Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Aura® Session Border Controller to support TalkTalk Business Voice over Ethernet - Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between an Avaya SIP enabled enterprise solution and the TalkTalk Business Voice over Ethernet Service. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Aura® Session Border Controller connected to the TalkTalk Business Voice over Ethernet Service. TalkTalk is a member of the Global SIP Service Provider Compliance 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 an Avaya SIP enabled enterprise solution and TalkTalk Business Voice over Ethernet Service. The Avaya solution consists of Avaya Aura® Session Manager 6.1 and Avaya Aura® Communication Manager 6.0.1 connected to an Avaya Aura® Session Border Controller (AASBC). Customers using this Avaya SIP-enabled enterprise solution with the TalkTalk Business Voice over Ethernet Service are able to place and receive PSTN calls via a dedicated Internet connection, using SIP protocol. This converged network solution is offered as an alternative to traditional PSTN ISDN trunks. This approach generally results in lower operational costs and more flexibility 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 Session Manager and Communication Manager with all SIP traffic routed through an AASBC to the TalkTalk SIP network. The enterprise site was configured to use the SIP Trunk Service provided by Talk Talk.

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 TalkTalk. Incoming PSTN calls were made to H.323, SIP, Digital and Analog telephones at the enterprise side.
- Outgoing calls from the enterprise side were completed via the Voice over Ethernet Service to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made using H.323, SIP, Digital and Analogue telephones.
- Calls were made using G.729 and G.711A codecs.
- DTMF transmission using RFC 2833 with successful Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by TalkTalk requiring Avaya responses and sent by Avaya requiring TalkTalk responses.
- T.38 Fax transmission was tested in both directions, using G.711 and G.729 setup.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Voice over Ethernet Service with the following observations:

- The identity of an enterprise caller is hidden if the Calling Line Identity (CLI) is withheld at the enterprise side. In this scenario, the Voice over Ethernet Service trunk CLID is presented to the called party.
- Inbound PSTN calls which were answered and transferred to PSTN destinations failed, the call drops when the PSTN called party answers.
- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- Routing to emergency numbers (such as 999) was not tested.
- SIP Network Call Redirect (NCR) using REFER does not work, the Voice over Ethernet Service responds with a BYE message.

2.3. Support

For technical support on TalkTalk products please use the following web link.
http://www.talktalkbusiness.co.uk/contact-us/

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Voice over Ethernet Service. Located at the enterprise site are a Session Manager and Communication Manager. Endpoints are an Avaya Desktop Video Device, Avaya 9600 series IP telephones (H323 and SIP), Avaya 4600 series IP telephones (with H.323 firmware), Avaya 2400 series Digital telephone, an Analogue Telephone and a Fax machine. All SIP traffic from the enterprise site is via the AASBC. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

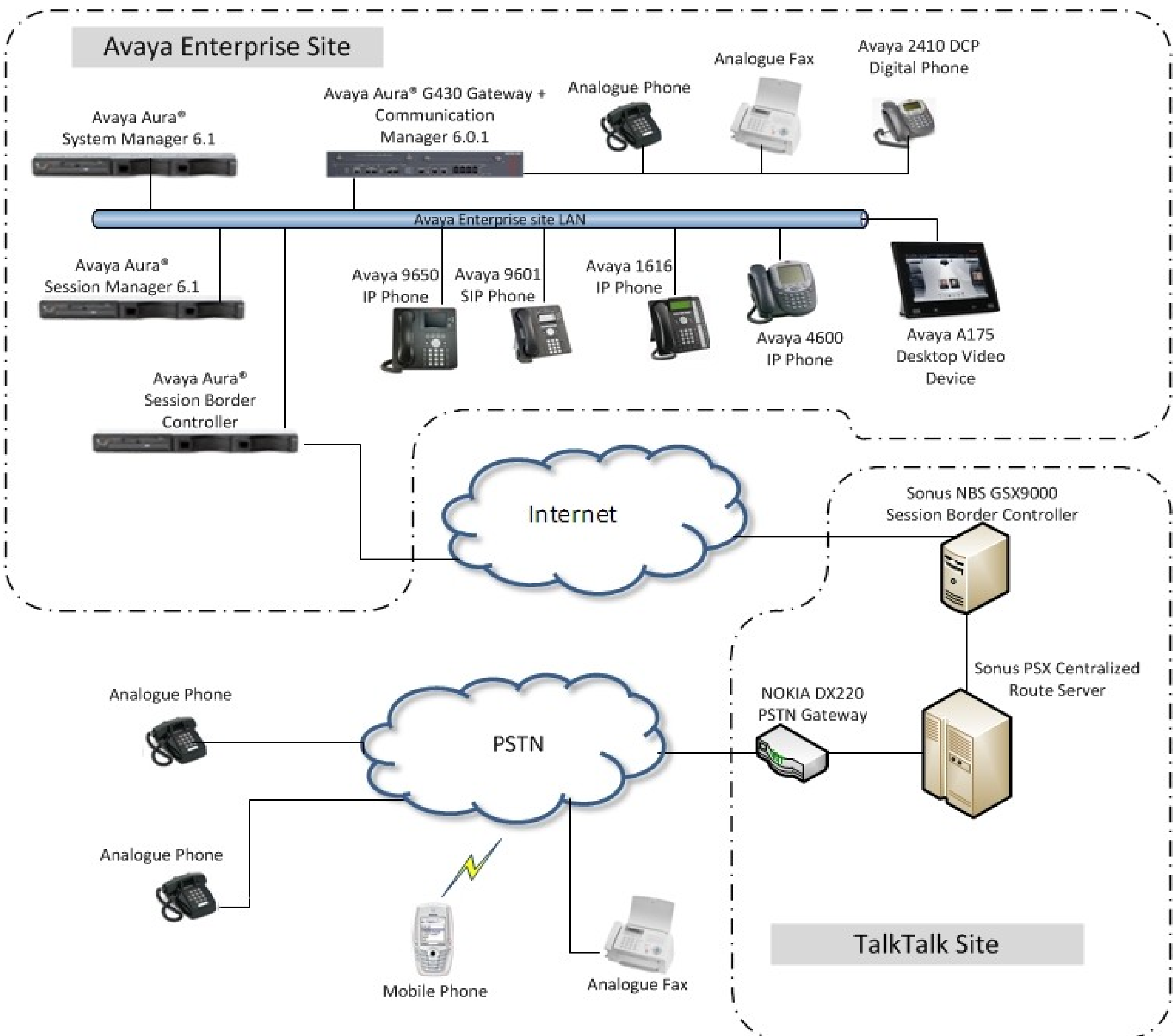


Figure 1: TalkTalk Test Configuration

4. Equipment and Software Validated

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

Equipment	Software
Avaya G430 Media Gateway MM711AP MM712AP	31.19.2 HW33 FW095 HW07 FW014
Avaya S8300D Media Server	Avaya Aura® Communication Manager R6.0.1 (6.1.3.0.613006)
Avaya S8800 Media Server	Avaya Aura® Session Manager R6.1 (6.1.3.0.613006)
Avaya S8800 Media Server	Avaya Aura® SBC E362P4 48236
Avaya S8800 Media Server	Avaya Aura® System Manager R6.1 6.1.5.0 Build Number 6.1.0.0.7345 Patch 6.1.5.112 Build Number 6.1.7.1.1260
Avaya Desktop Video Device	Avaya Flare® Experience Release 1.0.2
Avaya 9650 Phone (H.323)	3.102S
Avaya 9601 Phone (SIP)	2.6.4
Avaya 1616 Phone (H.323)	1.332B
Avaya 2410 Digital Phone	N/A
Avaya 4621 Phone (H.323)	2.9020
Analogue Phone	N/A
Service Provider	
Sonus NBS GSX9000 SBC	V07.02.10R000
Sonus PSX Centralizsed Route Server	V07.02.04R001
NOKIA DX220 PSTN Gateway	G4.1

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 Signaling associated with the Voice over Ethernet Service. For incoming calls, the Session Manager receives SIP messages from the TalkTalk network via the AASBC 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 and on to the TalkTalk 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 S8300D Server 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 TalkTalk 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: 4000  0
           Maximum Concurrently Registered IP Stations: 2400  5
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  0
                       Maximum Administered SIP Trunks: 4000  10
```

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
        (NOTE: You must logoff & login to effect the permission changes.)
```

Use the **display system-parameters features** command to verify the **Trunk-to-Trunk Transfer** field is set to y.

```
display system-parameters features                              Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
              Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

             Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n



            Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? 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. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SessionMngr** and **10.10.6.30** are the **Name** and **IP Address** for the Session Manager. Also note the **procr** name as this is the interface that the Communication Manager will use as the SIP signaling interface to Session Manager.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
SessionMngr         10.10.6.30
default             0.0.0.0
CMM                 10.10.6.13
procr               10.10.6.35
```

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 to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. This can remain at default.
- 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** will be used.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Defualt NR
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 20000                     IP Audio Hairpinning? n
   UDP Port Max: 65535
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. Enter the list of audio codecs eligible to be used in order of preference. For the interoperability test the codecs supported by TalkTalk were configured, namely G.711A and G.729.

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

                          IP Codec Set

    Codec Set: 1

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

On **Page 2** of the **IP Codec Set** form, configure the fax protocol by setting the **Fax Mode** to **t.38-standard,** as shown in the next screenshot.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:   384:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:   384:Kbits

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

5.5. Administer SIP Signaling Group

This signaling group (and trunk group) will be used for inbound and outbound PSTN calls to the Voice over Ethernet Service and will be configured using **tls** (Transport Layer Security) and a SIP port of **5061**. Configure the **Signaling Group** using the **add signaling-group** command as follows:

- Set the **Group Type** field to **sip**.
- The **Transport Method** field is set to **tls**.
- 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 **SessionMngr**), also shown in **Section 5.2**.
- Ensure that the recommended 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**.
- Ensure the **Far-end Domain** field is blank to allow calls from any domain.
- The **Direct IP-IP Audio Connections** field is set to **y**.

```
display signaling-group 2
                                SIGNALING GROUP

 Group Number: 2              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: SessionMngr
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         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** command. 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 previously configured in **Section 5.5**.
- Specify the **Number of Members** supported by this SIP trunk group.

