Application Notes for Configuring Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to support BT Global Services NOAS SIP Trunk - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between BT Global Services NOAS SIP Trunk and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Aura® Communication Manager as an Evolution Server, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise. BT is a member of the DevConnect Service Provider program.

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

1. Introduction

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

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Avaya SBCE. The enterprise site was configured to use the SIP Trunk service provided by BT.

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from mobile phones using the SIP Trunk provided by BT, calls made to SIP and H.323 telephones at the enterprise
- Outgoing fixed and mobile calls from the enterprise site completed via BT to PSTN and mobile destinations, calls made from SIP and H.323 telephones
- Calls using the G.711A and G.729A codecs
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones
- Call coverage and call forwarding for endpoints at the enterprise site
- Transmission and response of SIP OPTIONS messages sent by BT 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 Wholesale SIP Trunk service with the following observations:

- Inbound call hold and resume from BT was not tested as BT is unable to initiate the call-hold due to their environment set-up.
- PSTN called party hang-up during an active call did not cause the call to drop. Communication Manager caller must hang-up first, or wait for the PSTN T2ISUP timer to expire.
- When an outgoing call is attempted and there are no matching codes in the SDP offer and answer, the calls are not rejected by the network. Instead they are accepted and the media quality is very poor in line with mismatched codec's.
- G729 annex b (silence suppression) is not supported by BT SIP Trunk Service and thus was not tested.
- Incoming Toll-Free numbers were not tested as they were not available for test.
- Emergency Calls were not tested as a test call was not booked with the Operator

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 use the following web link. http://btbusiness.custhelp.com/app/contact

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the BT NOAS SIP Trunk service. Located at the Enterprise site is an Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96xx, 46xx series IP telephones (with SIP and H.323 firmware), Avaya digital telephones, Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was Avaya one-X® Communicator and Avaya Flare Experience for Windows softphones running on a laptop PC configured for SIP & H.323.

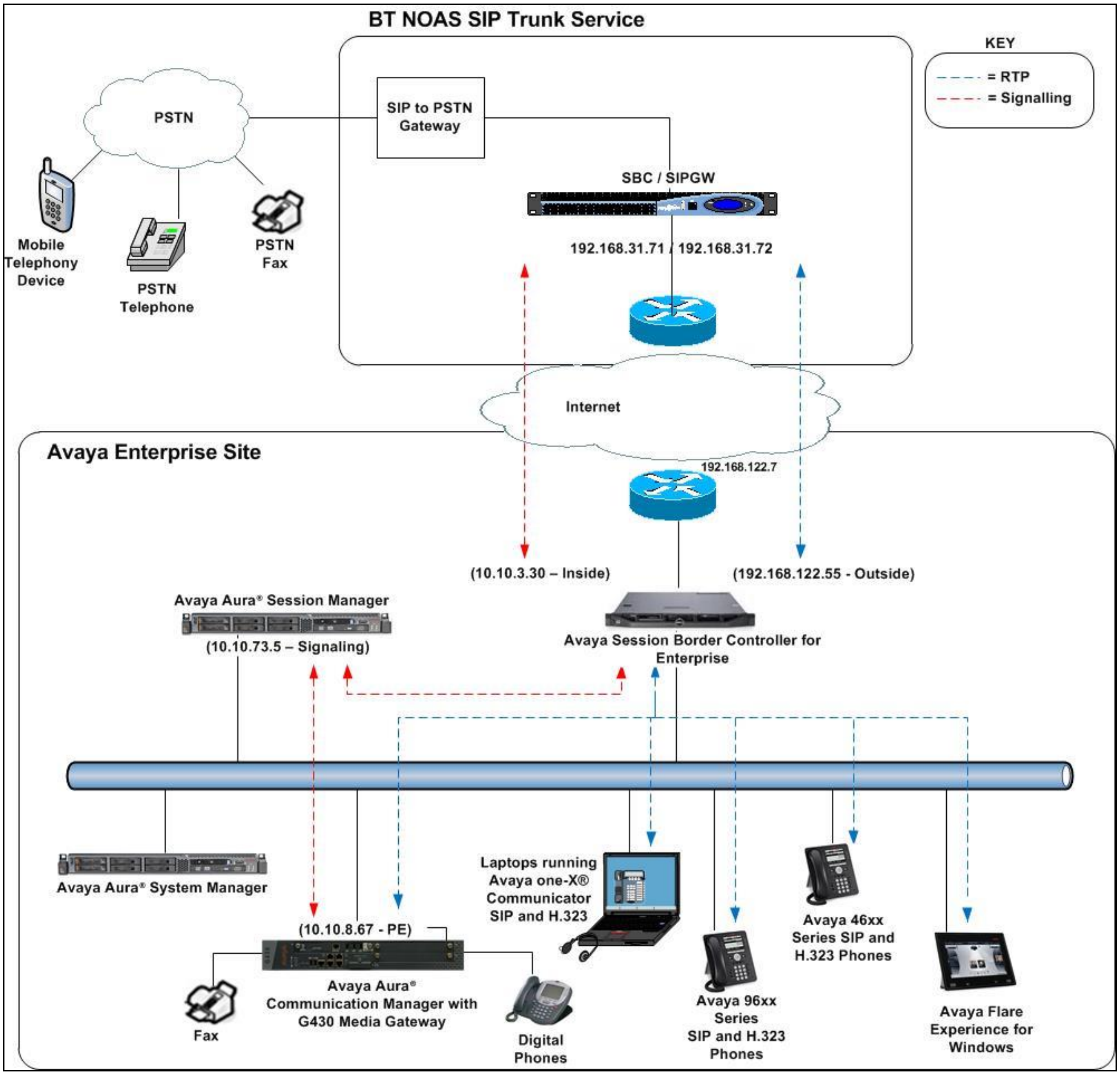

BT NOAS SIP Trunk Service
KEY
- - - - = RTP
- - - - = Signalling
PSTN
SIP to PSTN Gateway
SBC / SIPGW
192.168.31.71 / 192.168.31.72
Mobile Telephony Device
PSTN Telephone
PSTN Fax
Internet
Avaya Enterprise Site
192.168.122.7
(10.10.3.30 – Inside)
(192.168.122.55 - Outside)
Avaya Aura® Session Manager
(10.10.73.5 – Signaling)
Avaya Session Border Controller for Enterprise
Avaya Aura® System Manager
Laptops running Avaya one-X® Communicator SIP and H.323
(10.10.8.67 - PE)
Avaya Aura® Communication Manager with G430 Media Gateway
Fax
Digital Phones
Avaya 96xx Series SIP and H.323 Phones
Avaya 46xx Series SIP and H.323 Phones
Avaya Flare Experience for Windows

Figure 1: BT NOAS to Avaya Enterprise SIP Trunk Topology

4. Equipment and Software Validated

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

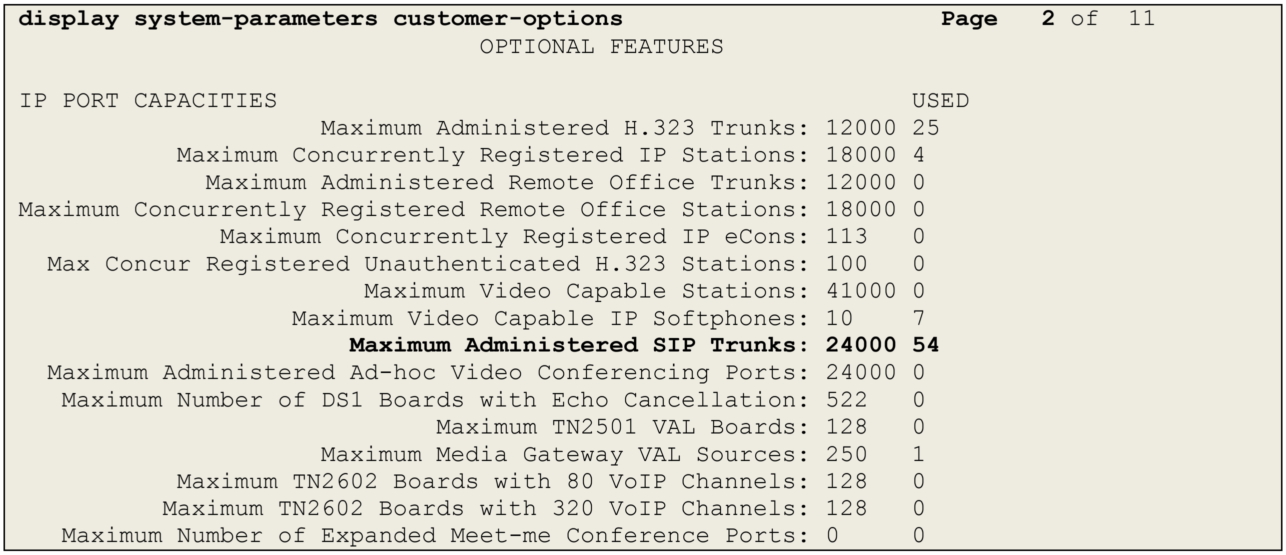
Equipment/Software	Release/Version
Avaya	
Dell PowerEdge R620 running Session Manager on VM Version 8	R6.3.6 - 6.3.6.0.636005
Dell PowerEdge R620 running System Manager on VM Version 8	R6.3.6 - Build No. - 6.3.0.8.5682-6.3.8.3007 Software Update Revision No: 6.3.6.6.2103
Avaya S8800 Server running Communication Manager	R016x.03.0.124.0 -21291
Avaya Session Border Controller for Enterprise	6.2.1.Q07
Avaya 9670 IP Deskphone (H.323)	6.3
Avaya 9621 IP Deskphone (SIP)	6.2.2
Avaya 9611 IP Deskphone (SIP)	6.2.2
Avaya 9608 IP Deskphone (SIP)	6.2.2
Avaya 9641 IP Deskphone (SIP)	6.2.2
Avaya 9608 IP Deskphone (SIP)	R6.2 SP1
Avaya Flare Experience for Windows	1.1.3.14
Avaya one–X® Communicator on Lenovo T510 Laptop PC	6.1.8.06-SP8-40314
Avaya 2420 Digital Handset	R6
Analogue Handset	N/A
Analogue Fax	N/A
BT	
Acme Packet Net-Net 4250 Session border Controller	SC6.1.0 MR-11 patch 1 (build 1036)

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP signalling associated with the BT NOAS SIP Trunk service. For incoming calls, Session Manager receives SIP messages from the Avaya SBCE and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to Session Manager. Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that 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 Servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the BT NOAS 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 25
           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: 41000 0
                   Maximum Video Capable IP Softphones: 10    7
                       Maximum Administered SIP Trunks: 24000 54
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

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

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

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                        ISDN Feature Plus? 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? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                 Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
```

5.2. Administer IP Node Names

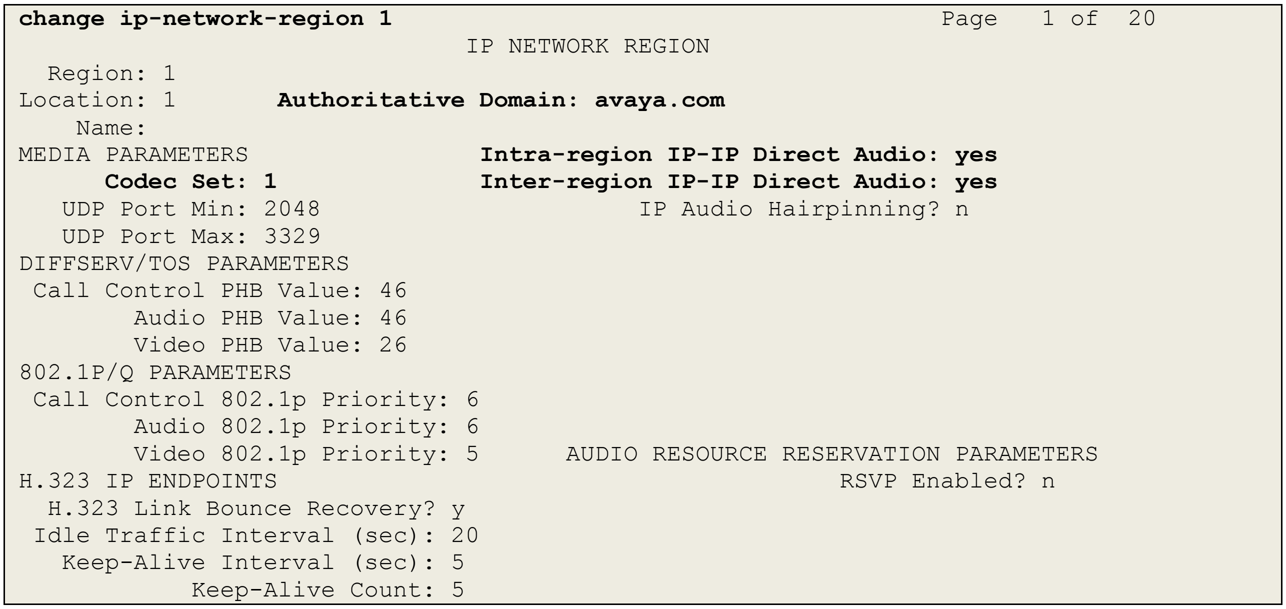
The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for Session Manager. In this case, **SM100** and **10.10.73.5** are the **Name** and **IP Address** for Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
SM100               10.10.73.5
default             0.0.0.0
procr               10.10.8.67
procr6              ::
```

5.3. Administer IP Network Region

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

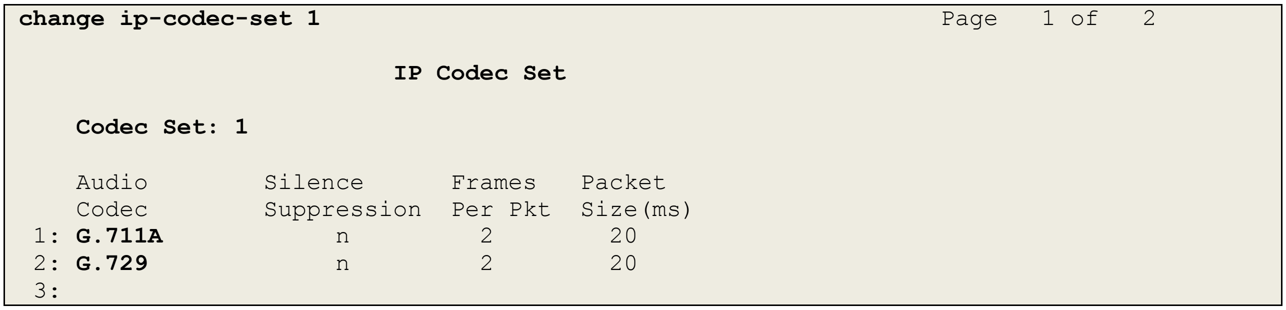
- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra**- and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly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



```
change ip-network-region 1                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.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
```

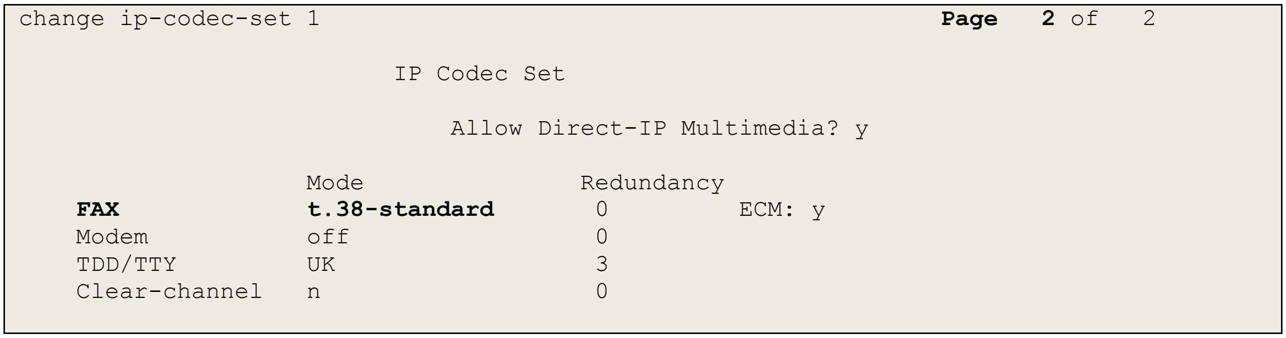
5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form in **Section 5.3.** Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec's supported by BT 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
 3:
```

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



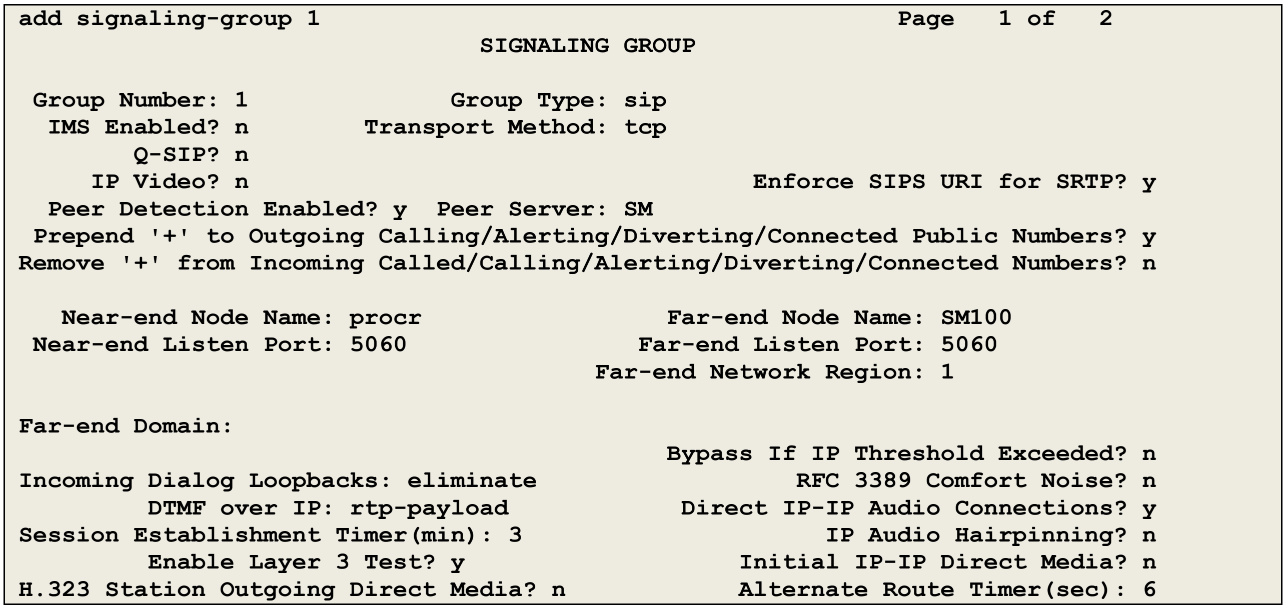
```
change ip-codec-set 1                                             Page   2 of   2

