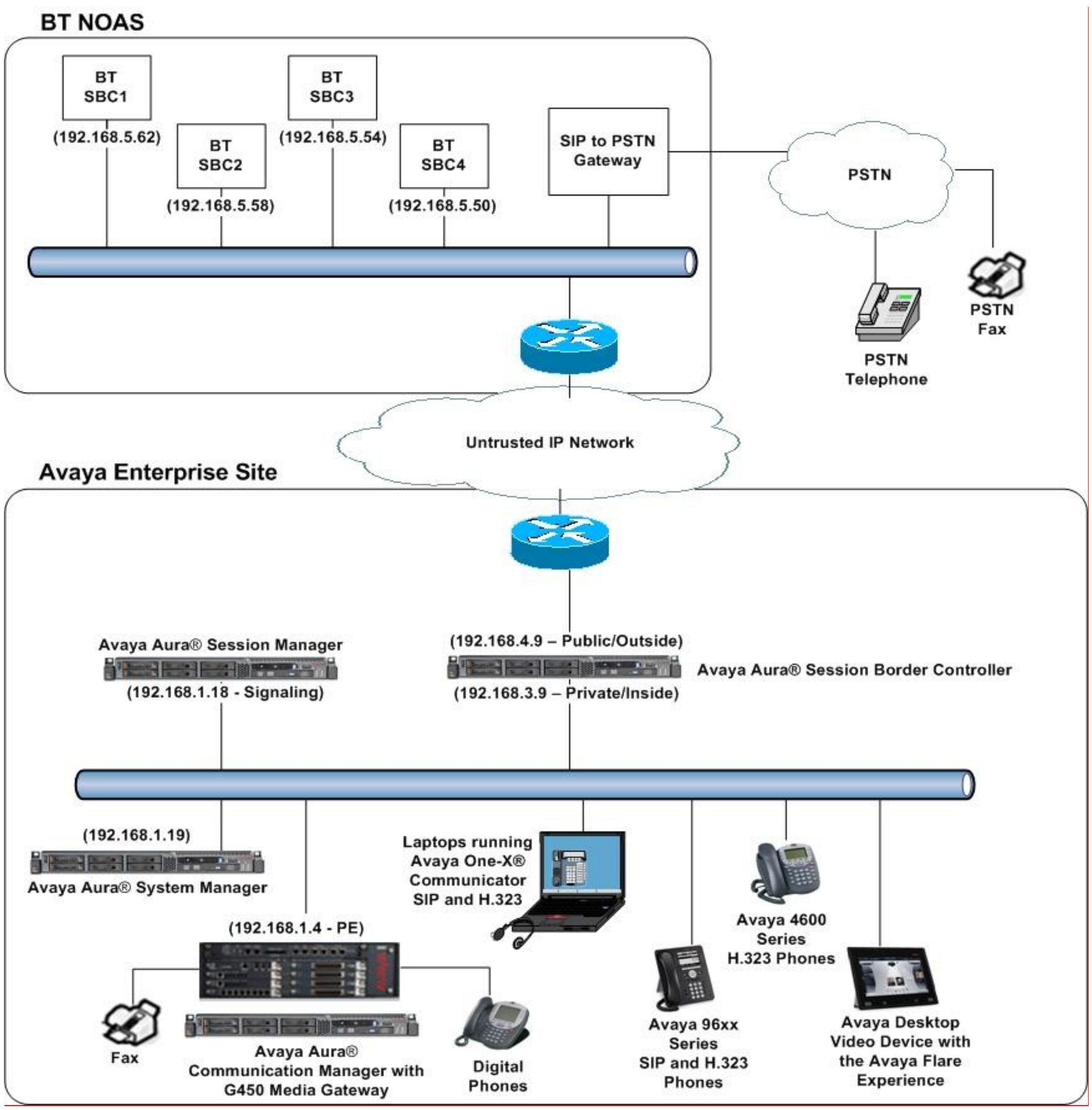


Figure 1: BT Sample Configuration

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server	Avaya Aura® Communication Manager R6.0.1 (R016x.00.1.510.1) Service Pack 18621 (System Platform 6.0.2.1.5)
Avaya G450 Media Gateway	FW 31.17.1
Avaya S8800 Server	Avaya Aura® Session Manager R6.1 (6.1.0.0.610023)
Avaya S8800 Server	Avaya Aura® System Manager R6.1 (System Platform 6.0.2.0.5, Template 6.1.4.0)
Avaya S8800 Media Server	Avaya Aura® Session Border Controller R6.1 (System Platform 6.0.3.0.3, Template E362P4)
Avaya 9620 Phone (H.323)	3.1.1
Avaya 9620 Phone (SIP)	2.6.1
Avaya 9621 Phone (H.323)	s9621_41HAL_R6_0r58_V4r52
Avaya 4621 Phone (H.323)	2.9.1
Avaya Desktop Video Device, A175, incorporating the Avaya Flare experience	1.0.0
One–X® Communicator (SIP)	6.0.1.16-SP1-25226
One–X® Communicator (H.323)	6.0.1.16-SP1-25226
Digital Phone 2420	N/A
BT SIP Trunk Service	2.1.0.8

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 Signaling associated with BT SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the SBC 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 signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the AASBC; the AASBC then sends the SIP messages to the BT 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 Server and Avaya G450 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 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 10
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 113   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 24000 24
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
```

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

```
isplay 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? y
                  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 signaling group between Communication Manager and Session Manager. Use the **change node-name ip** command and assign the node **Name** and **IP Address** for the Session Manager. In this case, **rom_sm6** and **192.168.1.18** are the **Name** and **IP Address** for the Session Manager. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signaling interface to Session Manager.

```
change node-names ip
                                  IP NODE NAMES
    Name              IP Address
procr               192.168.1.4
rom_sm6             192.168.1.18
default             0.0.0.0
```

5.3. Administer IP Network Region

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

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager (**Section 6.2**). In this configuration, the domain name is **rom2.bt.com**.
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is enabled to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled the enterprise end point will talk directly to the public interface of the BT Session Border Controller.
- 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 which is configured in **Section 5.4**.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: rom2.bt.com
    Name:
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

Use the **change ip-codec-set x** command to configure the codec set specified in the **IP Network Region** form and enter the list of audio codecs eligible to be used in order of preference. For the interoperability test the codecs supported by BT were configured, namely G.729 and G.711A. During compliance testing, other codec set configurations were also verified.

```
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.729             n          2        20
 2: G.711A            n          2        20
 3: G.723             n          2        20
```

BT SIP Trunk Service supports the T.38 fax protocol. Configure the T.38 fax protocol by setting the **Fax Mode** to **t.38-standard** on **Page 2** of the codec set form as shown below.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

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

5.5. Administer SIP Signaling Groups

This signaling group (and trunk group) will be used for inbound and outbound PSTN calls to BT SIP Trunk Service and will be configured using TLS (Transport Layer Security) and the default TLS port of 5061. Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set the **Group Type** field to **sip.**
- The **Transport Method** field is set to **tls** (Transport Layer Security).
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication.
- Manager to automatically detect if the peer server is a Session Manager.
- Set the **Near-end Node Name** to the processor interface (node name **procr**). This value is taken from the **IP Node Names** form shown in **Section 5.2.**
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **rom_sm6**), as shown in **Section 5.2.**
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 5.3**. This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- Set the **Far-end Domain** field to the domain of the enterprise.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.

Default values were used for other fields.

```
add signaling-group 4                                            Page   1 of   1
                                SIGNALING GROUP

 Group Number: 4              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n                                                SIP Enabled LSP? 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: rom_sm6
 Near-end Listen Port: 5061                  Far-end Listen Port: 5061
                                          Far-end Network Region: 1

Far-end Domain: rom2.bt.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 5                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? y             Alternate Route Timer(sec): 6
```

5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group 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 **tie**.
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as configured in **Section 5.5**.
- Specify the **Number of Members** supported by this SIP trunk group.

```
add trunk-group 4                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 4                    Group Type: sip           CDR Reports: y
  Group Name: sip trunk to Rom SM6        COR: 1        TN: 1        TAC: 104
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 4
                                                     Number of Members: 4
```

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 to prevent unnecessary SIP messages during call setup. Also note that the value for **Redirect On OPTIM Failure** was set to **8000** to allow additional set-up time for calls destined for an EC500 destination.

```
add trunk-group 4                                        Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS
     Unicode Name: auto
                                        Redirect On OPTIM Failure: 8000

            SCCAN? n                              Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 1800
```

On **Page 3**, set the **Numbering Format** field to **public**.

```
add trunk-group 4                                                    Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: both
                                                          Maintenance Tests? y

                     Numbering Format: public
                                                UUI Treatment: service-provider
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

On **Page 4,** set the **Mark Users as Phone** to **y**, this field inserts a parameter to SIP requests indicating to any receiving SIP entity that the user part of the request URI should be treated as a telephone number. Set **Send Transferring Party Information** to **y,** to allow trunk to trunk transfers. Set **Telephone Event Payload Type** to **101** the value preferred by BT.

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

                      Mark Users as Phone? y
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? y
                 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? y
       Identity for Calling Party Display: P-Asserted-Identity
                             Enable Q-SIP? n
```

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number. In the sample configuration, all stations with a **4-digit** extension beginning with **39** will send the calling party number **44207111111x** to BT SIP Trunk Service, where **x** is the last digit of the 4-digit extension. This calling party number will be sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones.

```
change public-unknown-numbering 0                                  Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext             Trk       CPN           CPN
Len Code            Grp(s)    Prefix        Len
                                                  Total Administered: 1
 4  39              4          44207111111    12       Maximum Entries: 240
```

5.8. Administer Route Selection for Outbound Calls

In these Application Notes, the Automatic Route Selection (ARS) feature will be used to route outbound calls via the SIP trunk to BT SIP Trunk Service. In the sample configuration, the single digit 9 is used as the ARS access code. Avaya telephone users will dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure or observe 9 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:
                       Answer Back 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 dialed digits following the first digit 9. A small sample of dial patterns is illustrated here. Further administration of ARS is beyond the scope of these Application Notes. The example entries shown will match outgoing calls to numbers beginning **0207** or **0208**. Calls are sent to **Route Pattern 5**.

```
change ars analysis 02                                          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
    0207                 4    11    5        pubu         n
    0208                 4    11    5        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 **5** is used to route calls to trunk group **4**.

```
change route-pattern 5                                          Page   1 of   3
                    Pattern Number: 5   Pattern Name: sip trk to SM6
                             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: 4    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                                        none
 2: y y y y y n  n            rest                                        none
```

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from BT can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DID numbers provided by BT correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers 02071111111 and 02081111111 to a 4 digit extension by deleting all of the incoming digits and inserting an extension.

```
change inc-call-handling-trmt trunk-group 1                    Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    11  02071111111    all  3936
 public-ntwrk    11  02081111111    all  3934
```

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 3910. Use the command **change off-pbx-telephone station mapping x**, where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate.
- For **Application** enter **EC500.**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration.
- For the **Phone Number** field enter the phone that will also be called (e.g., **07880111111**).
- Set the **Trunk Selection** to **ars** so that the ARS tables will be used to determine how Communication Manager will route to the Phone Number destination.
- Set the **Config Set** to **1.**

Default values were used for other fields.