```
add trunk-group 2                                                 Page   1 of  21
                                TRUNK GROUP

Group Number: 2                    Group Type: sip           CDR Reports: y
  Group Name: Outbound                    COR: 1        TN: 1        TAC: 702
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 2
                                                    Number of Members: 5
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a reasonable value to prevent unnecessary SIP messages during call setup. A value of **300** was used in this reference configuration.

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

TRUNK PARAMETERS

     Unicode Name: auto

                                           Redirect On OPTIM Failure: 5000

            SCCAN? n                              Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 300

 Disconnect Supervision - In? y  Out? y


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

On **Page 3** set the **Numbering Format** field to **private**.

```
add trunk-group 2                                                    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** 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.

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

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

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

5.7. 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 the Voice over Ethernet Service. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise telephone users will dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure or confirm **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: *01
         Abbreviated Dialing List2 Access Code: *02
         Abbreviated Dialing List3 Access Code: *03
Abbreviated Dial - Prgm Group List Access Code: *04
                      Announcement Access Code: *05
                       Answer Back Access Code: *06
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 0
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *07    Deactivation: #07
Call Forwarding Activation Busy/DA: *08    All: *09    Deactivation: #09
   Call Forwarding Enhanced Status: *10    Act: *11    Deactivation: #11
```

Use the **change ars analysis 0** 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 sample entries shown will match outgoing calls to numbers beginning 0. Calls are sent to **Route Pattern 2**, which will contain the previously configured **SIP Trunk Group 2**.

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

          Dialed           Total      Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd

    0                     9    14     2        pubu         n
    00                    3    14     2        pubu         n
```

Use the **change route-pattern 2** command to add the SIP trunk group to the route pattern that ARS selects. In this configuration entry **1** in **Grp No** will be set to the value **2**. Set the **Numbering Format** to **unk-unk**.

```
change route-pattern 2                                         Page   1 of   3
                    Pattern Number: 2   Pattern Name: Outgoing
                             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: 2    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
```

5.8. 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 TalkTalk 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 TalkTalk were mapped to the internal extensions assigned within Communication Manager. The entries displayed below translate incoming DID numbers starting with **0161** (obscured for security reasons) to a four or five digit extension. Each incoming DID number has a corresponding internal extension number associated with it and this extension number replaces all the digits in the incoming DID call.

```
change inc-call-handling-trmt trunk-group 2                     Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 tie             11 XXXXX780000      all 1531
 tie             11 XXXXX780001      all 59022
 tie             11 XXXXX780002      all 59024
 tie             11 XXXXX780003      all 59023
 tie             11 XXXXX780004      all 59027
 tie             11 XXXXX780005      all 59029
 tie             11 XXXXX780006      all 59021
 tie             11 XXXXX780007      all 1502
 tie             11 XXXXX780008      all 1543
 tie             11 XXXXX780009      all 1544
```

5.9. Administer Private Unknown Numbering

Use the change p**rivate-unknown-numbering 0** command to ensure outgoing calls have the correct Caller Line ID. Each outgoing call must be an E.164 number. The full public number is contained in the **Private Prefix,** which is populated with one of the assigned DID numbers. Each four or five digit telephone extension is mapped to a unique **Private Prefix**.

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

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 4  1502             2          XXXX780007       10    Total Administered: 9
 4  1531             2          XXXX780000       10       Maximum Entries: 540
 5  59021            2          XXXX780006       10
 5  59022            2          XXXX780001       10
 5  59023            2          XXXX780003       10
 5  59024            2          XXXX780002       10
 5  59026            2          XXXX780004       10
 5  59027            2          XXXX780008       10
 5  59029            2          XXXX780005       10
```

This completes the Communication Manager configuration steps. Save the 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:

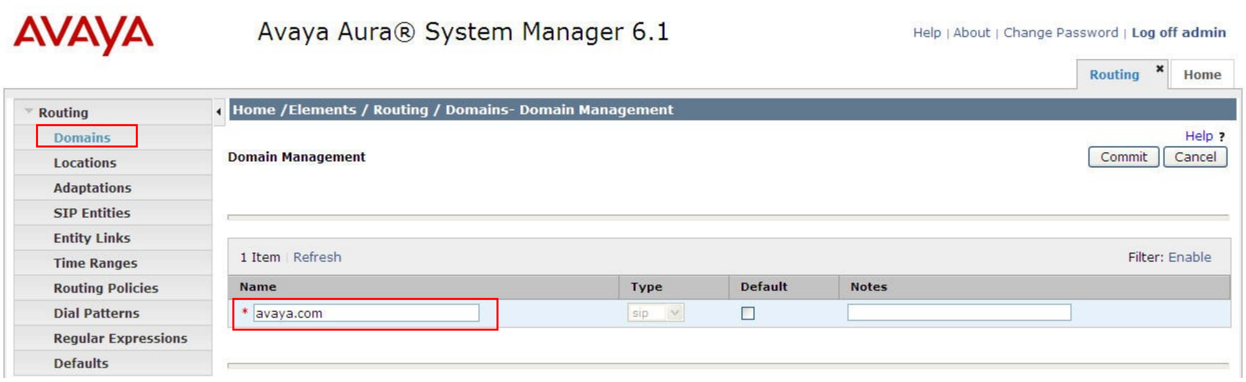
- Log in to Avaya Aura® Session Manager
- Administer SIP domain
- Administer Locations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Avaya Aura® Communication Manager
- Configure a SIP phone

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 page will be presented with menu options shown below.

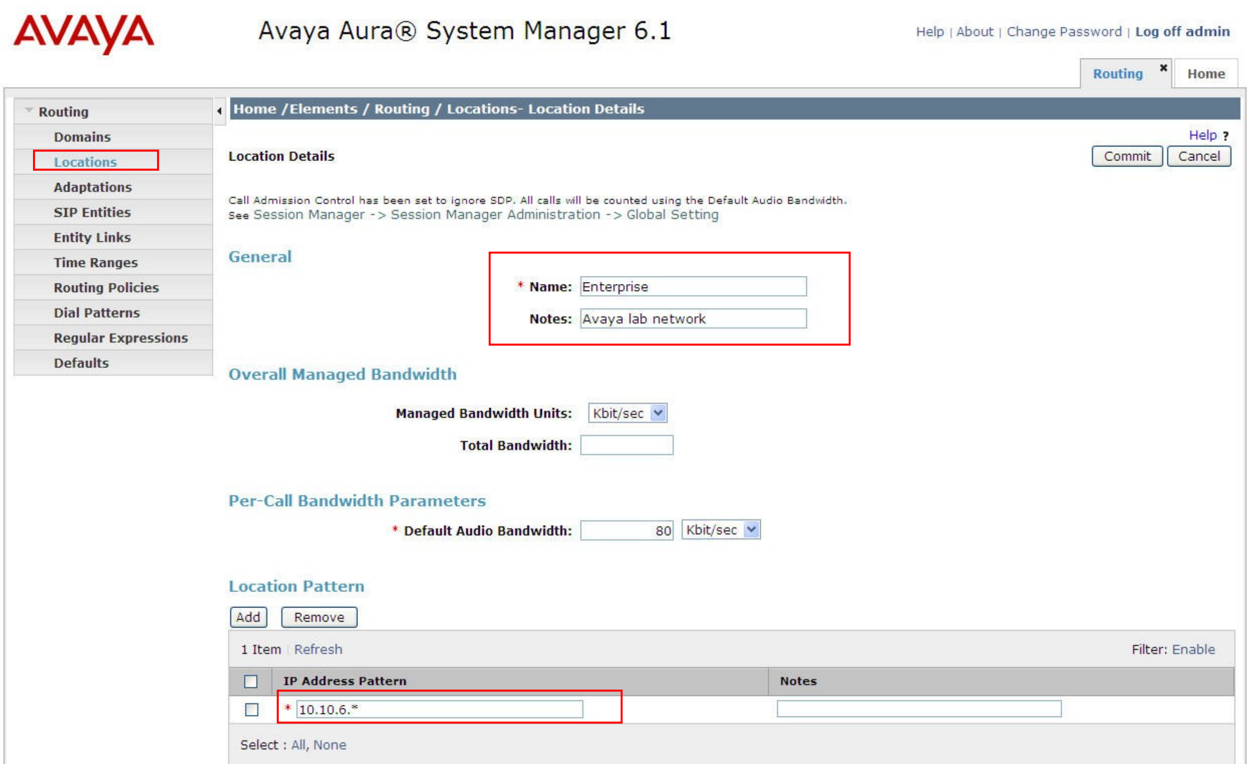
6.2. Administer SIP domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Elements Home** tab menu and in the resulting new page select **Domains** from left hand menu. Click the **New** button (not shown) to create a new SIP domain entry. In the **Name** field, enter the domain name (e.g., **Avaya.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes.



6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management. One location is added to the sample configuration for the enterprise SIP entities. Under the **Routing** tab, select **Locations** from the left hand menu and click the **New** button in the resulting page. 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 site. Click on the **Commit** button when finished.