                          IP Codec Set

                              Allow Direct-IP Multimedia? y

                Mode                Redundancy
    FAX         t.38-standard        0          ECM: y
    Modem       off                  0
    TDD/TTY     UK                   3
    Clear-channel   n                0
```

5.5. Administer SIP Signaling Groups

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

- Set **Group Type** to **sip**
- Set **Transport Method** to **tcp**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to Session Manager (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region **1**)
- Leave **Far-end Domain** blank (allows the CM to accept calls from any SIP domain on the associated trunk)
- Set **Direct IP-IP Audio Connections** to **y**
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.

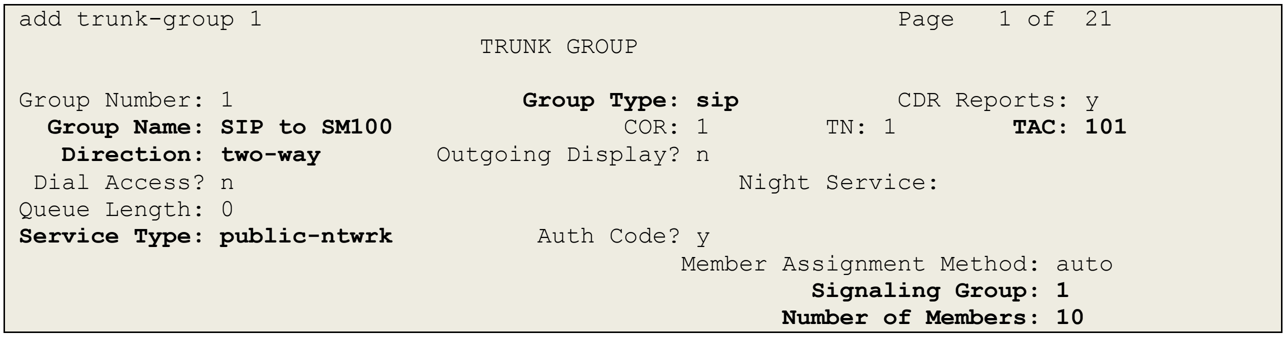


```
add signaling-group 1                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

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

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

5.6. Administer SIP Trunk Group

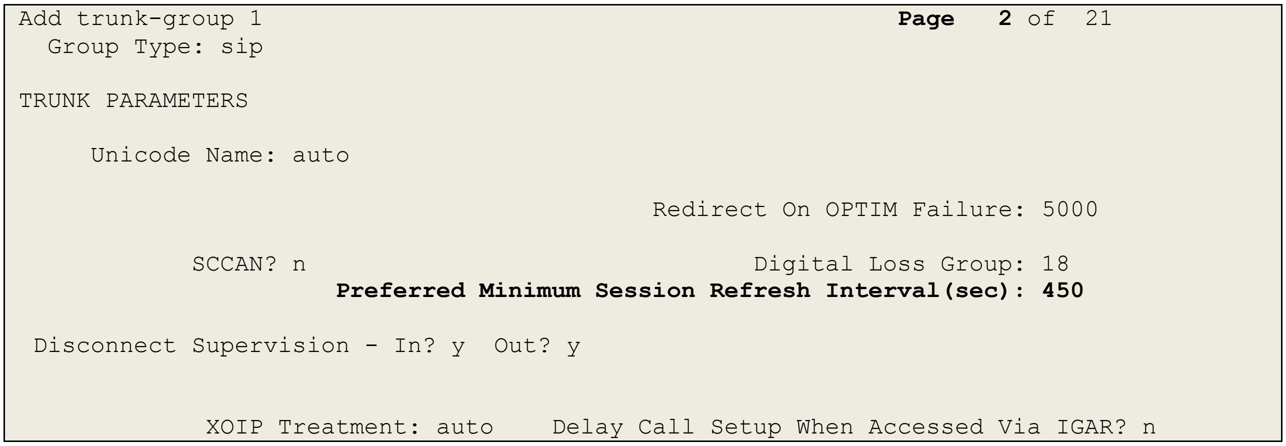
A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group x** command, where **x** is an available trunk group. On **Page 1** of this form:

- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **public-ntwrk**
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the **Number of Members** supported by this SIP trunk group



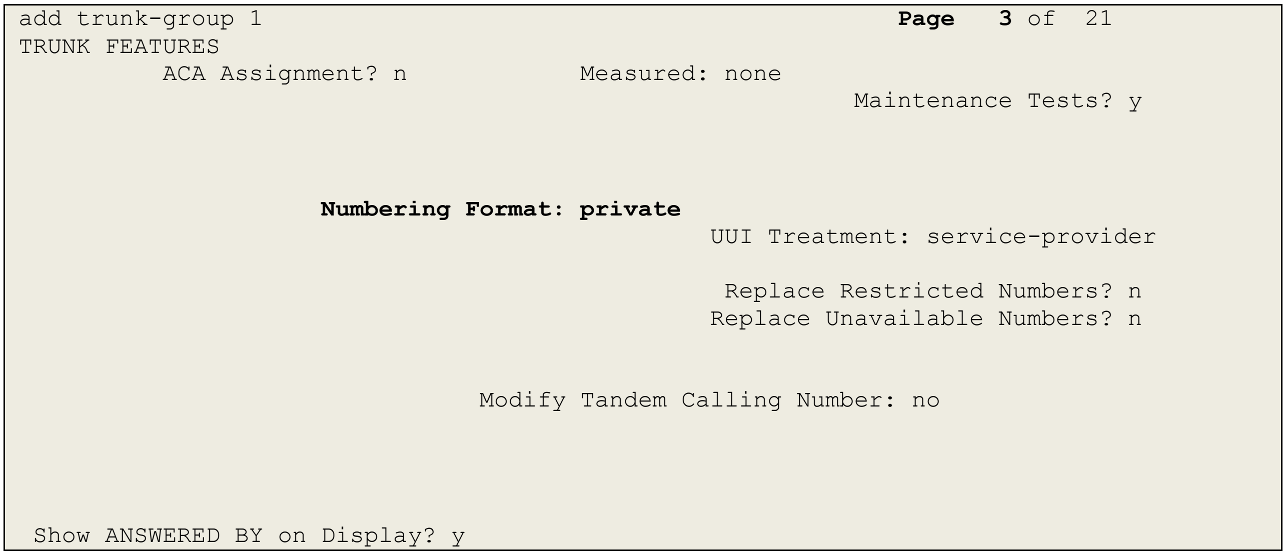
```
add trunk-group 1                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: SIP to SM100                COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? y
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

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



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

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 450

 Disconnect Supervision - In? y  Out? y


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

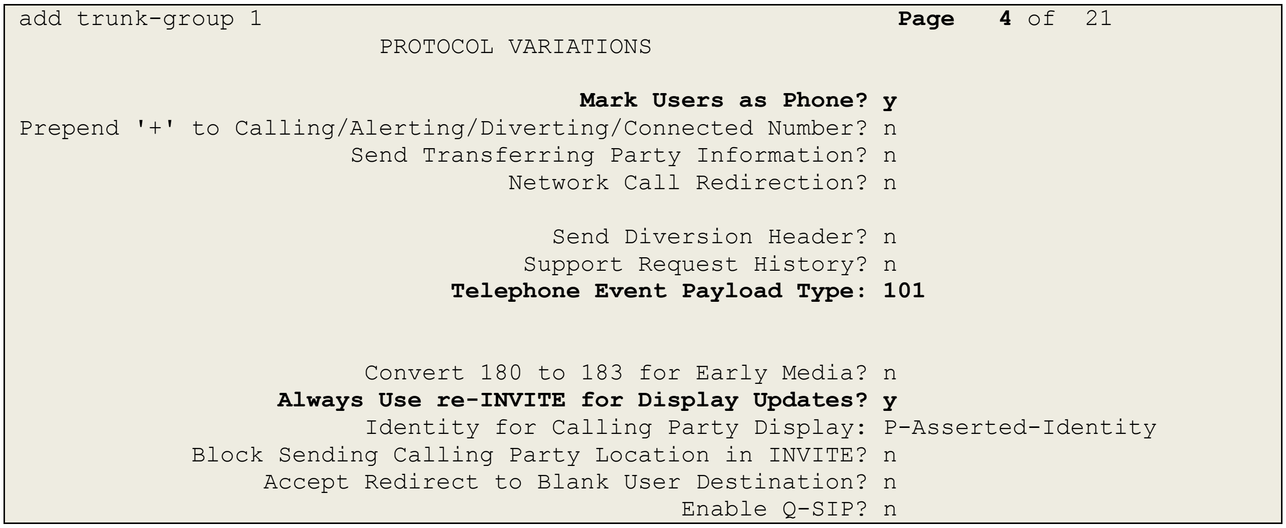
On **Page 3**, set the **Numbering Format** field to **private**.



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



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

On **Page 4** of this form:

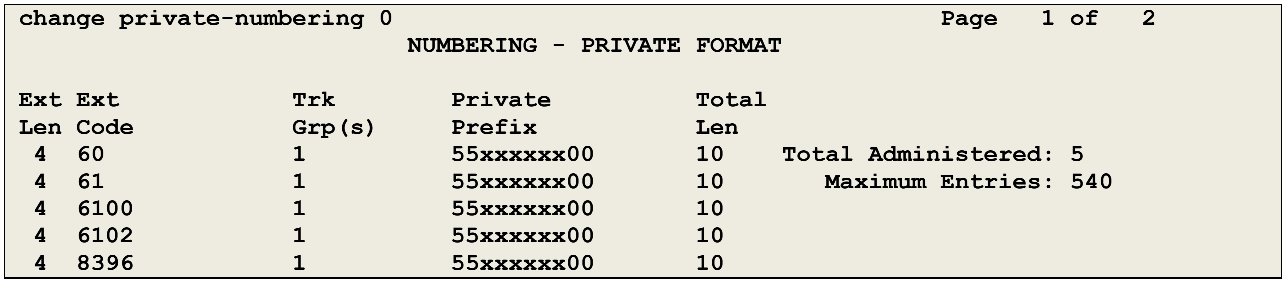
- Set **Mark Users as Phone** to **y**
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by BT (this Payload Type is not applied to calls from SIP end-points)
- Set **Always Use re-INVITE for Display Updates** to **y**



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

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

                                     Send Diversion Header? n
                                   Support Request History? n
                              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
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```

5.7. Administer Calling Party Number Information

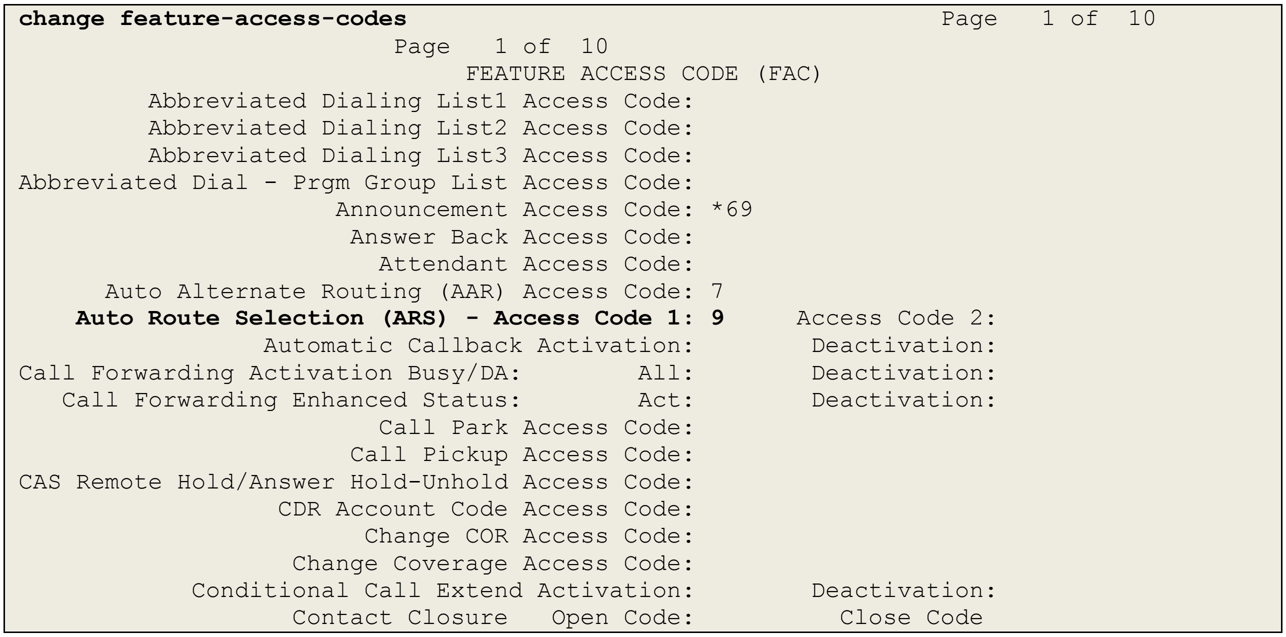
Use the **change private-numbering** command to configure Communication Manager to send the calling party number. In the test configuration, individual stations were mapped to send numbers allocated from the BT DDI range supplied. This calling party number is sent in the SIP From, Contact and PAI headers,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



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

Ext Ext             Trk        Private          Total
Len Code            Grp(s)     Prefix           Len
 4  60              1          55xxxxxx00       10    Total Administered: 5
 4  61              1          55xxxxxx00       10       Maximum Entries: 540
 4  6100            1          55xxxxxx00       10
 4  6102            1          55xxxxxx00       10
 4  8396            1          55xxxxxx00       10
```

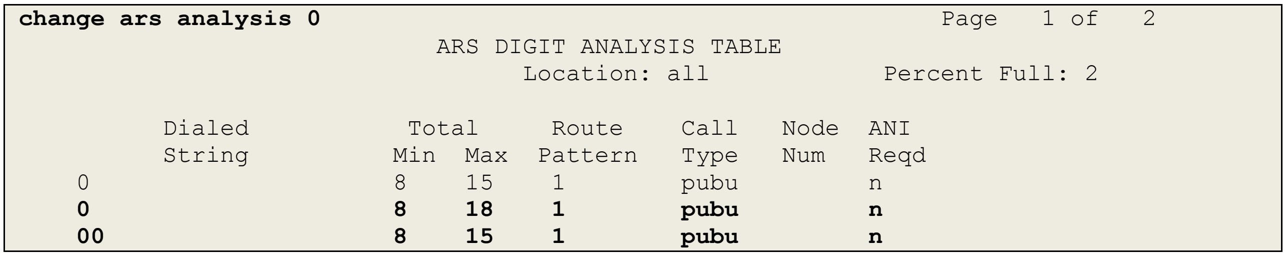
5.8. Administer Route Selection for Outbound Calls

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



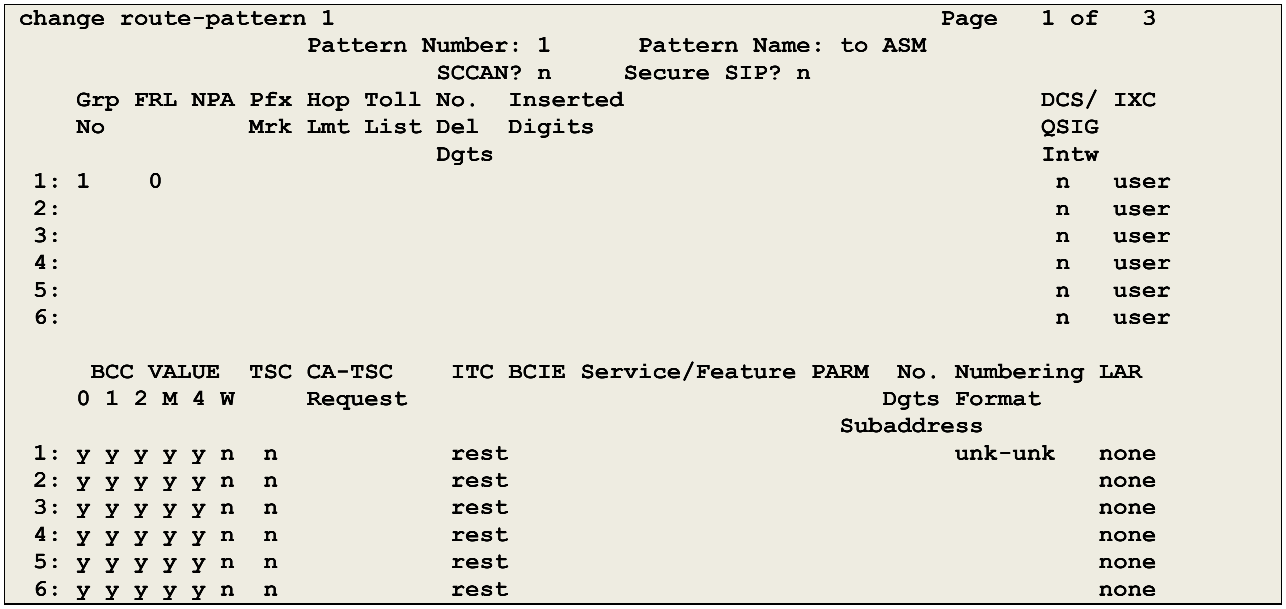
```
change feature-access-codes                                     Page   1 of  10
                          Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *69
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 7
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code
```

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to two UK area codes and one international country code. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.



