Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.3, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise R6.2 to Support Gamma IP Direct Connect SIP Trunking Service – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Gamma IP Direct Connect SIP Trunking Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Session Border Controller for Enterprise. Gamma Telecom is a member of the DevConnect Global SIP Service Provider program.

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Gamma IP Direct Connect SIP Trunking Service and an Avaya SIP enabled enterprise solution. IP Direct Connect (IPDC) is the product name for Gamma's SIP Trunking service, marketed and sold within the UK via authorised Channel Partners. The service provides VoIP connectivity for certified PBXs, allowing inbound and outbound telephony through Gamma's network for termination to both national and international destinations.

The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Session Border Controller for Enterprise (Avaya SBCE). Customers using this Avaya SIP-enabled enterprise solution with the Gamma IPDC service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

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

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DDI numbers assigned by Gamma. Incoming PSTN calls were made to H.323, SIP, Digital and Analog telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via Gamma to PSTN destinations using H.323, SIP, Digital and Analog telephones.
- Calls using G.729 and G.711A codec's.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using G.711 (T.38 is the only Avaya supported method of fax transmission).
- 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.
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones, and the Avaya Desktop Video Device (Avaya DVD) running Flare Experience.

- Call coverage and call forwarding for endpoints at the enterprise site.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Gamma IPDC service with the following observations:

- During Test, SIP 491 "Request Pending" message was seen on a small number of seemingly random outgoing calls with no noticeable effect.
- During test, the Avaya DVD running Flare started to fail to send media following the re-INVITE for shuffling. This was resolved by rebooting the Avaya DVD.
- No test call was made to the Emergency Services Operator as no test was booked.
- No Privacy header was received on incoming calls with withheld CLI. In this case, the equipment displays the user portion of the "From" URI.
- T.38 Fax is not supported.

2.3. Support

For technical support on Gamma SIP trunking, please contact an authorised Gamma Partner or visit the website at www.gamma.co.uk

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to Gamma IPDC. Located at the Enterprise site is an Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with SIP and H.323 firmware), Avaya A175 Desktop Video Device running Flare Experience, Avaya 2420 Digital telephone, Avaya analog telephone and fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Flare for Windows running on a laptop PC.

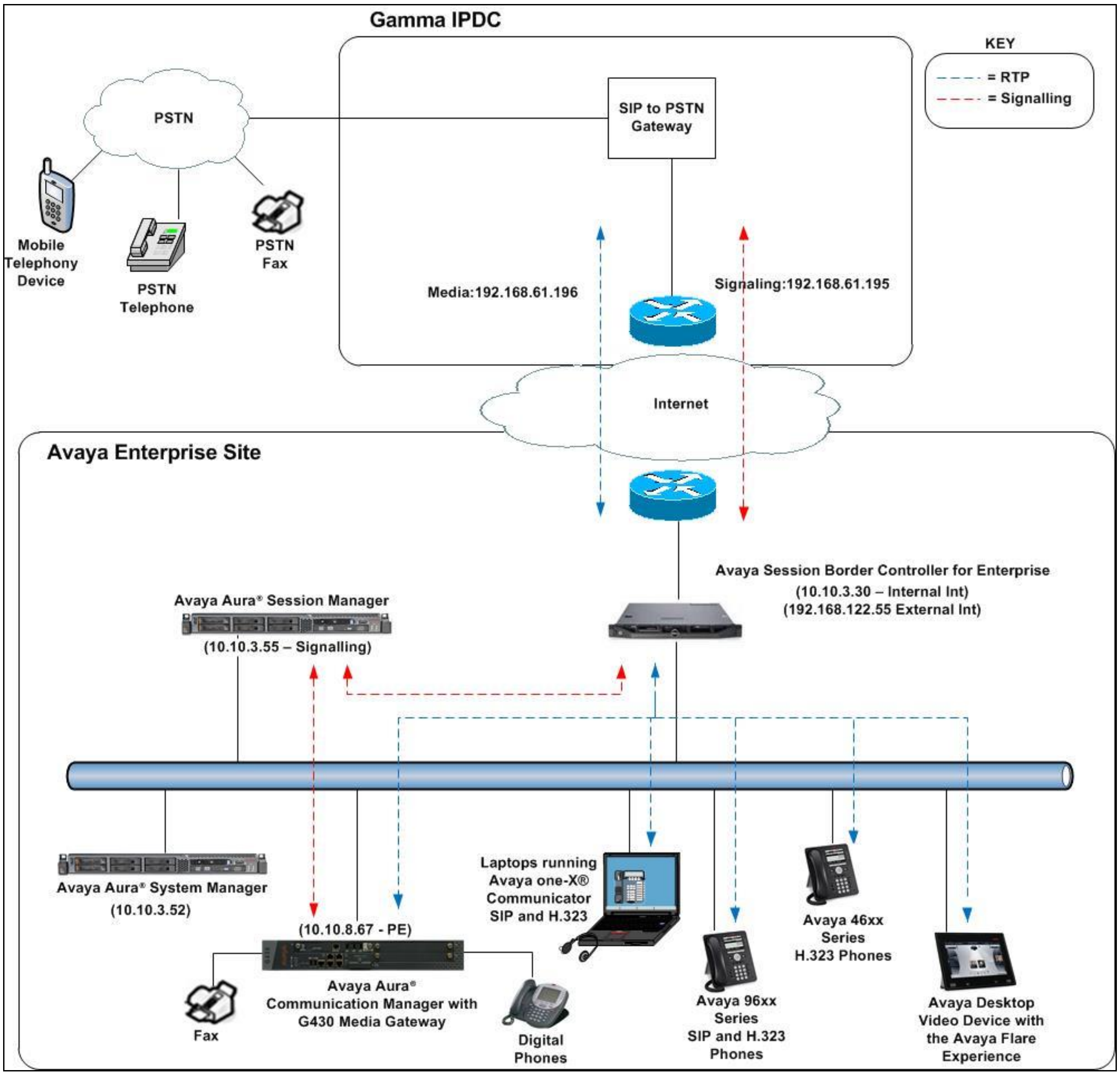


Figure 1: Gamma IP Direct Connect Solution Topology

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.3 Build R016x.03.0.124.0
Avaya G430 Media Gateway	FW 33.13.0
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.3 Build 6.3.3.0.633004
Avaya Aura® System Manager running on Avaya S8800 Server	R6.3 (Build No - 6.3.0.8.5682 -6.3.8.1814)
Avaya Session Border Controller running on Dell R210 V2 server	6.2.0.Q36
Avaya 9650 Phone (H.323)	3.171B
Avaya 9621 Phone (SIP)	6.2.0.72
Avaya 2420 Digital Phone	N/A
Analog Phone	N/A
Avaya 4620 Phone (H.323)	1.2200
Avaya 9611 Phone (SIP)	6.2.0.72
Avaya one-X® Communicator	6.1.3.06-SP3-35509
Avaya A175 Desktop Video Device (SIP)	Flare Experience Release 1.1
Gamma	
Genband S3 SBC	Code version 7.1.14.0
Ericsson TSS4 Softswitch	Code version R1F.5R.514.052
Marconi XCD Softswitch	Code version 4.2.1

5. Configure Avaya Aura ® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP signalling associated with the Gamma IPDC service. For incoming calls, the Session Manager receives SIP messages from the Avaya Session Border Controller for Enterprise (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 the Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Gamma 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 Gamma network, and any other SIP trunks used.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 12
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

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

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

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

           IP Attendant Consoles? y
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM100** and **10.10.3.55** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
SM100               10.10.3.55
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: default
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                   RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.4. Administer IP Codec Set

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

The Gamma IPDC service does not currently support T.38 for transmission of fax. Although not supported as a standard configuration by Avaya, G.711 transmission of fax was tested. To configure the CM to accept any fax transmission method, navigate to **Page 2** and configure by setting the **Fax Mode** to **off** as shown below.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n


                    Mode                   Redundancy
    FAX             off                     0              ECM: y
    Modem           off                     0
    TDD/TTY         US                      3
    Clear-channel   n                       0
```

5.5. Administer SIP Signaling Groups

The signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Gamma IPDC 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, where **x** is an available signalling group, as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tcp**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region **1**)
- Leave **Far-end Domain** blank (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 signalling 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 (in the test system the dial plan includes 1 as a three digit dac – not shown)
- 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 upon with Gamma 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): 1800

 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
```

On **Page 4** of this form:

- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Gamma
- Set **Always Use re-INVITE for Display Updates** to **y** as the most effective method employed by the CM of modifying an existing dialogue

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

                                       Mark Users as Phone? n
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 Gamma 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 1                                          Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 4  60               1          1635xxxxx0       10    Total Administered: 5
 4  61               1          1635xxxxx0       10    Maximum Entries: 540
 4  6100             1          1635xxxxx0       10
 4  6102             1          1635xxxxx0       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 Gamma IPDC service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

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

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to national, international and some Operator numbers. 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: 0

          Dialed          Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
    0                    8    14     1       pubu         n
    00                   13   17     1       pubu         n
    00353                10   14     1       pubu         n
    0044                 12   14     1       pubu         n
    01                   7    14     1       pubu         n
    0800                 11   11     1       pubu         n
    118                  5    6      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:
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 1    0                                                               n   user
 2:                                                                      n   user
 3:                                                                      n   user
 4:                                                                      n   user
 5:                                                                      n   user
 6:                                                                      n   user

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

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Gamma can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by Gamma for testing are assigned to the internal extensions of the test equipment configured within the Communication Manager. The **change inc-call-handling-trmt trunk-group 1** command is used to translate numbers **01635xxxxx0** to **01635xxxxx8** to the 4 digit extension by deleting **all** of the incoming digits and inserting the extension number. Note that the significant digits beyond the city code have been obscured.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of   3
                         INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    11 01635xxxxx0      all 6100
 public-ntwrk    11 01635xxxxx2      all 6102
 public-ntwrk    11 01635xxxxx3      all 6003
 public-ntwrk    11 01635xxxxx4      all 6004
 public-ntwrk    11 01635xxxxx5      all 6005
 public-ntwrk    11 01635xxxxx6      all 8501
 public-ntwrk    11 01635xxxxx7      all 6104
 public-ntwrk    11 01635xxxxx8      all 6006
```

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 6100. Use the command **change off-pbx-telephone station mapping x** where **x** is the Communication Manager station.

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