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:**

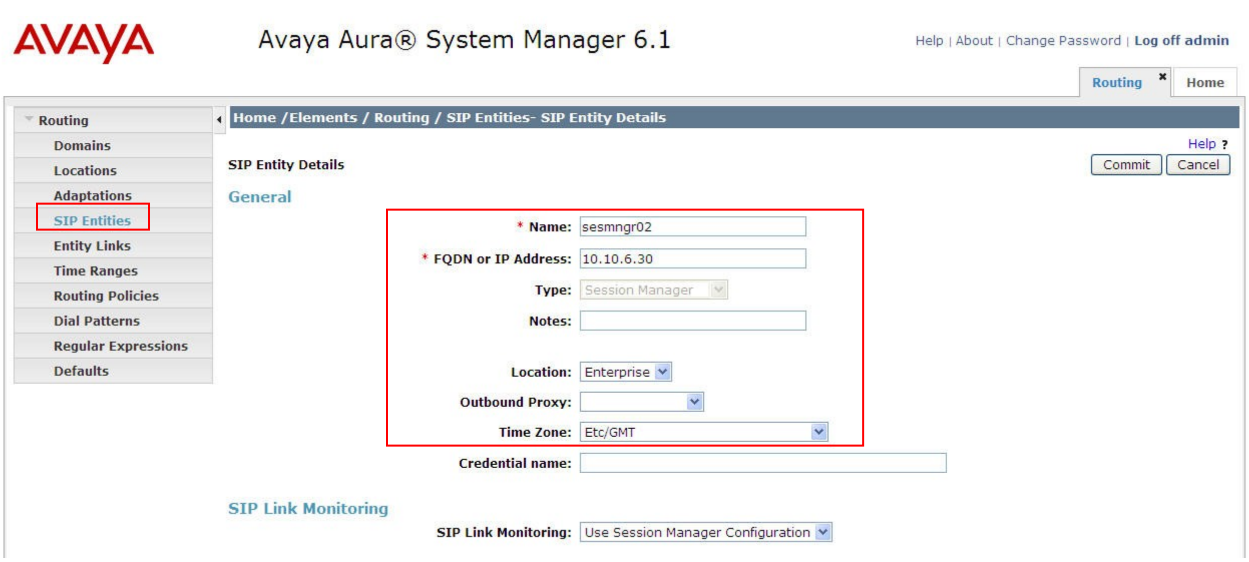
- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of the SIP entity being configured.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **Gateway** for the AASBC SIP entity.
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field select the time zone for the SIP Entity.

In this test configuration there are three SIP Entities configured.

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

6.4.1. Avaya Aura® Session Manager SIP Entity

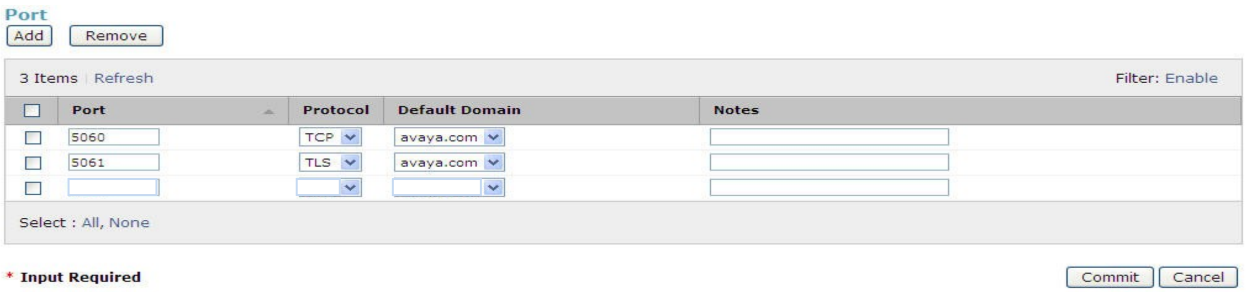
The following screens show the SIP entity for Session Manager. The **Name** is typically the Session manager hostname. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signaling interface. **Type** is set to Session Manager.



The Session Manager must be configured with the port numbers and the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the **SIP Entity Details** 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**.

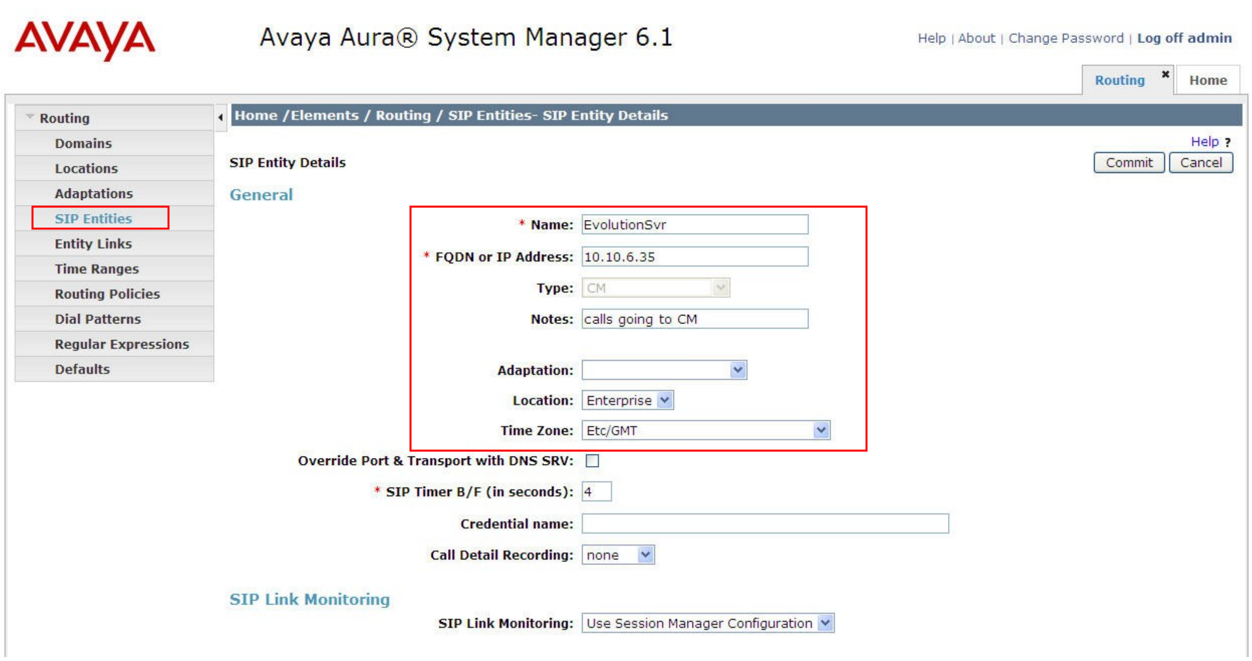
Two entries are required as different protocols will be used to communicate with each SIP entity. When finished, click of the **Commit** button. See the following screenshot for the configuration used.



6.4.2. Avaya Aura® Communication Manager SIP Entity

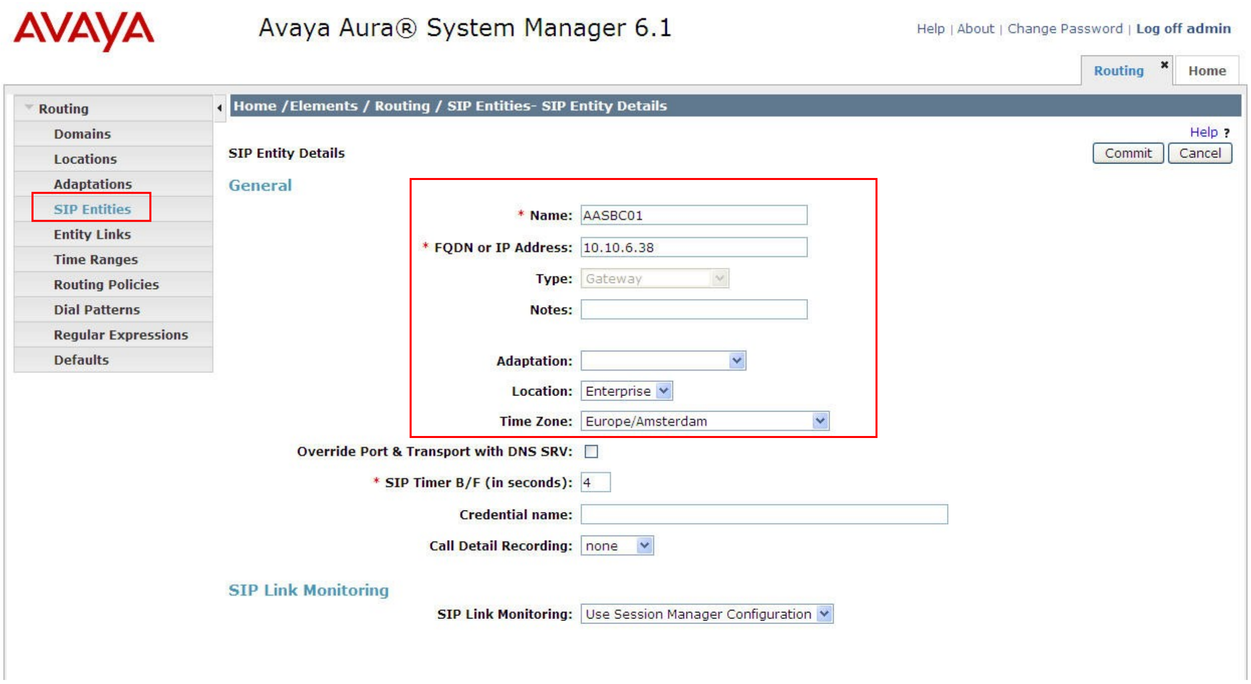
The following screen shows the SIP entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of the Interface that will be providing SIP signaling (value set in **Section 5.2** for **procr**).

Set the **Type** field to **CM** and click on the **Commit** button to save.



6.4.3. Avaya Aura® Session Border Controller SIP Entity

The ASSBC used for the SIP trunk connection to TalkTalk must be added to Session Manager as a SIP entity. The **FQDN or IP Address** field is set to the private side IP address of the SBC. See the following screenshot for **AASBC** entity configuration details.