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

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    0                     8    15    1        pubu         n
    0                     8    18    1        pubu         n
    00                    8    15    1        pubu         n
```

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**.



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

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

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming 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 **55xxxxxxx** to a 4 digit extension by deleting all of the incoming digits and inserting an extension. Public DID numbers have been masked for security purposes.

```
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    10 55xxxxxx00       all 6010
 public-ntwrk    10 55xxxxxx01       all 6012
 public-ntwrk    10 55xxxxxx02       all 6102
```

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 6102. Use the command **change off-pbx-telephone station-mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386nnnnnnn**)
- Set the **Trunk Selection** to the trunk group defined in **section 5.6** for the SIP Trunk, in test it was **1**
- Set the **Config Set** to **1**

```
change off-pbx-telephone station-mapping 6102                   Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 6102             EC500         -     0035386nnnnnnn   1          1
                                -
```

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

6. Configuring Avaya Aura® Session Manager

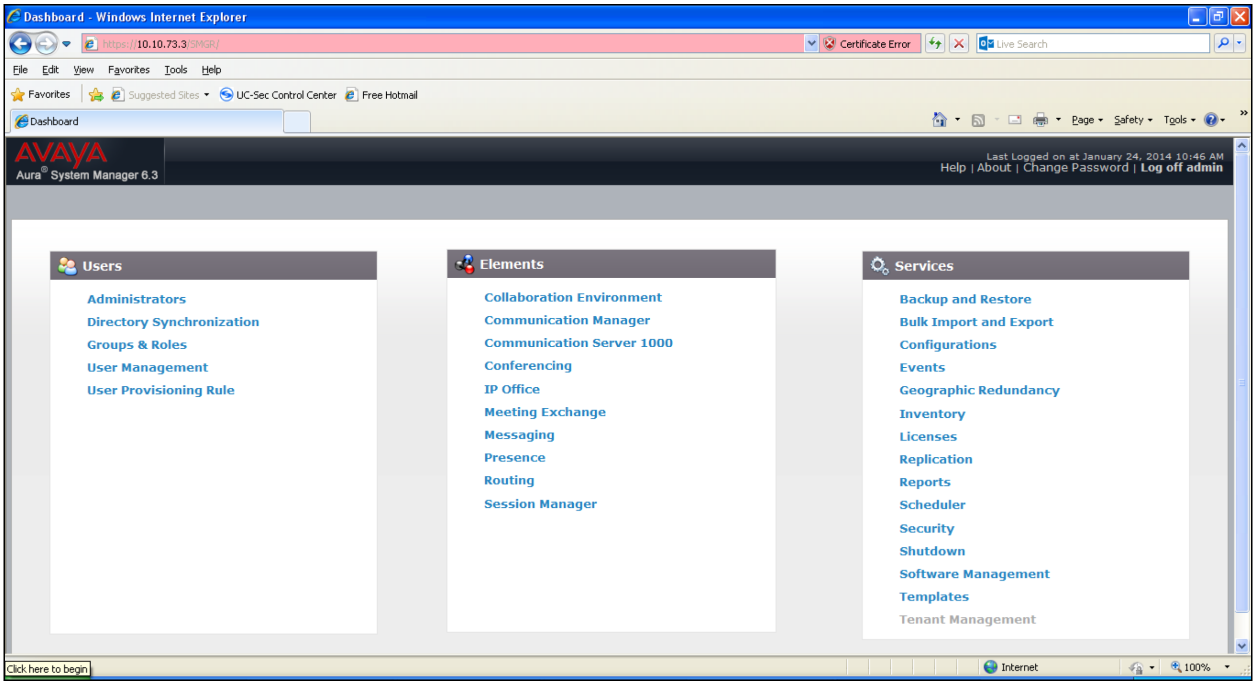
This section provides the procedures for configuring Session Manager. Session Manager is configured via the System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns

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

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser 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.

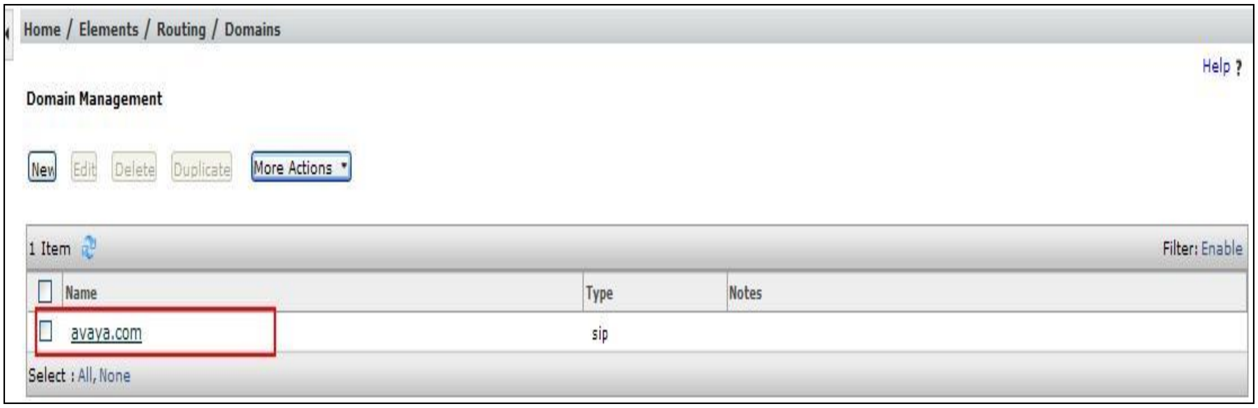


6.2. Administer SIP Domain

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

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

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



□	Name	Type	Notes
□	avaya.com	sip	

6.3. Administer Locations

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

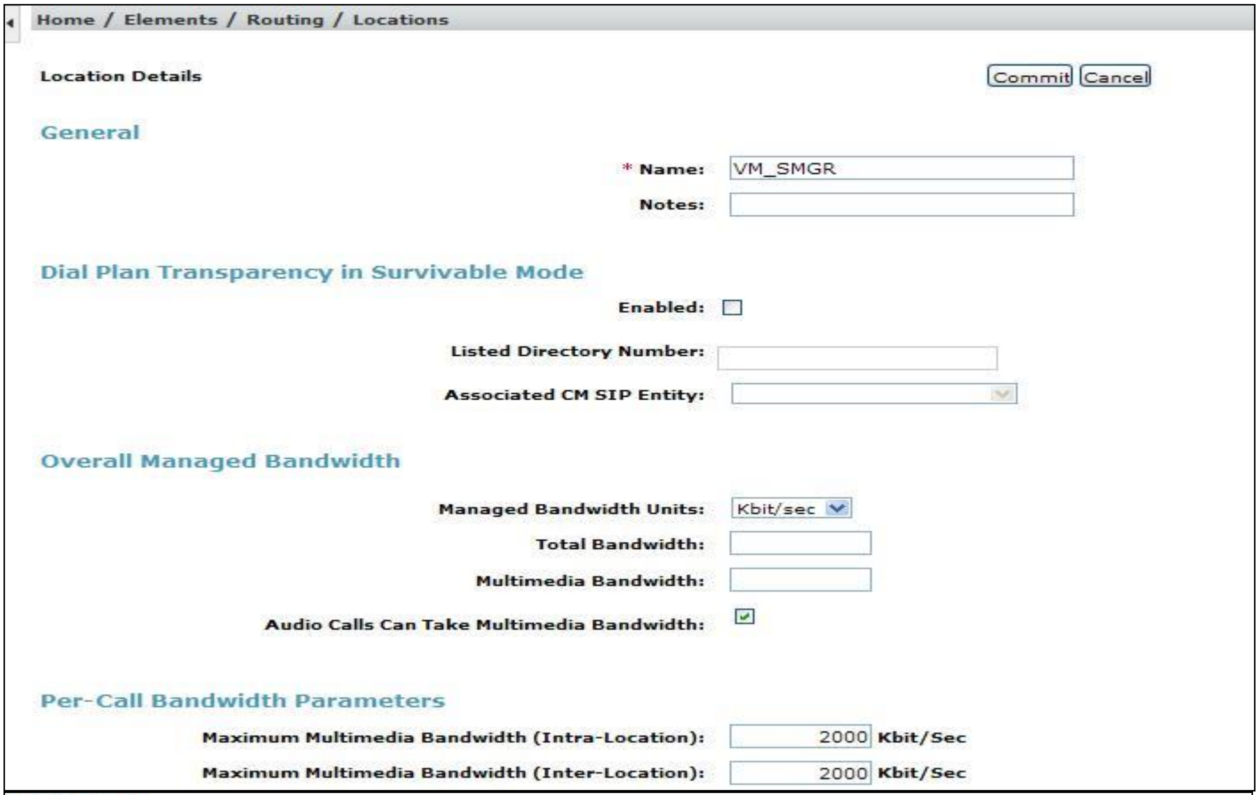
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

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

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

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

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



Home / Elements / Routing / Locations

Location Details

General

* Name:	VM_SMGR
Notes:	

Dial Plan Transparency in Survivable Mode

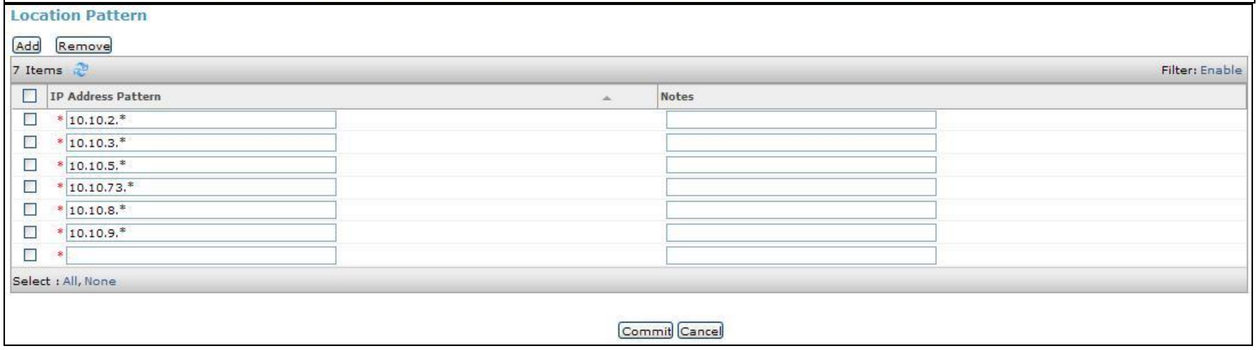
Enabled:	□
Listed Directory Number:	
Associated CM SIP Entity:	

Overall Managed Bandwidth

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

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):	2000 Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location):	2000 Kbit/Sec



Location Pattern

7 Items

Filter: Enable

□	IP Address Pattern	Notes
□	* 10.10.2.*	
□	* 10.10.3.*	
□	* 10.10.5.*	
□	* 10.10.73.*	
□	* 10.10.8.*	
□	* 10.10.9.*	
□	*	

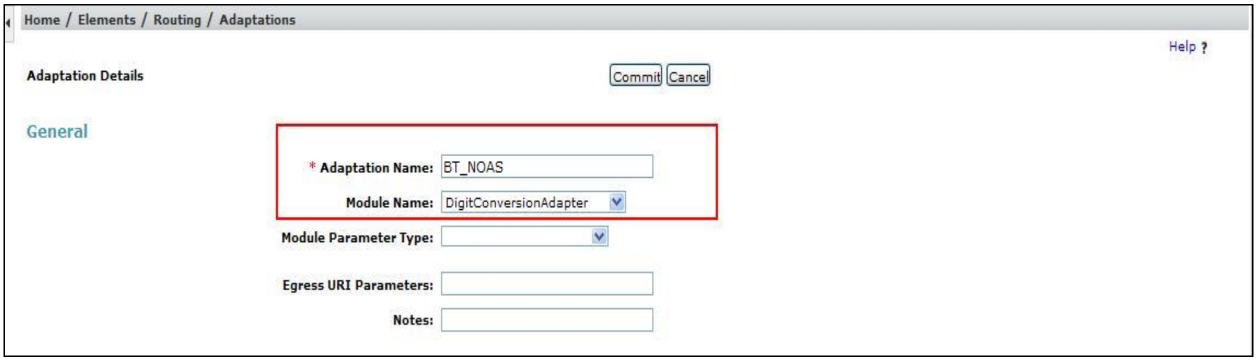
Select : All, None

6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. The example below was applied to the Avaya SBCE SIP Entity and was used in test to convert numbers being passed between the Avaya SBCE and Session Manager.

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

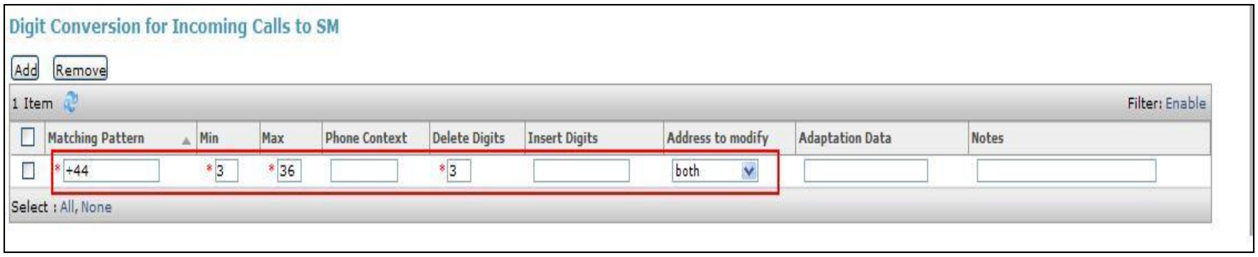
- In the **Adaptation name** field enter an informative name.
- In the **Module name** field click on the down arrow and then select the <**click to add module**> entry from the drop down list and type **DigitConversionAdapter** in the resulting New Module Name field.



* Adaptation Name:	BT_NOAS
Module Name:	DigitConversionAdapter
Module Parameter Type:	
Egress URI Parameters:	
Notes:	

Scroll down the page and 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.



□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
□	* +44	* 3	* 36		* 3		both		

This will ensure any incoming 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 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:**

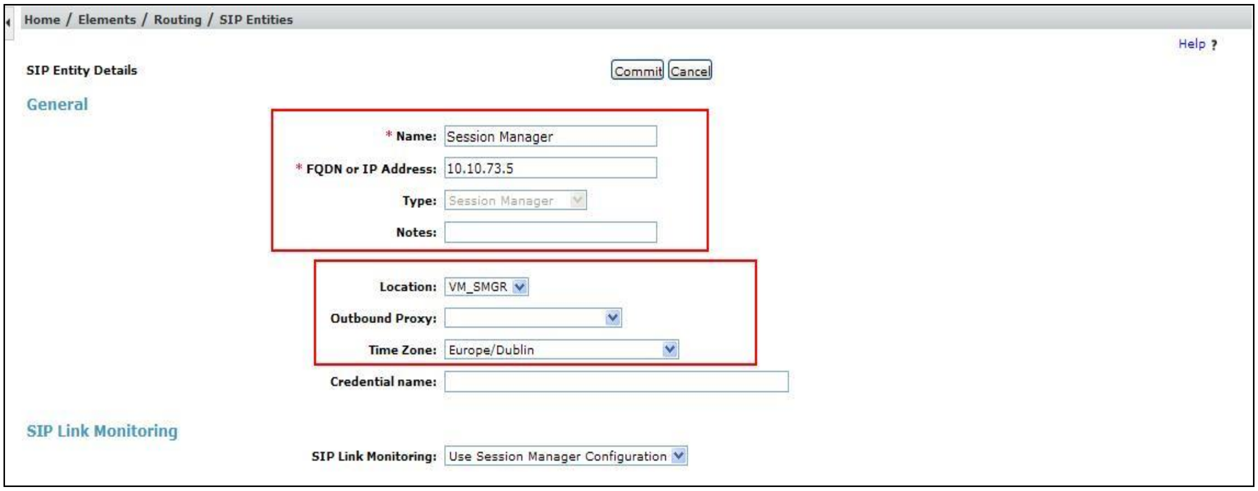
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **SIP Trunk** for the Avaya SBCE 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