```
change off-pbx-telephone station-mapping 6100                   Page   1 of   3
                    STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number     Trunk       Config  Dual
 Extension                 Prefix                      Selection   Set     Mode
 6100            EC500         -      0035386xxxxxxx    1          1
                               -
```

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

6. Configuring Avaya Aura® Session Manager

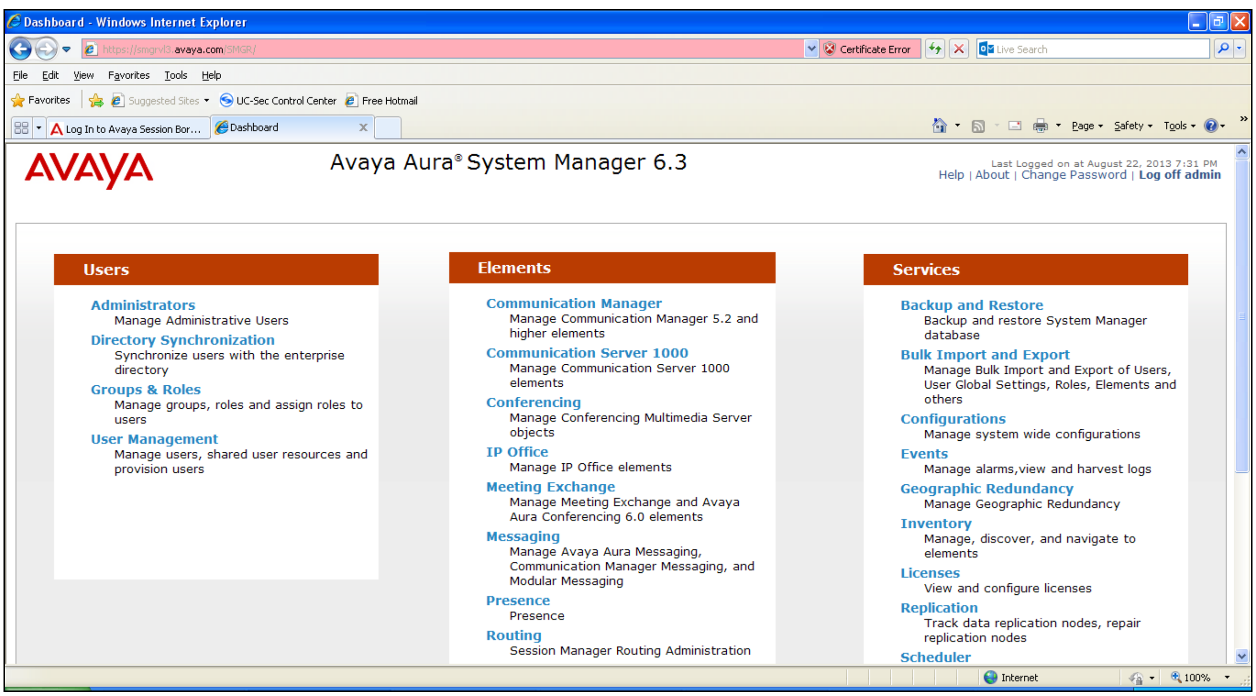
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager.
- Administer SIP domain.
- Administer SIP Location.
- 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

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL https://<ip-address>/SMGR, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed.



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.

6.3. Administer Locations

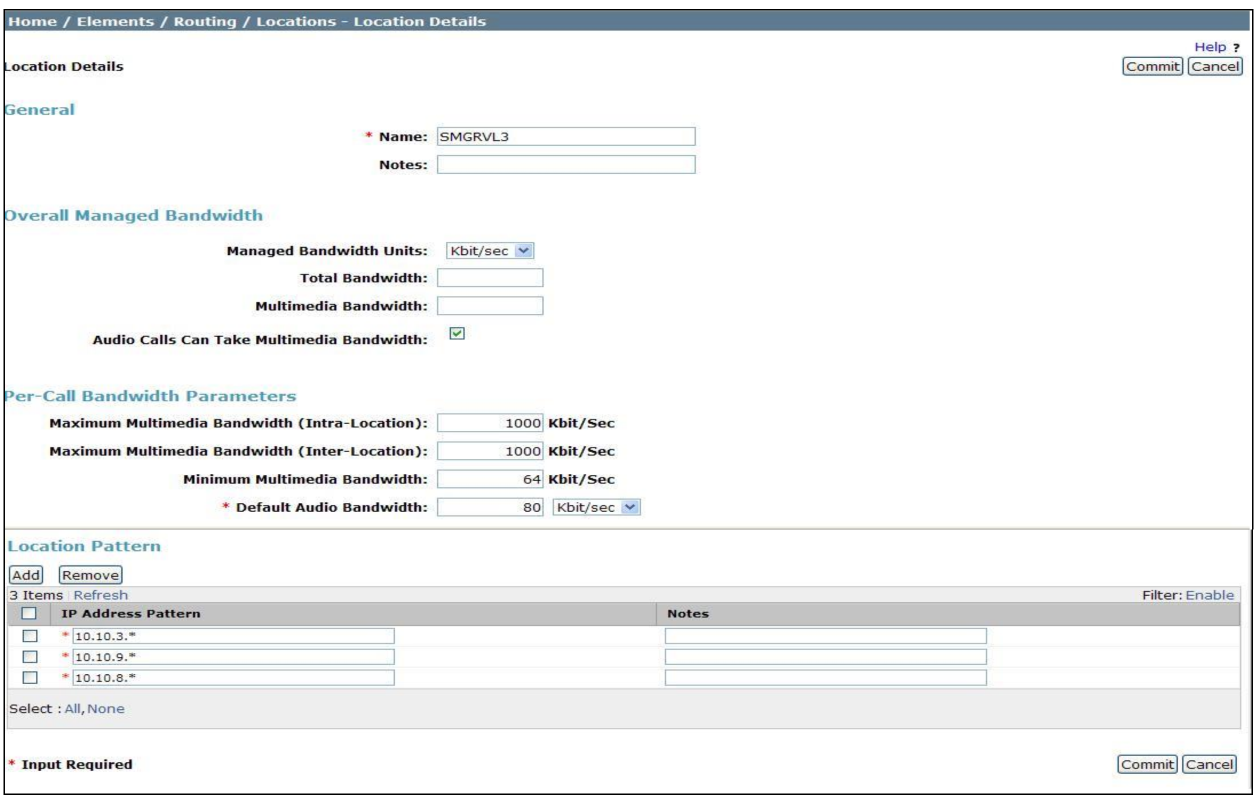
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). 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 **SMGRVL3** defined for the compliance testing.



6.4. Administer SIP Entities

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

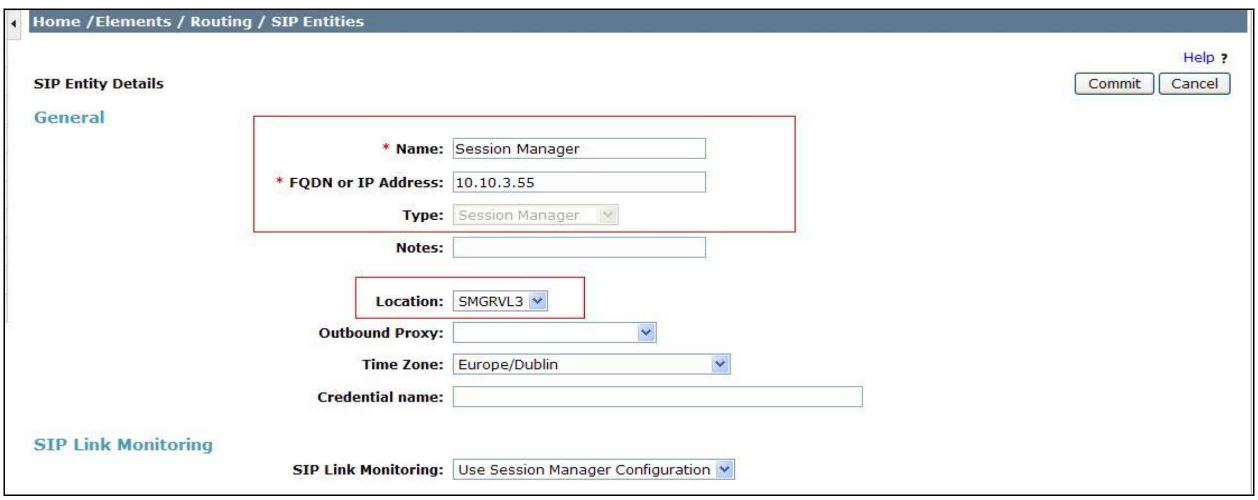
- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP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

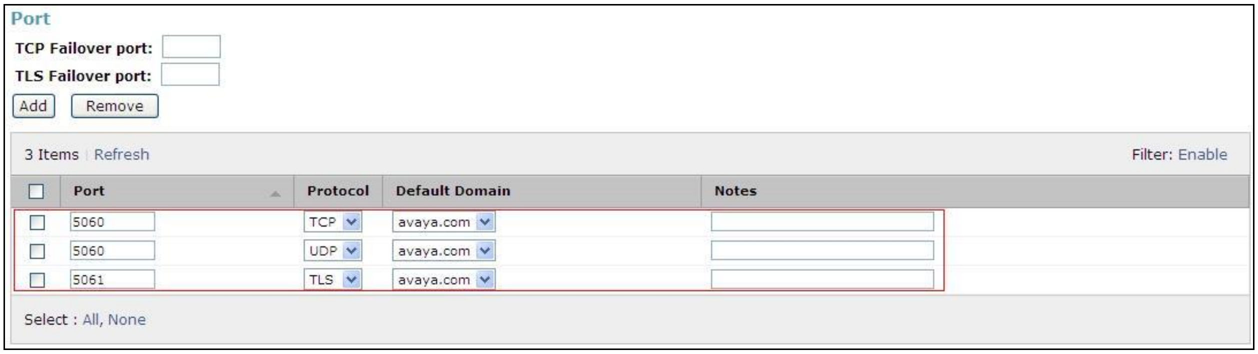
6.4.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface.



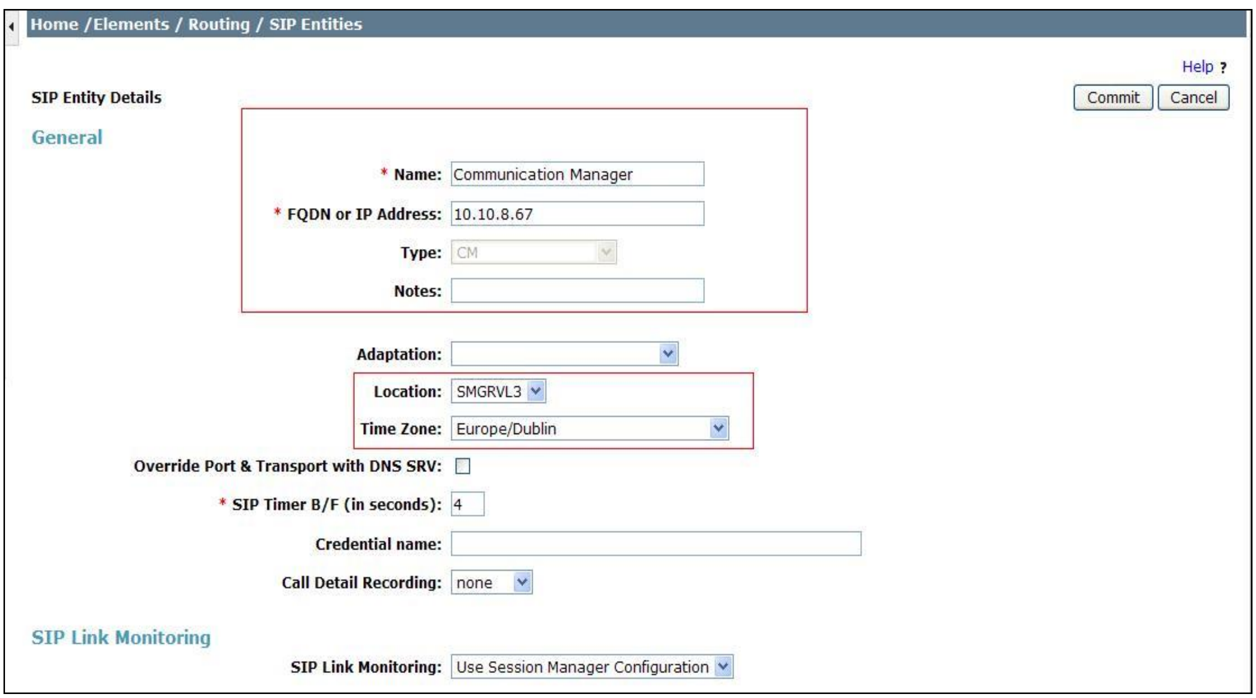
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these, scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

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