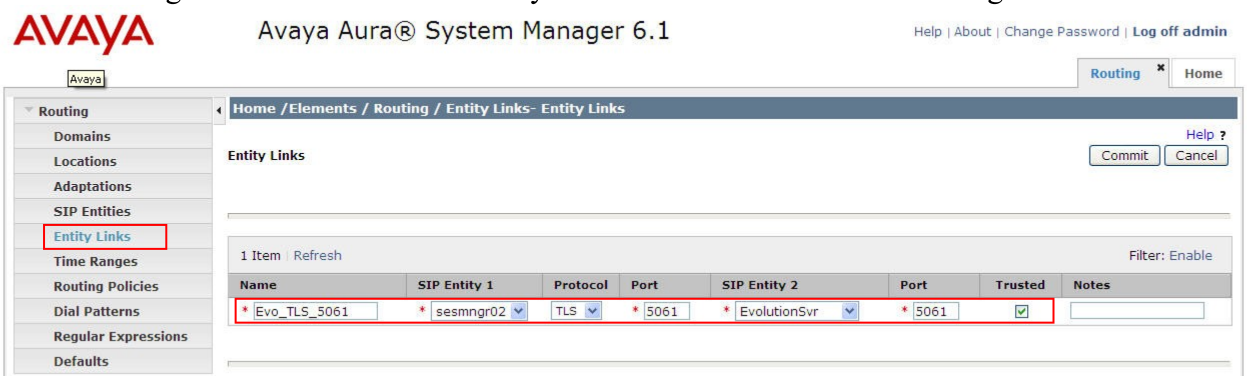


6.5. Administer Entity Links

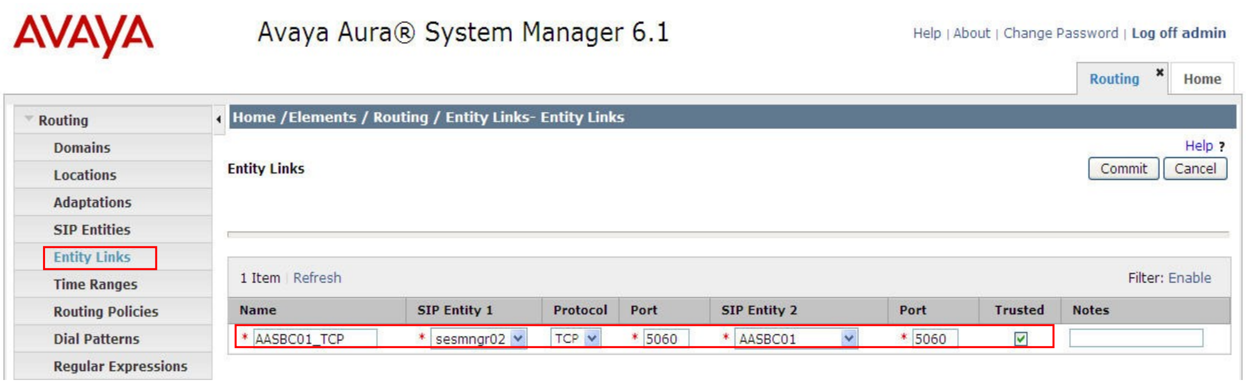
A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu of the following screenshot and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field always select **sessmngr02.**
- In the **Port** field **for SIP Entity 1**, enter the port number to which the other system sends the SIP requests.
- In the **SIP Entity 2** field enter one of the other SIP Entities created in **Sections 6.5**.
- In the **Port** field for **SIP Entity 2**, 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 select the transport protocol to be used to send SIP requests.

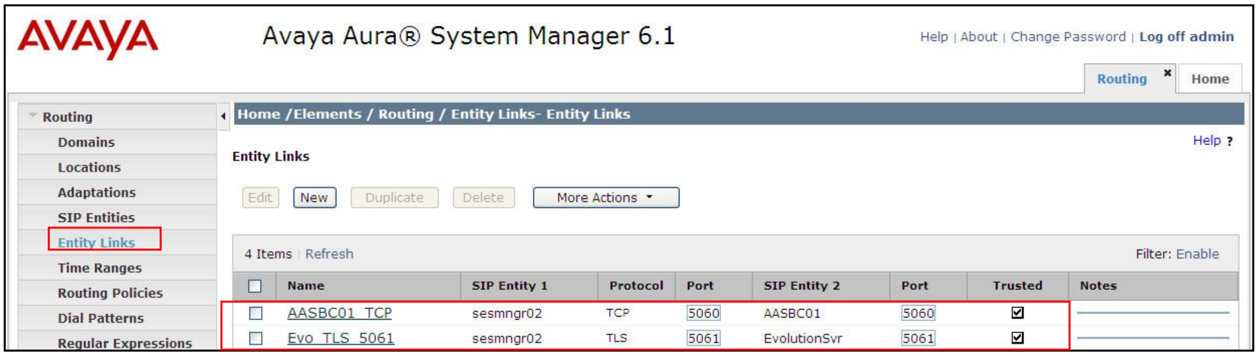
The following screenshot shows the Entity Link for the Communication Manger.



Repeat this step to configure the AASBC. The following screenshot shows the AASBC configuration. Click **Commit** to save the changes.



The following screen shows all the Entity Links used in this configuration.

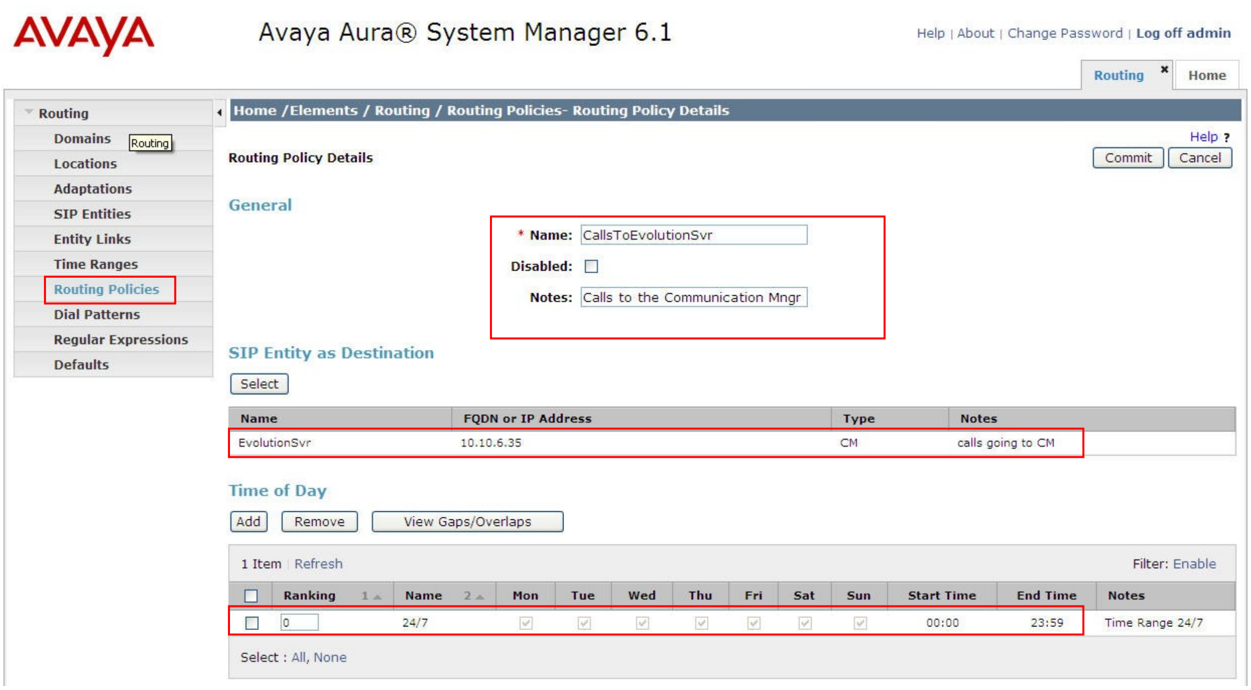


6.6. Administer Routing Policies

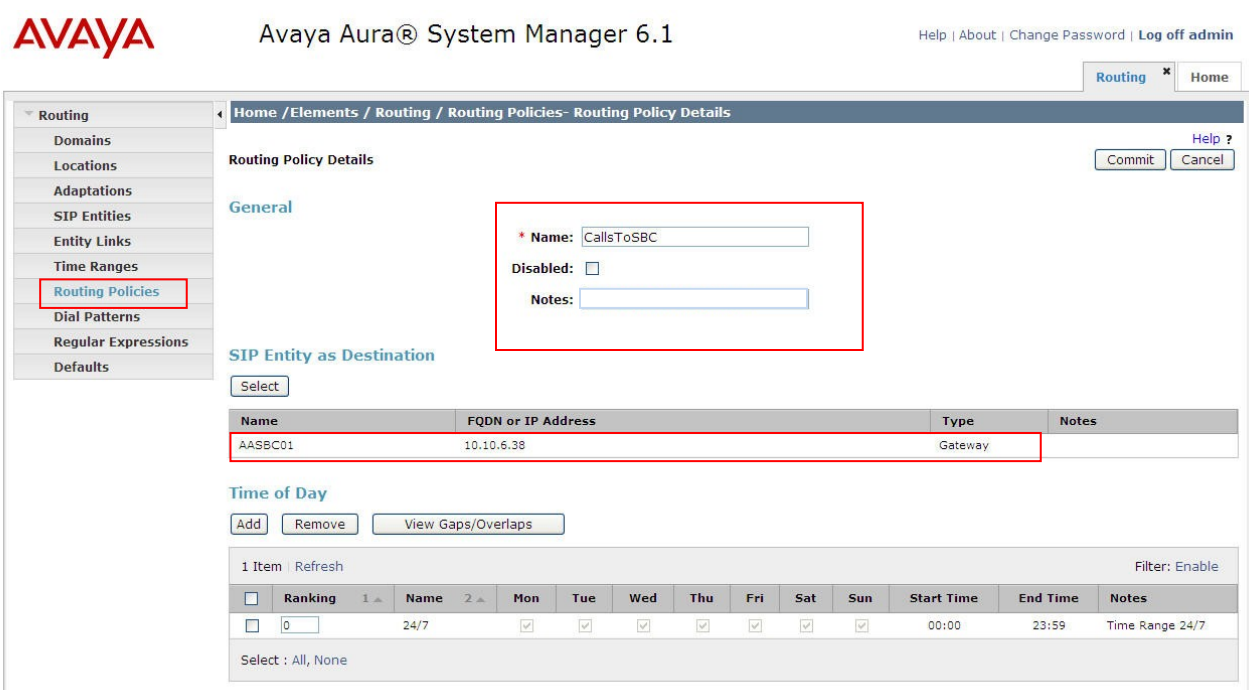
Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu (see next screenshot) and then click on the **New** button (not shown).

- Under **General** enter an informative name in the Name field.
- Under **SIP Entity as Destination**, click the **Select** button, a new page will appear (not shown) with a list of SIP entities. Select the appropriate SIP entity to which this routing policy will apply.
- Under **Time of Day**, click **Add**, and then set a time range with a **Start Time** of **00:00** and a **Stop Time** of **23:59**. Ensure each day of the week is checked.