- Avaya SBCE 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 signalling interface and **TYPE** is **Session Manager**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.



Home / Elements / Routing / SIP Entities

Help ?

SIP Entity Details

Commit Cancel

General

* Name: Session Manager

* FQDN or IP Address: 10.10.73.5

Type: Session Manager

Notes:

Location: VM_SMGR

Outbound Proxy:

Time Zone: Europe/Dublin

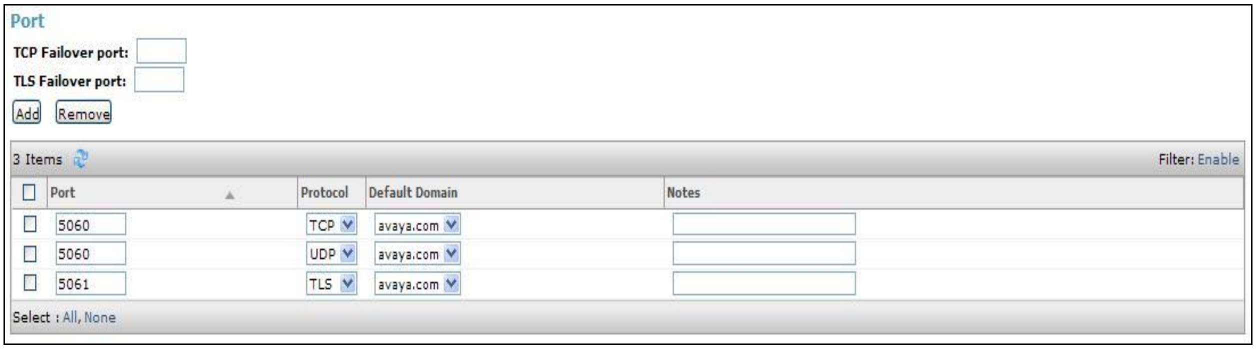
Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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

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



Port

TCP Failover port:

TLS Failover port:

Add Remove

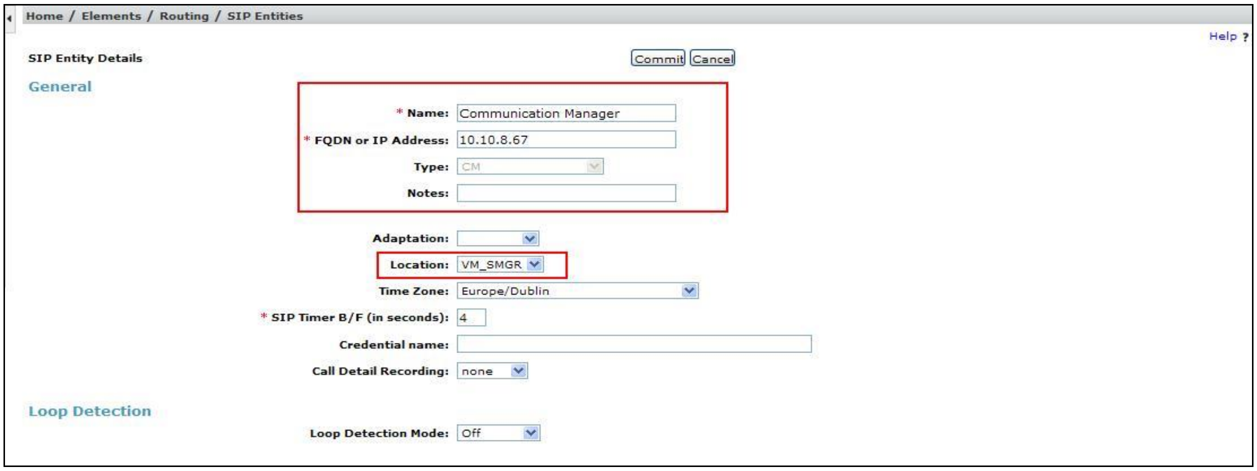
3 Items Filter: Enable

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

Select : All, None

6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signaling and **Type** is **CM**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.



SIP Entity Details

General

* Name: Communication Manager

* FQDN or IP Address: 10.10.8.67

Type: CM

Notes:

Adaptation:

Location: VM_SMGR

Time Zone: Europe/Dublin

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

Credential name:

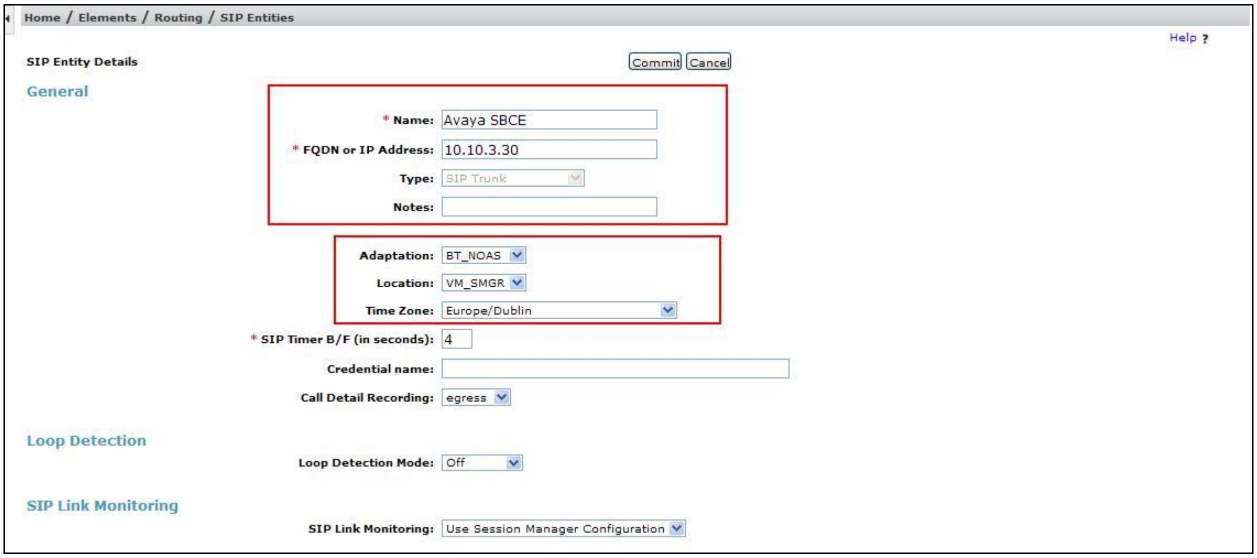
Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set **Type** to **SIP Trunk** and **Adaptation** to that defined in **Section 6.4**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.



SIP Entity Details

General

* Name: Avaya SBCE

* FQDN or IP Address: 10.10.3.30

Type: SIP Trunk

Notes:

Adaptation: BT_NOAS

Location: VM_SMGR

Time Zone: Europe/Dublin

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

Credential name:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

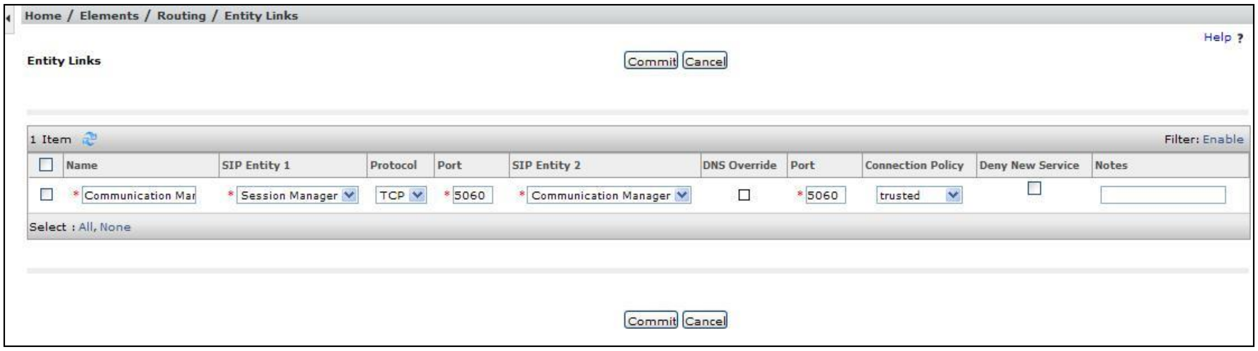
SIP Link Monitoring: Use Session Manager Configuration

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

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select **Session Manager**
- 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** to save changes. The following screen shows the Entity Link for the Communication Manager.

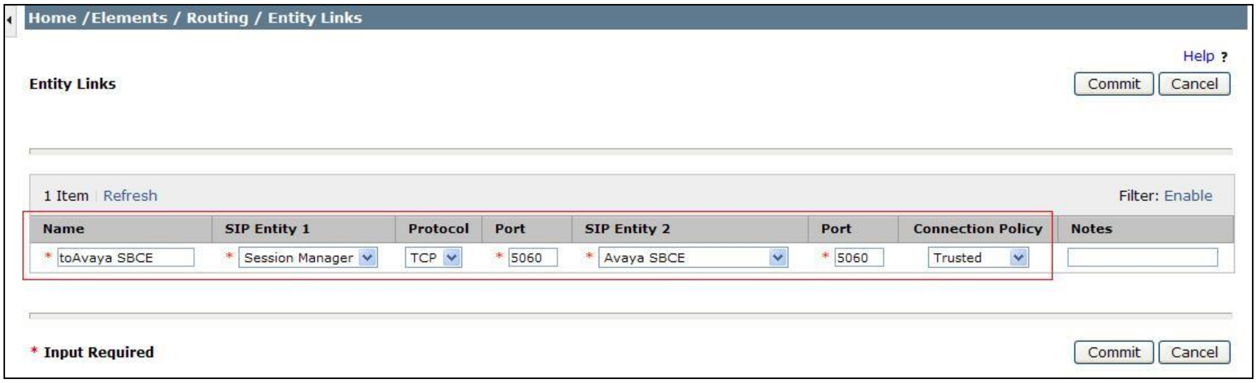


Entity Links

1 Item

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
□	* Communication Mar	* Session Manager	TCP	* 5060	* Communication Manager	□	* 5060	trusted	□	

The following screen shows the Entity Link for the Avaya SBCE.



Entity Links

1 Item

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* toAvaya SBCE	* Session Manager	TCP	* 5060	* Avaya SBCE	* 5060	Trusted	

* Input Required

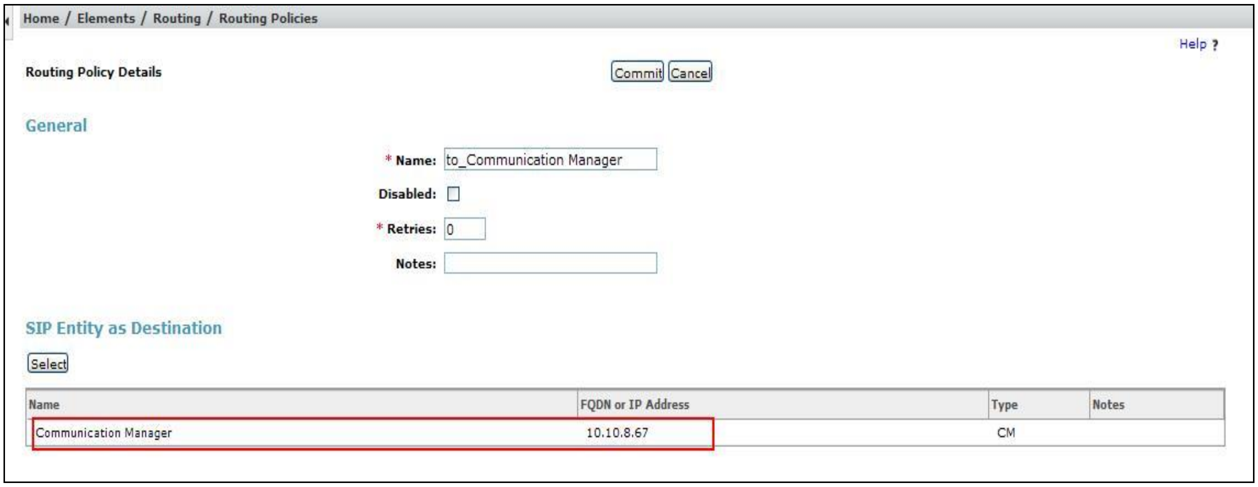
6.7. Administer Routing Policies

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

Under **General**:

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

The following screen shows the routing policy for Communication Manager.



Routing Policy Details

General

* Name: to_Communication Manager

Disabled: □

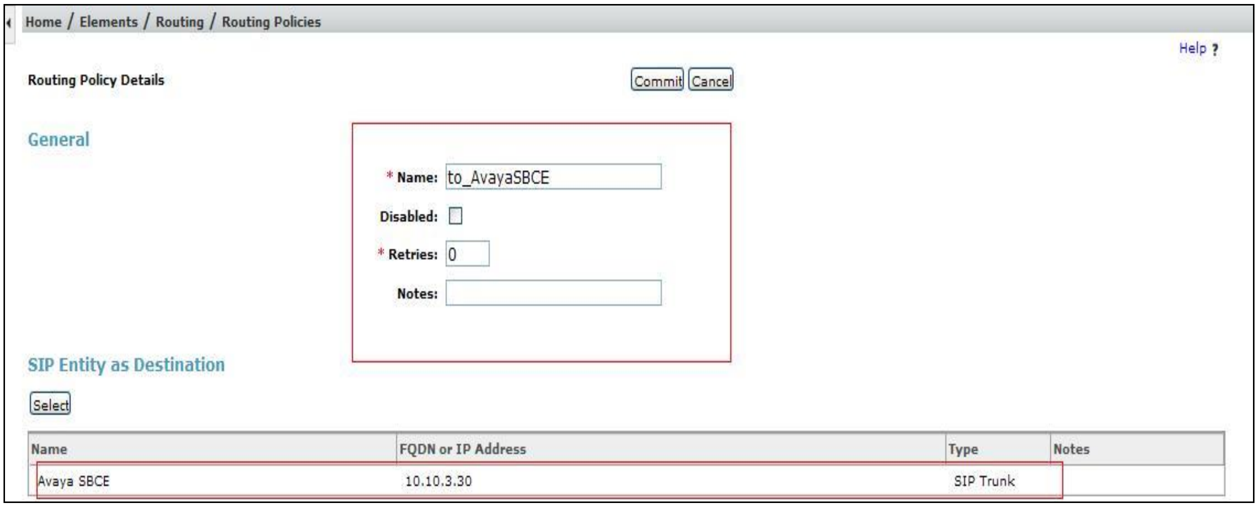
* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Communication Manager	10.10.8.67	CM	

The following screen shows the routing policy for the Avaya SBCE.



Routing Policy Details

General

* Name: to_AvayaSBCE

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.10.3.30	SIP Trunk	

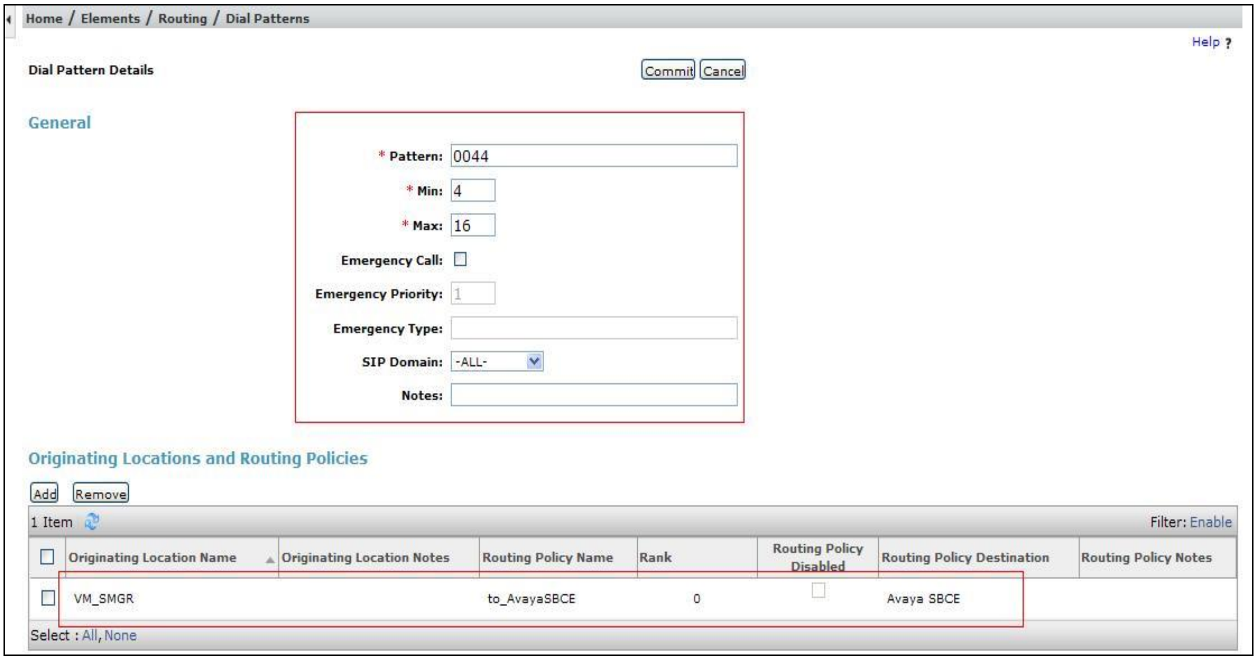
6.8. Administer Dial Patterns

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

Under **General**:

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

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown), under **Originating Location** select the location defined in **Section 6.3** or **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 the Avaya SBCE which will route the calls out to the BT NOAS SIP Trunk service.



Dial Pattern Details

General

* Pattern: 0044

* Min: 4

* Max: 16

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

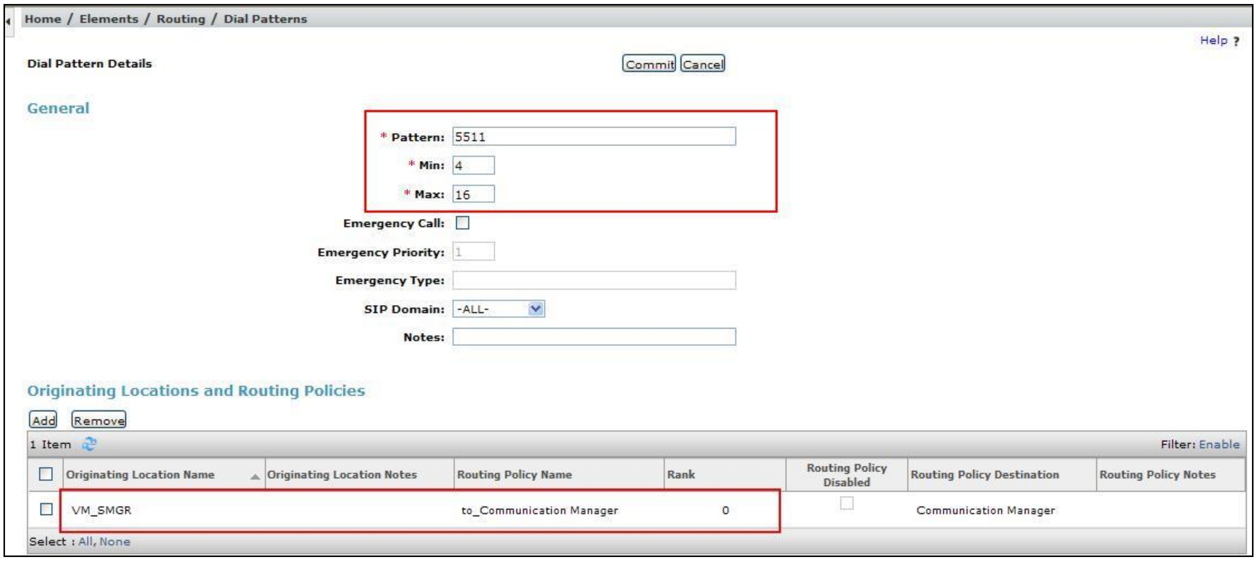
Notes:

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	VM_SMGR		to_AvayaSBCE	0	□	Avaya SBCE	

Select : All, None

The following screen shows the test dial pattern configured for Communication Manager.



Dial Pattern Details

General

* Pattern:	5511
* Min:	4
* Max:	16
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

1 Item Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	VM_SMGR		to_Communication Manager	0	□	Communication Manager	

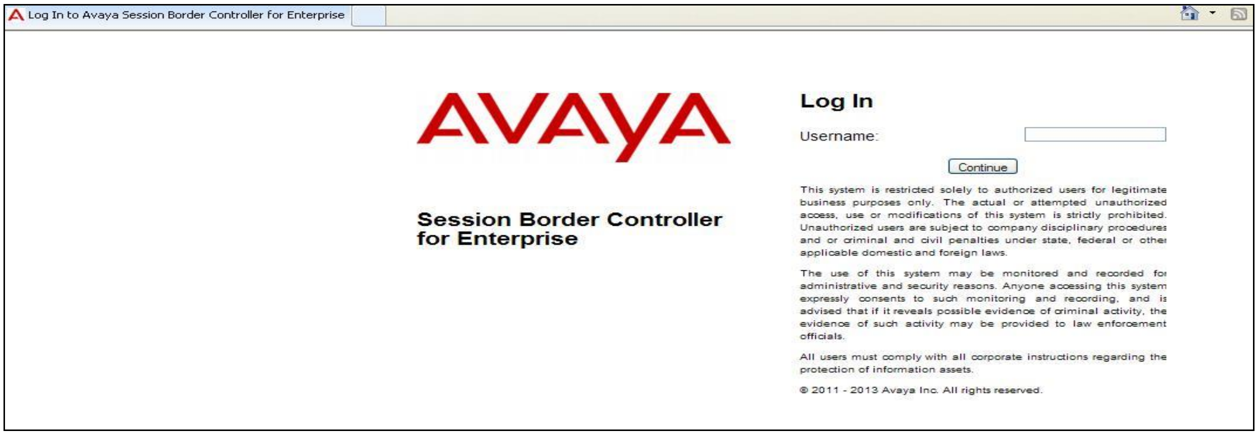
Select : All, None

7. Configure Avaya Session Border Controller for Enterpriser

This section describes the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed.