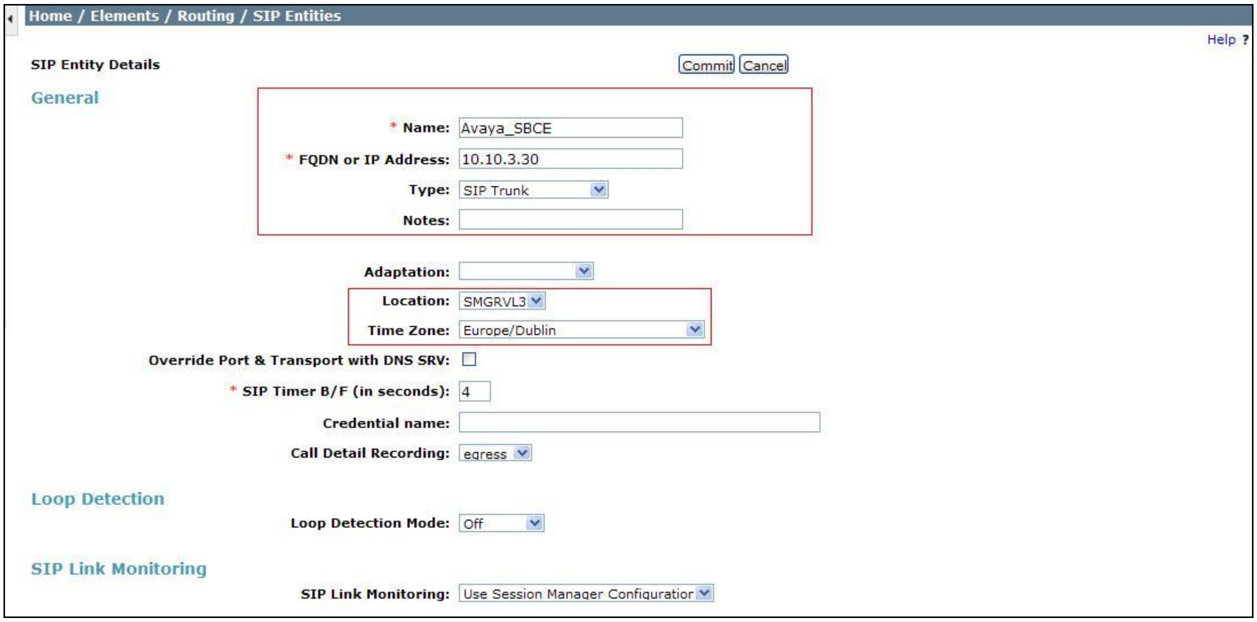
6.4.2. Avaya Aura® Communication Manager SIP Entity

The following screens show 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 signalling. The entity **Type** is set to **CM**. Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.



6.4.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP entity for the Avaya SBCE used for routing calls. The **FQDN or IP Address** field is set to the IP address of the private interfaces administered in **Section 7** of this document. Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

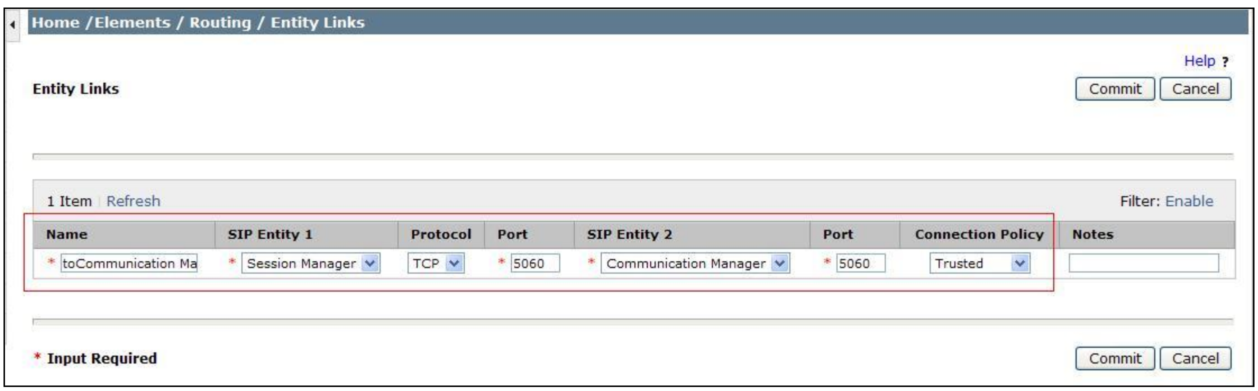


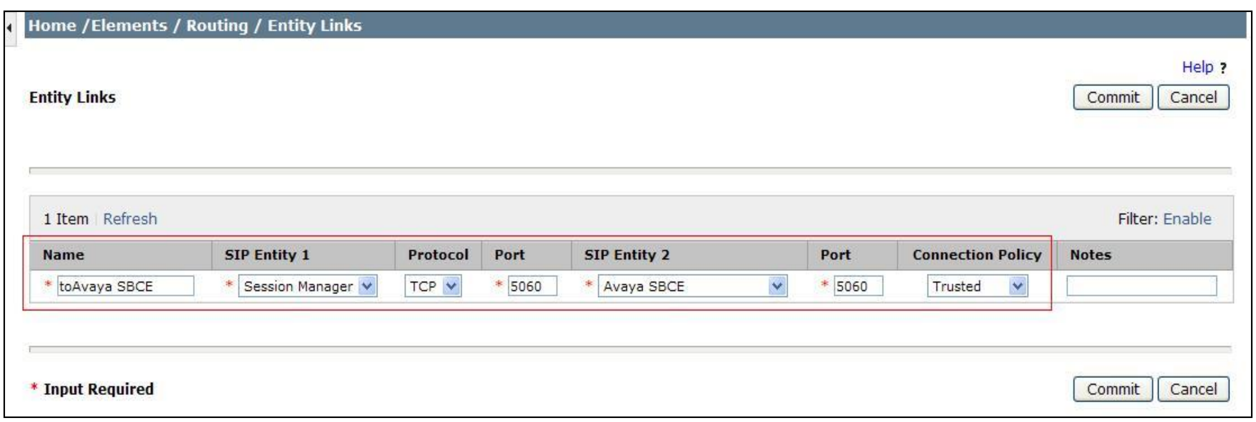
6.5. Administer Entity Links

A SIP trunk between 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 6.4**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Select **Trusted** from the drop down menu to make the other system trusted.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.

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





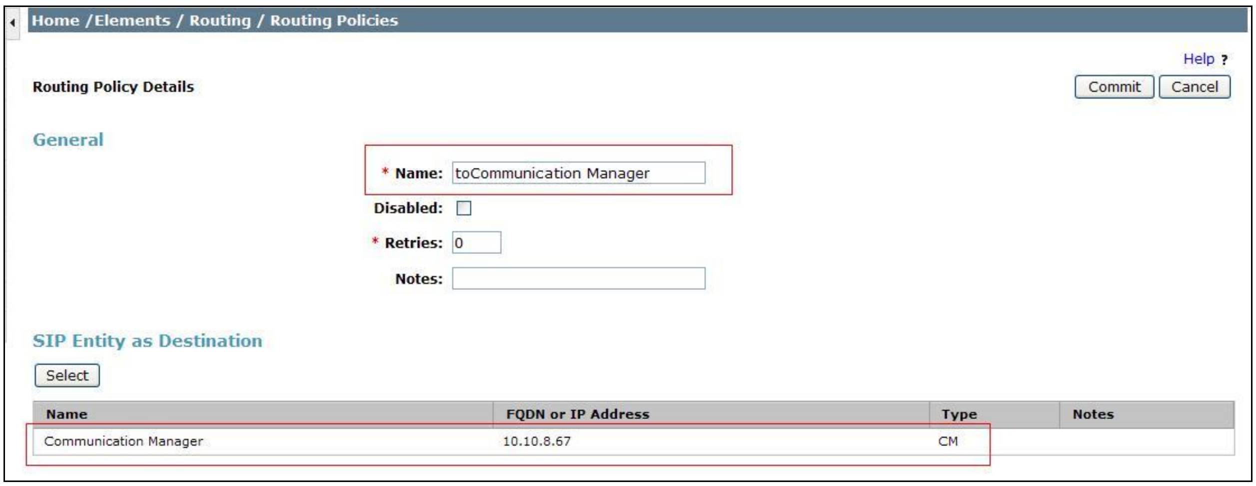
6.6. Administer Routing Policies

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

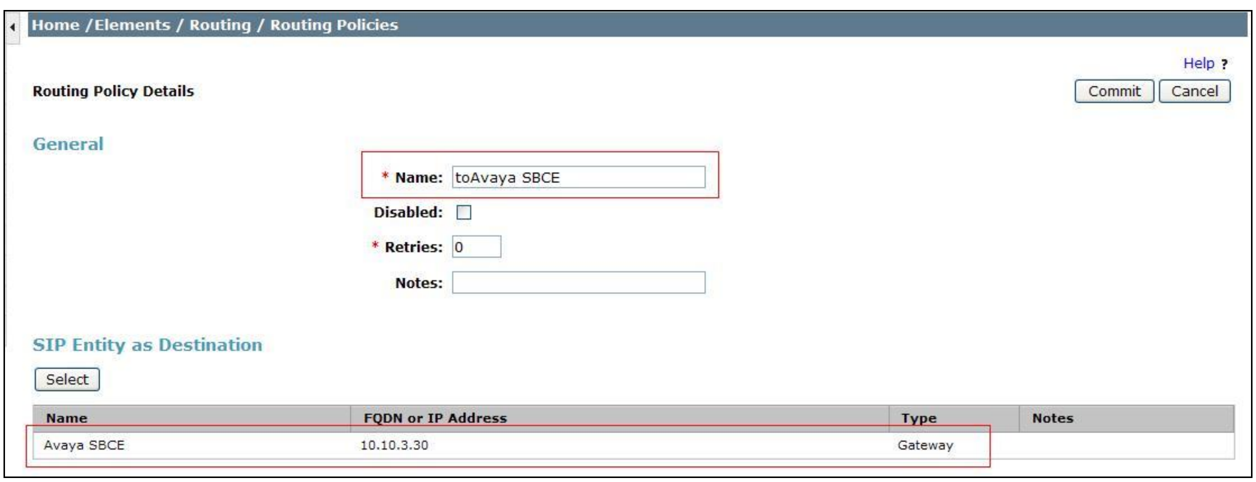
Under **General**:

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

The following screen shows the routing policy for Communication Manager:



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



6.7. Administer Dial Patterns

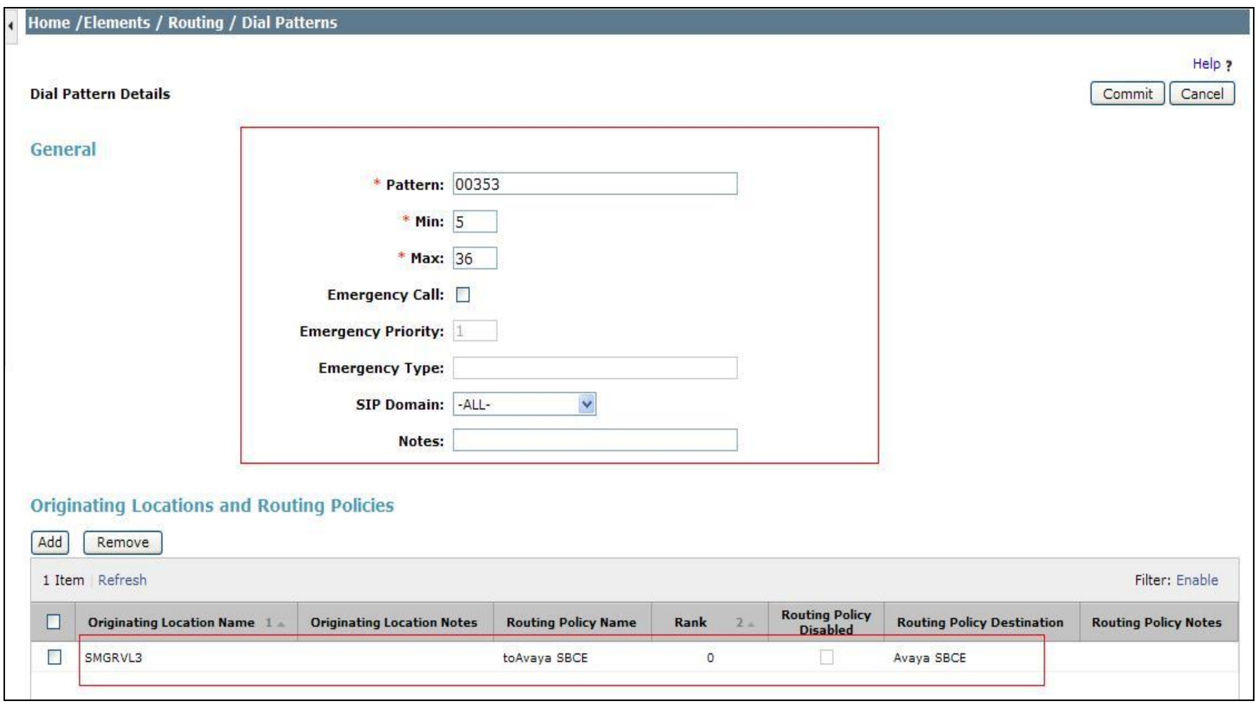
A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

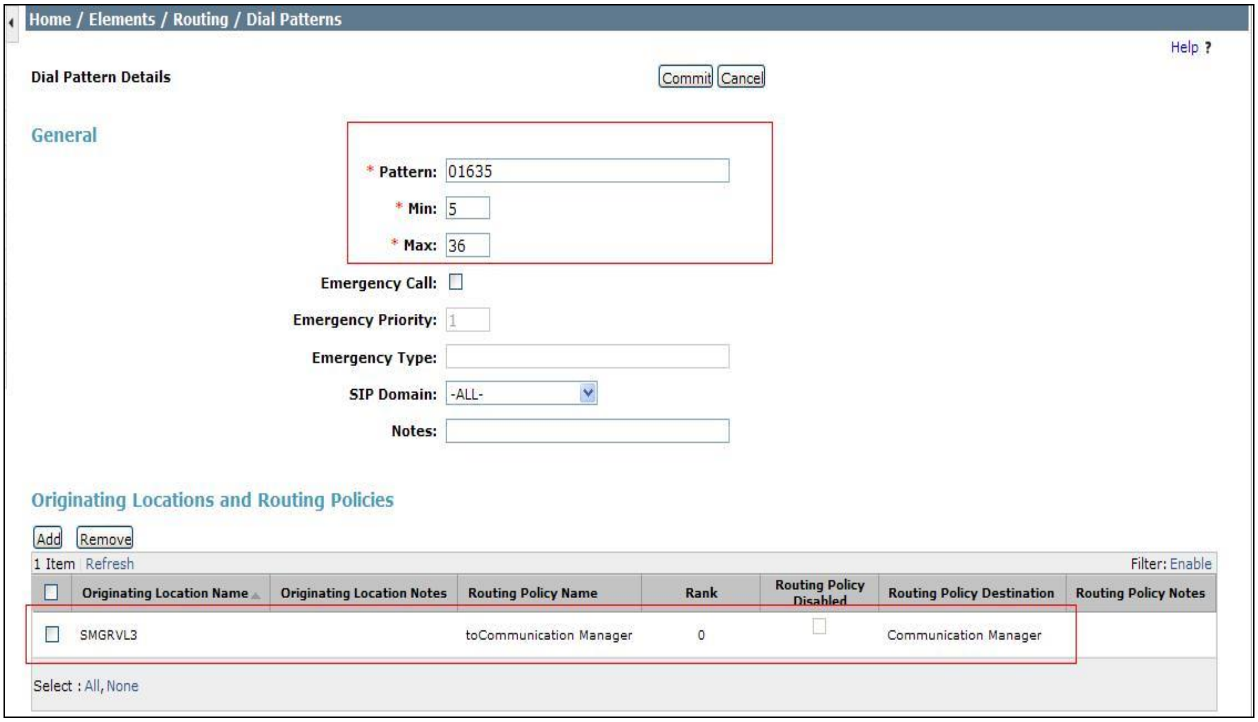
- In the **Pattern** field enter a dialled number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialled number.