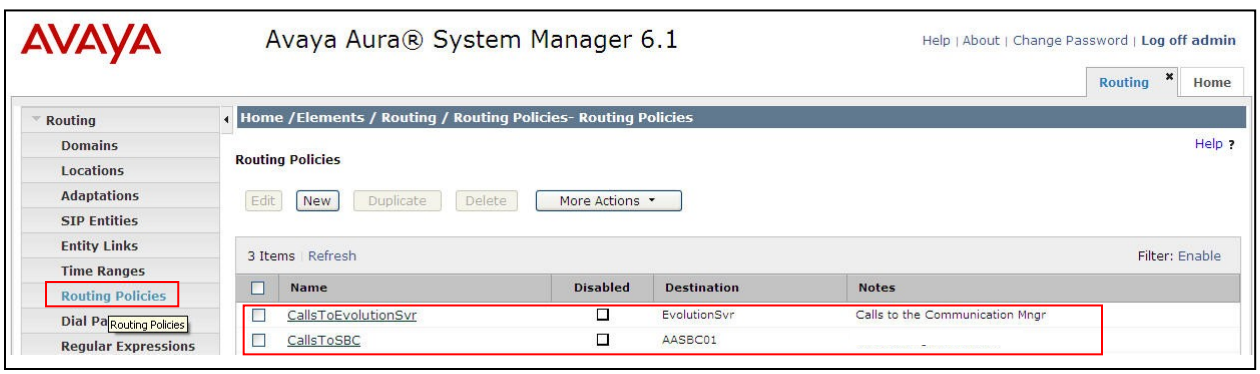
The following screen shows the routing policy defined for the Communication Manager SIP entity using the above procedure. The **SIP Entity as Destination** value is chosen as **EvolutionSvr** (previously configured in **Section 6.4.2**). The **Time of Day** is set to 24 hour by 7 day operation.



The following screenshot shows the routing policy created for the AASBC SIP entity defined in **Section 6.4.3**.



The next screenshot shows all routing policies used during TalkTalk compliance testing.

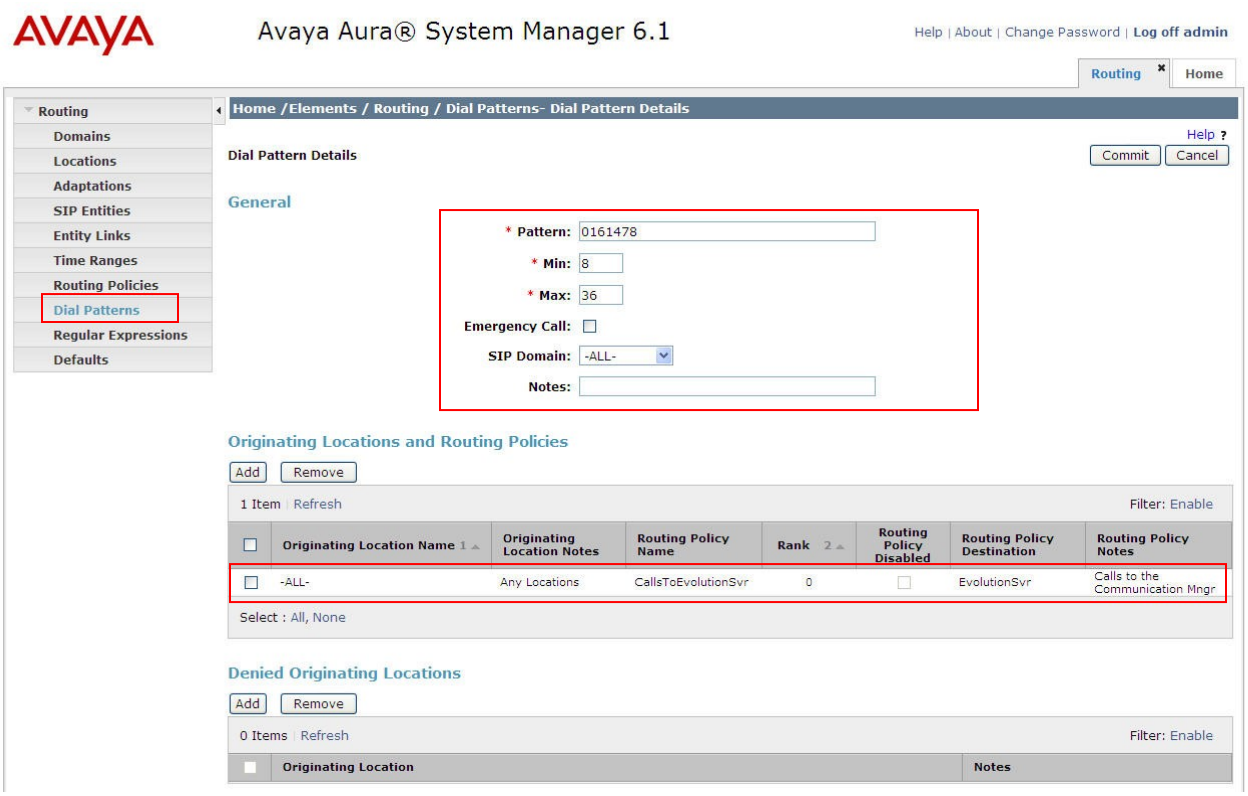


6.7. Administer Dial Patterns

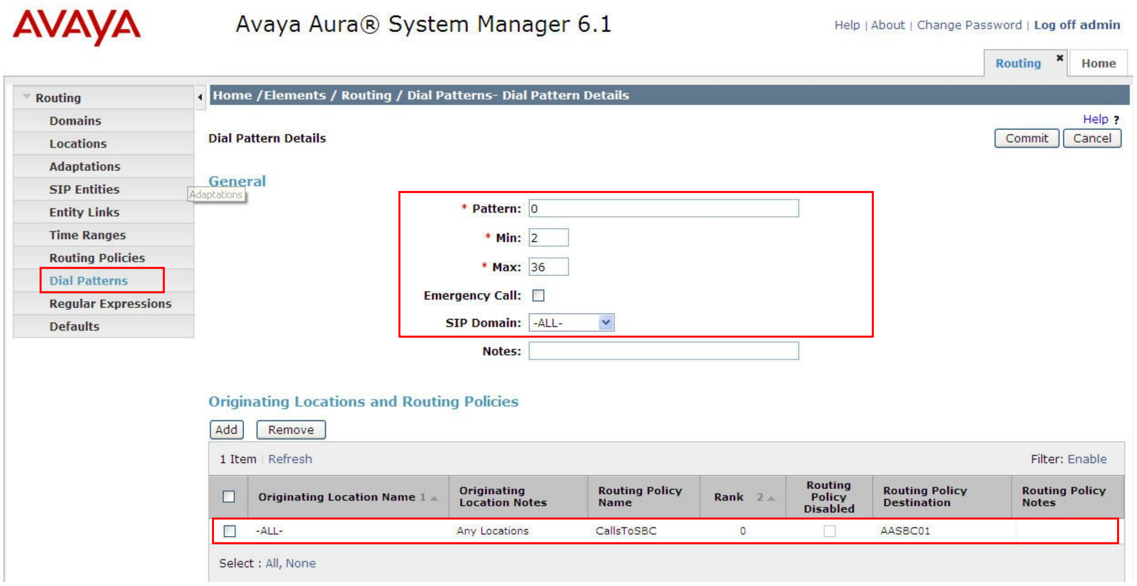
A dial pattern must be defined to direct calls to the appropriate telephony element. To configure a dial pattern select **Dial Patterns** on the left panel menu (see below) and then click on the **New** button (not shown). In section **General**:

- 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 value **ALL** from the drop down list.

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 a sample dial pattern configured for the Voice over Ethernet Service. All incoming calls beginning with 0161478 (first six digits of TalkTalk DID range assigned for test purposes) are sent to Communication Manager for further processing.

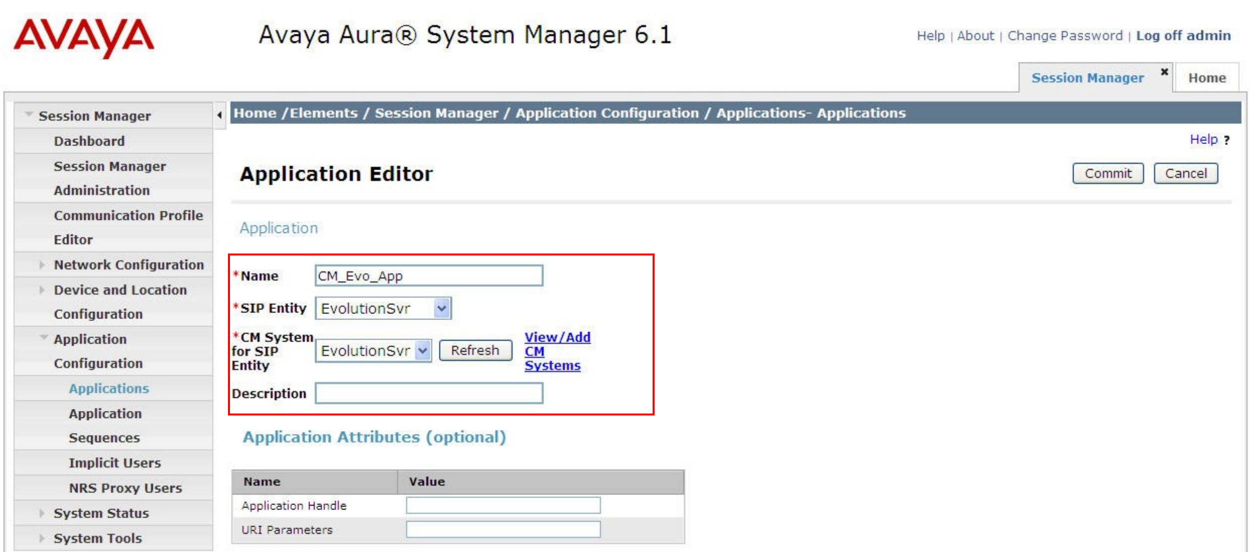


The following screen shows a sample dial pattern configured for calls to the AASBC.