7.1. Access Avaya Session Border Controller for Enterprise

Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.


Log In to Avaya Session Border Controller for Enterprise
AVAYA
Session Border Controller for Enterprise
Continue

Log In

Username:

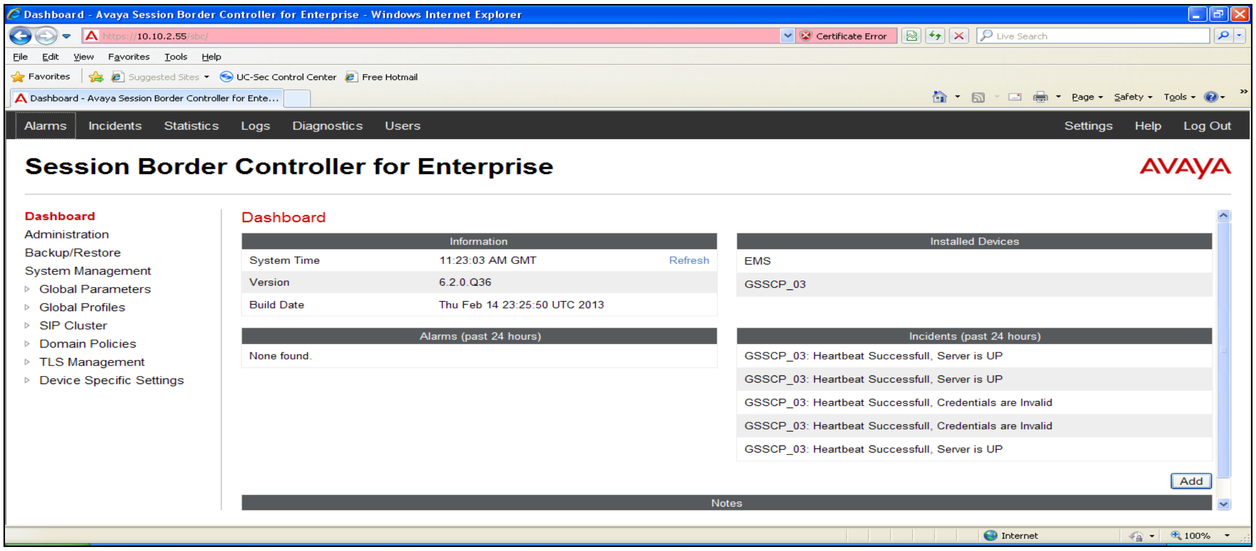
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

The main page of the Avaya SBCE will appear.



Dashboard

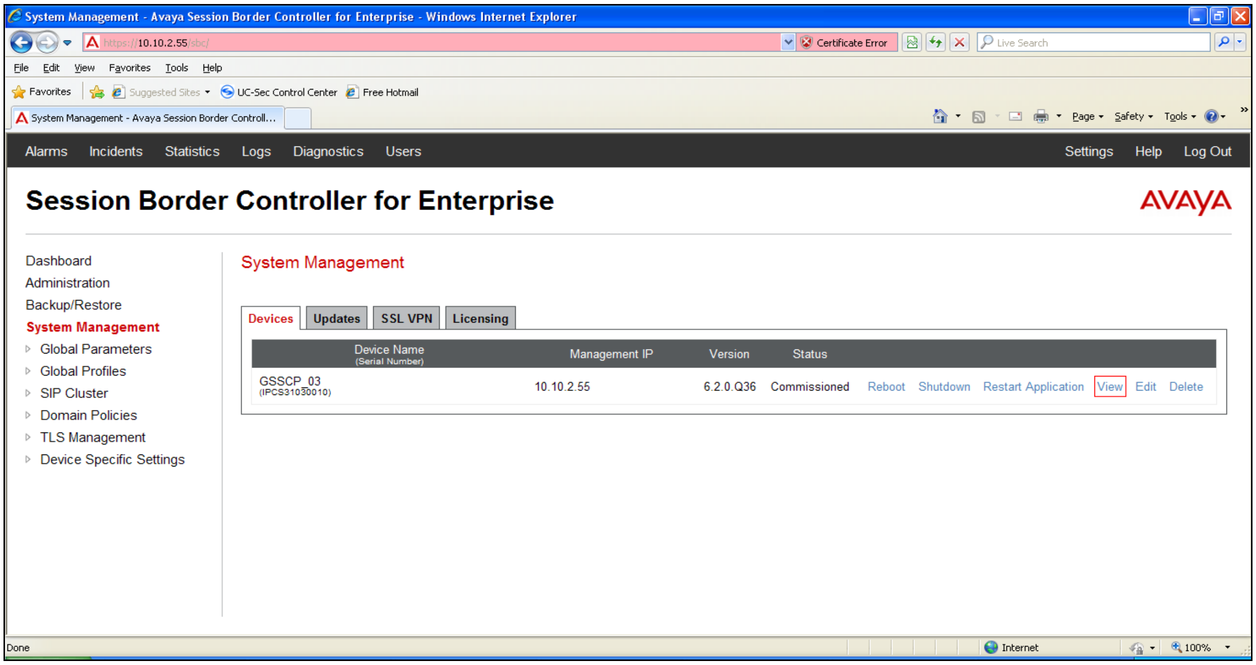
Information		
System Time	11:23:03 AM GMT	Refresh
Version	6.2.0.Q36	
Build Date	Thu Feb 14 23:25:50 UTC 2013	

Installed Devices
EMS
GSSCP_03

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
GSSCP_03: Heartbeat Successfull, Server is UP
GSSCP_03: Heartbeat Successfull, Server is UP
GSSCP_03: Heartbeat Successfull, Credentials are Invalid
GSSCP_03: Heartbeat Successfull, Credentials are Invalid
GSSCP_03: Heartbeat Successfull, Server is UP

To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP_03** is shown. To view the configuration of this device, click **View** (the third option from the right).

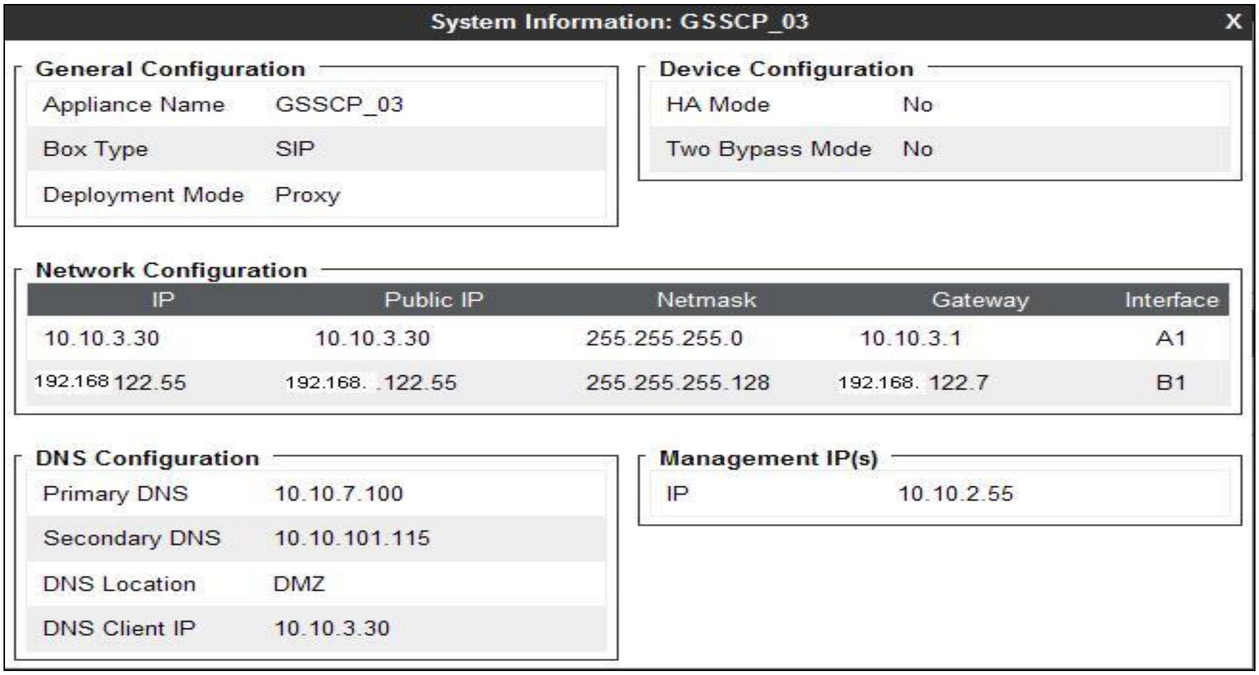


Session Border Controller for Enterprise

System Management

Device Name (Serial Number)	Management IP	Version	Status						
GSSCP_03 (IPCS31030010)	10.10.2.55	6.2.0.Q36	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Delete

The System Information screen shows the **Appliance Name**, **Device Settings** and **DNS Configuration** information.


System Information: GSSCP_03

General Configuration

Appliance Name	GSSCP_03
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.10.3.30	10.10.3.30	255.255.255.0	10.10.3.1	A1
192.168 122.55	192.168. .122.55	255.255.255.128	192.168. 122.7	B1

DNS Configuration

Primary DNS	10.10.7.100
Secondary DNS	10.10.101.115
DNS Location	DMZ
DNS Client IP	10.10.3.30

Management IP(s)

IP	10.10.2.55

7.2. Global Profiles

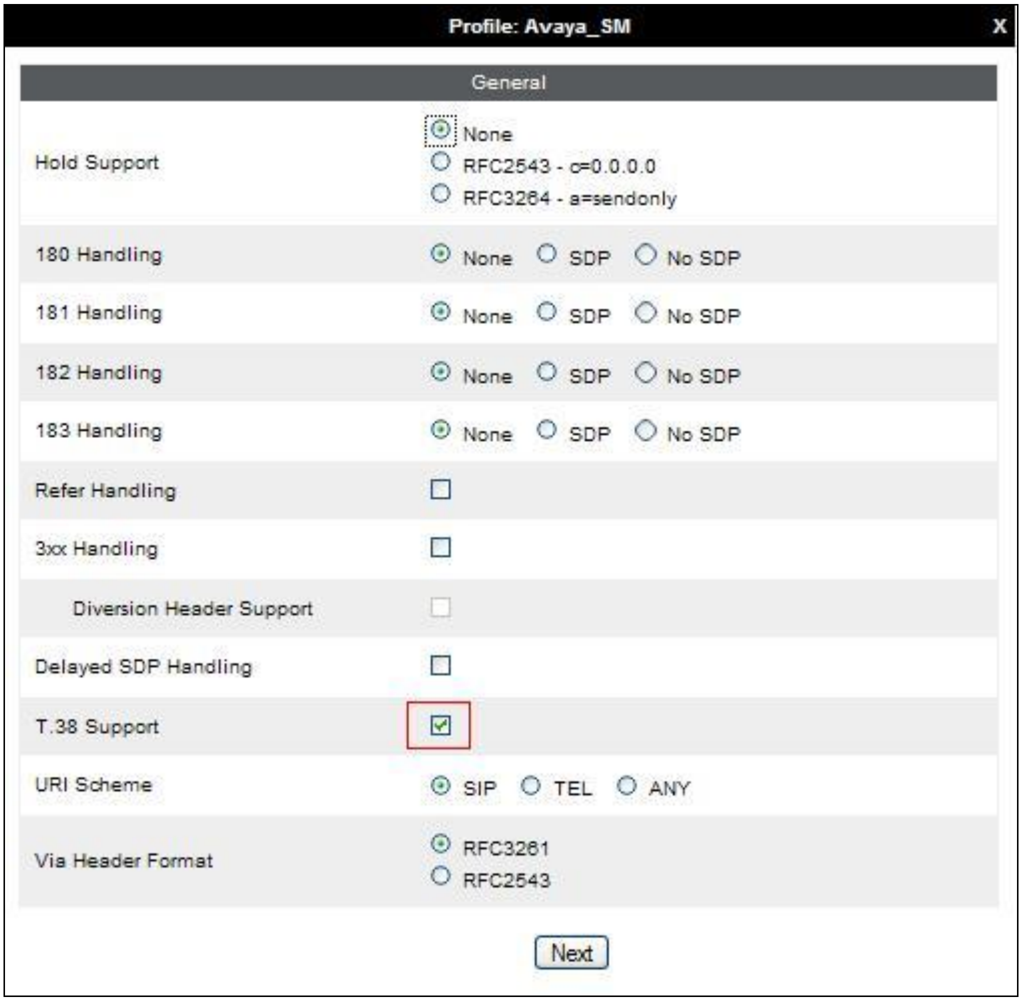
When selected, Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.2.1. Server Internetworking - Avaya

Server Internetworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles → Server Interworking** and click on **Add Profile.**

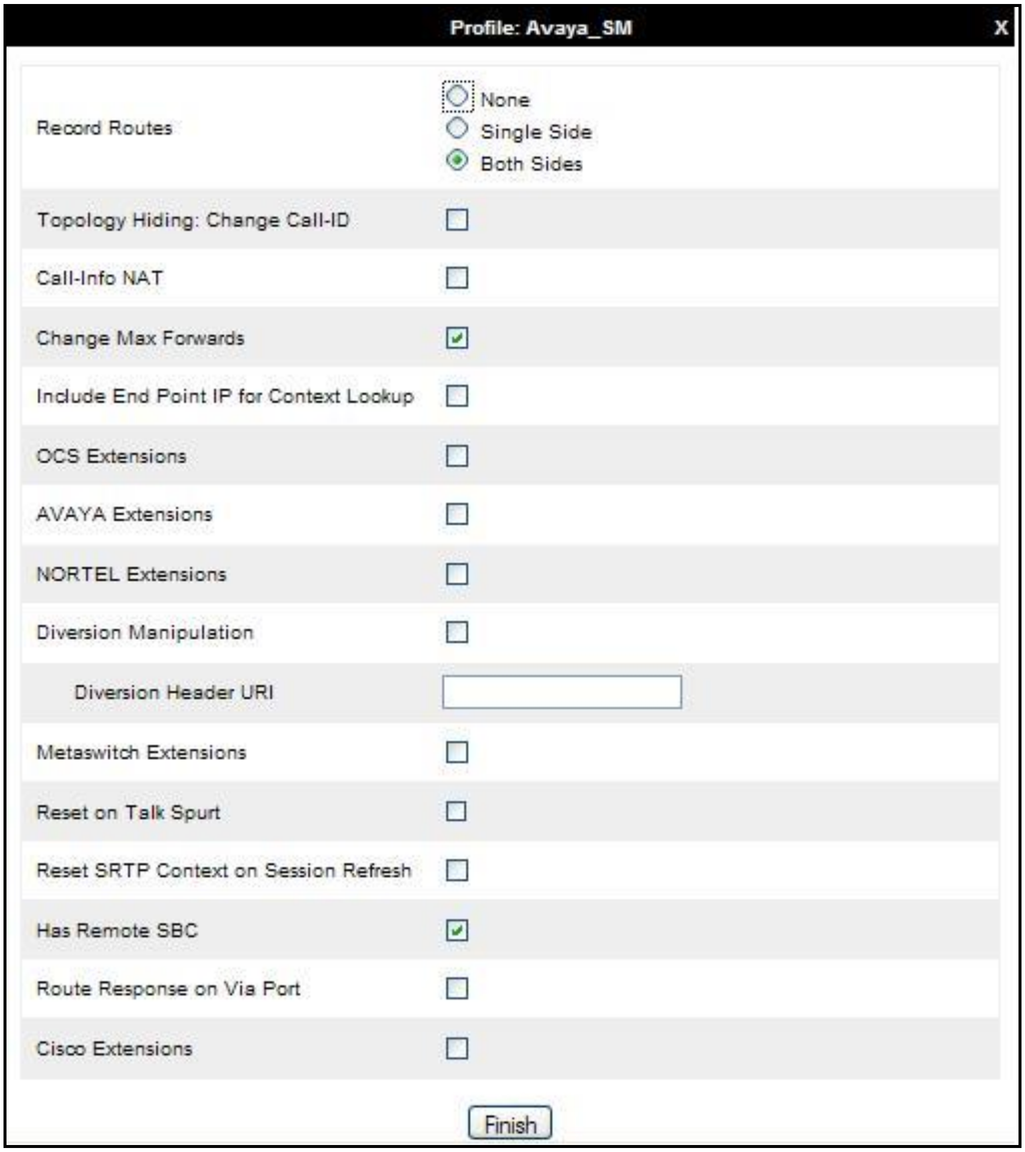
- Enter profile name such as **Avaya_SM** and click **Next** (Not Shown)
- **Check Hold Support=None**
- **Check T.38 Support**
- All other options on the **General** Tab can be left at default

Click on **Next** on the following screens and then **Finish**.



Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

Default values can be used for the **Advanced Settings** window. Click **Finish**



Profile: Avaya_SM

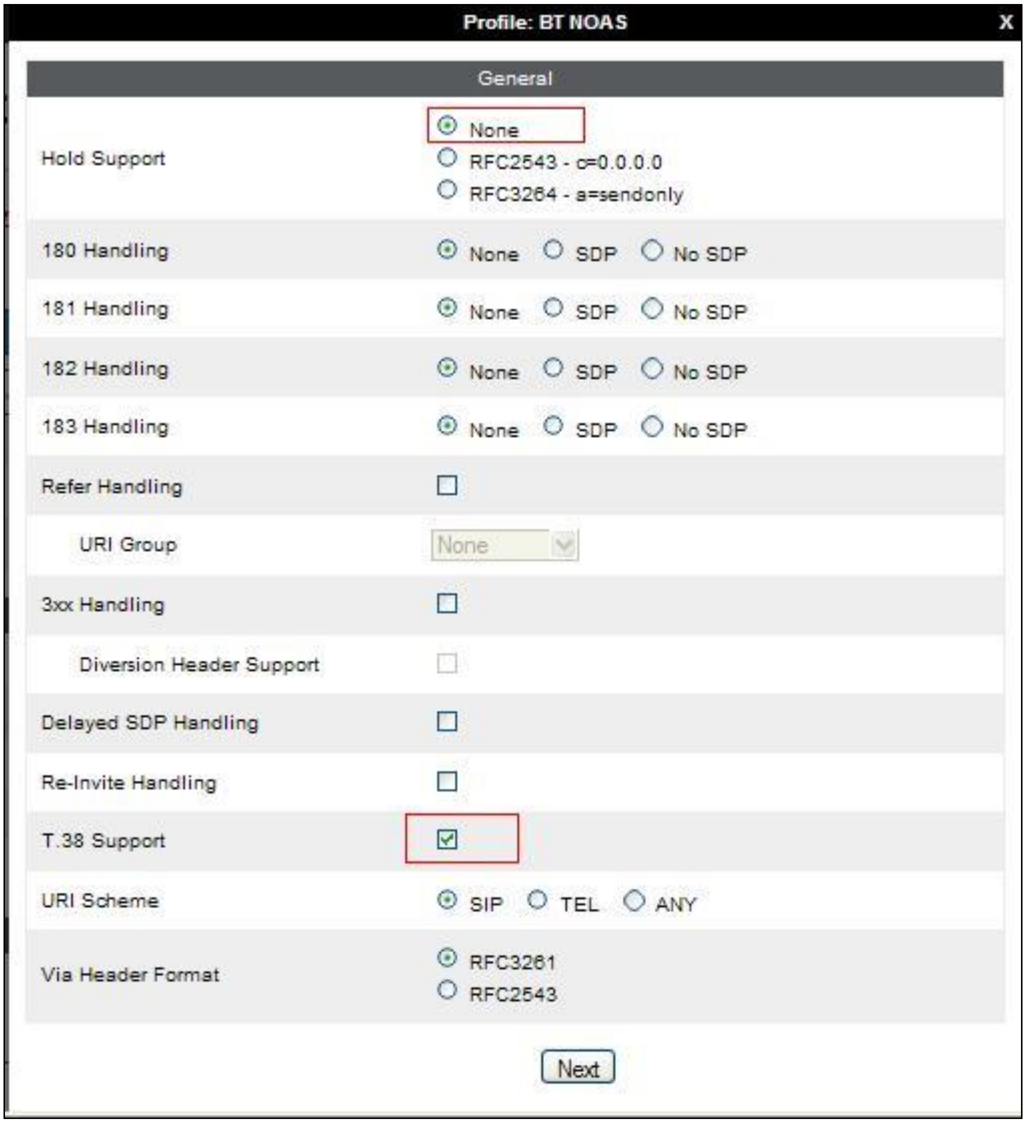
Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	□
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	□
NORTEL Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

7.2.2. Server Internetworking – BT NOAS

Server Internetworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles → Server Interworking** and click on **Add Profile**.

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

Click on **Next** on the following screens and then **Finish**.

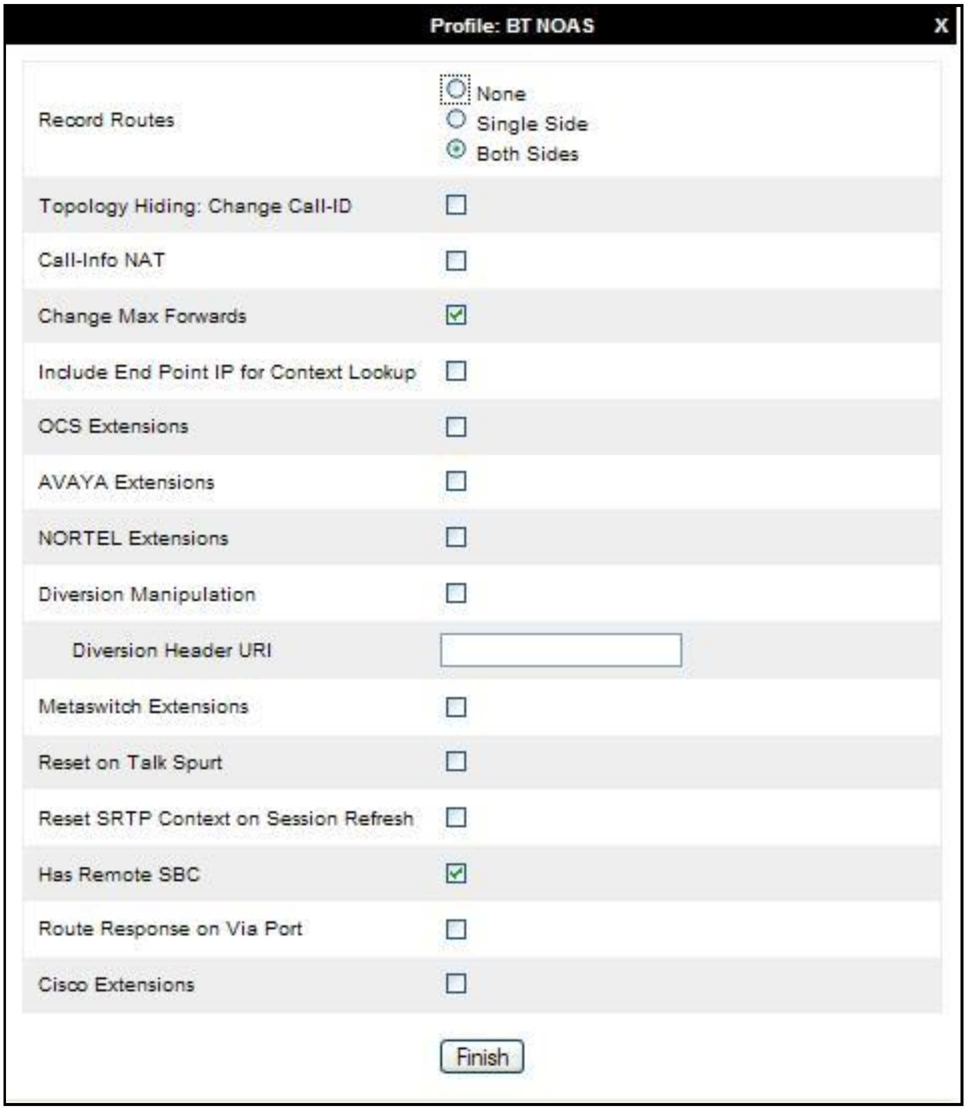


Profile: BT NOAS

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

Default values can be used for the **Advanced Settings** window. Click **Finish**.



Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	□
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	□
NORTEL Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

7.2.3. Routing

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

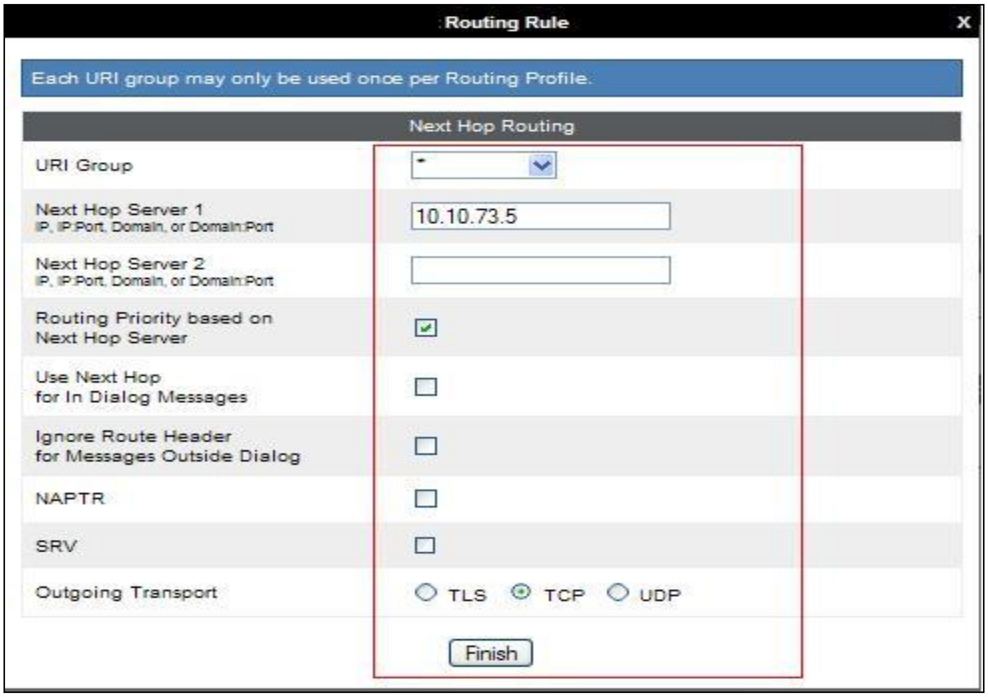
Routing information is required for routing to Session Manager on the internal side and the BT NOAS addresses on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is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

Create a Routing Profile for both Session Manager and BT NOAS SIP trunk. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **URI Group:** Select "*****" from the drop down box
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server, e.g. Session Manager
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server
- **Routing Priority Based on Next Hop Server**: Checked
- **Use Next Hop for In-Dialog Messages**: Select only if there is no secondary Next Hopserver
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets

Click **Finish**.

The following screen shows the Routing Profile to Session Manager

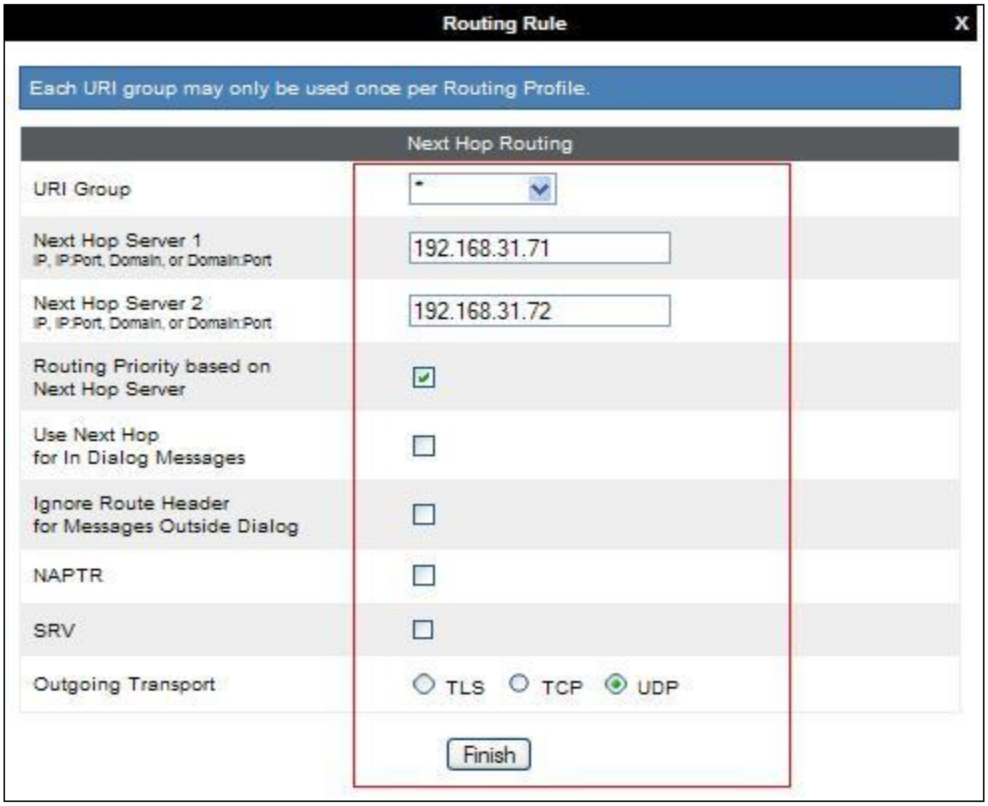


Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	10.10.73.5