- In the **Max** field enter the maximum length of the dialled number.
- In the **SIP Domain** field select **–ALL-**.

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown) under **Originating Location** select **Locations** created in **Section 6.3** and under **Routing Policies** select one of the routing policies defined in **Section 6.6**. Click **Select** button to save (not shown).

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the PSTN via the Gamma SIP Trunk Service.



The following screen shows the test dial pattern configured for Communication Manager. Note that the number format received from Gamma was national with leading 0.

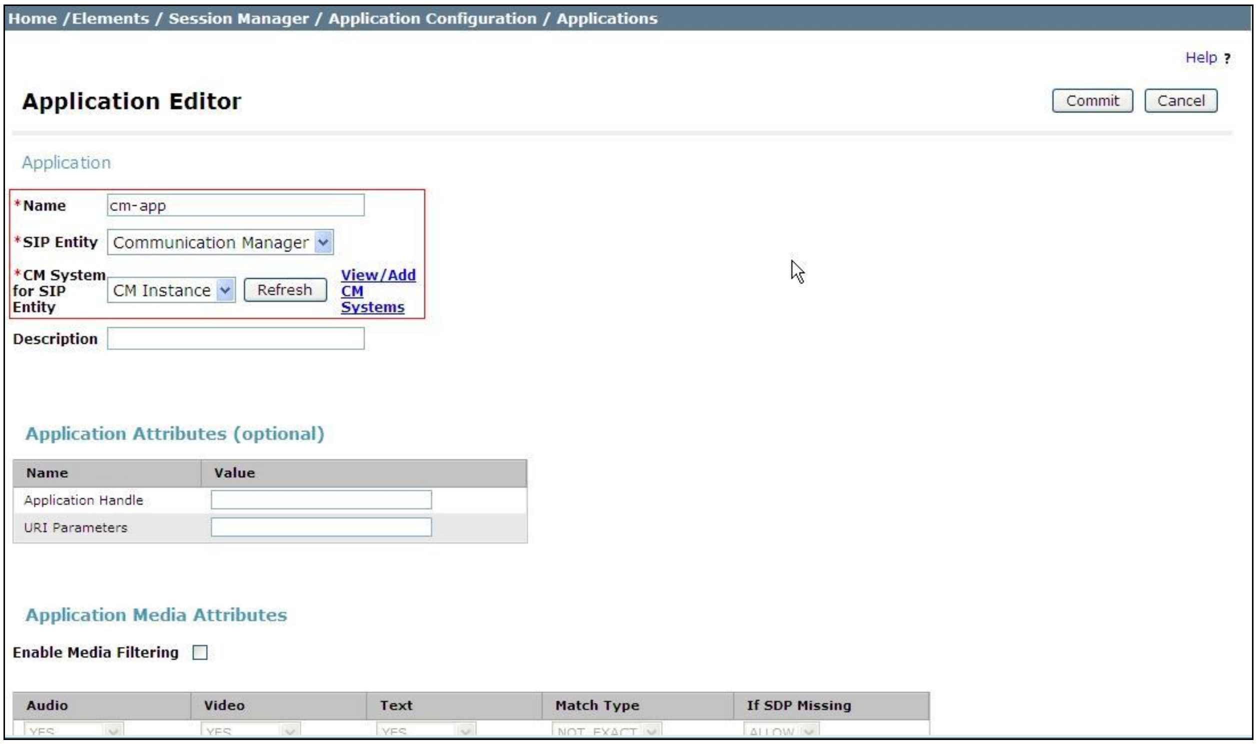


6.8. Administer Application for Avaya Aura® Communication Manager

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

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

Select **Commit** to save the configuration.

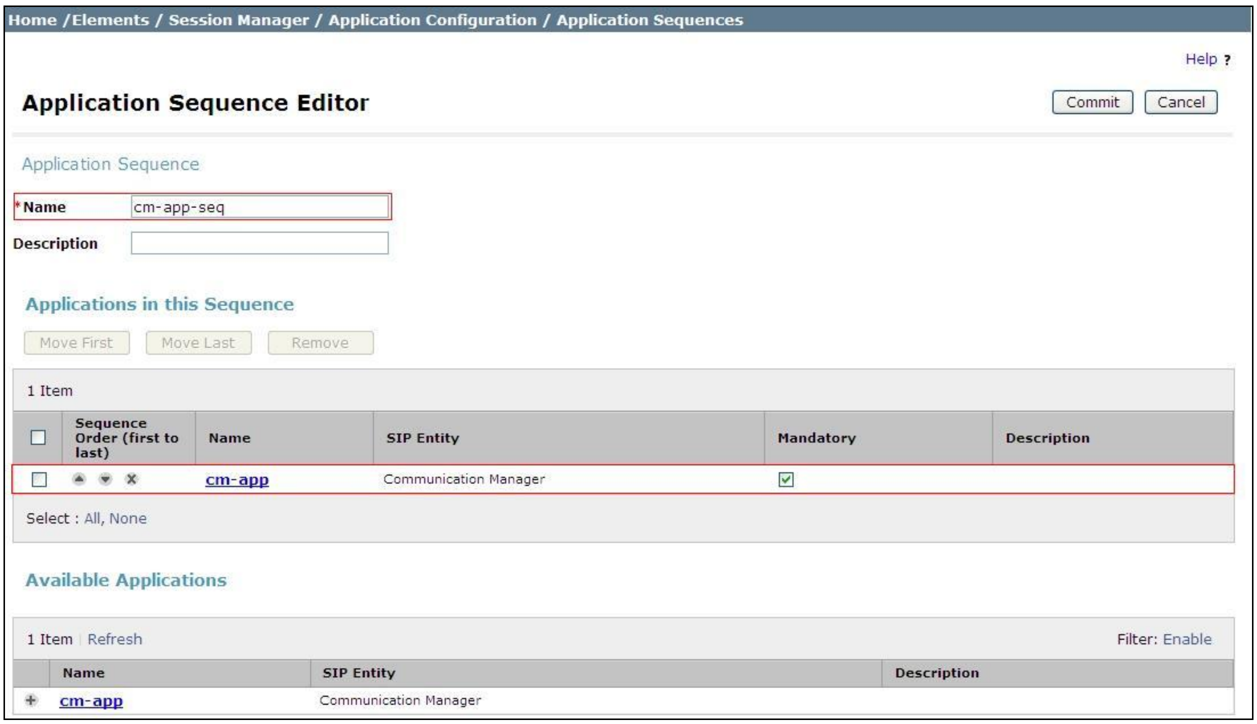


6.9. Administer Application Sequence for Avaya Aura® Communication Manager

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

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

Select **Commit**.

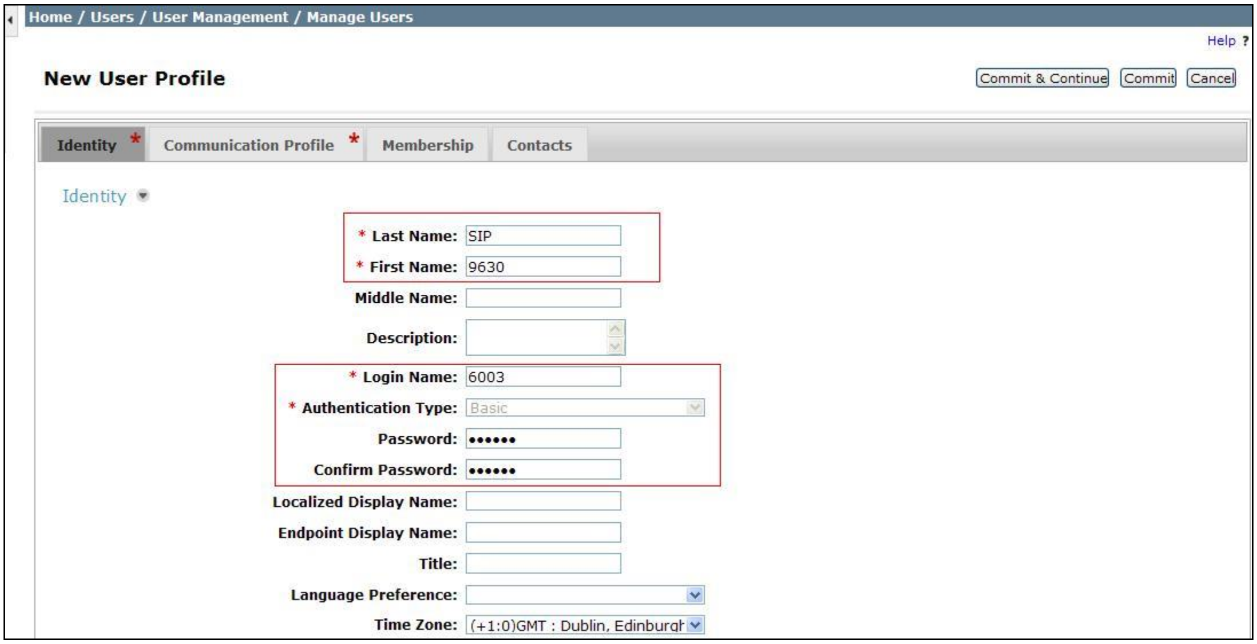


6.10. Administer SIP Extensions

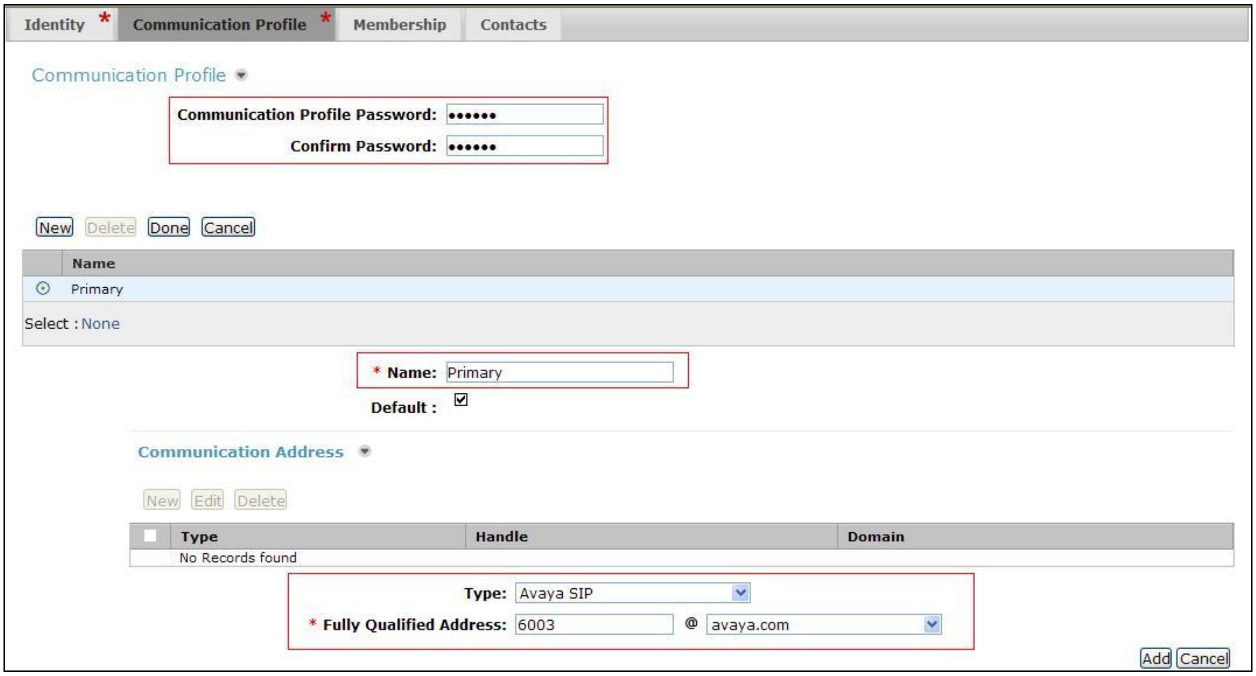
SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the Home tab, select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of **user@domain** (e.g.**6003@avaya.com**) which is used to create the user's primary handle
- The **Authentication Type** should be **Basic**