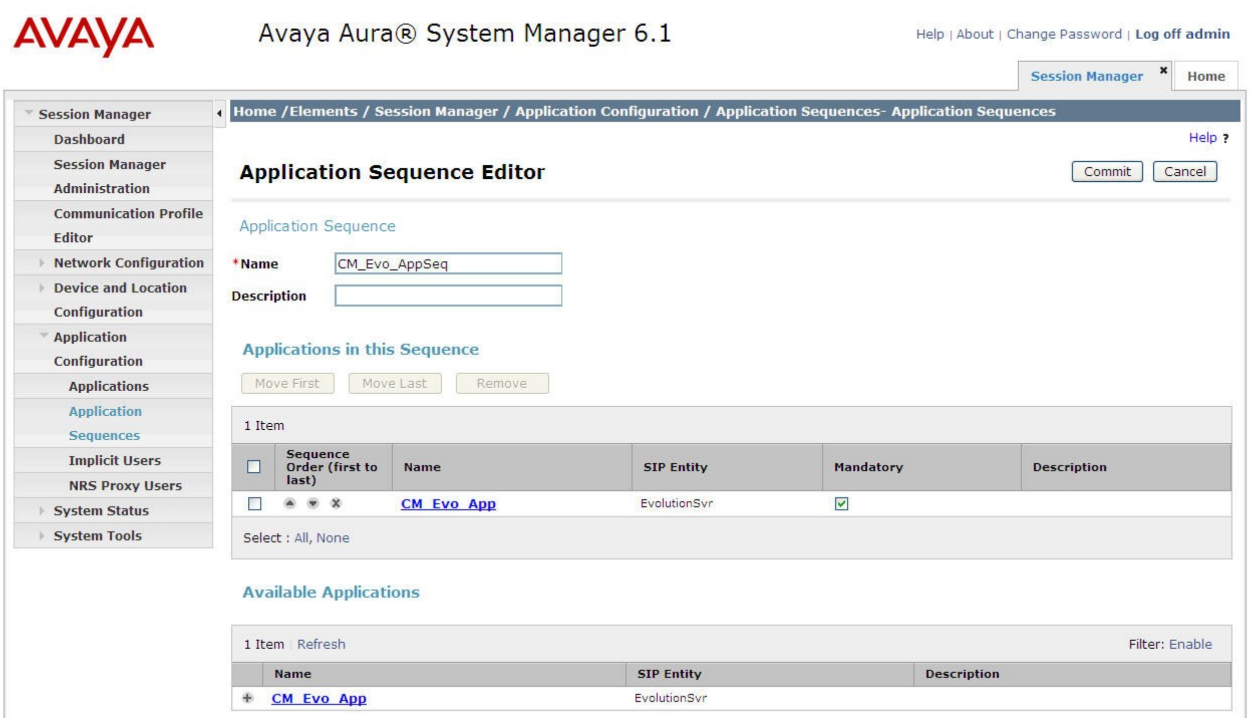
6.8. Administer Application for Avaya Aura® Communication Manager

SIP telephones require an application to be configured on Session Manager. To configure an application, click on **Application Configuration** then **Applications** from the side menu. Click on the **New** button (not shown) then enter a **Name** for the application, select Communication Manager (**EvolutionSvr**) defined in **Section 6.4.2** from the drop down list as the **SIP Entity**. Select **EvolutionSvr** as the **CM system for SIP Entity**. Text can be entered in the **Description** field to describe the application purpose. When finished, click on the **Commit** button.



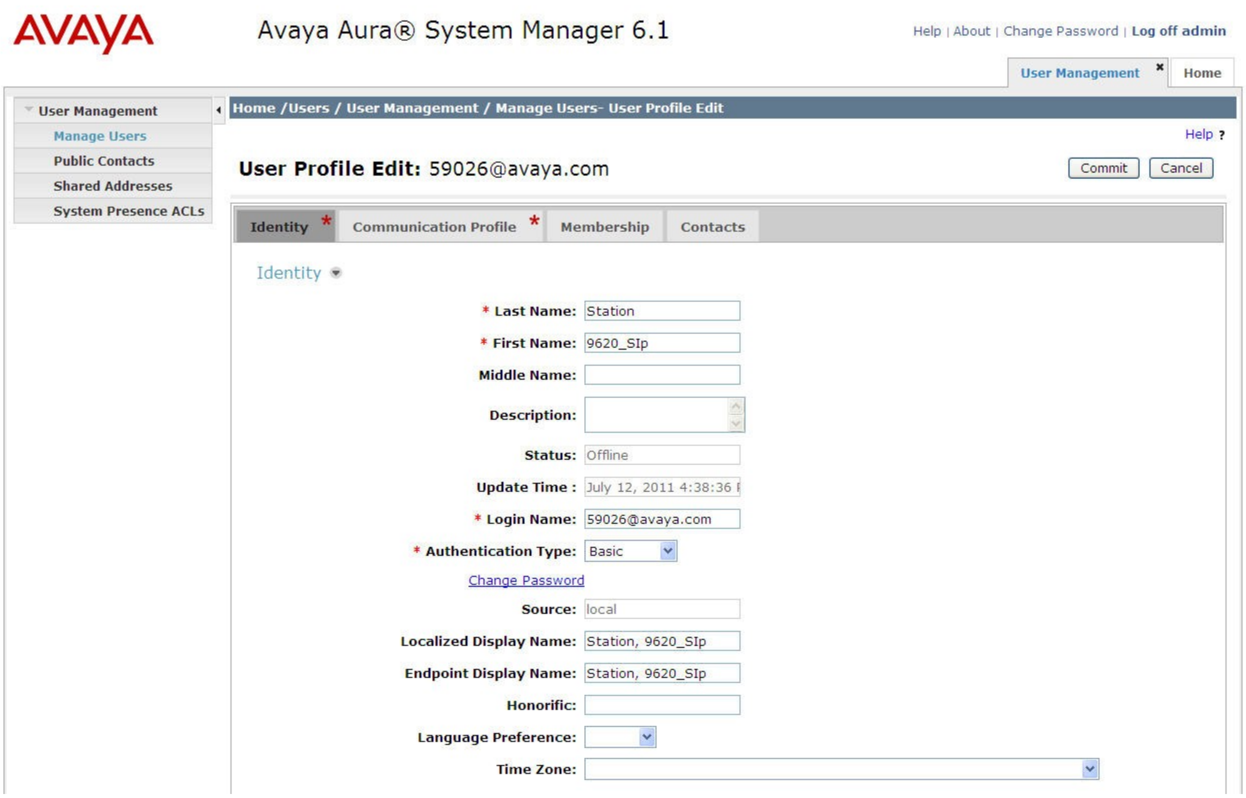
6.9. Administer Application Sequence for Avaya Aura® Communication Manager

Click on **Application Configuration** in the side menu, and then click on **Application Sequences**. Click on the **New** button (not shown), then enter a **Name** for the application sequence. Move down the page to the **Available Applications** area and click on the plus symbol next to the application sequence created in the previous step (see following screenshot). Ensure the sequence just added is the first (or only) application in this sequence; use the **Move First** and **Move Last** buttons to change the application order. Click on the Commit button when finished.

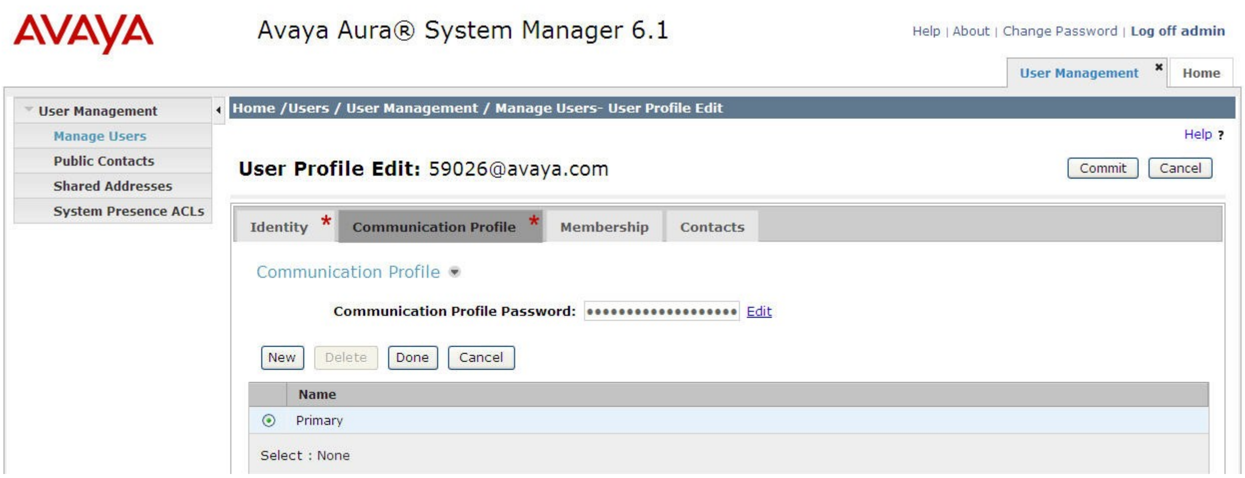


6.10. Configure a SIP phone

SIP telephones are configured on the Session Manager. Click on the **User Management** entry in the **Home** menu, and then select the **Manage Users** entry from the side menu. Click on the **New** button (not shown). Click on the **Identity** tab and fill in the user's **First** and **Last** names. Configure a **Login Name** and **Password** for the user. The **Localized Display Name** and **Endpoint Display Name** fields are auto populated based on the values entered for the user's first and last names. See the following screenshot for an example of a SIP telephone configuration.



When ready, click on the **Communication Profile** tab. Enter the user's **Communication Profile Password** (this is the SIP phone logon password).



Move down the page to the **Communication Address** area, click on the **New** button (not shown) and select Avaya SIP from the **Type** drop down list. Enter the same value for **Fully Qualified Address:** as used previously for Login Name: (see the first screenshot in **Section 6.10**). Click the **Add** button when completed.

The following screenshot shows the configured Communication Address.