```
change off-pbx-telephone station-mapping 3910                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 3910             EC500         -     07880111111      ars        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:

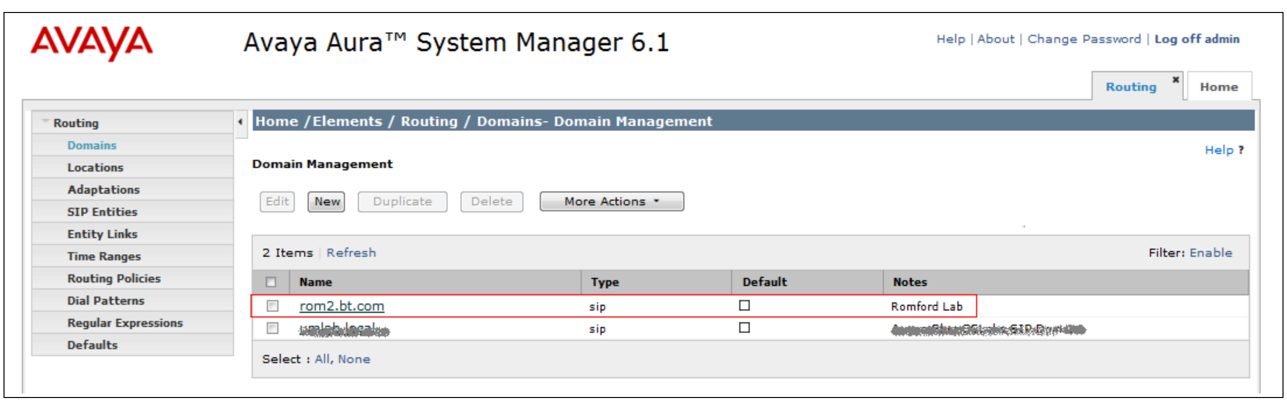
- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Avaya Aura® Communication Manager as Managed Element
- Administer Application for Avaya Aura®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

6.1. Log in to Avaya Aura® System Manager

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

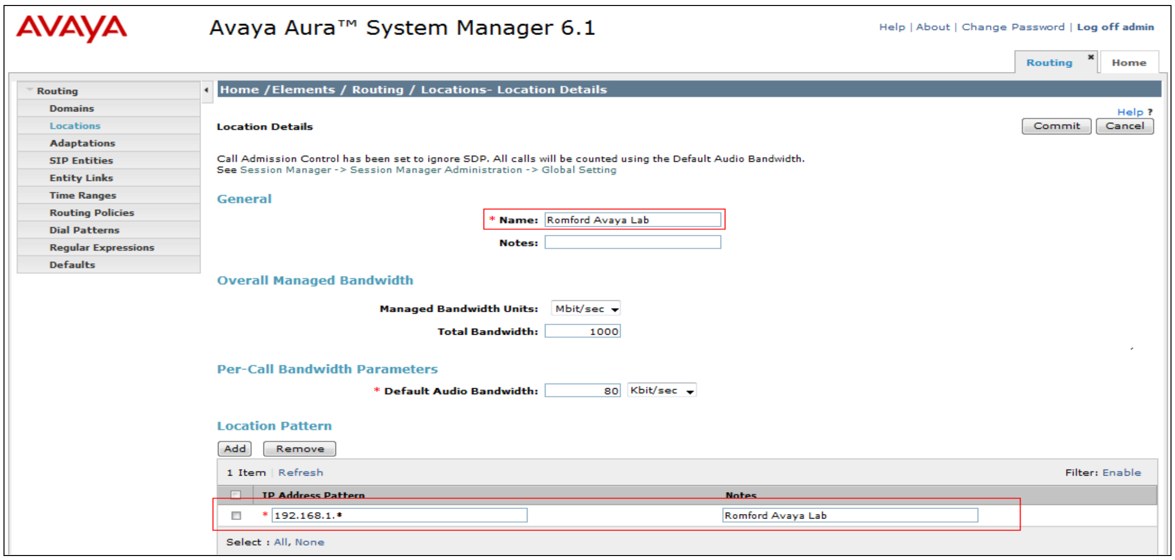
6.2. Administer SIP domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu (not shown) 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., **rom2.bt.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** (not shown) to save changes.



6.3. Administer Locations

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

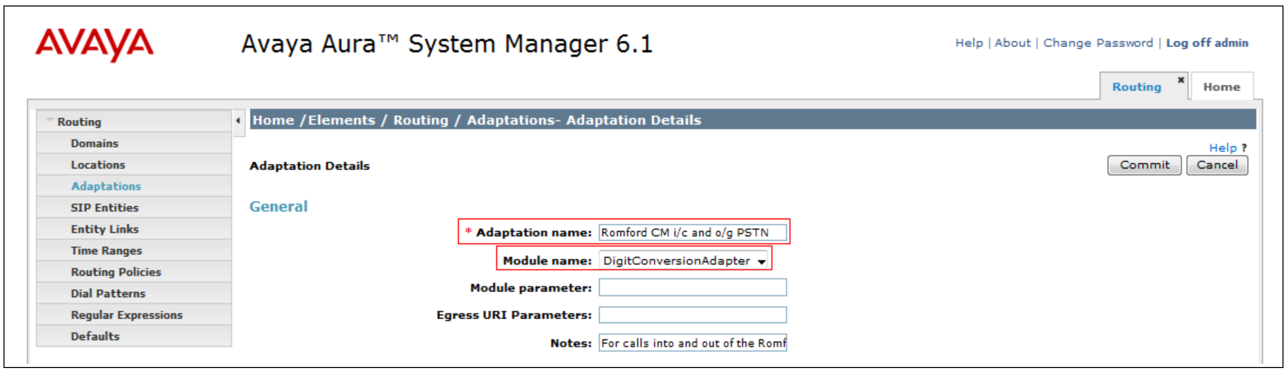


6.4. Administer Adaptations

In order to ensure that the E.164 numbering format is used between the enterprise and BT SIP Trunk Service, an adaptation module is used to perform some digit manipulation. This adaptation is applied to the Communication Manager SIP entity. To add an adaptation, on the **Routing** tab select **Adaptations** on the left hand menu and then click on the **New** button (not shown).

Under **General:**

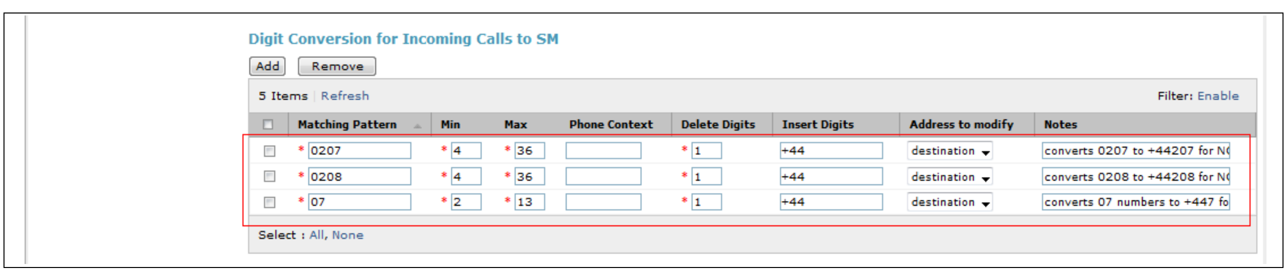
- In the **Adaptation Name** field enter an informative name.
- In the **Module Name** field select **<click to add module>** from the drop down list and enter **DigitConversionAdapter** in the resulting **New Module Name** field.



Under **Digit Conversion for Incoming Calls to 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. In this configuration the dialed number is the target so **destination** has been selected.

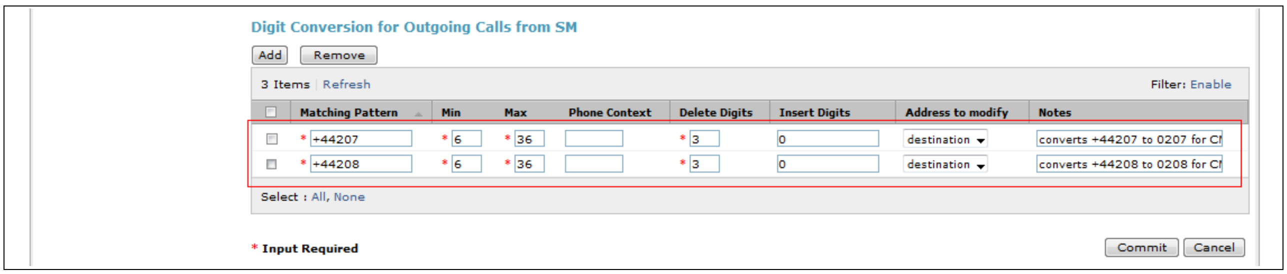
This will ensure any destination numbers received from Communication Manager are converted to the E.164 numbering format before being processed by Session Manager



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. In this configuration the dialed number is the target so **destination** has been selected.

This will ensure any destination numbers will have the + symbol and international dialing code removed before being presented to Communication Manager.



6.5. Administer SIP Entities

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

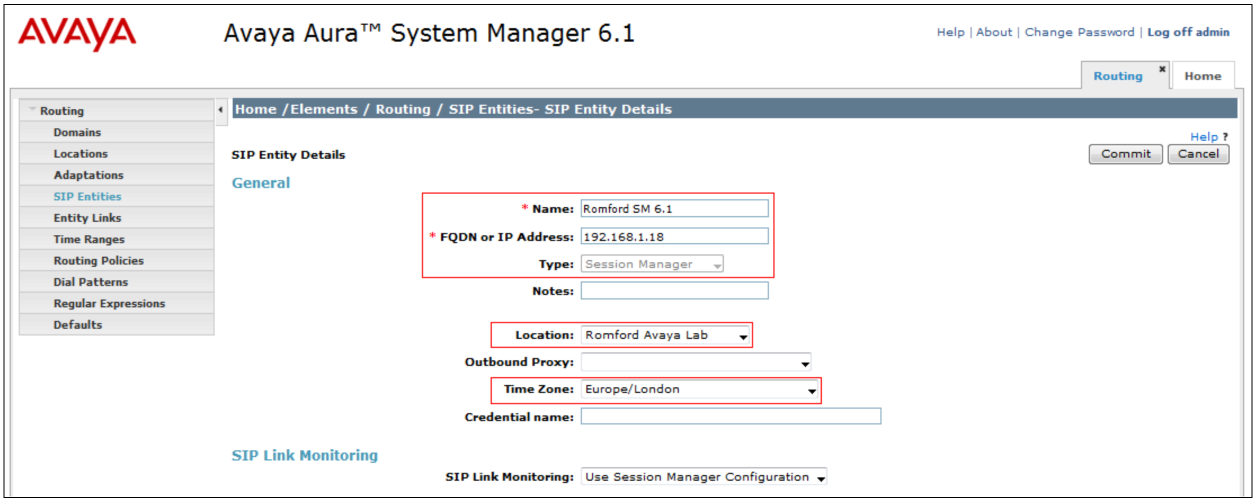
- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **Other** for the AASBC 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.

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Session Border Controller SIP Entity

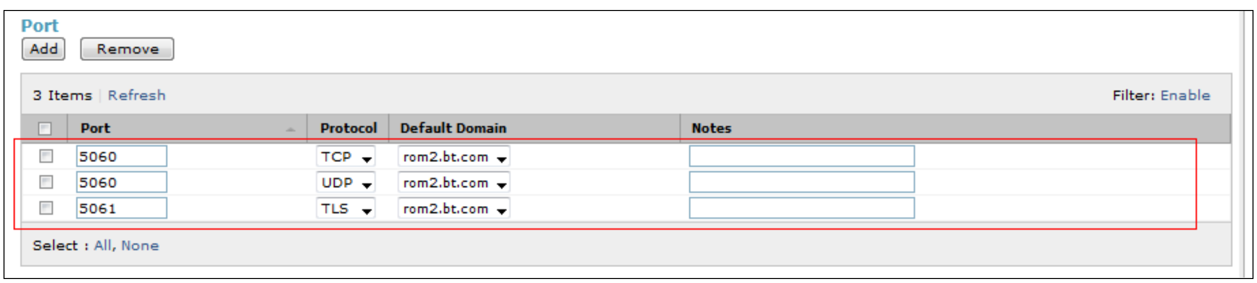
6.5.1. Avaya Aura® Session Manager SIP Entity

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 signaling interface.