- In the **Password/Confirm Password** fields enter an alphanumeric password

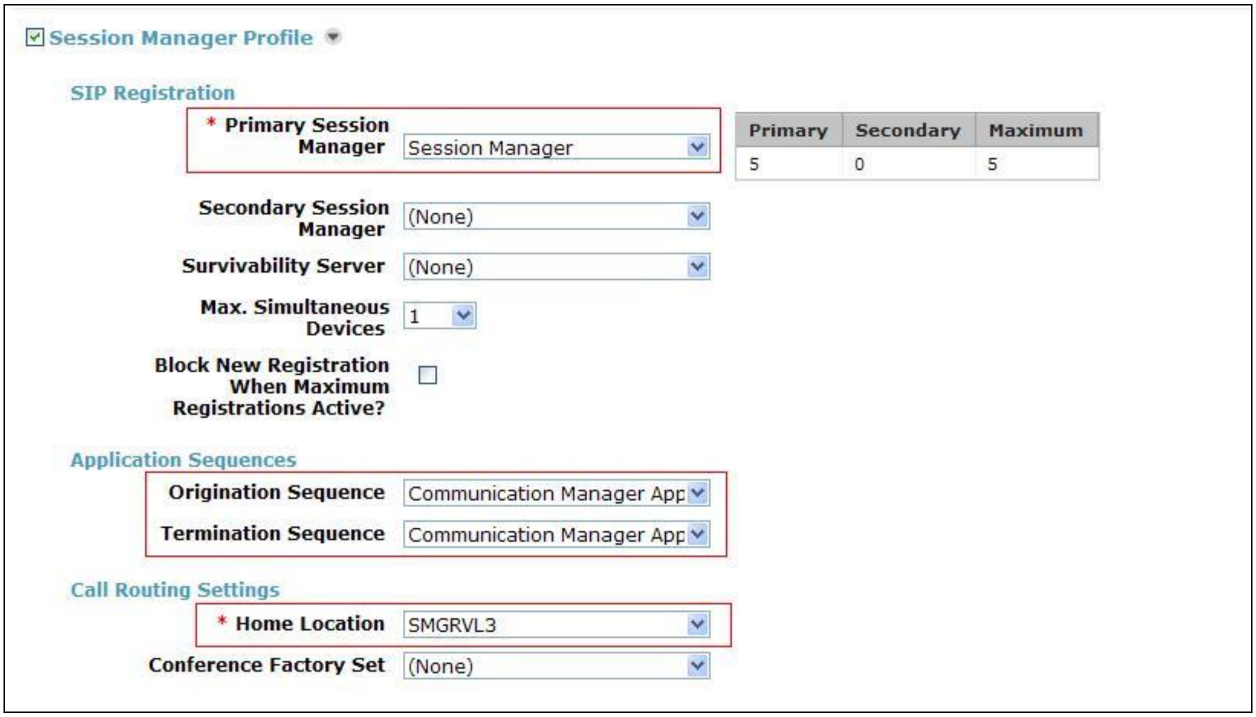


On the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it, then expand the **Communication Address** section and click **New**. For the **Type** field, select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension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



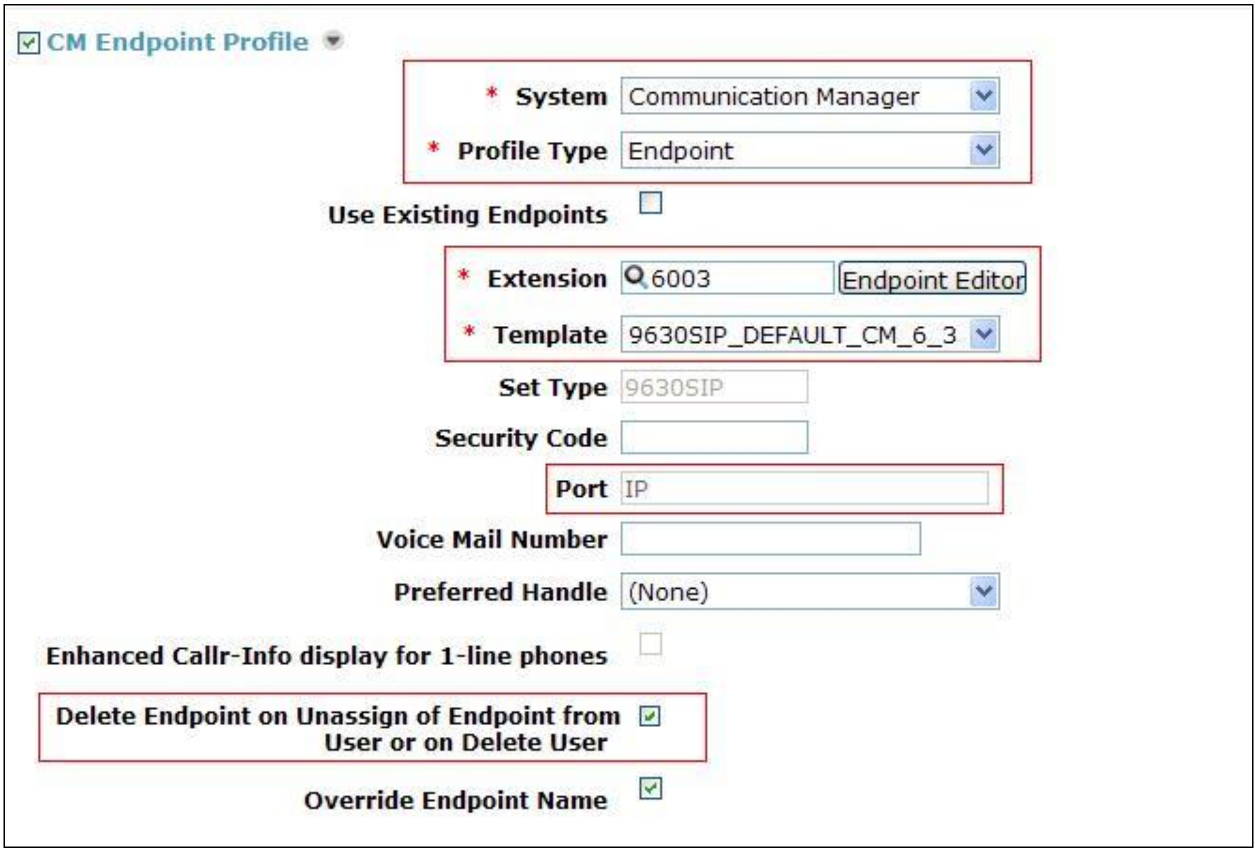
Expand the **Session Manager Profile** section.

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



Expand the **Endpoint Profile** section.

- Select the Communication Manager SIP Entity from the **System** drop-down menu
- Select **Endpoint** from the drop-down menu for **Profile Type**
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- For the **Port** field select **IP**
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box
- Select **Commit** (not shown) to save changes and the System Manager will add the Communication Manager user configuration automatically

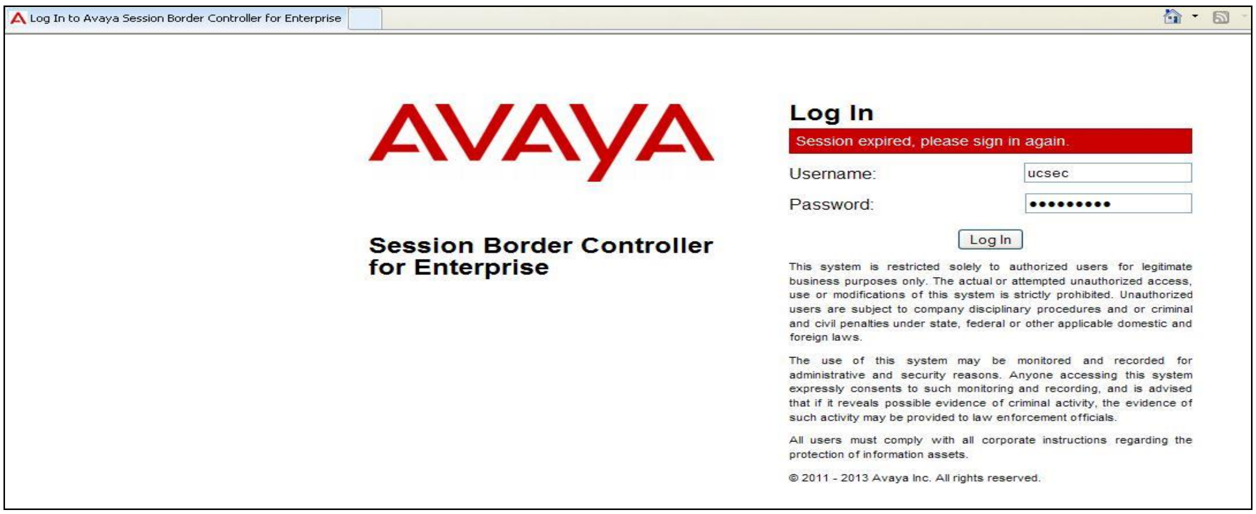


7. Configure Avaya Session Border Controller for Enterprise

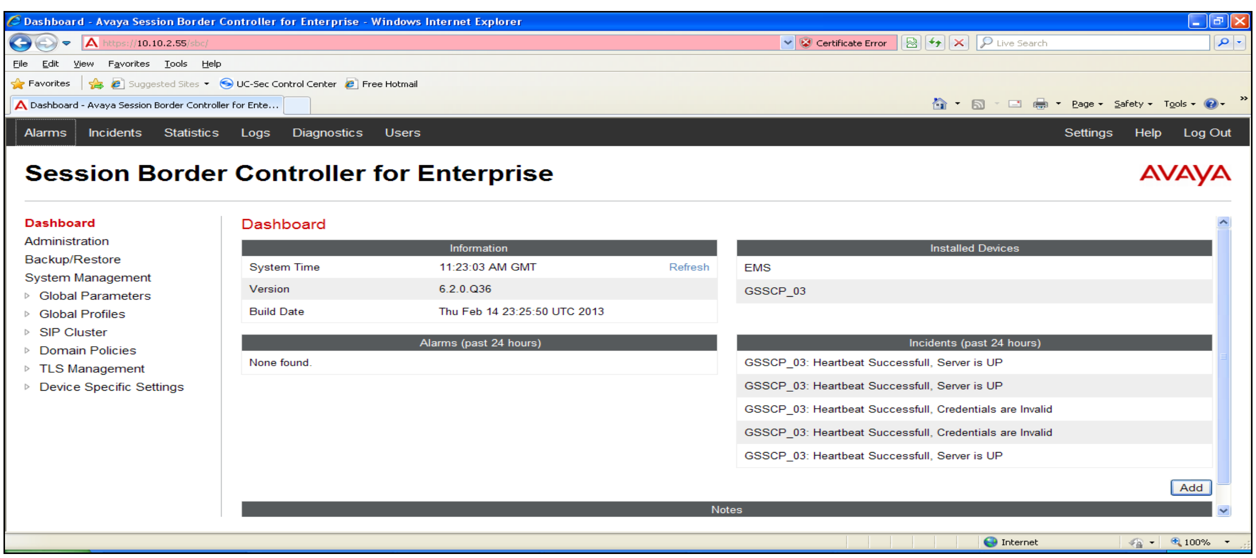
This section describes the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed.

7.1. Access Avaya Session Border Controller for Enterprise

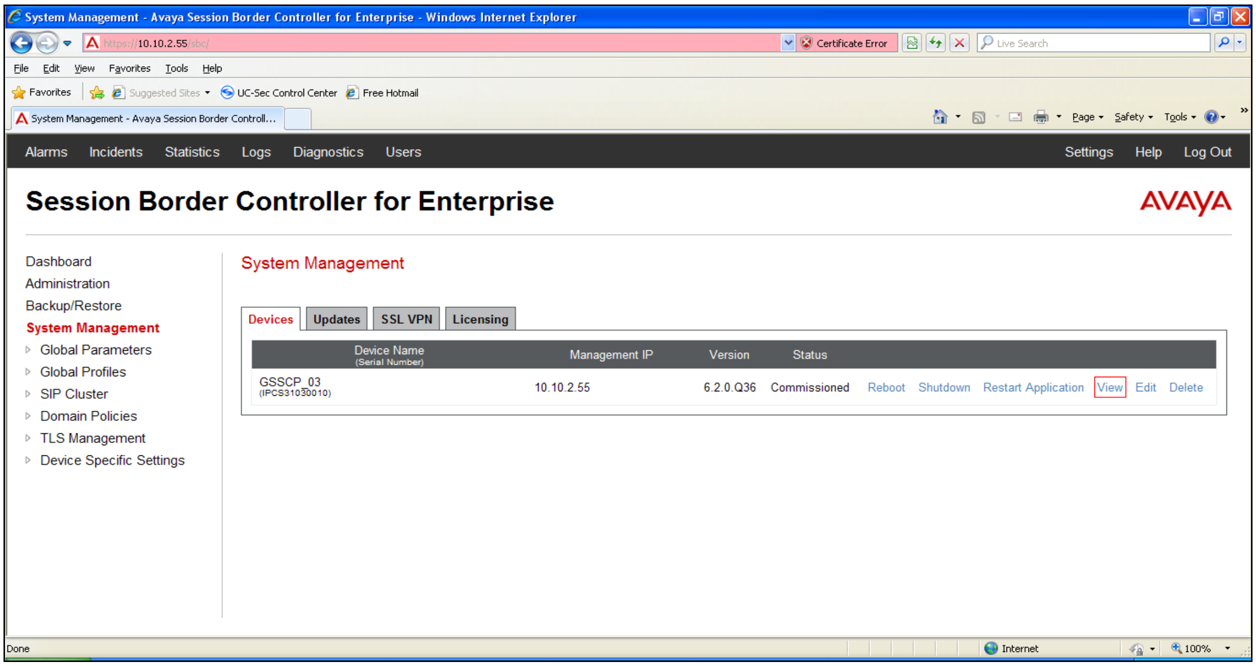
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



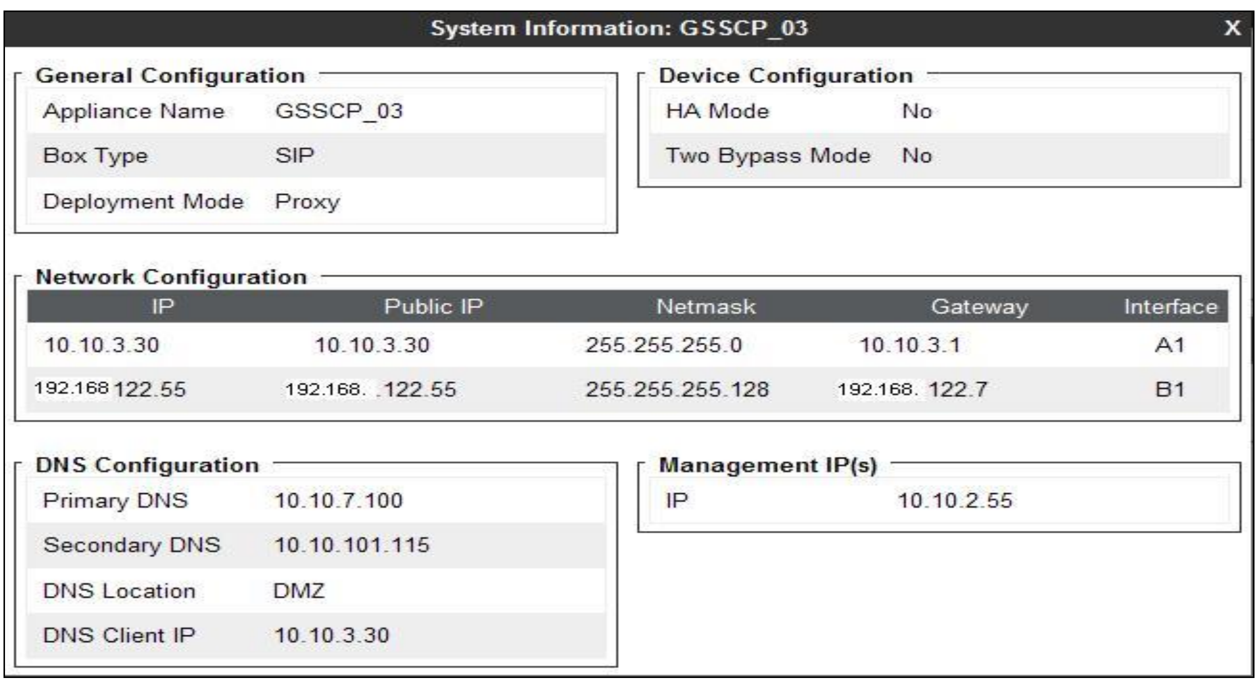
The main page of the Avaya SBCE will appear.



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).



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



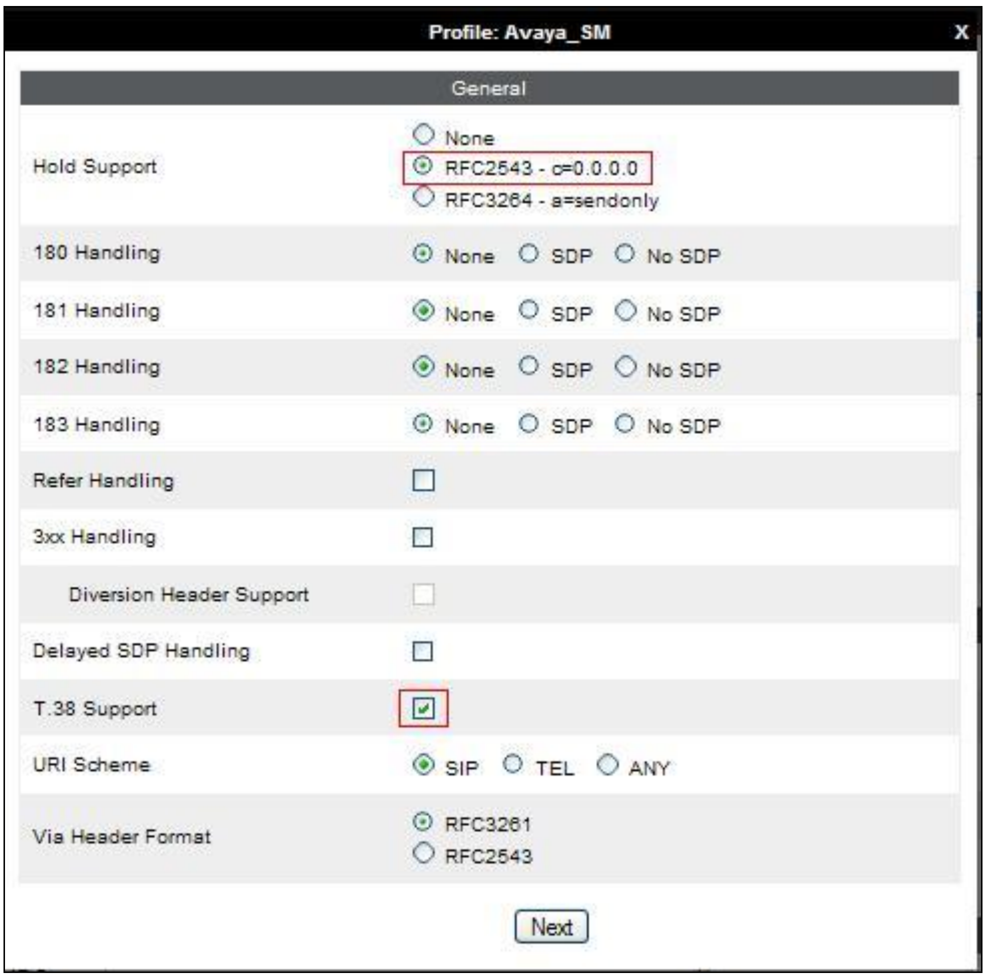
7.2. Global Profiles