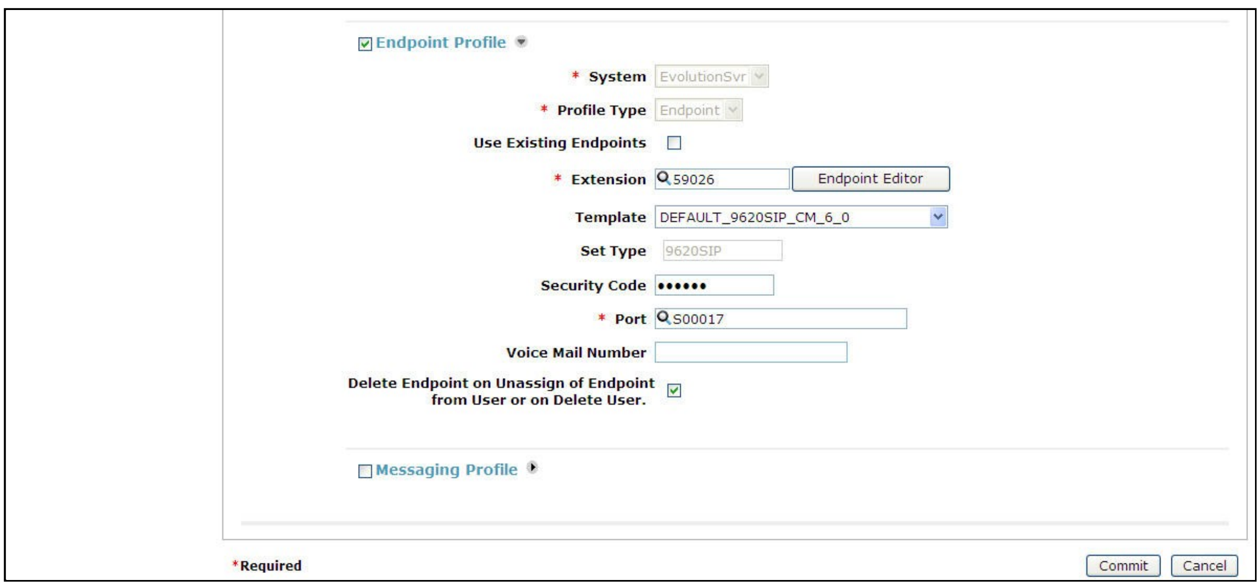
Scroll down the page to the **Session Manager Profile** section, click the checkbox and click on the arrow to the right. Enter the following values:

- For **Primary Session Manager**, select the name configured in **Section 6.4.1**.
- For **Origination Application Sequence**, select the name configured in **Section 6.9**.
- For **Termination Application Sequence**, select the name configured in **Section 6.9**.
- For **Home Location**, select the location configured in **Section 6.3**.

Scroll down to the **Endpoint Profile** section, click the checkbox and click on the arrow to the right. Enter the following values:

- For **System**, select the Communication Manager previously configured in **Section 6.4.2**.
- Set the **Profile Type** to Endpoint.
- Populate the **Extension** box with a phone number.
- Select the correct template for the SIP phone being configured.
- Enter a **Security Code** (a string of digits).
- Ensure the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** checkbox is ticked.

Click on the **Commit** button when finished. The following screenshot shows the **Endpoint Profile** configuration used. This completes the configuration required for the Session Manager.



7. Configure Avaya Aura® Session Border Controller

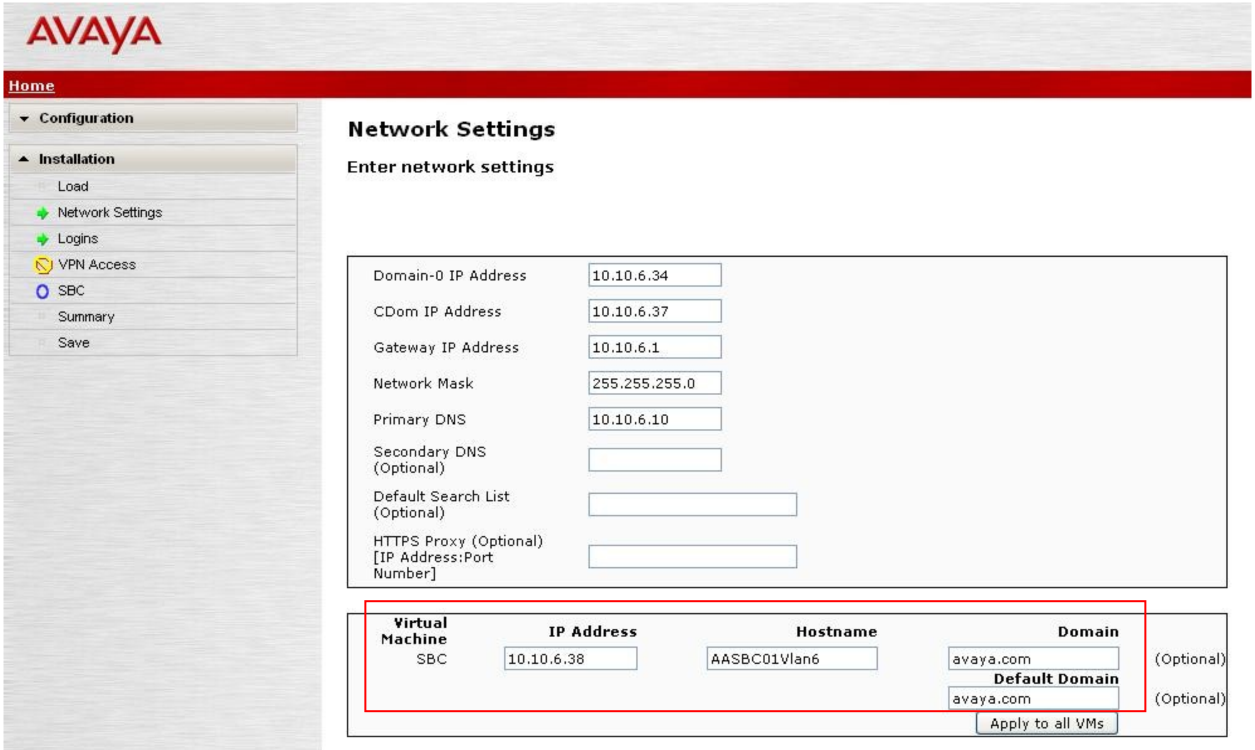
This section shows the configuration for AASBC to allow routing of SIP messages from the Session Manager to the Voice over Ethernet Service. These Application Notes will not cover the AASBC installation in its entirety but will include the use of the installation wizard. For information on installing the System Platform and the loading of the AASBC template see documents **[1]** and **[2]** in **Section 11**.

7.1. Installation Wizard

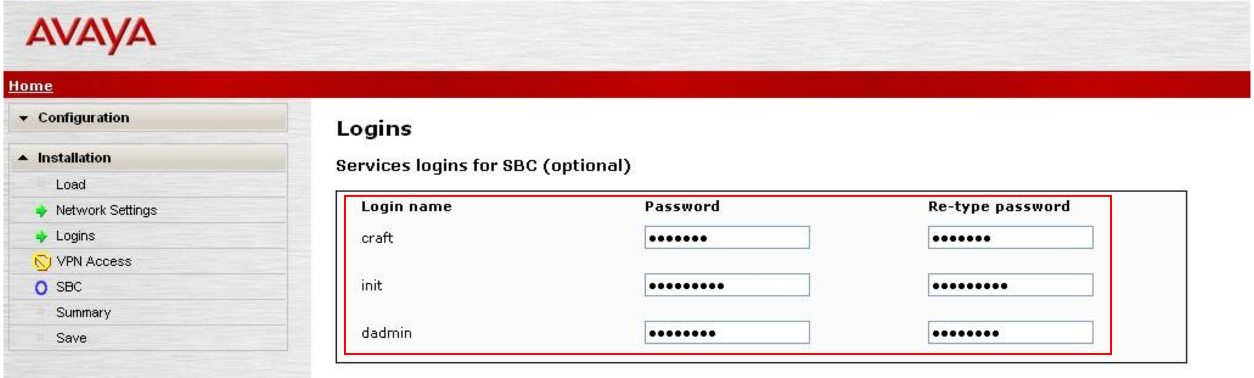
During the installation of the AASBC template, the installation wizard will prompt the installer for information which will be used to create the initial configuration of the SBC. The first screen of the installation wizard is the **Network Settings** screen. Fill in the fields as described below and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

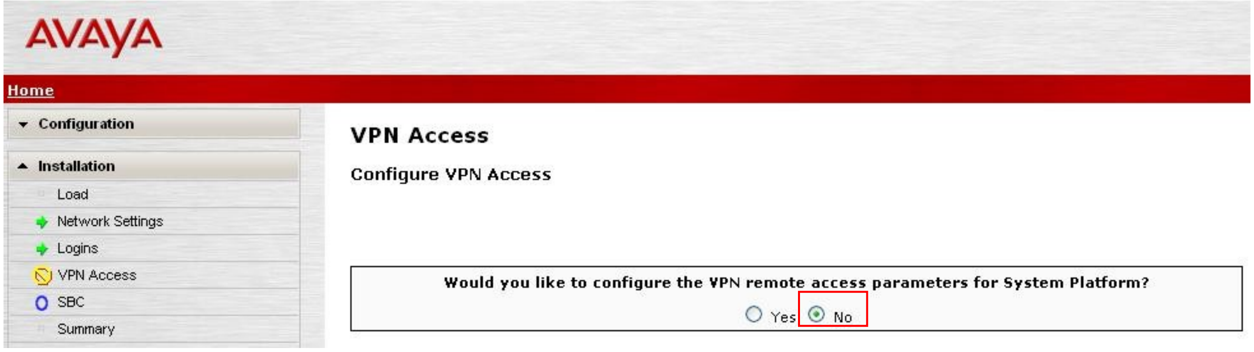
Click **Next Step** (not shown) to continue.



From the **Logins** screen (see next screenshot) specify passwords for the services logins to the AASBC. Click **Next Step** (not shown) to continue.



VPN remote access to the SBC was not required for the compliance test. Therefore on the **VPN Access** screen, select **No** to the question, **Would you like to configure the VPN remote access parameters for System Platform?** (see the following screenshot). Click **Next Step** (not shown) to continue.