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	☑
Use Next Hop for In Dialog Messages	□
Ignore Route Header for Messages Outside Dialog	□
NAPTR	□
SRV	□
Outgoing Transport	○ TLS ● TCP ○ UDP

The following screen shows the Routing Profile to BT NOAS.



Each URI group may only be used once per Routing Profile.

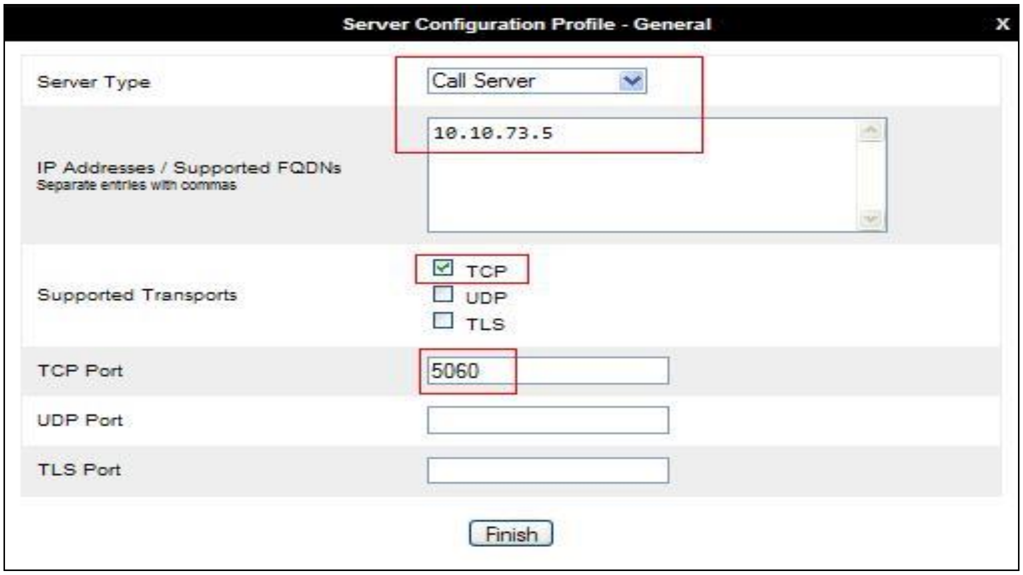
Next Hop Routing

URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	192.168.31.71
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	192.168.31.72
Routing Priority based on Next Hop Server	☑
Use Next Hop for In Dialog Messages	□
Ignore Route Header for Messages Outside Dialog	□
NAPTR	□
SRV	□
Outgoing Transport	○ TLS ○ TCP ● UDP

7.2.4. Server Configuration– Avaya Aura® Session Manager

Servers are defined for each server connected to the Avaya SBCE. In this case, BT NOAS is connected as the Trunk Server and Session Manager is connected as the Call Server.
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add Profile** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**
- Enter **IP Addresses / Supported FQDNs** to **10.10.73.5** (Session Manager IP Address)
- For **Supported Transports,** check **TCP**
- **TCP Port:5060**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs

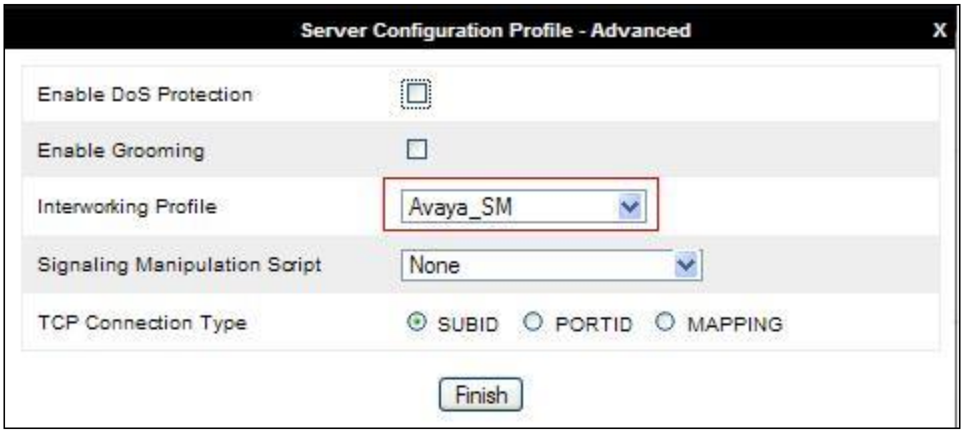


Server Configuration Profile - General

Server Type	Call Server
IP Addresses / Supported FQDNs Separate entries with commas	10.10.73.5
Supported Transports	☑ TCP □ UDP □ TLS
TCP Port	5060
UDP Port	
TLS Port	

On the **Advanced** tab:

- Select **Avaya_SM** for **Interworking Profile**
- Click **Finish**



Server Configuration Profile - Advanced

Enable DoS Protection □

Enable Grooming □

Interworking Profile: Avaya_SM

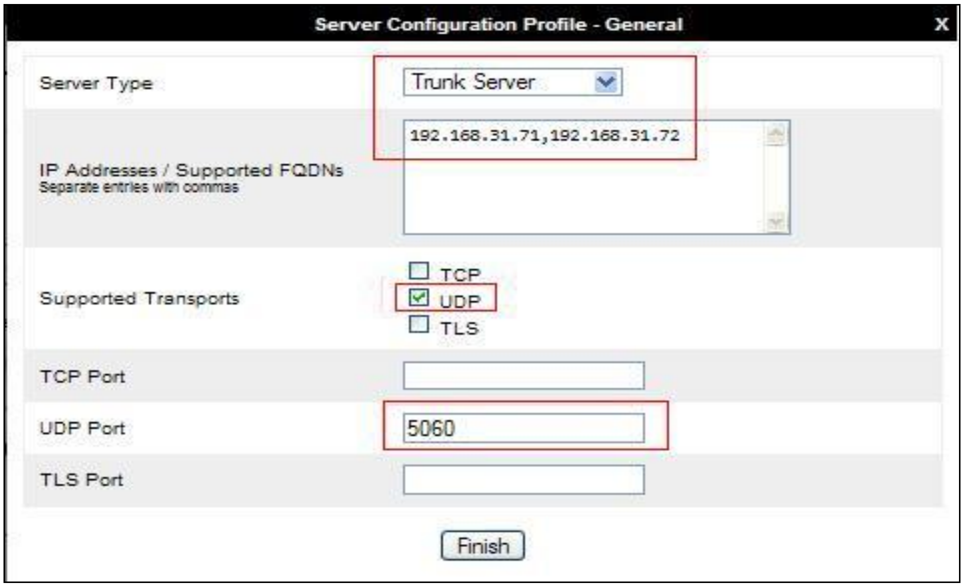
Signaling Manipulation Script: None

TCP Connection Type: ● SUBID ○ PORTID ○ MAPPING

7.2.5. Server Configuration– BT NOAS

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

- Select **Server Type** as **Trunk Server**
- Set **IP Address** to **192.168.31.71 and 192.168.31.72** (BT NOAS SIP Trunks)
- **Supported Transports**: Check **UDP**
- **UDP Port: 5060**
- Hit **Next**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs



Server Configuration Profile - General

Server Type: Trunk Server

IP Addresses / Supported FQDNs
Separate entries with commas: 192.168.31.71,192.168.31.72

Supported Transports: □ TCP ☑ UDP □ TLS

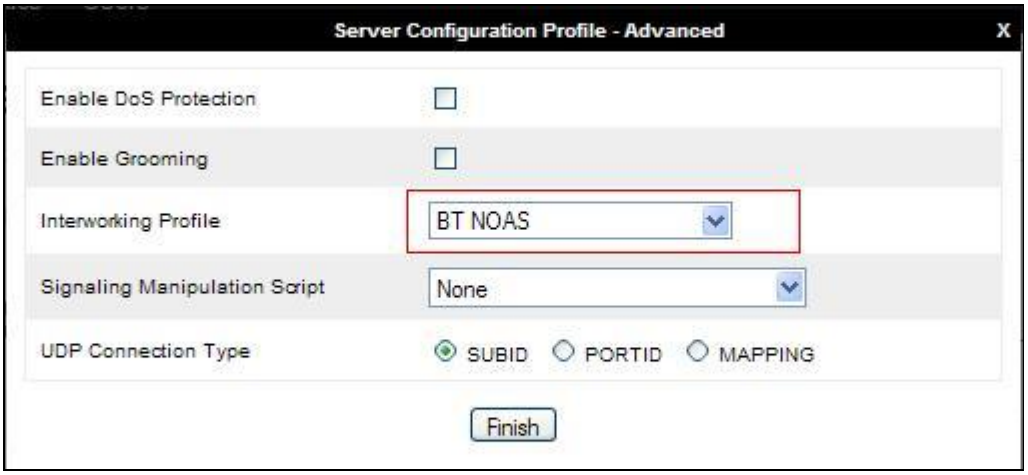
TCP Port:

UDP Port: 5060

TLS Port:

On the **Advanced** tab:

- Select **BT NOAS** for **Interworking Profile**
- Click **Finish**



Server Configuration Profile - Advanced

Enable DoS Protection □

Enable Grooming □

Interworking Profile: BT NOAS

Signaling Manipulation Script: None

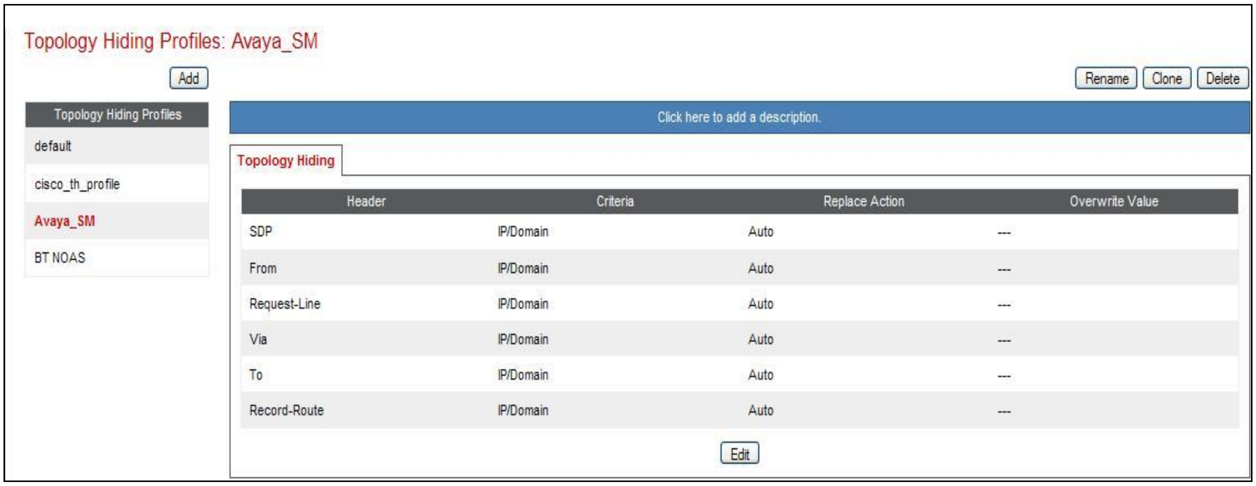
UDP Connection Type: ● SUBID ○ PORTID ○ MAPPING

7.2.6. Topology Hiding

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

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

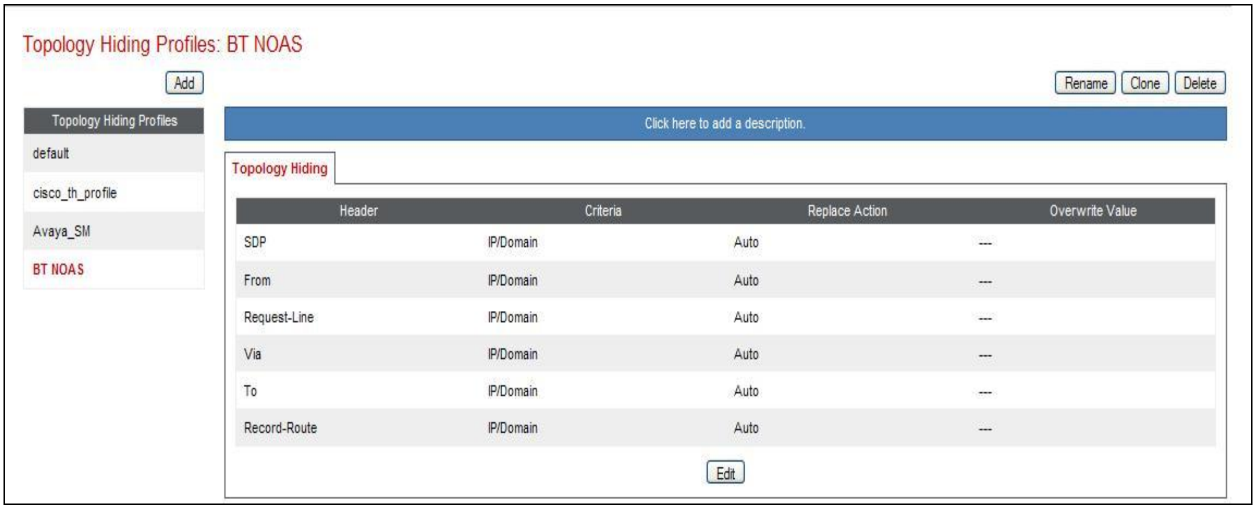
- In the **Profile Name** field enter a descriptive name for Session Manager and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **Request-Line, To** and **From** as the required headers from the **Header** drop down menu
- Select the required action from the **Required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



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

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

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



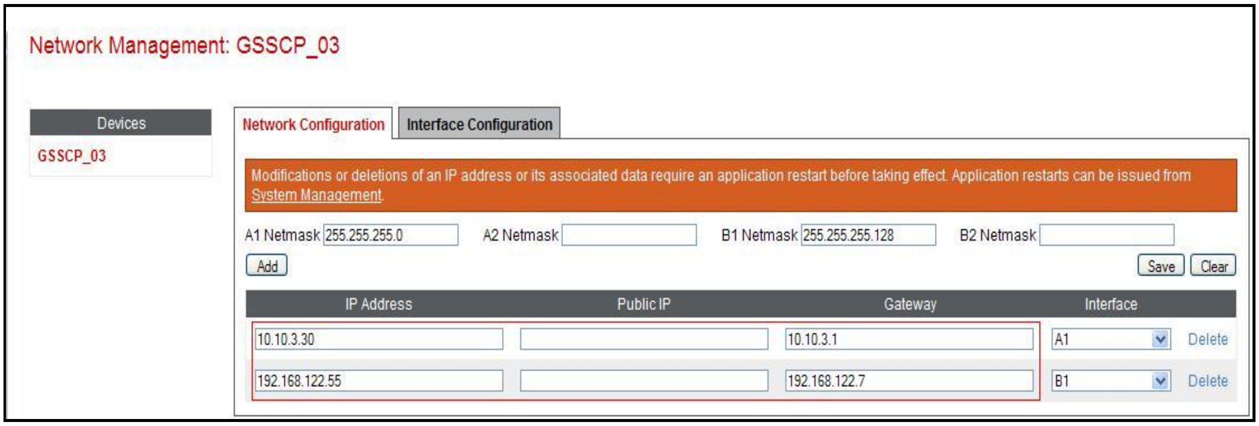
Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

7.3. Define Network Information

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

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

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



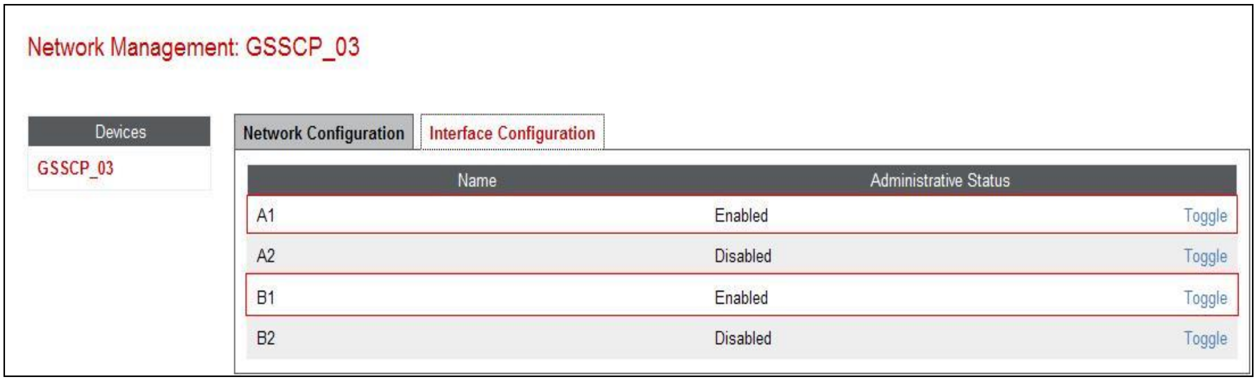
Network Management: GSSCP_03

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

A1 Netmask 255.255.255.0 A2 Netmask B1 Netmask 255.255.255.128 B2 Netmask

IP Address	Public IP	Gateway	Interface
10.10.3.30		10.10.3.1	A1
192.168.122.55		192.168.122.7	B1

Select the **Interface Configuration** tab and click on **Toggle State** to enable the interfaces.



Network Management: GSSCP_03

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

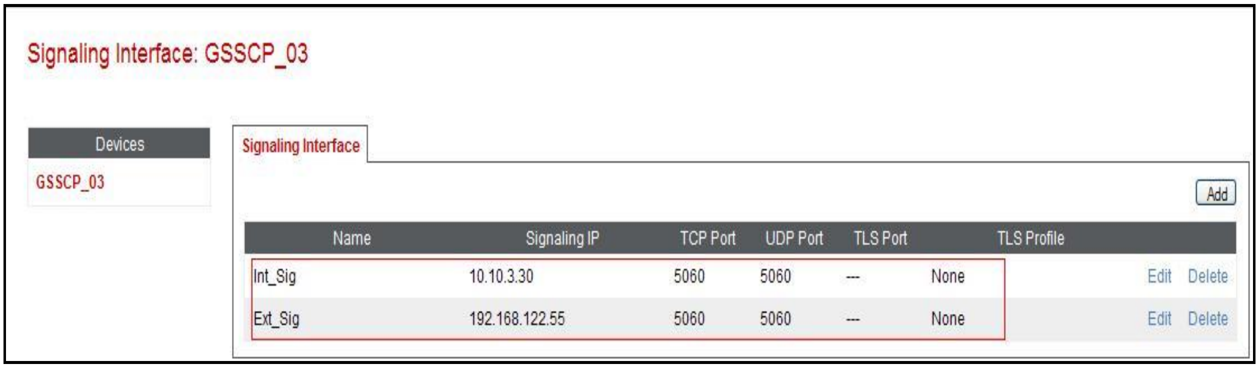
7.4. Define Interfaces

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

7.4.1. Signalling Interfaces

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

- Select **Add Signaling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal signalling interface