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

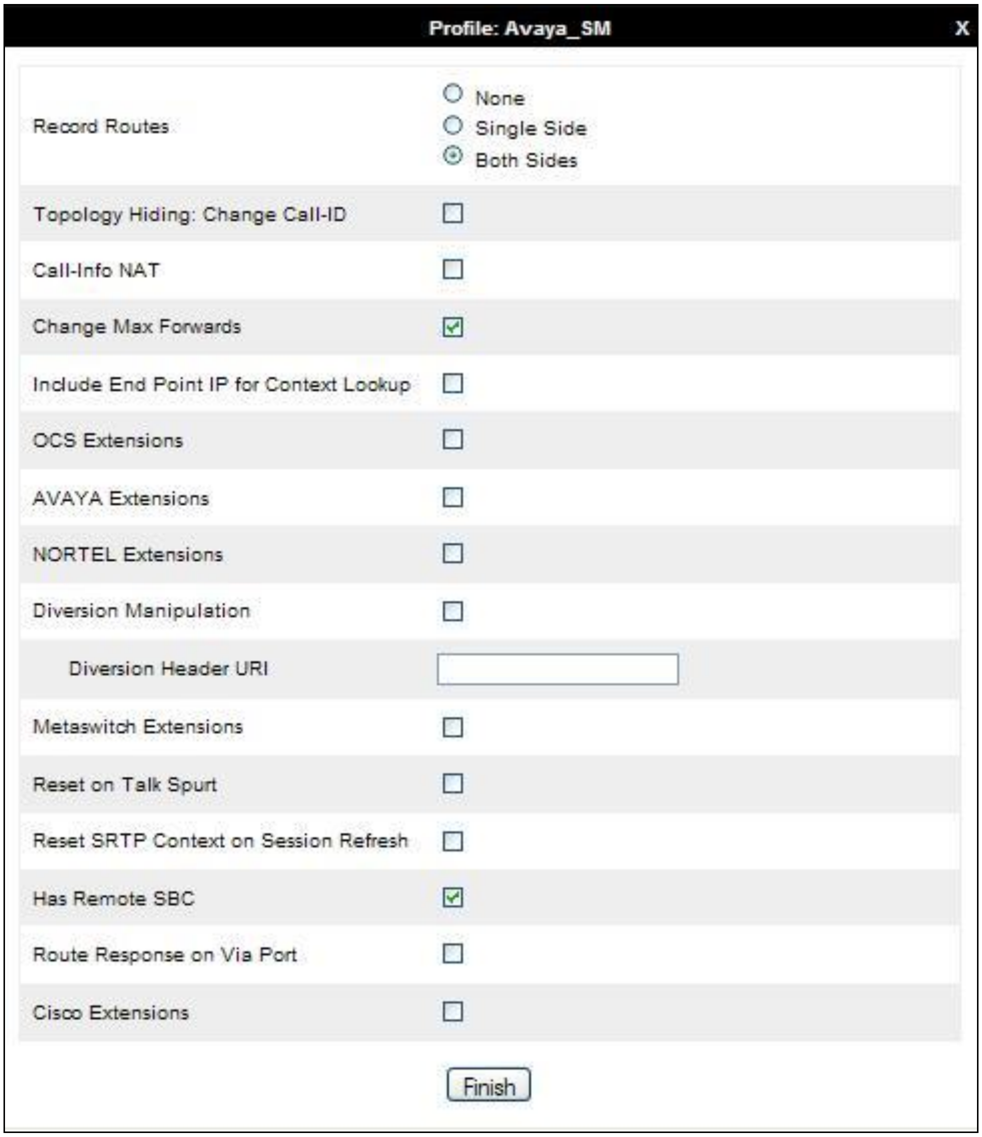
7.2.1. Server Internetworking - Avaya

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** = **RFC2543**
- Check **T.38 Support**
- All other options on the **General** Tab can be left at default



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

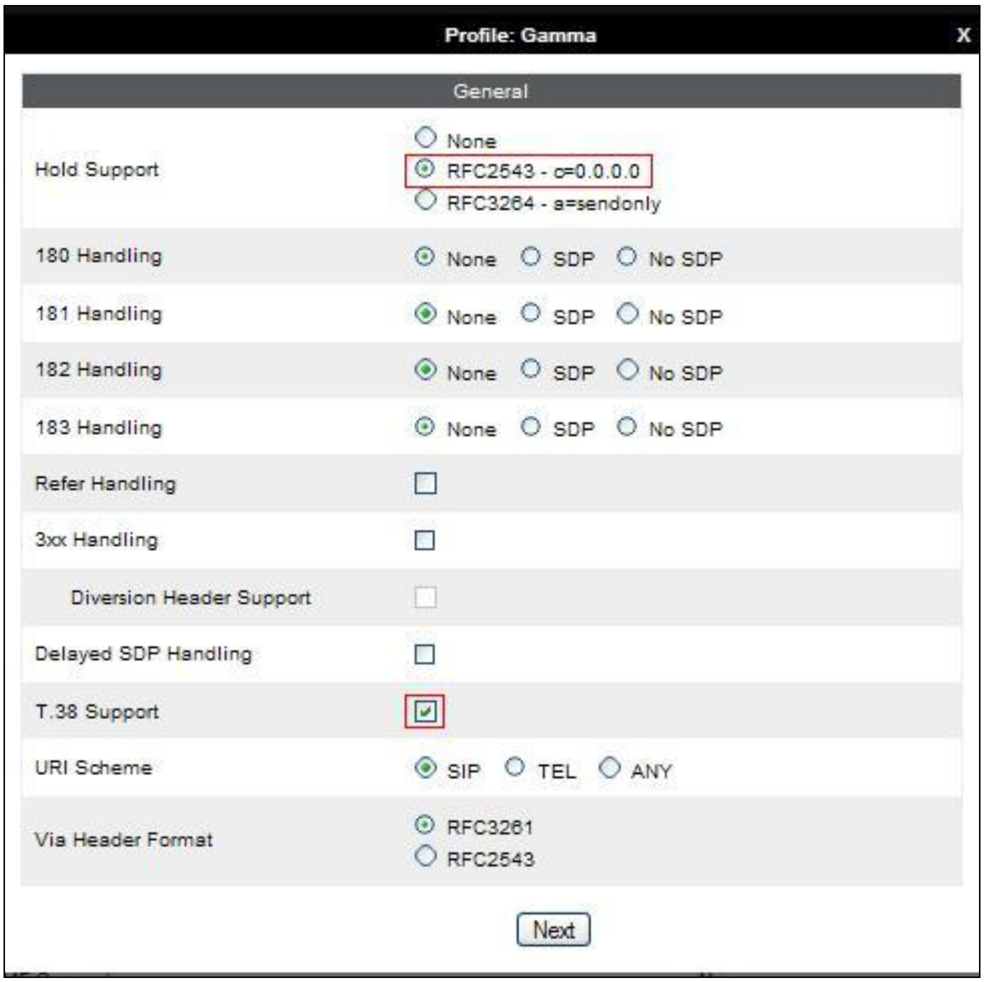


7.2.2. Server Internetworking – Gamma

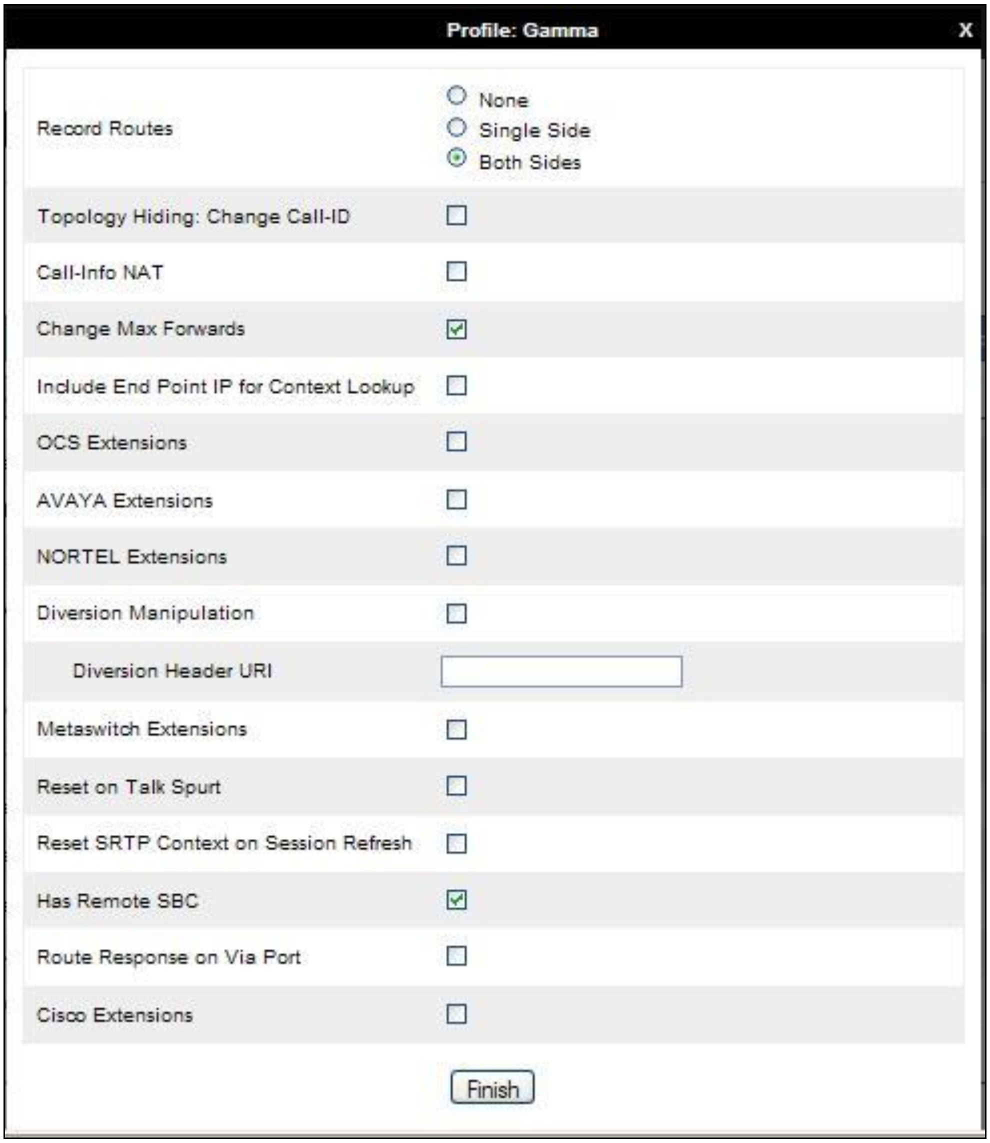
Server Internetworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38. From the lefthand menu select **Global Profiles → Server Interworking** and click on **Add Profile**.

- Enter profile name such as **Gamma** and click **Next** (Not Shown)
- Check **Hold Support = RFC2543**
- 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**



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



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 Gamma IPDC 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.

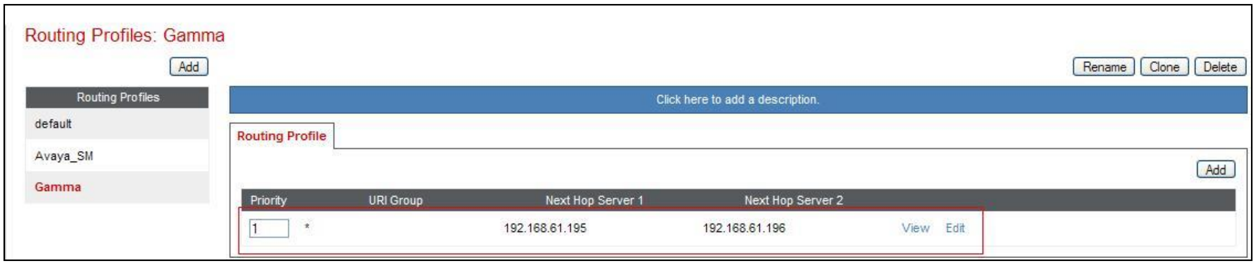
Create a Routing Profile for both Session Manager and Gamma IPDC service. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.
In the new window that appears, enter the following 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 Hop Server
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signalling packets

Click **Finish**.

The following screen shows the Routing Profile to Session Manager

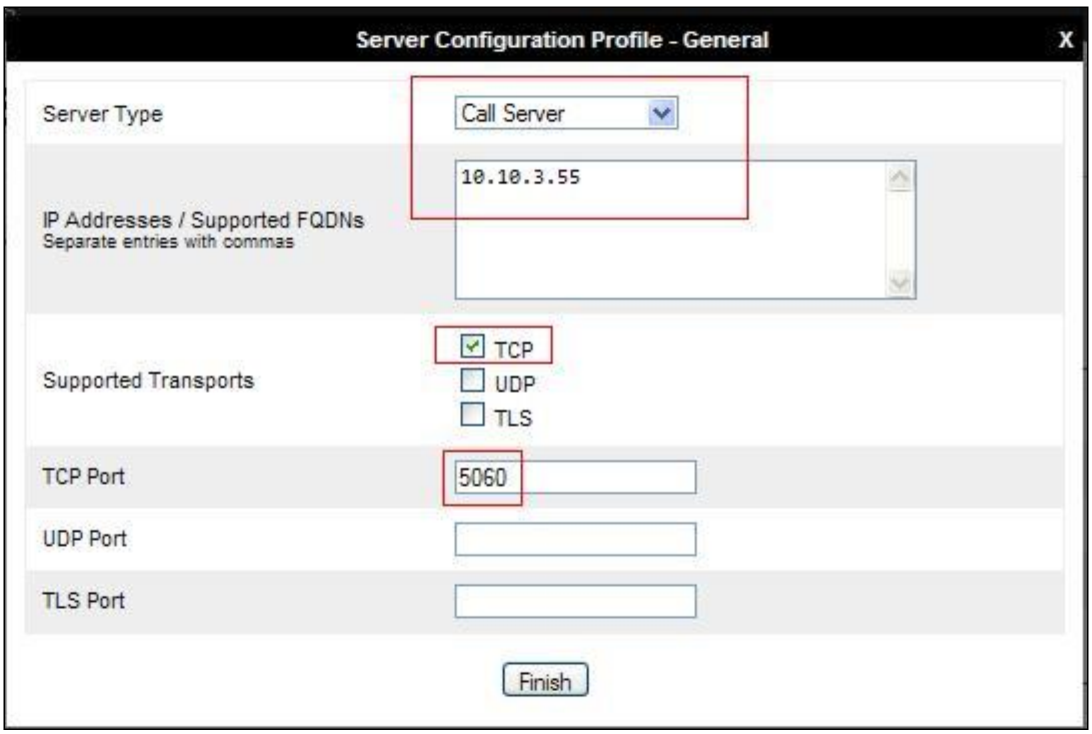
The following screen shows the Routing Profile to Gamma.



7.2.4. Server Configuration – Avaya Aura® Session Manager

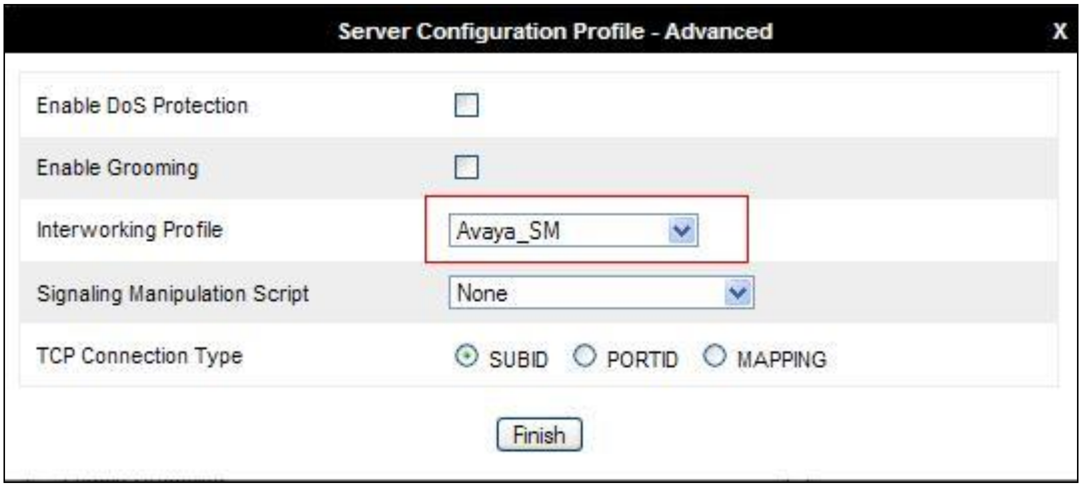