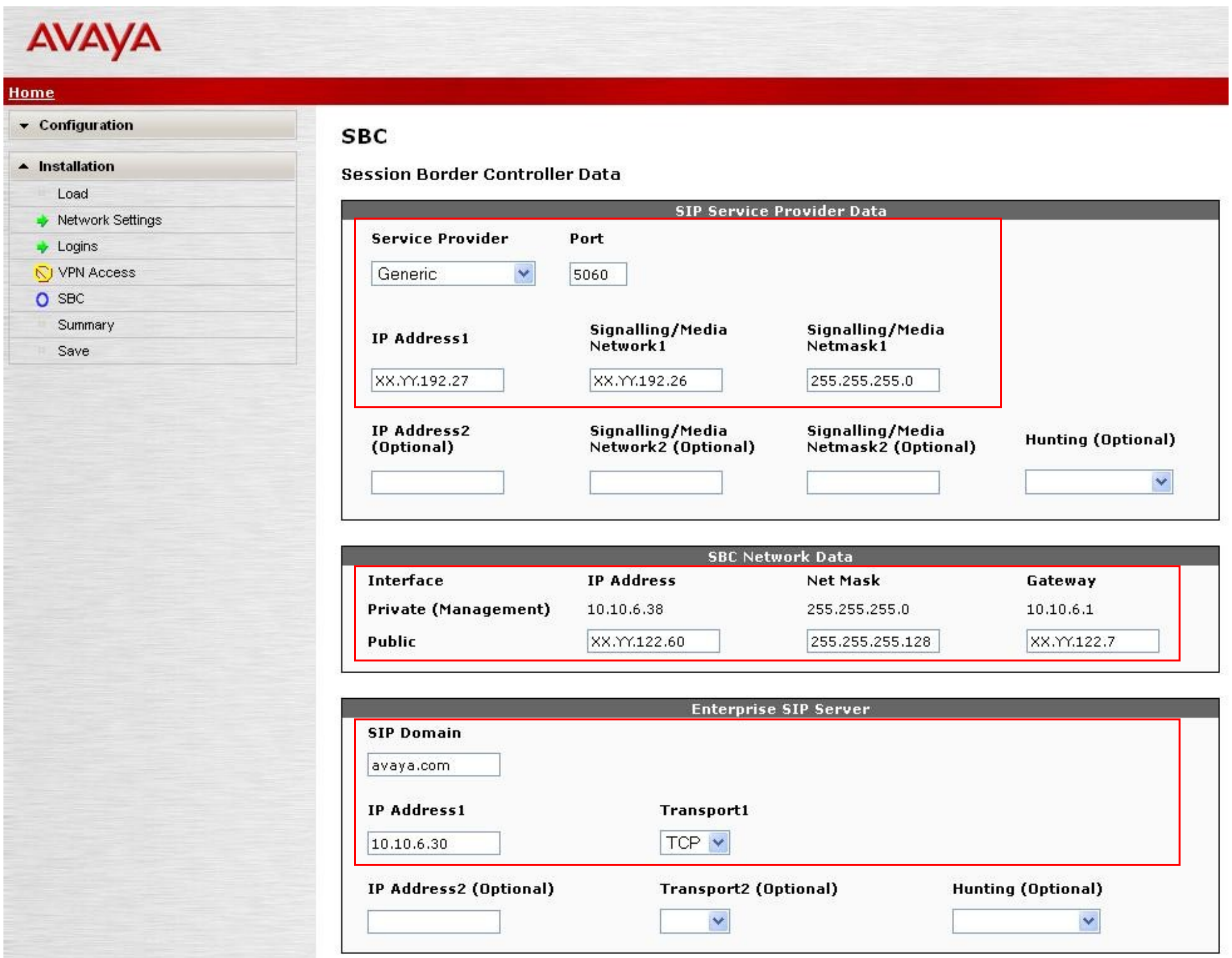


On the **SBC** screen, fill in the fields as described below and shown in the following screenshot:

- In the **Service Provider** area select the name of the **Service Provider** the AASBC will connect to. This allows the wizard to select a pre-existing configuration file. At time of compliance testing a configuration file did not exist for the Voice over Ethernet Service, therefore **Generic** was chosen.
- In the **Port** field enter the port number the Voice over Ethernet Service uses for SIP traffic.
- In the **IP Address1** field enter the public SIP signaling IP address of the Sonus NBS GSX9000 SBC (SIP Trunk provider equipment - see **Figure 1**).
- In the **Signaling/Media Network1** field enter the public media traffic IP address of the Sonus NBS GSX9000 SBC (see **Figure 1**). In the **Signaling/Media Netmask** field enter the netmask corresponding to the Media Network.
- In the **Public IP Address** field enter the IP address of the public side of**AASBC**.
- In the **Public Net Mask** field enter the netmask associated with the public network to which the SBC connects.

- In the **Public Gateway** field enter the default gateway of the public network.
- In the **IP Address1** 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** (not shown) 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. This completes the AASBC configuration.



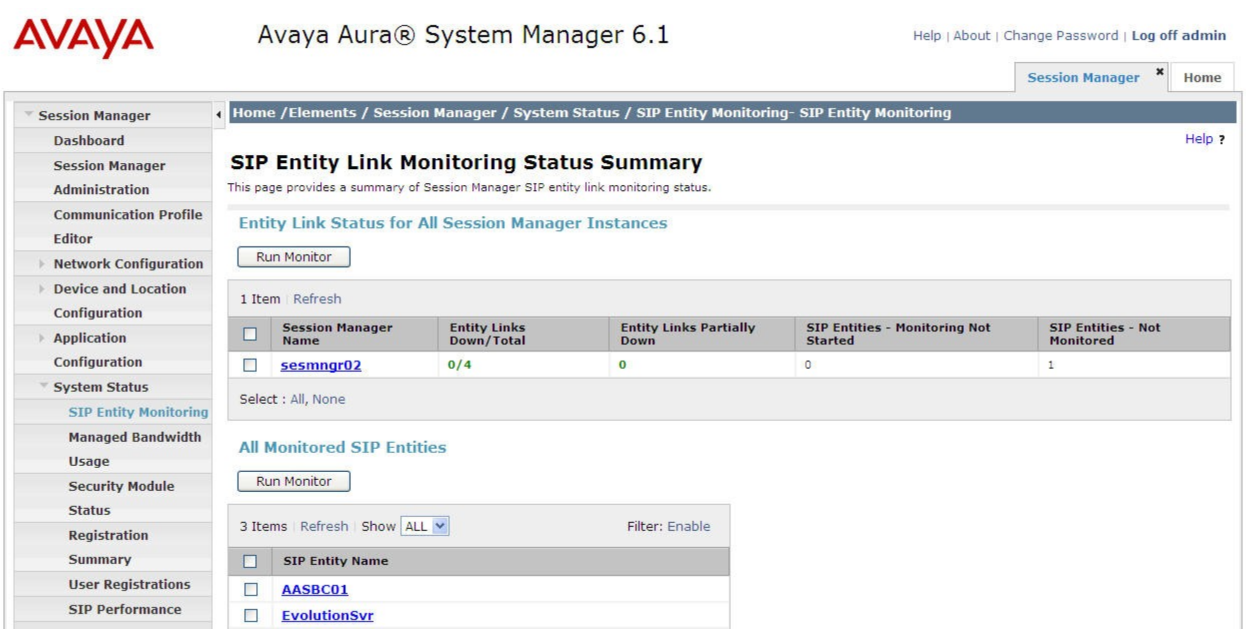
8. SIP Provider Trunk configuration

Other than the basic network diagram and general configuration for the SIP Trunk solution testing shown in **Figure 1**; specific Voice over Ethernet Service configuration and discussion of the operational and technical characteristics are outside the scope of these Application Notes. Please contact TalkTalk using the contact details provide in **Section 2.3** for detailed information on their Voice over Ethernet Service.

9. Verification Steps

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

1. From System Manager left hand side menu, click on **Session Manager** and navigate to **System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Entity Links Down** and **Entity Links Partially Down** values are greater than zero. Check the **SIP Entity Name** in the **All Monitored SIP Entities** area. See the following screenshot for details.



2. From the Communication Manager SAT interface run the command **status trunk 2** where **2** is the previously configured SIP trunk group (see **Section 5.6**). Observe whether all channels on the trunk group display **in-service/ idle**.

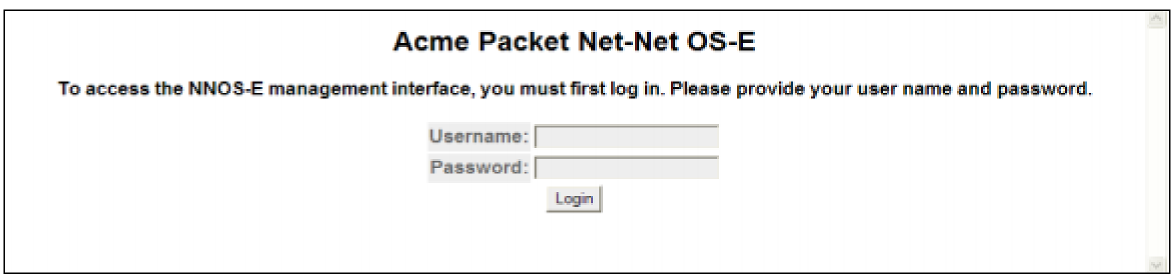
```
status trunk 2

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0002/001 T00001   in-service/idle    no
0002/002 T00007   in-service/idle    no
0002/003 T00008   in-service/idle    no
0002/004 T00009   in-service/idle    no
0002/005 T00010   in-service/idle    no
```

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call remains active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Access the Avaya Aura® SBC using a web browser by entering the **URL https://<ip-address>**, where **<ip-address>** is the private IP address configured.
   A logon screen is presented, logon with a valid **Username** and **Password** and confirm access is granted to the configuration screens (not shown).



10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager and Avaya Aura® Session Manager to TalkTalk Business Voice over Ethernet Service. It was observed during testing that inbound calls which were transferred (either supervised or unsupervised) to PSTN destinations failed to complete (call dropped after 2 seconds). Inbound calls which were redirected using the SIP REFER method to PSTN destinations also failed.

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,* May 2009, *D*ocument 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*, January 2011, Document Number 03-603473
[7] *Administering Avaya Aura® Session Manager,* March 2011, Document Number 03-603324.
[8] RFC 3261 *SIP: Session Initiation Protocol,* http://www.ietf.org/

For information on TalkTalk please use the contact information provided in **Section 2.3**.

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.