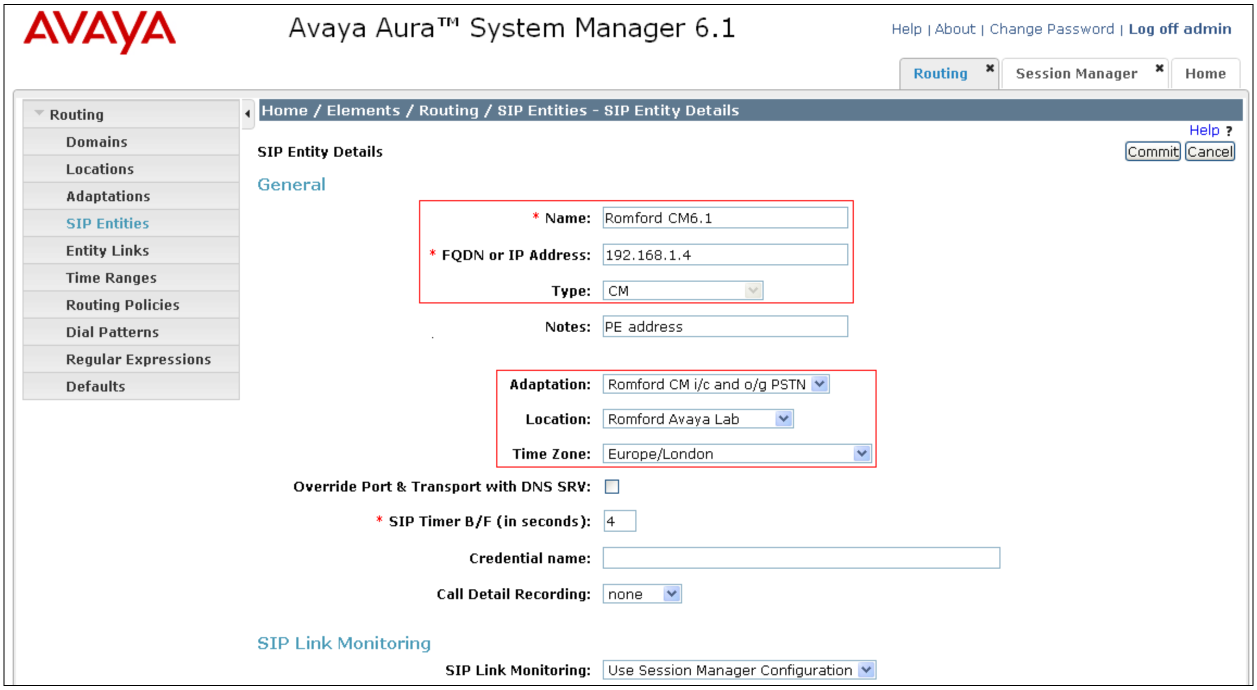
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add,** then edit the fields in the resulting new row.

- In the **Port** field enter the port number on which the system listens for SIP requests.
- In the **Protocol** field enter the transport protocol to be used for SIP requests.
- In the **Default Domain** field, from the drop down menu select **rom2.bt.com** as the default domain.



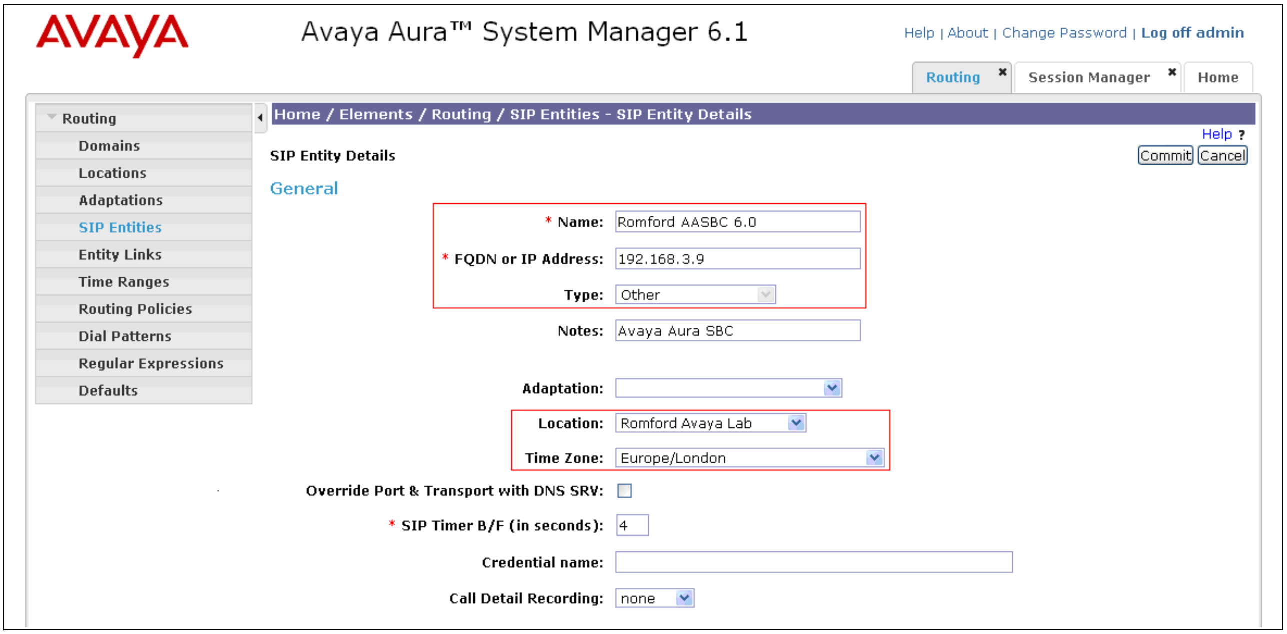
6.5.2. Avaya Aura® Communication Manager SIP Entities

The following screens show 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 signaling. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **Section 6.4**.



6.5.3. Avaya Aura® Session Border Controller SIP Entity

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

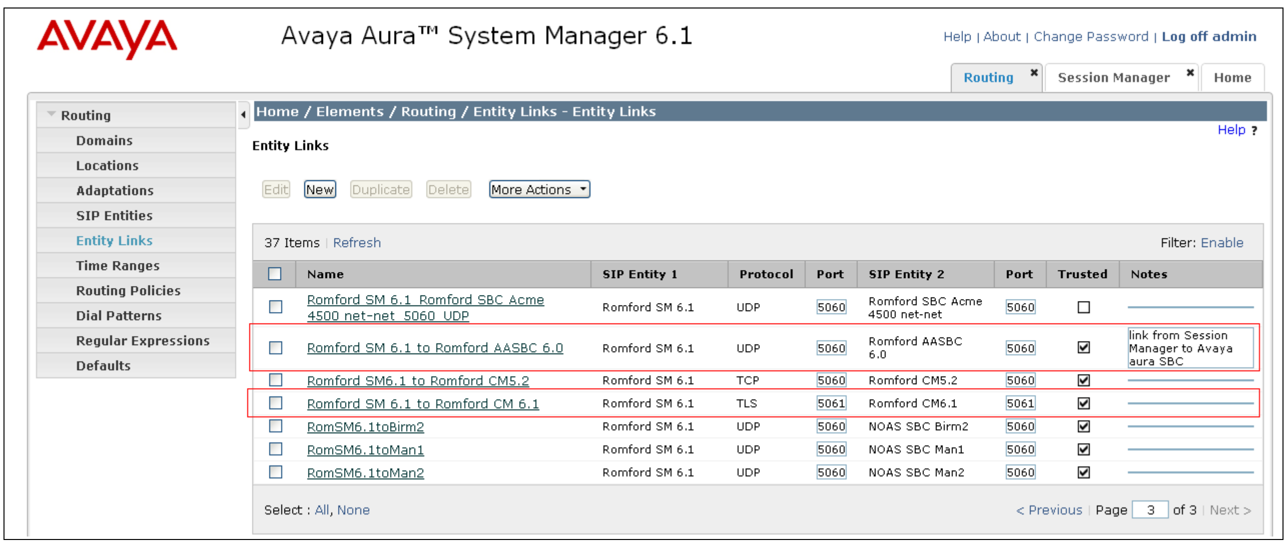


6.6. Administer Entity Links

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. In the resulting screen fill in the following fields displayed in the new row.

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **Romford SM 6.1**.
- 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 6.5**.
- 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** (not shown) to save changes. The following screen shows the Entity Links used in this configuration.



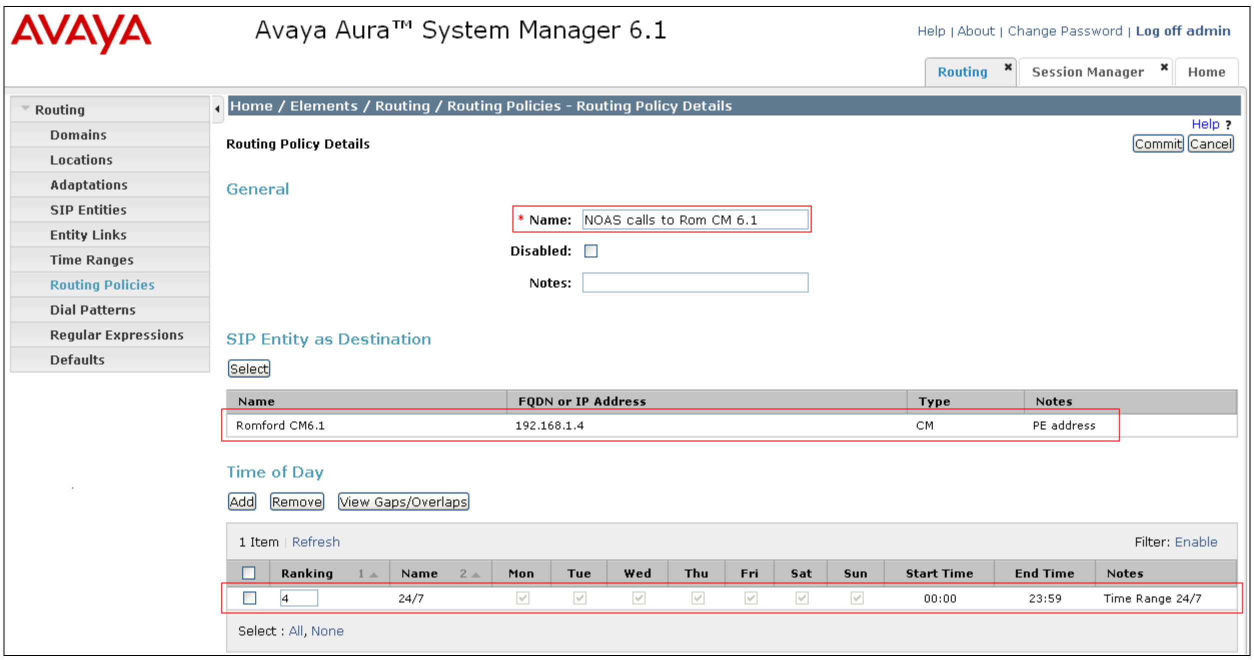
6.7. Administer Routing Policies

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).

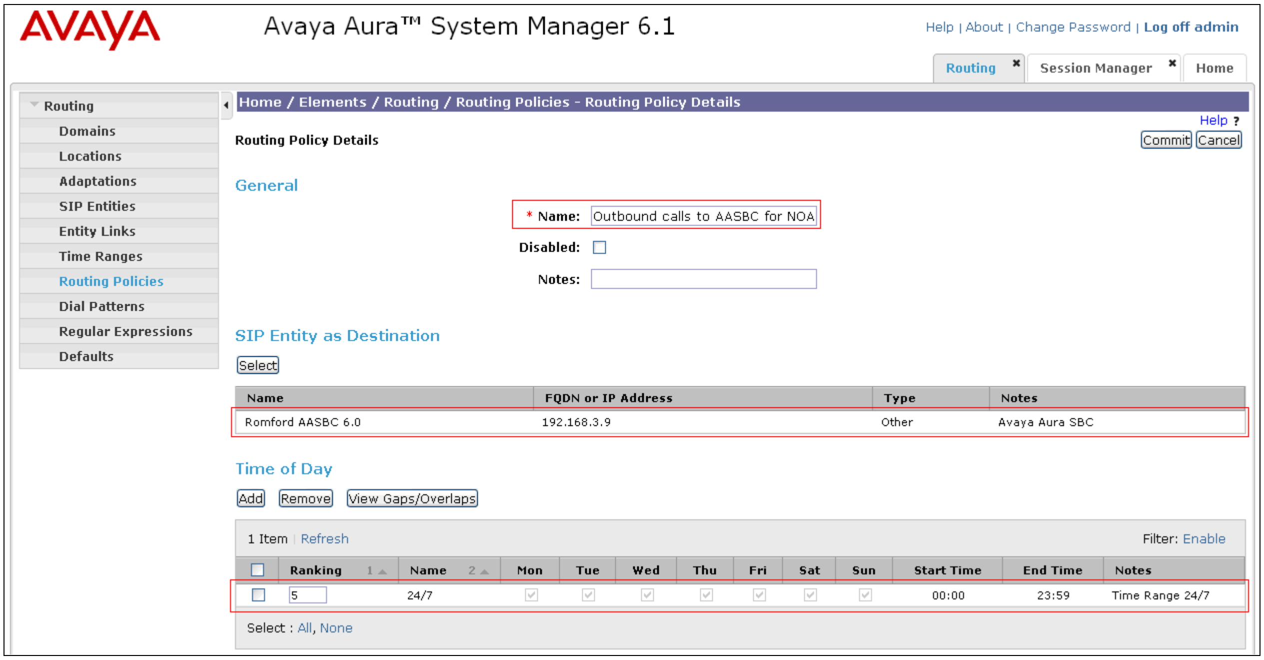
Under **General:**

- Enter an informative name in the **Name** field.
- Under **SIP Entity as Destination**, click **Select**, and in the resulting window (not shown) select the appropriate SIP entity to which this routing policy applies.
- Under **Time of Day**, click **Add**, and then select the time range.