Servers are defined for each server connected to the Avaya SBCE. In this case, the Gamma IPDC service is connected as the Trunk Server and Session Manager is connected as the Call Server. The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. 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 signalling parameters and some advanced options. From the lefthand 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 **10.10.3.55** (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



On the **Advanced** tab:

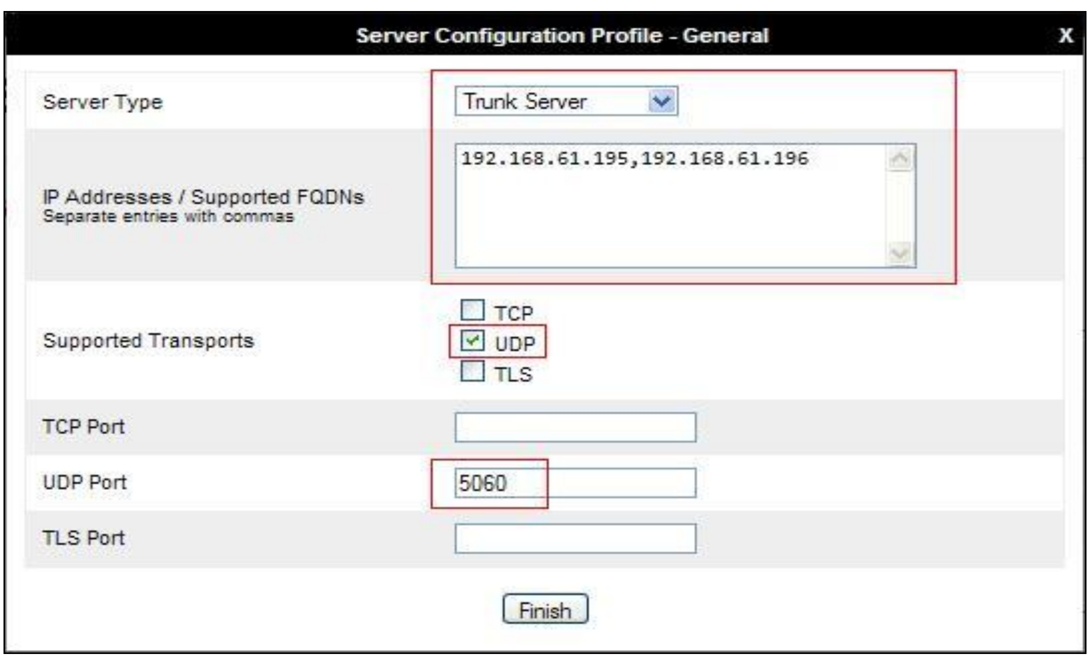
- Select **Avaya_SM** for **Interworking Profile**
- Click **Finish**



7.2.5. Server Configuration – Gamma

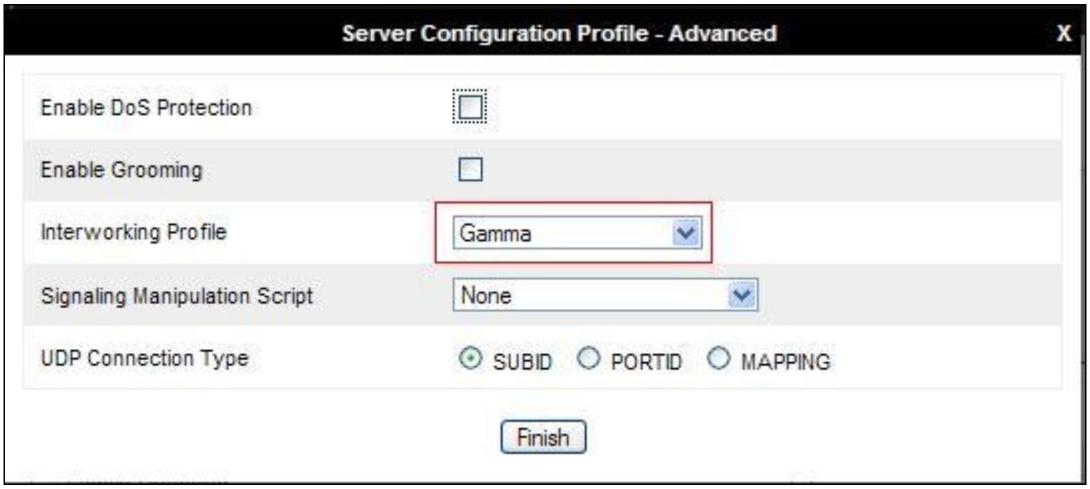
To define the Gamma IPDC Trunk Server, navigate to select **Global Profiles → Server Configuration** and click on **Add Profile** and enter a descriptive name. On the **Add Server Configuration Profile** tab, click on **Edit** and set the following:

- Select **Server Type** as **Trunk Server**
- Set **IP Address's** to **192.168.61.195 & 192.168.61.196** (Gamma IPDC)
- **Supported Transports**: Check **UDP**
- **UDP Port**: **5060**
- Hit **Next**
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs



On the **Advanced** tab:

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

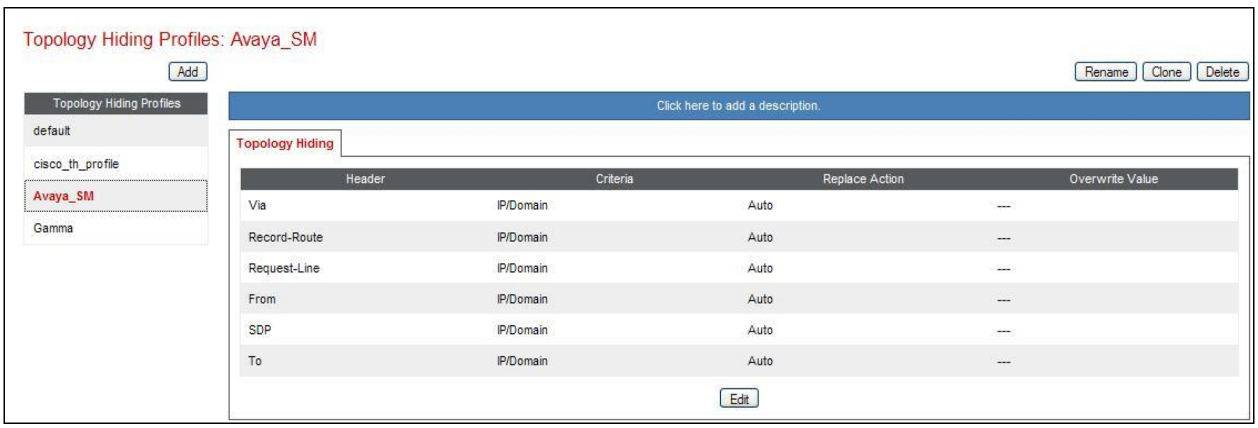


7.2.6. Topology Hiding

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.

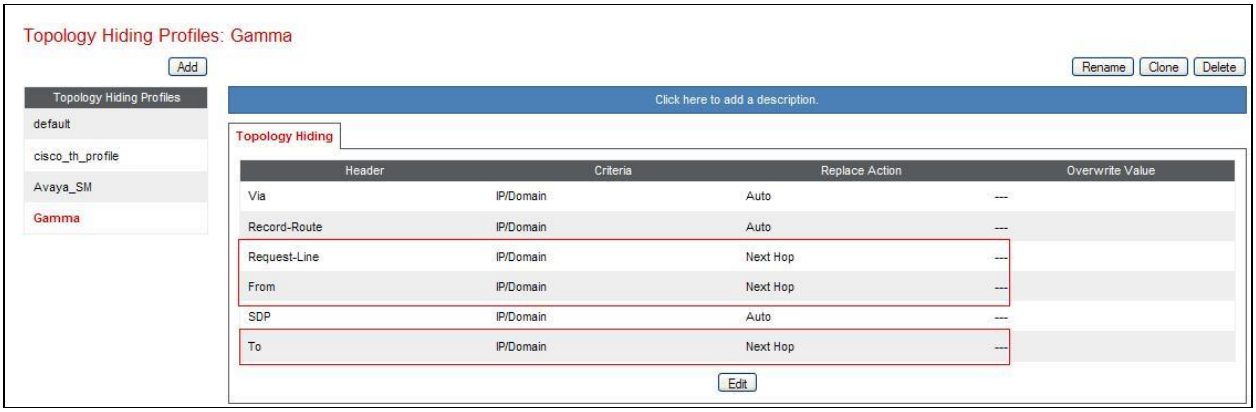
To define Topology Hiding for the Session Manager, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- 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