- For **Signaling IP**, select an **internal** signalling interface IP address defined in **Section 7.3**
- Select **UDP** and **TCP** port numbers, **5060** is used for the Session Manager
- Select **Add Signaling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external signalling interface
- For **Signaling IP**, select an **external** signalling interface IP address defined in **Section 7.3**
- Select **UDP** and **TCP** port numbers, **5060** is used for BT NOAS

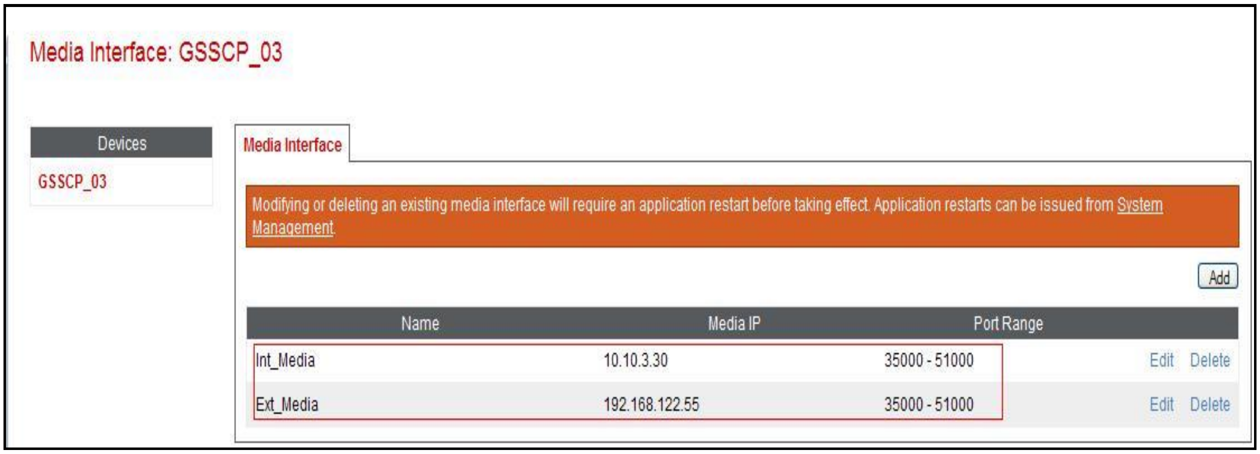


Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.3.30	5060	5060	---	None	Edit Delete
Ext_Sig	192.168.122.55	5060	5060	---	None	Edit Delete

7.4.2. Media Interfaces

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

- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface
- For **Media IP**, select an **internal** media interface IP address defined in **Section 7.3**
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external media interface
- For **Media IP**, select an **external** media interface IP address defined in **Section 7.3**
- Select **RTP port** ranges for the media path with BT NOAS SIP Trunk service



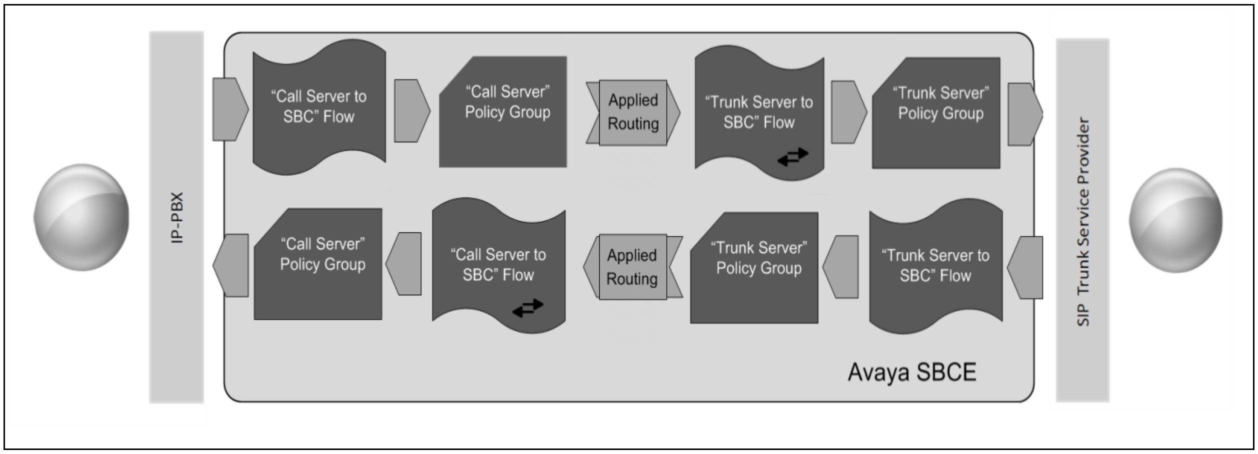
Media Interface: GSSCP_03

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

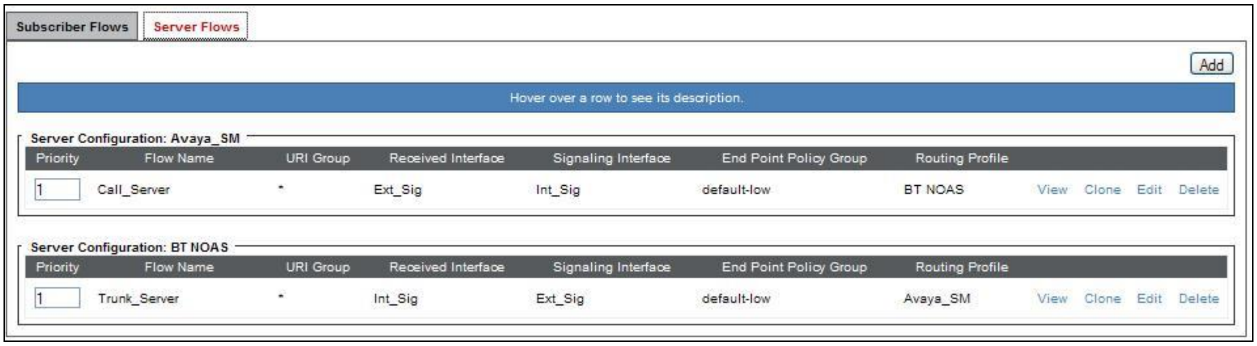
Name	Media IP	Port Range	
Int_Media	10.10.3.30	35000 - 51000	Edit Delete
Ext_Media	192.168.122.55	35000 - 51000	Edit Delete

7.5. Server Flows

When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.


IP-PBX
"Call Server to SBC" Flow
"Call Server" Policy Group
Applied Routing
"Trunk Server to SBC" Flow
"Trunk Server" Policy Group
"Call Server" Policy Group
"Call Server to SBC" Flow
Applied Routing
"Trunk Server" Policy Group
"Trunk Server to SBC" Flow
SIP Trunk Service Provider
Avaya SBCE

This configuration ties all the previously entered information together so that calls can be routed from Session Manager to BT NOAS SIP Trunk service and vice versa. The following screenshot shows both flows.



Server Configuration: Avaya_SM

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Call_Server	*	Ext_Sig	Int_Sig	default-low	BT NOAS	View	Clone	Edit	Delete

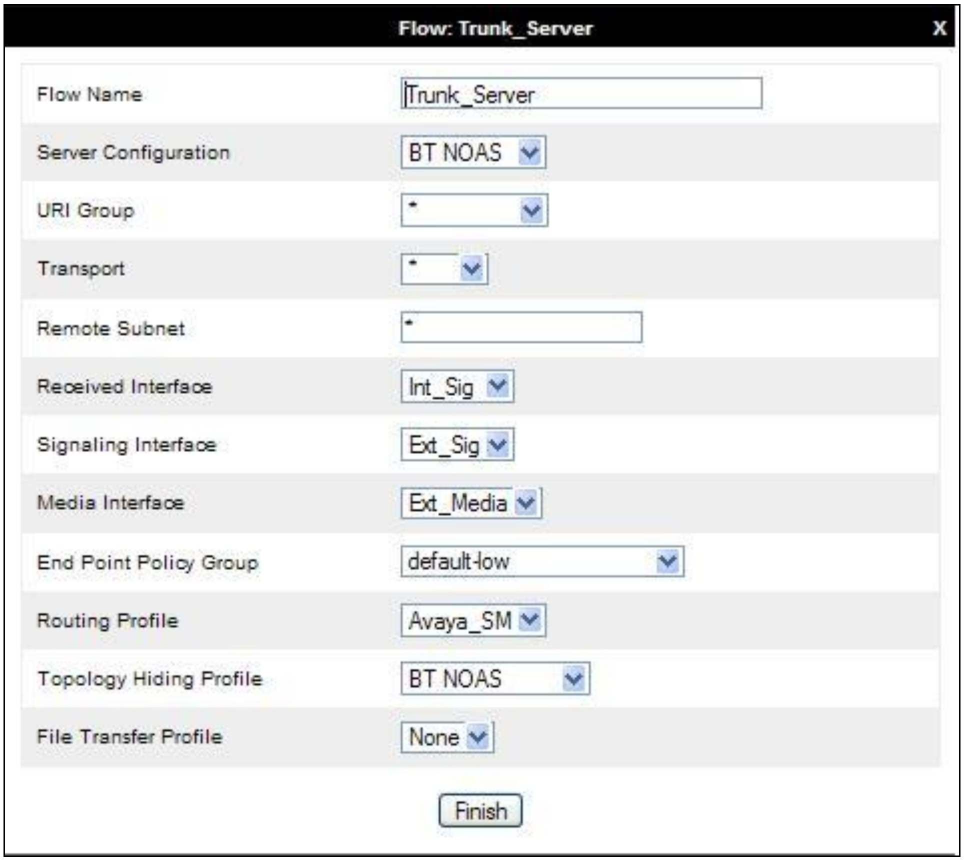
Server Configuration: BT NOAS

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Trunk_Server	*	Int_Sig	Ext_Sig	default-low	Avaya_SM	View	Clone	Edit	Delete

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

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the outgoing server flow to the BT NOAS SIP Trunk service
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**

- In the **Signalling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.2.3**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the BT NOAS SIP Trunk service defined in **Section 7.2.6** and click **Finish**



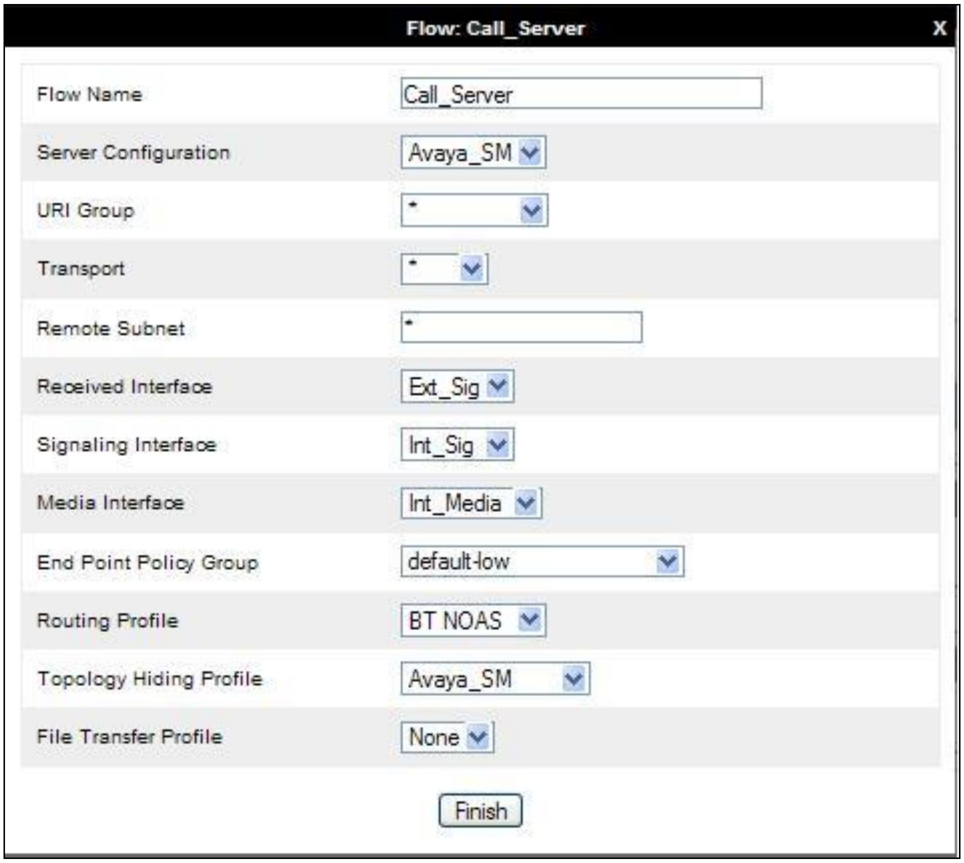
Flow: Trunk_Server

Flow Name	Trunk_Server
Server Configuration	BT NOAS
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
End Point Policy Group	default-low
Routing Profile	Avaya_SM
Topology Hiding Profile	BT NOAS
File Transfer Profile	None

The incoming Server Flows are defined as a reversal of the outgoing Server Flows

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the incoming server flow to Session Manager
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**
- In the **Signalling Interface** drop-down menu, select the internal SIP signalling defined in **Section 7.4.1**
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.4.2**

- In the **Routing Profile** drop-down menu, select the routing profile of the BT NOAS SIP Trunk service defined in **Section 7.2.3**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.2.6** and click **Finish**



Flow: Call_Server

Flow Name	Call_Server
Server Configuration	Avaya_SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Media
End Point Policy Group	default-low
Routing Profile	BT NOAS
Topology Hiding Profile	Avaya_SM
File Transfer Profile	None

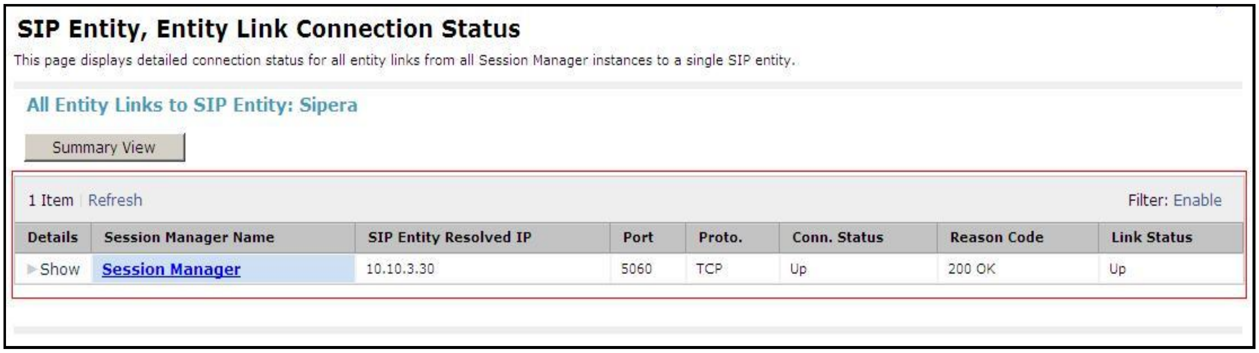
8. BT NOAS Configuration

The configuration of the BT NOAS equipment used to support the BT NOAS SIP Trunk service is outside of the scope of 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 Entities from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.



SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: Sipera

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶Show	Session Manager	10.10.3.30	5060	TCP	Up	200 OK	Up

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