The following screen shows the routing policy for Communication Manager.



The following screen shows the routing policy for the AASBC.



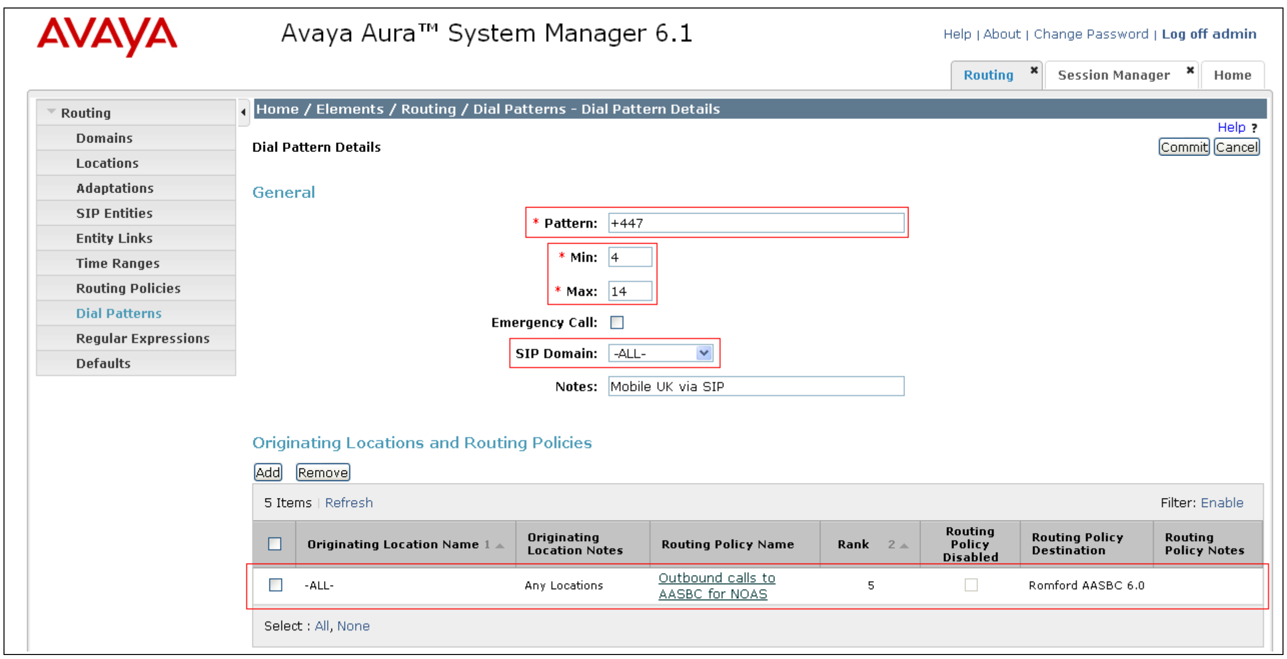
6.8. Administer Dial Patterns

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).

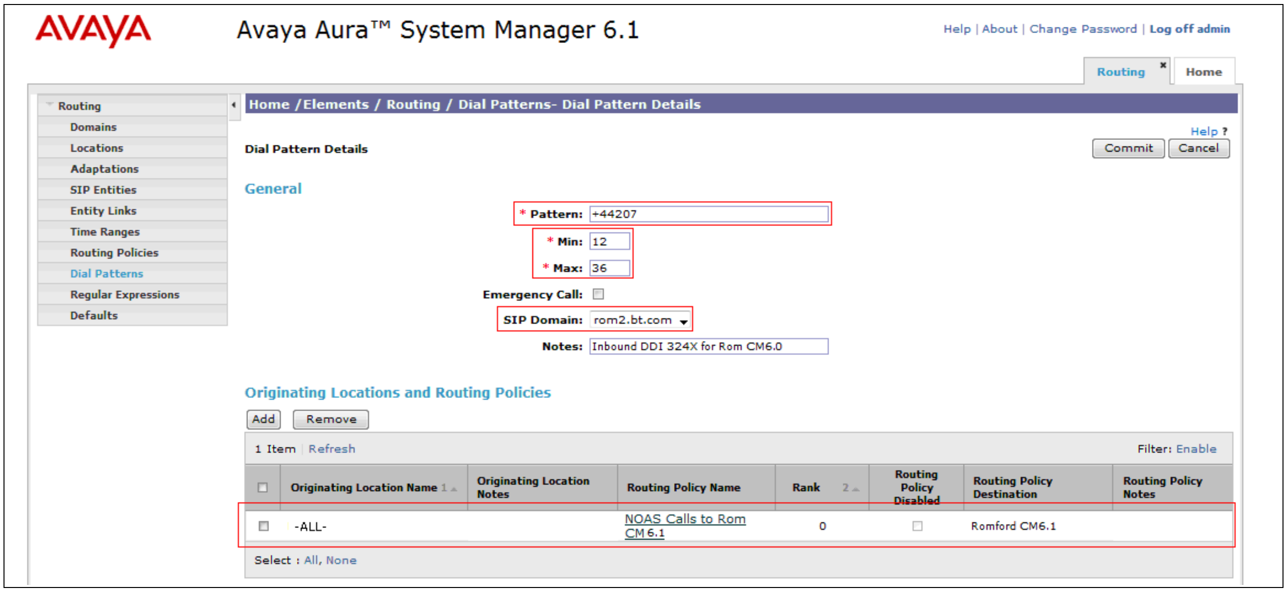
Under **General:**

- In the **Pattern** field, enter a dialed number or prefix to be matched.
- In the **Min** field, enter the minimum length of the dialed number.
- In the **Max** field, enter the maximum length of the dialed number.
- In the **SIP Domain** field, select the domain configured in **Section 6.2**.

Under **Originating Locations and Routing Policies.** Click **Add**, in the resulting screen (not shown), under **Originating Location** select **ALL** and under **Routing Policies** select one of the routing policies defined in **Section 6.7**. Click **Select** button to save. The following screen shows an example dial pattern configured for AASBC which will route the calls out to the BT SIP Trunk Service.



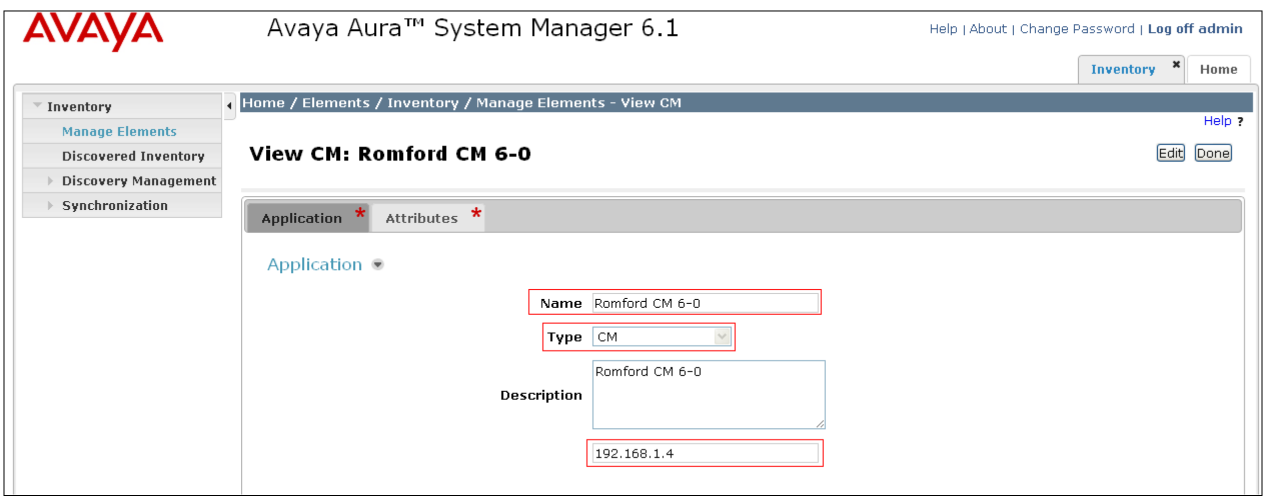
The following screen shows an example dial pattern configured for Communication Manager.



6.9. Administer Avaya Aura® Communication Manager as a Managed Element

From the Home tab select Inventory from the menu. In the resulting tab from the left panel menu select **Manage Elements** and click **New** (not shown)**.** On the **Application** tab, enter values in the following fields and use defaults for the remaining fields:

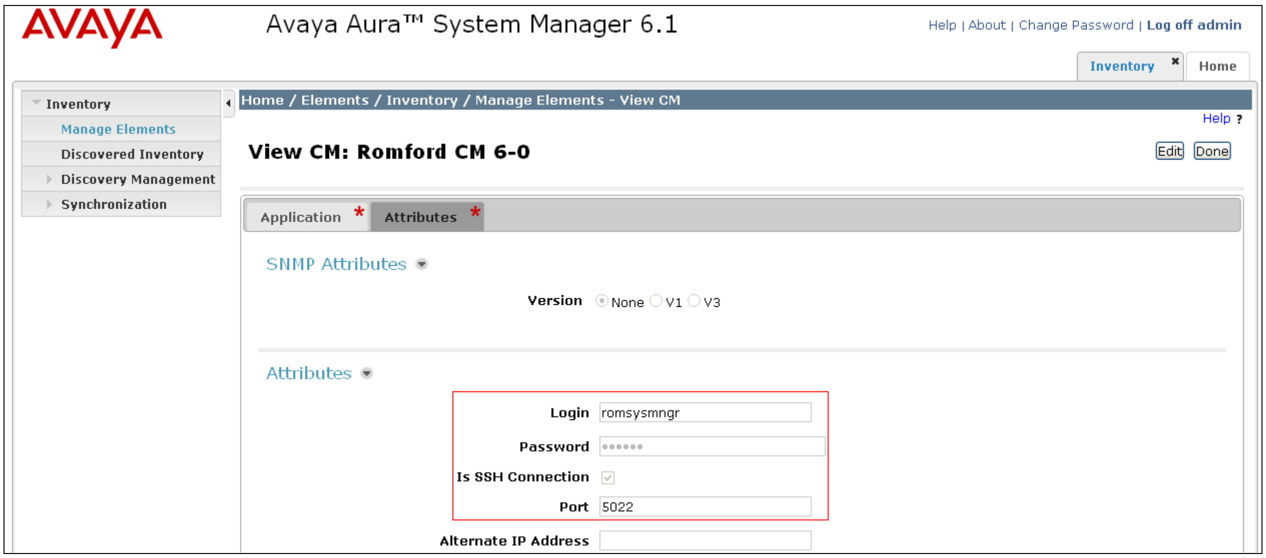
- In the **Name** field enter a descriptive name .
- In the **Type** field select CM from the drop-down menu.
- In the **Node** enter the IP address of the Communication Manager.



On the **Attributes** tab, under the **Attributes** heading, enter values in the following fields and use defaults for the remaining fields:

- In the **Login** field enter a login name for Communication Manager (SAT SSH login).
- In the **Password** field enter the password for Communication Manager (SAT SSH password).
- Select the **Is SSH Connection** check box if SSH is to be used.
- In the **Port** field enter the port number to use for SAT access.

Select **Commit** (not shown) to synchronize System Manager with the Communication Manager in the background.

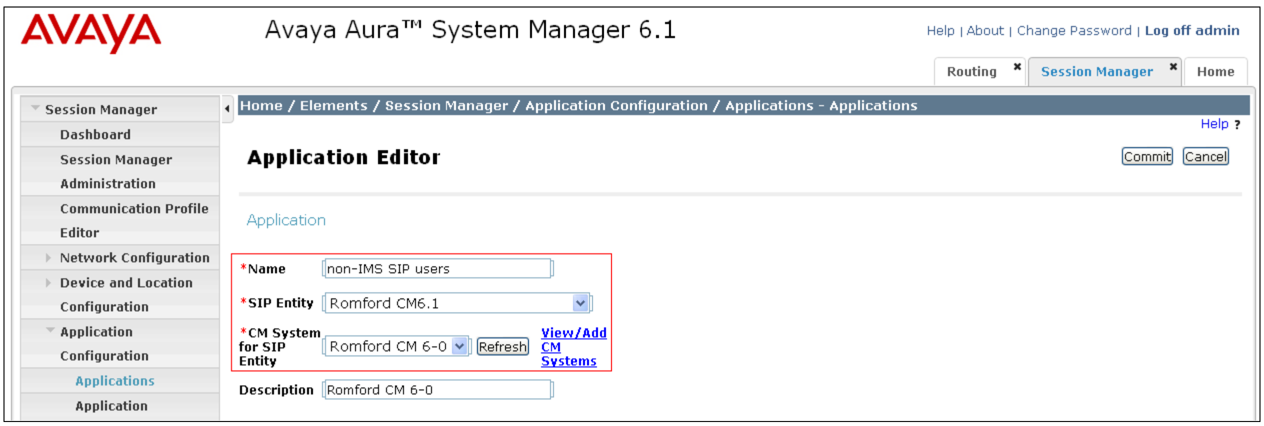


6.10. Administer Application for Avaya Aura® Communication Manager

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** (not shown) and configure as follows:

- In the **Name** field enter a name for the application.
- In the **SIP Entity** field select the SIP entity for the Communication Manager configured in **Section 6.5.2**.
- In the **CM System for SIP Entity** field select the managed element for the Communication Manager configured in **Section 6.9**.

Select **Commit** to save the configuration.

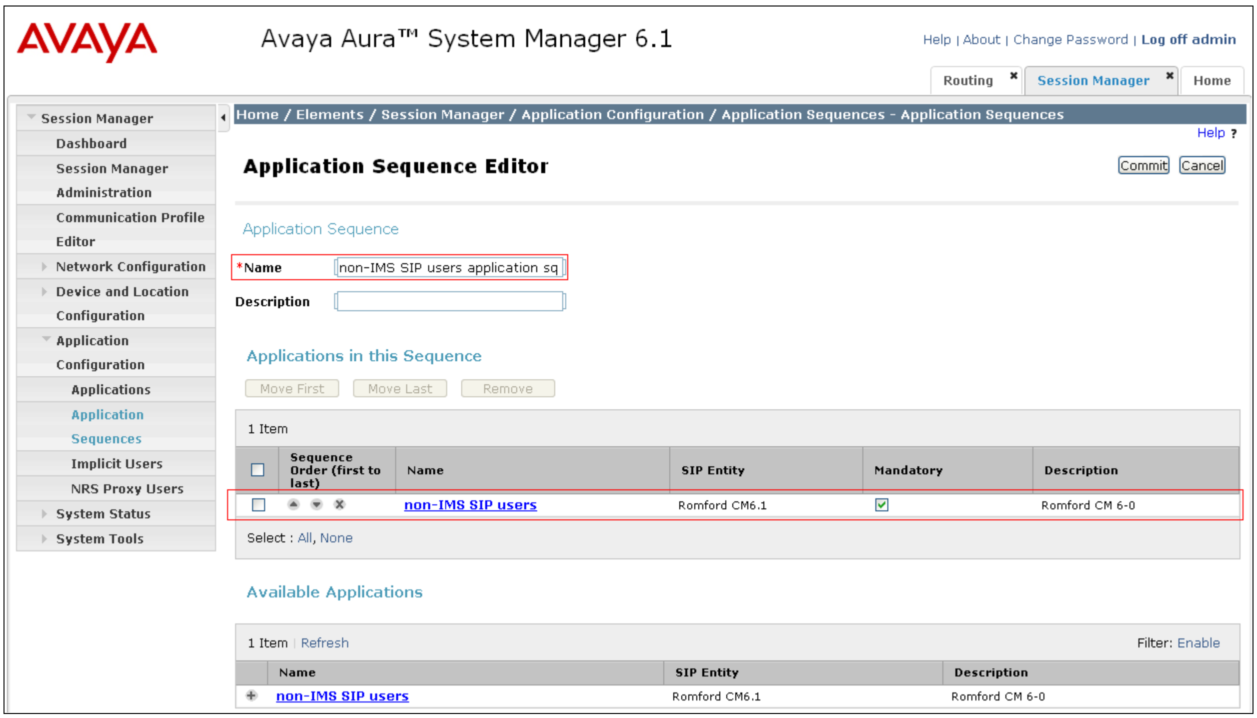


6.11. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Session Manager → Application Configuration → Application Sequences** and click on **New** (not shown).

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

Select **Commit**.

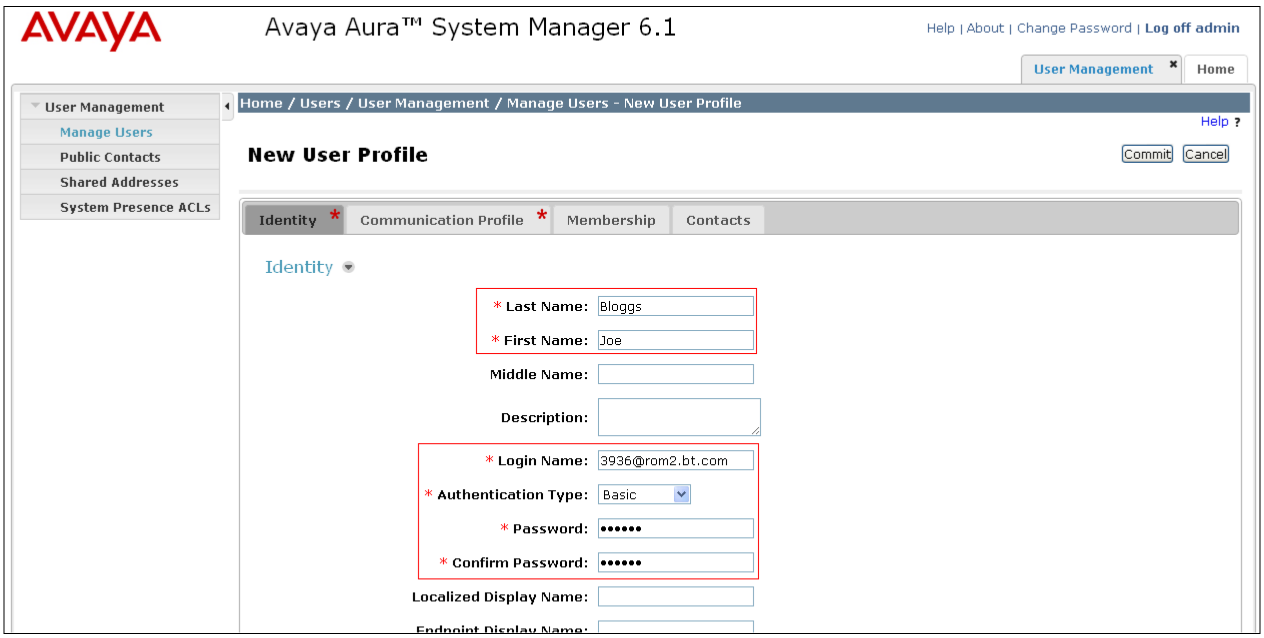


6.12. Administer SIP Extensions

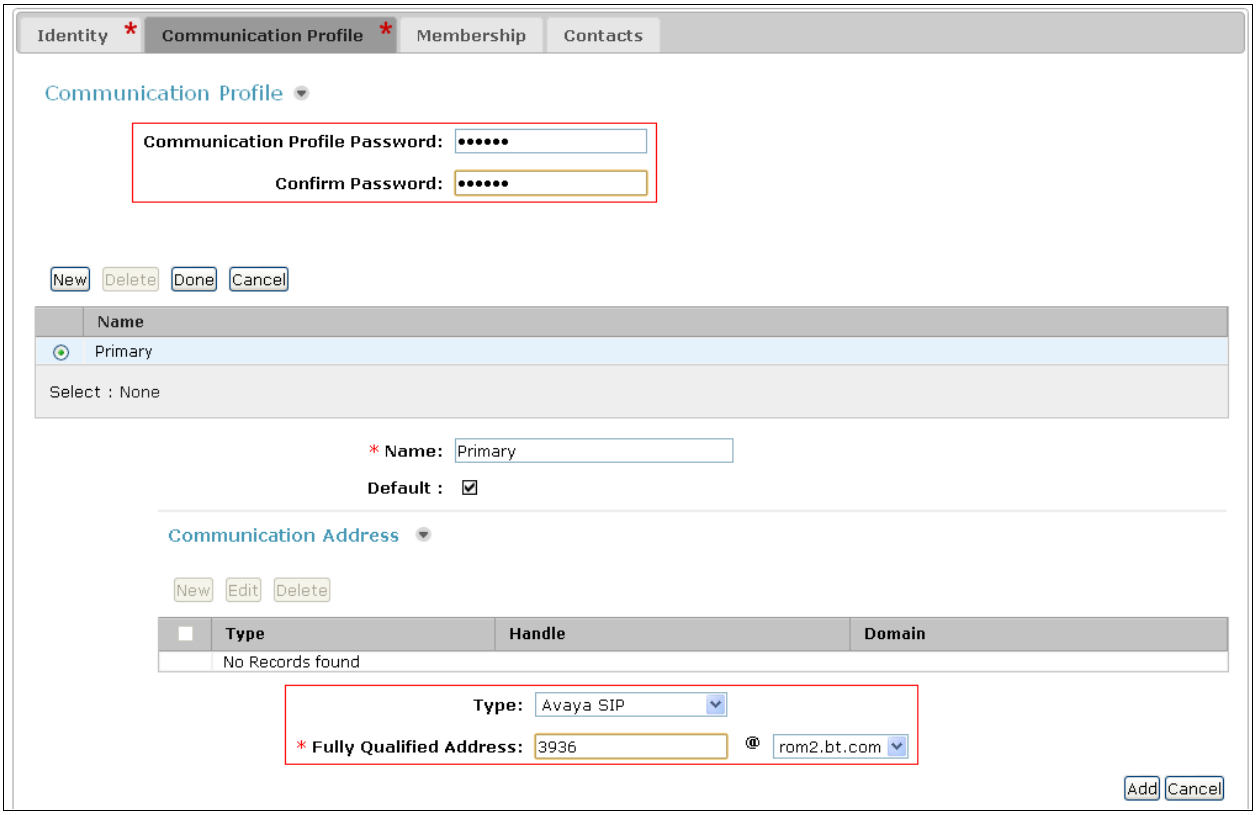
SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the Home tab select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

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. **3936@rom2.bt.com**) which is used to create the user's primary handle.
- The **Authentication Type** should be **Basic**.
- In the **Password/Confirm Password** fields enter an alphanumeric password.