```
status trunk 1

                                TRUNK GROUP STATUS

Member    Port     Service State       Mtce Connected Ports
                                       Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
```

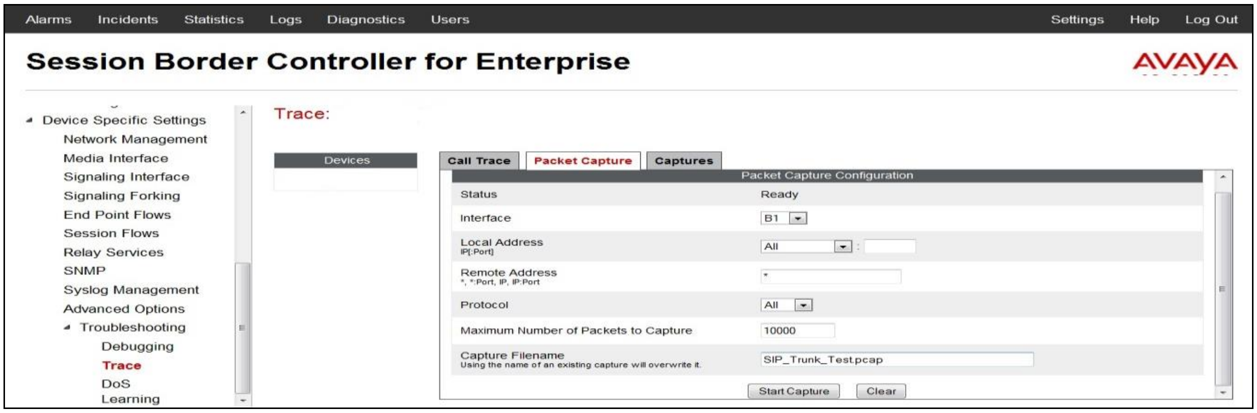
3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.

4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from the Session Manager via the Avaya SBCE to the network SBCs are receiving a response.

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

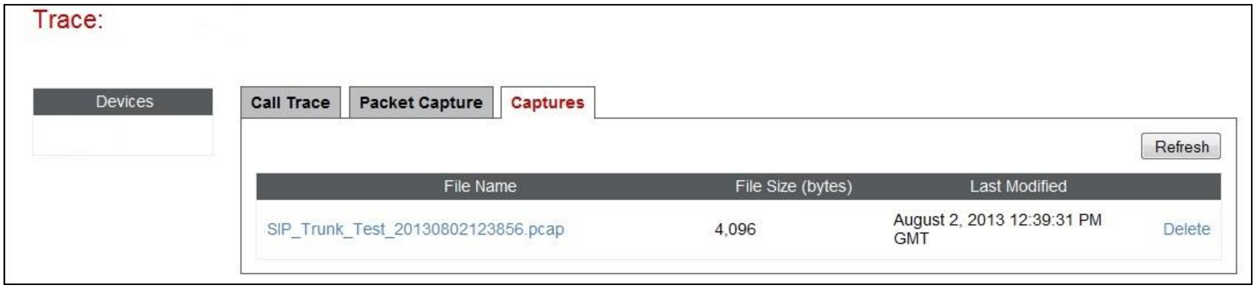
Select the SIP Trunk interface from the **Interface** drop down menu

- Select the signalling interface IP address from the **Local Address** drop down menu
- Enter the IP address of the Service Provider's SBC in the **Remote Address** field or enter a ***** to capture all traffic
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example
- Specify the filename of the resultant pcap file in the **Capture Filename** field
- Click on **Start Capture**.



Packet Capture Configuration	
Status	Ready
Interface	B1
Local Address IP[:Port]	All
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename Using the name of an existing capture will overwrite it.	SIP_Trunk_Test.pcap

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.



File Name	File Size (bytes)	Last Modified	
SIP_Trunk_Test_20130802123856.pcap	4,096	August 2, 2013 12:39:31 PM GMT	Delete

The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response in the form of a 200 OK will be seen from the Service Provider.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to BT NOAS SIP Trunk service. BT NOAS SIP Trunk service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

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

[1] [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3, May 2013.

[2] *Administering Avaya Aura® System Platform*, Release 6.3, May 2013.

[3] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, May 2013

[4] *Avaya Aura® Communication Manager 6.3 Documentation library*, August 2013.

[5] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013

[6] *Implementing Avaya Aura® System Manager* Release 6.3, May 2013

[7] *Upgrading Avaya Aura® System Manager to 6.3.2*, May 2013.

[8] *Administering Avaya Aura® System Manager* Release 6.3, May 2013

[9] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013

[10] *Implementing Avaya Aura® Session Manager* Release 6.3, May 2013

[11] *Upgrading Avaya Aura® Session Manager* Release 6.3, May 2013

[12] *Administering Avaya Aura® Session Manager* Release 6.3, June 2013,

[13] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2 June 2013

[14] *Upgrading Avaya Session Border Controller for Enterprise* Release 6.2 July 2013

[15] *Administering Avaya Session Border Controller for Enterprise* Release 6.2 March 2013

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

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