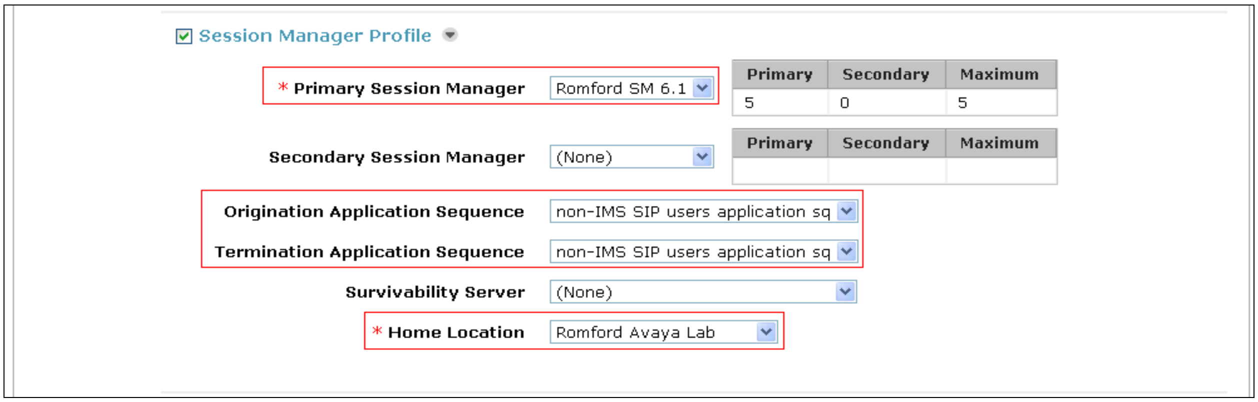


On the **Communication Profile** tab enter a numeric **Communication Profile Password** and confirm it, then click on the show/hide button for **Communication Address** and click **New**. For the **Type** field select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter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



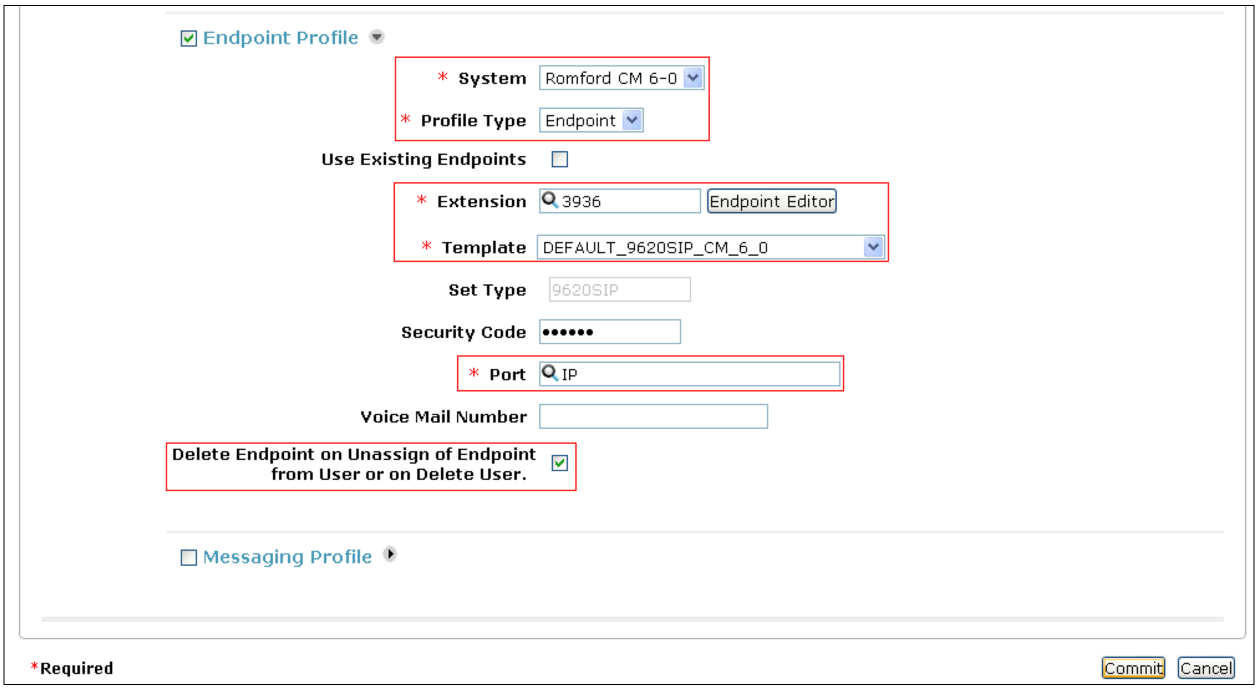
Click the show/hide button next to **Session Manager Profile**.

- 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 6.11**.
- Select the appropriate application sequence from the drop-down menu in the **Termination Application Sequence** field configured in **Section 6.11**.
- Select the appropriate location from the drop-down menu in the **Home Location** field configured in **Section 6.3**.



Click the show/hide button next to **Endpoint Profile** and configure as follows**:**

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



7. Configure Avaya Aura® Session Border Controller

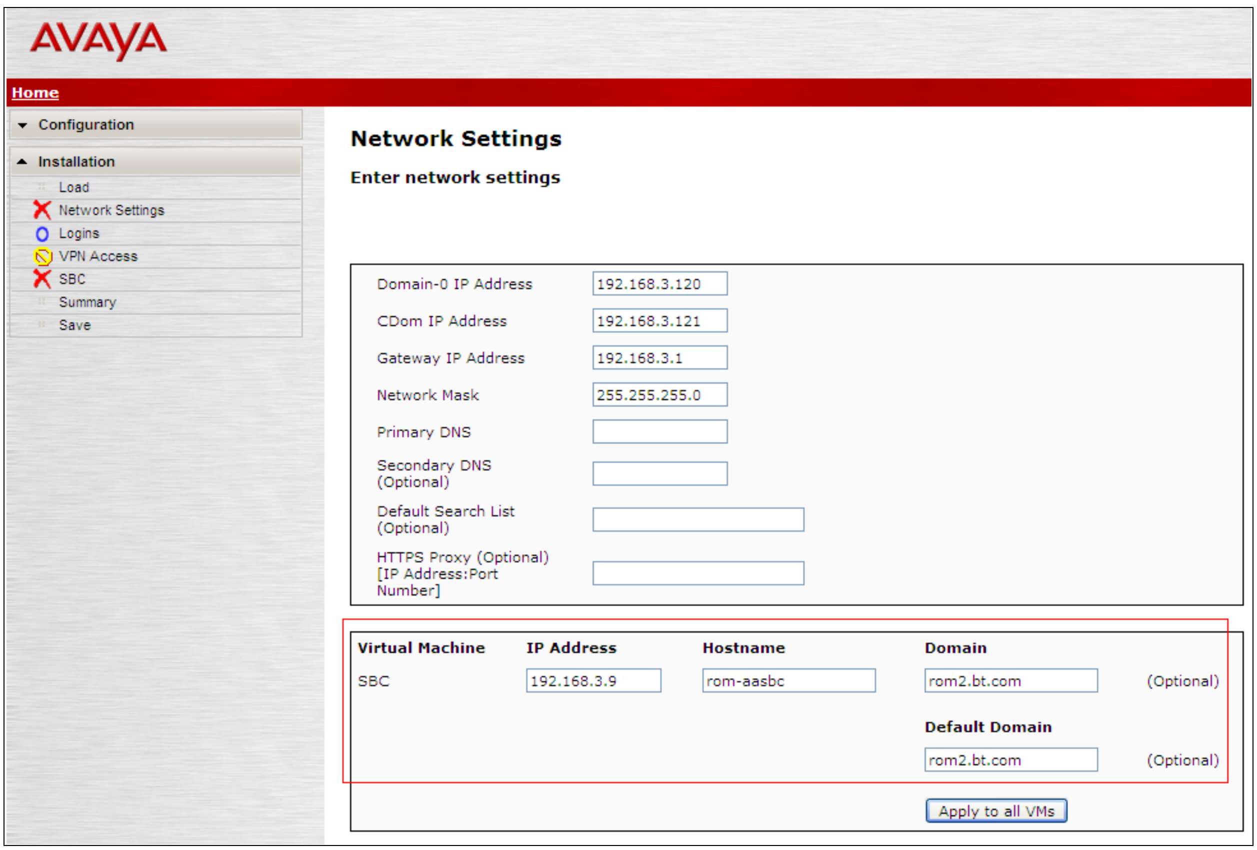
This section describes the configuration of the AASBC. This configuration is done in two parts. The first part is done during the AASBC installation via the installation wizard. These Application Notes will not cover the AASBC installation in its entirety but will include the use of the installation wizard. For information on installing the System Platform and the loading of the AASBC template see **[8]** & **[9]**. The second part of the configuration is done after the installation is complete using the AASBC management interface.

7.1. Installation Wizard

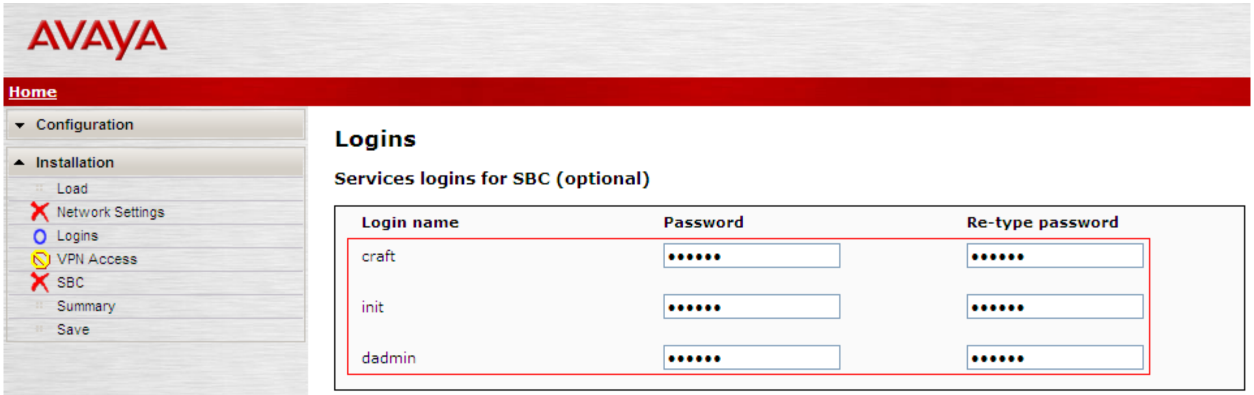
During the installation of the AASBC template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the AASBC. The first screen of the installation wizard is the Network Settings screen. Fill in the fields as described below and shown in the following screen:

- In the **IP Address** field enter the IP address of the private side of the AASBC.
- In the **Hostname** field enter a host name for the AASBC.
- Specify a domain in the **Domain** and **Default Domain** fields.

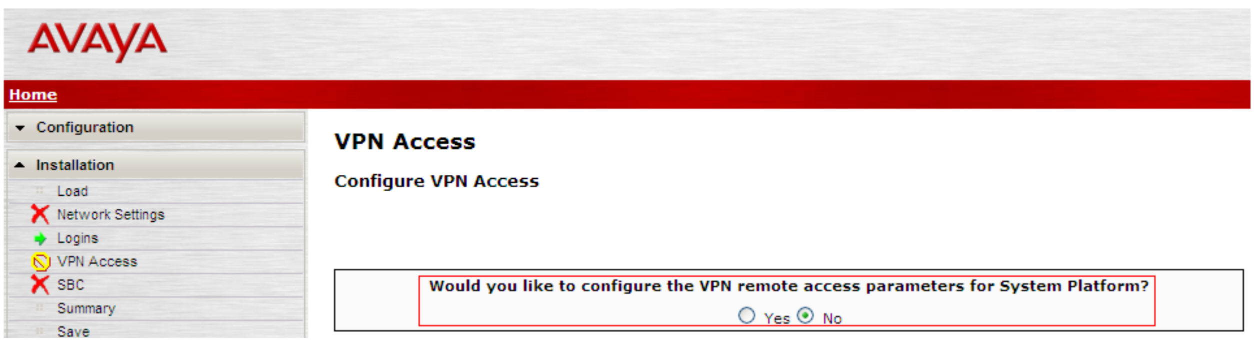
Click **Next Step** (not shown) to continue.



From the Logins screen specify passwords for the services logins to the AASBC.



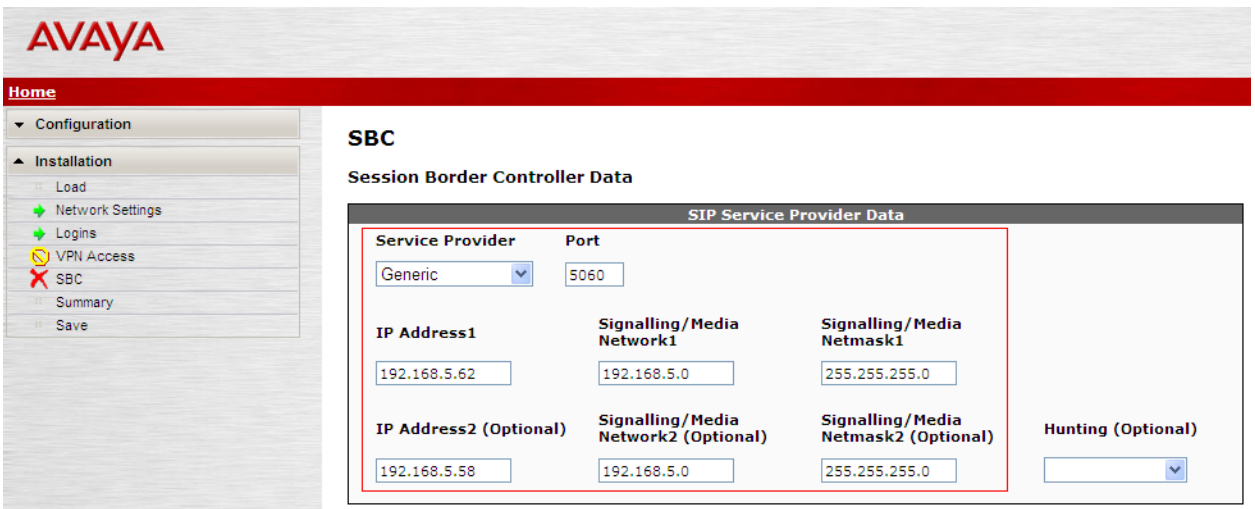
VPN remote access to the AASBC was not part of the compliance test. Thus, on the VPN Access screen, select **No** to the question, **Would you like to configure the VPN remote access parameters for System Platform?**



On the **SBC** screen, in the **SIP Service Provider Data** section fill in the fields as described below and shown in the following screen.

- In the **Service Provider** select the name of the service provider to which the AASBC will connect. This will allow the wizard to select a configuration file customized for this service provider. At the time of the compliance test, a customized configuration file did not exist for BT. Thus, **Generic** was chosen.
- In the **Port** field enter the port number that BT uses to listen for SIP traffic.
- In the **IP Address1** and **IP Address2** fields enter the first two BT provided IP addresses for the SIP Trunk Service. The remaining IP addresses used during testing will be added after the AASBC template is installed **(Section 7.3).**
- In the **Signaling/Media Network1** field enter the BT provided subnet where media traffic will originate. An additional subnet can be provided for **Signaling/Media Network2.**
- In the **Media Netmask** field enter the netmask corresponding to the Media Network.

Scroll down to continue



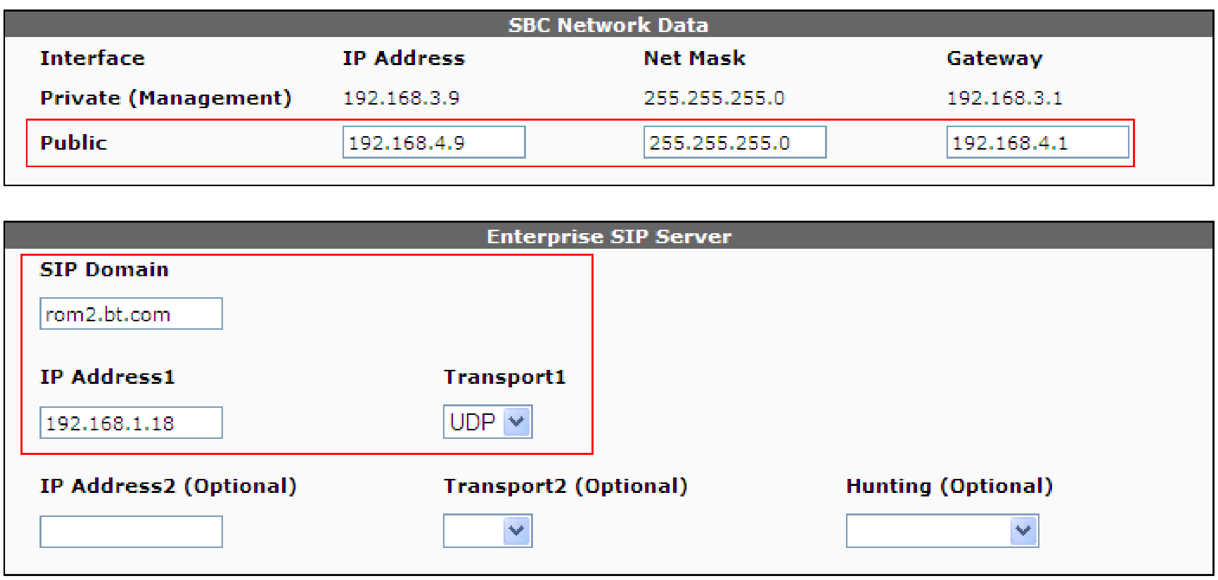
Further down on the same **SBC** screen, in the **SBC Network Data** section fill in the fields as described below:

- In the **Public IP Address** field enter the IP address of the public side of the AASBC.
- In the **Public Net Mask** field enter the netmask associated with the public network to which the AASBC connects.
- In the **Public Gateway** field enter the default gateway of the public network.

In the **Enterprise SIP Server** section fills in the fields as described below:

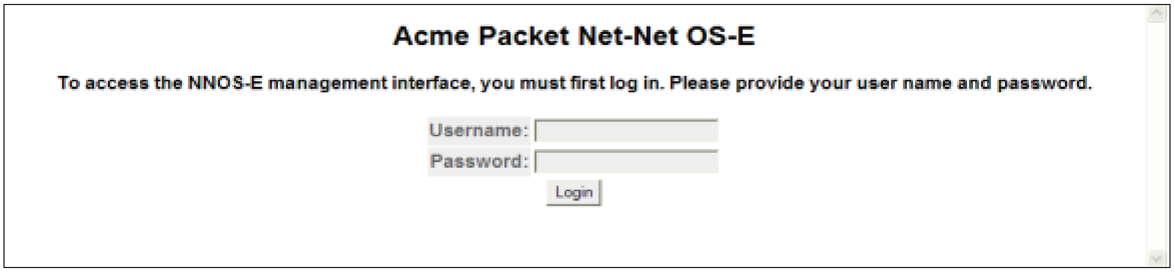
- In the **IP Address** field enter the IP address of the Enterprise SIP Server to which the AASBC will connect. In the case of the compliance test, this is the IP address of the Session Manager SIP signaling interface.
- In the **Transport1** field select the transport protocol to be used for SIP traffic between the AASBC and Session Manager.
- In the **SIP Domain** field enter the enterprise SIP domain.

Click **Next Step** to continue. A summary screen will be displayed (not shown). Check the displayed values and click **Next Step** again to install the template with the values entered.



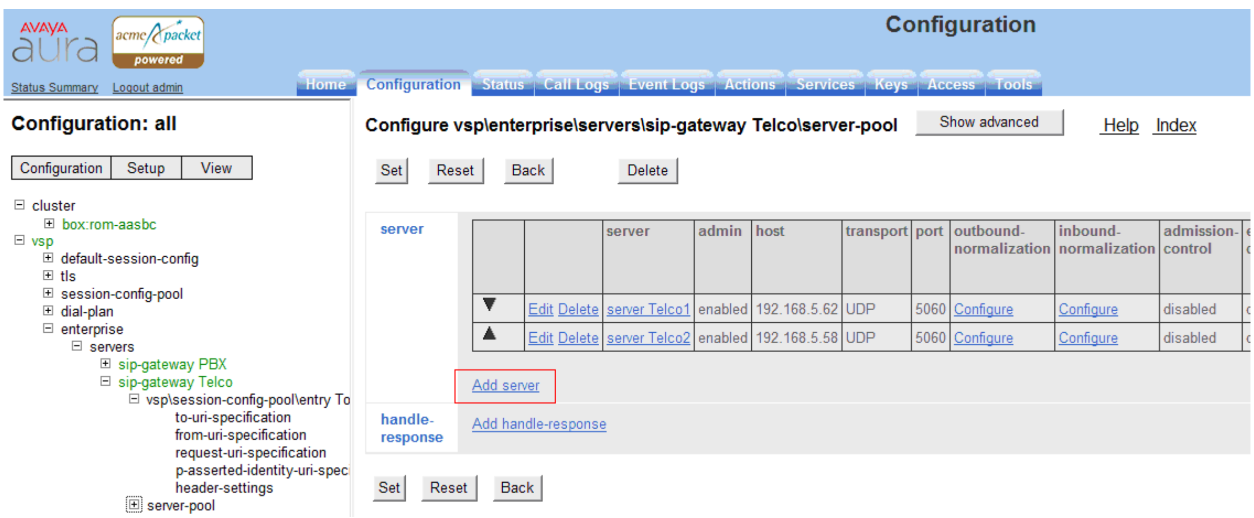
7.2. Access Avaya Aura® Session Border Controller

Access the AASBC using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured in **Section 7.1**. Log in with appropriate credentials.

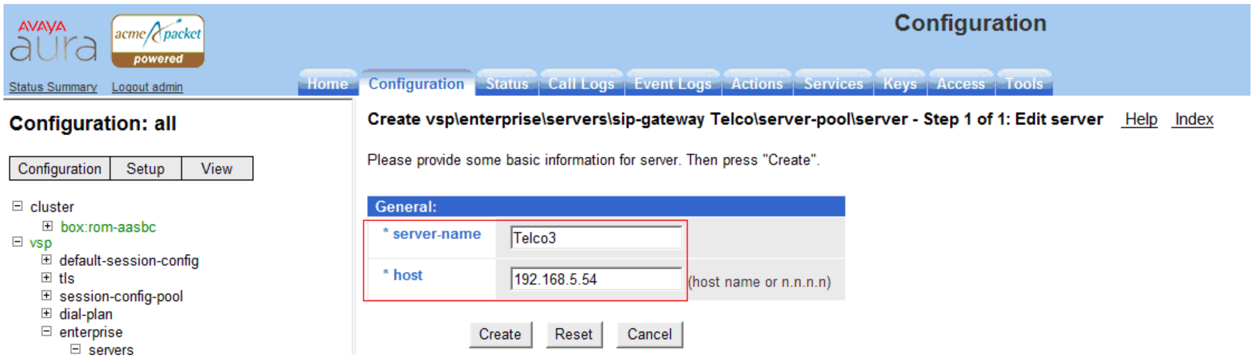


7.3. Add Additional Service Provider IP Addresses

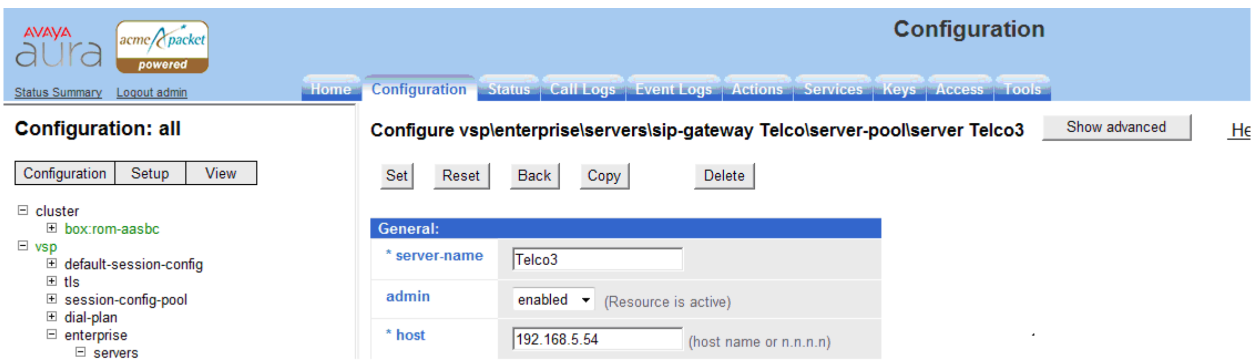
To add the additional IP addresses for the remaining BT SBCs that were not configured during the AASBC installation click on the **Configuration** tab and browse to **vsp → enterprise → servers → sip-gateway Telco → server-pool**. A list of the IP addresses already configured in the server pool is displayed in the right hand pane. Click the **Add server** link.



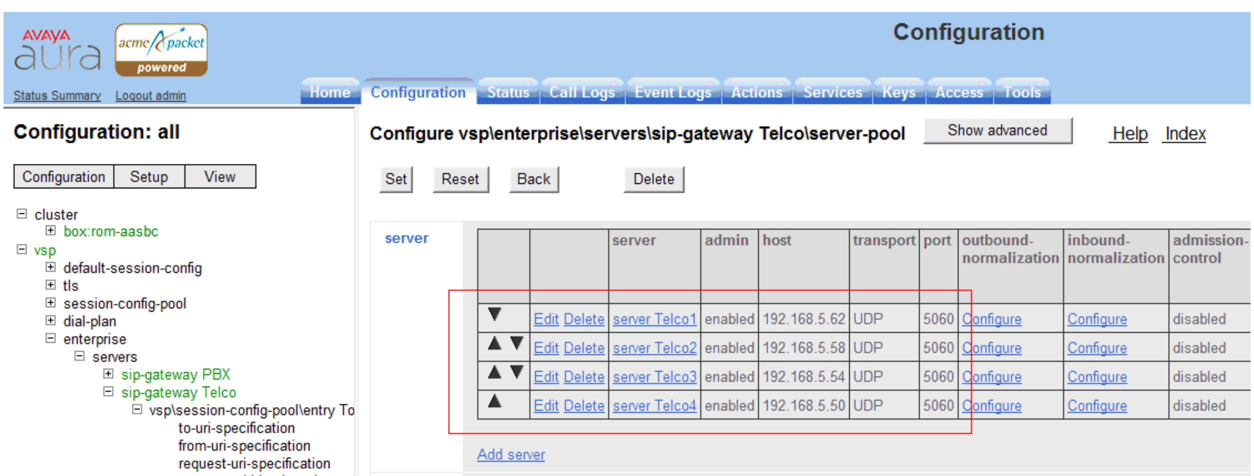
In the resulting page enter a name for the server in the **server-name** field and an IP address in the **host** field. Click **Create** to continue.



In the resulting page verify the details entered and click the **Set** button.

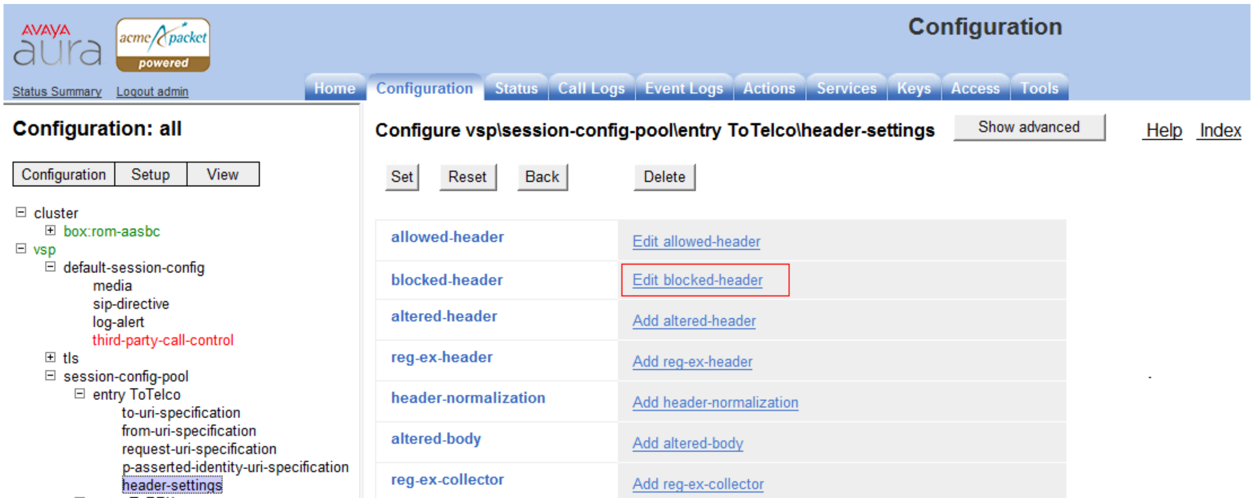


Repeat these steps for each additional IP address that needs to be added to the AASBC server pool. The screen below shows the server pool that was configured during testing.

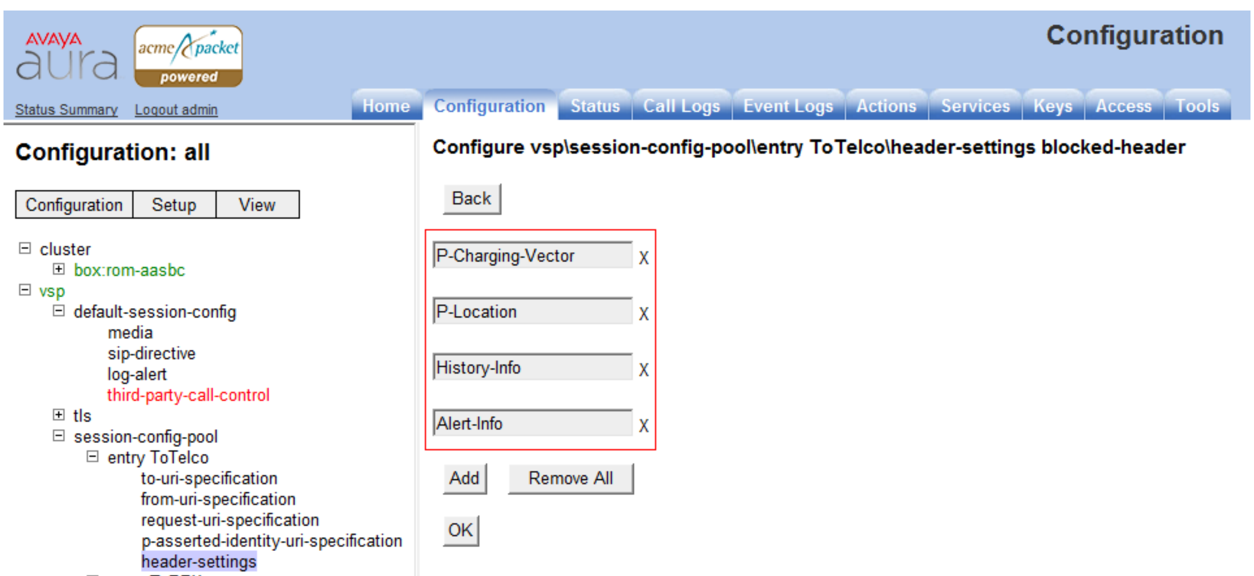


7.4. Stripping SIP Headers

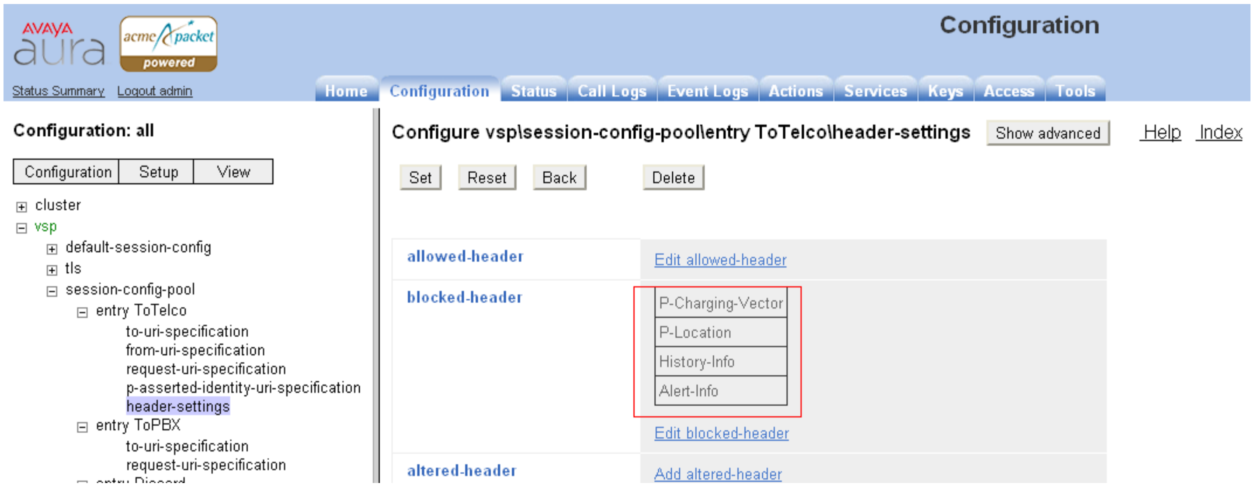
The AASBC can be used to strip SIP headers to prevent the header from being sent to the public SIP Service Provider. To strip a SIP header navigate to **vsp → session-config-pool → entry ToTelco → header-settings** and click on the **Edit blocked-header** link.



In the resulting page click the **Add** button to open a new entry field and enter the name of the header to be removed, repeat this action for all the headers to be removed. Click the **OK** button when finished.

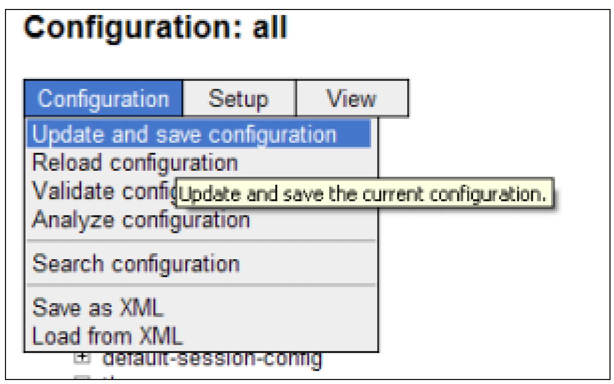


The following screen shows the headers being stripped during testing.



7.5. Save the Configuration

To save the configuration, click on **Configuration** in the left pane to display the configuration menu. Next, select **Update and save configuration**.



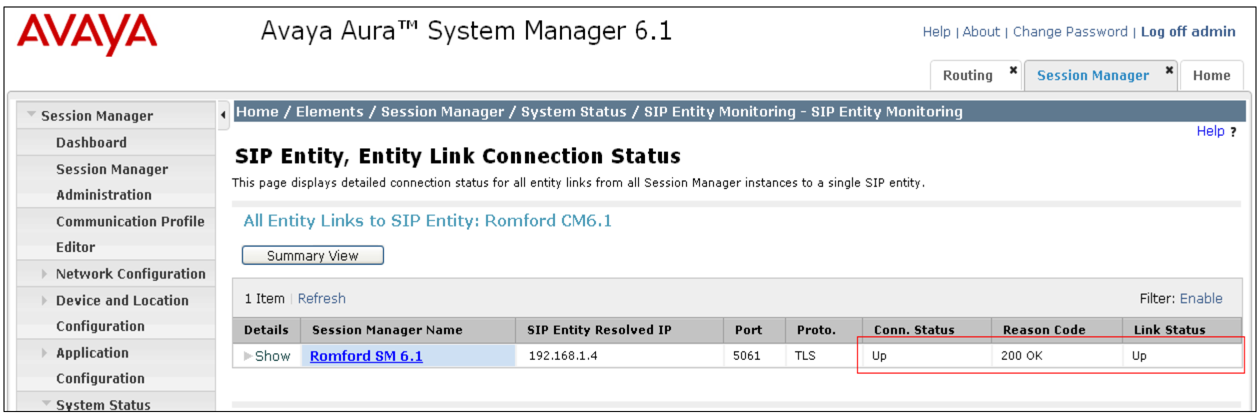
8. Service Provider Configuration

The configuration of the BT equipment used to support the BT SIP trunk service is outside of the scope for these application notes and will not be covered. To obtain further information on BT equipment and system configuration please contact an authorized BT 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.**



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 4

                            TRUNK GROUP STATUS

Member    Port     Service State      Mtce Connected Ports
                                      Busy

0004/001 T00001   in-service/idle    no
0004/002 T00007   in-service/idle    no
0004/003 T00008   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 Aura® Session Border Controller to BT SIP Trunk Service. BT SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

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, June 2010.

[2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.

[3] *Administering Avaya Aura® Communication Manager*, August 2010, Document Number 03-300509.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* August 2010, Document Number 555-245-205.

[5] *Installing and Upgrading Avaya Aura® System ManagerRelease6.1*, November 2010.

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

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

[8] *Avaya Aura® Session Border Controller System Administration*, September 2010

[9] *Installing and Configuring Avaya Aura Session Border Controller*, May 2011

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

.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.