To define Topology Hiding for the Gamma IPDC, 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 Gamma IPDC 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, **Next Hop** was used for test

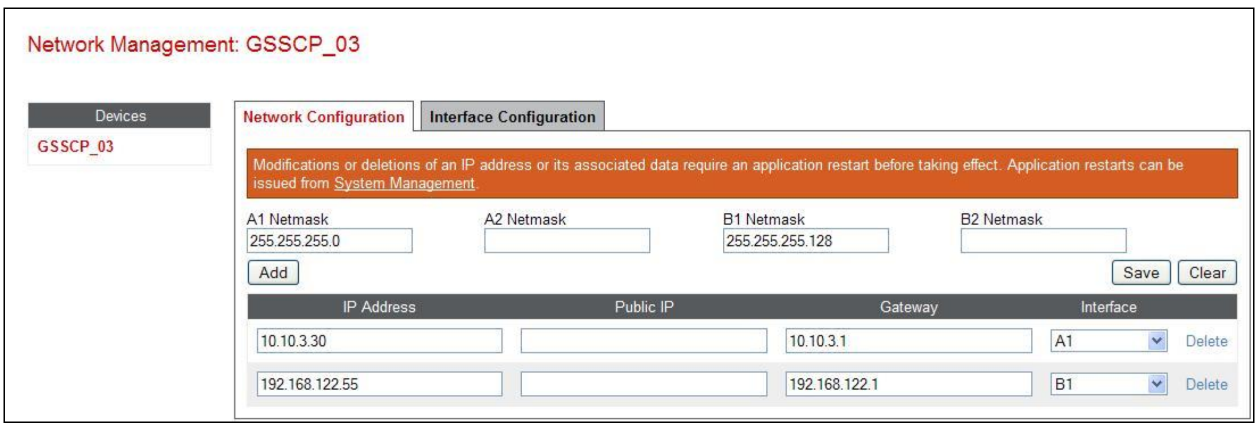


7.3. Define Network Information

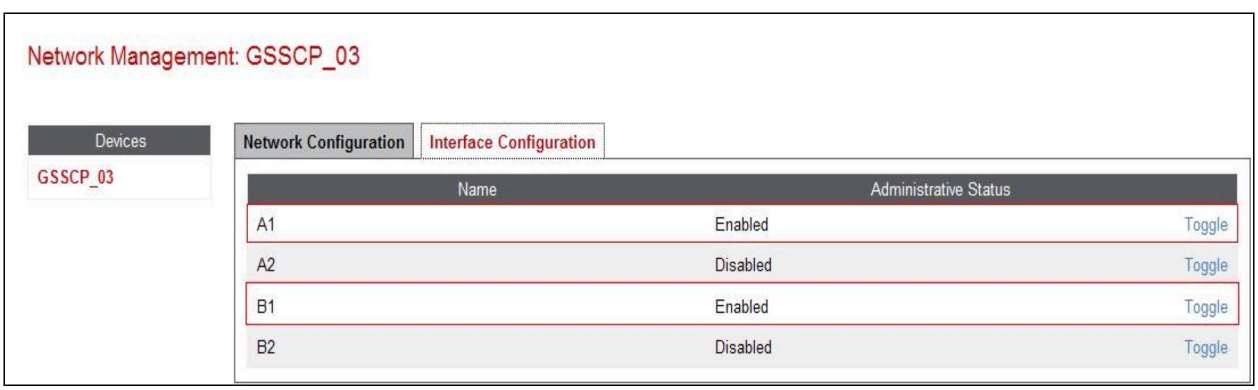
Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one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



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



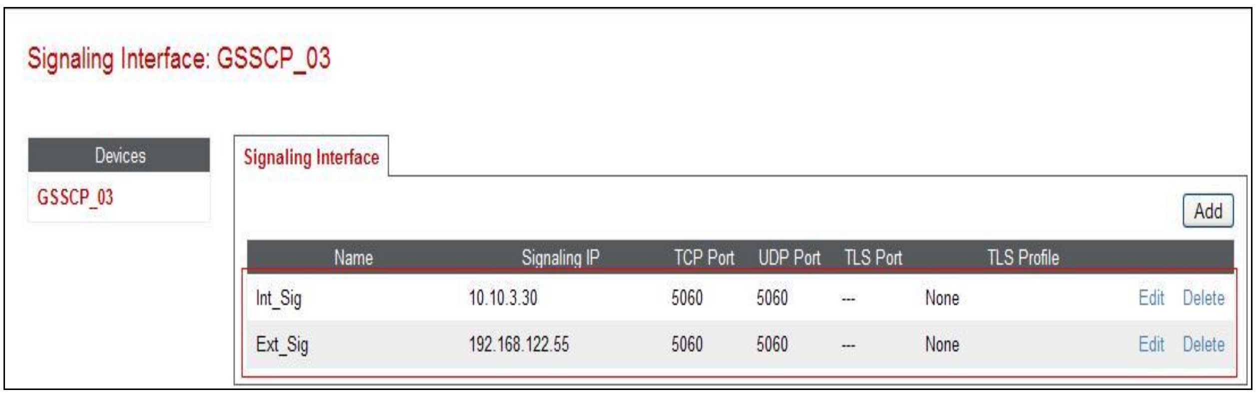
7.4. Define Interfaces

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

7.4.1. Signaling 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

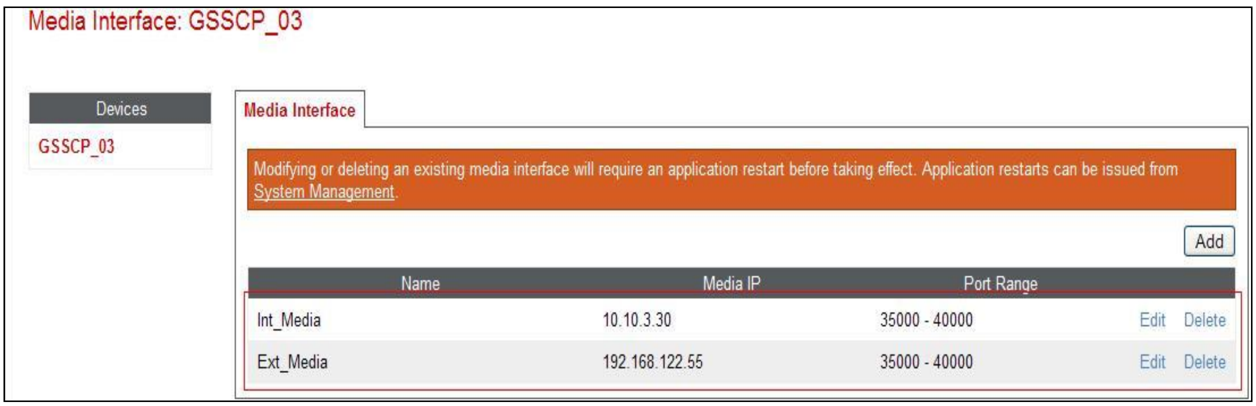
- Select **Add Signaling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal signalling interface
- For **Signaling IP**, select an **internal** signalling interface IP address defined in **Section 7.3**
- Select **UDP** and **TCP** port 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 Gamma



7.4.2. Media Interfaces

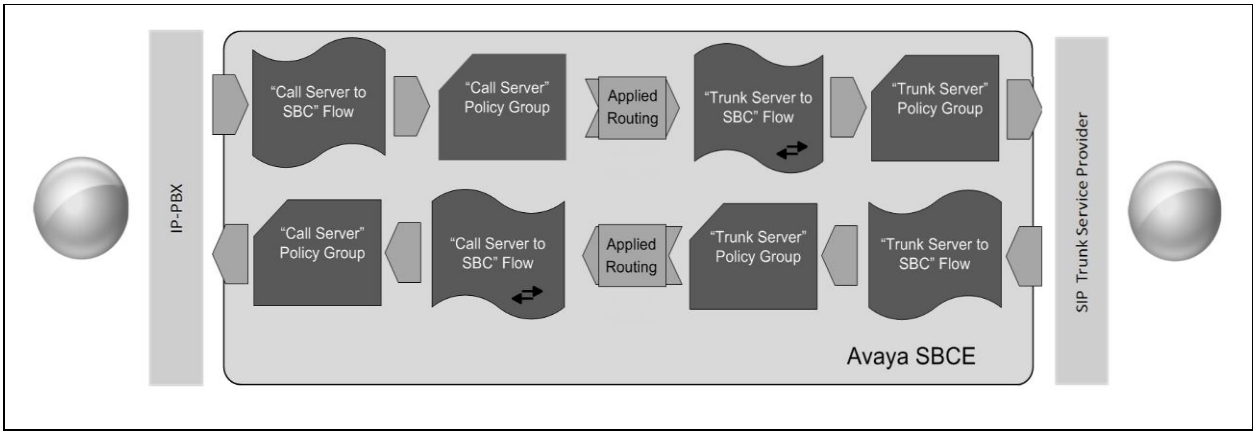
To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Media Interface** in the **UC-Sec Control Center** menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can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

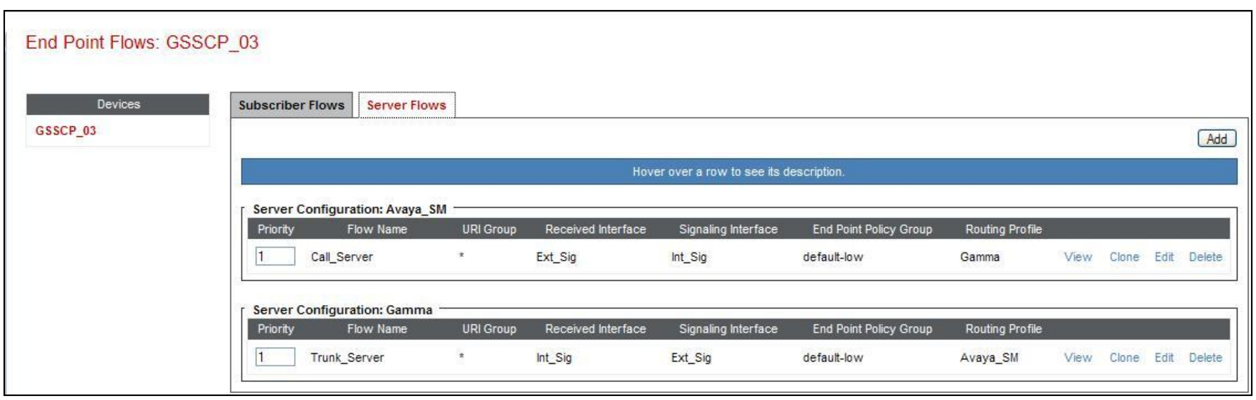


7.5. Server Flows

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.

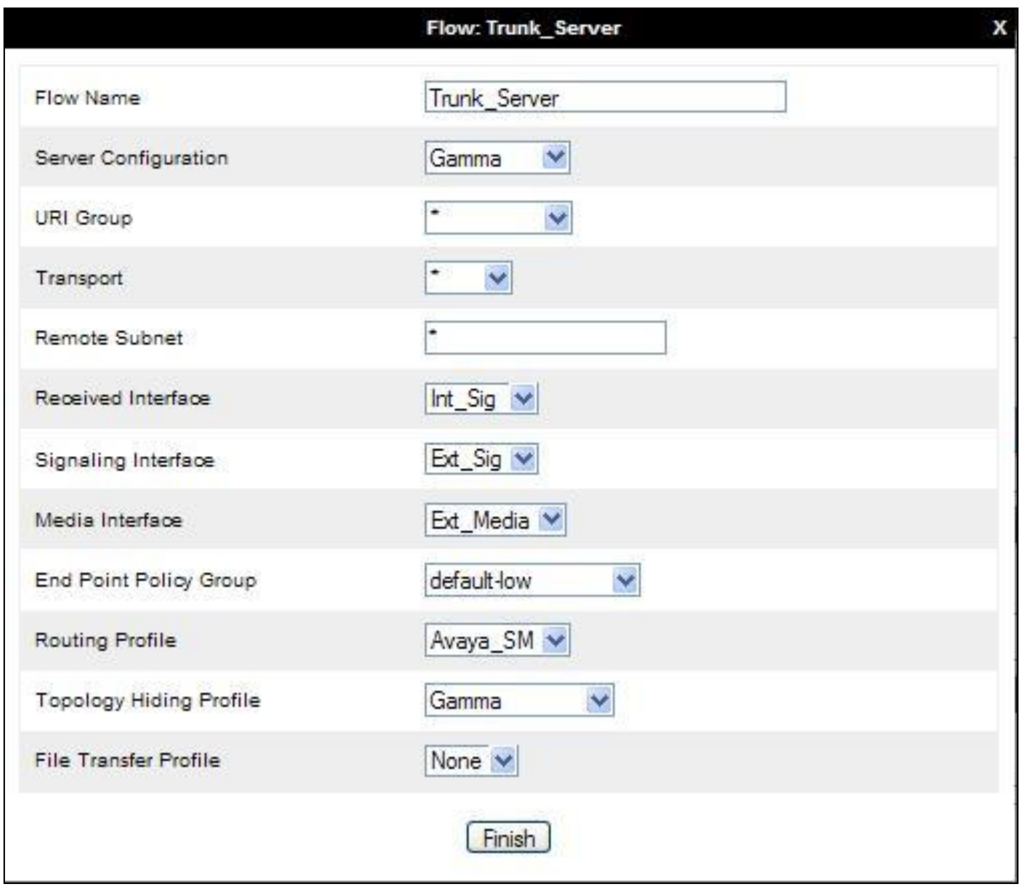


This configuration ties all the previously entered information together so that calls can be routed from Session Manager to the Gamma IPDC service and vice versa. The following screenshot shows both flows:



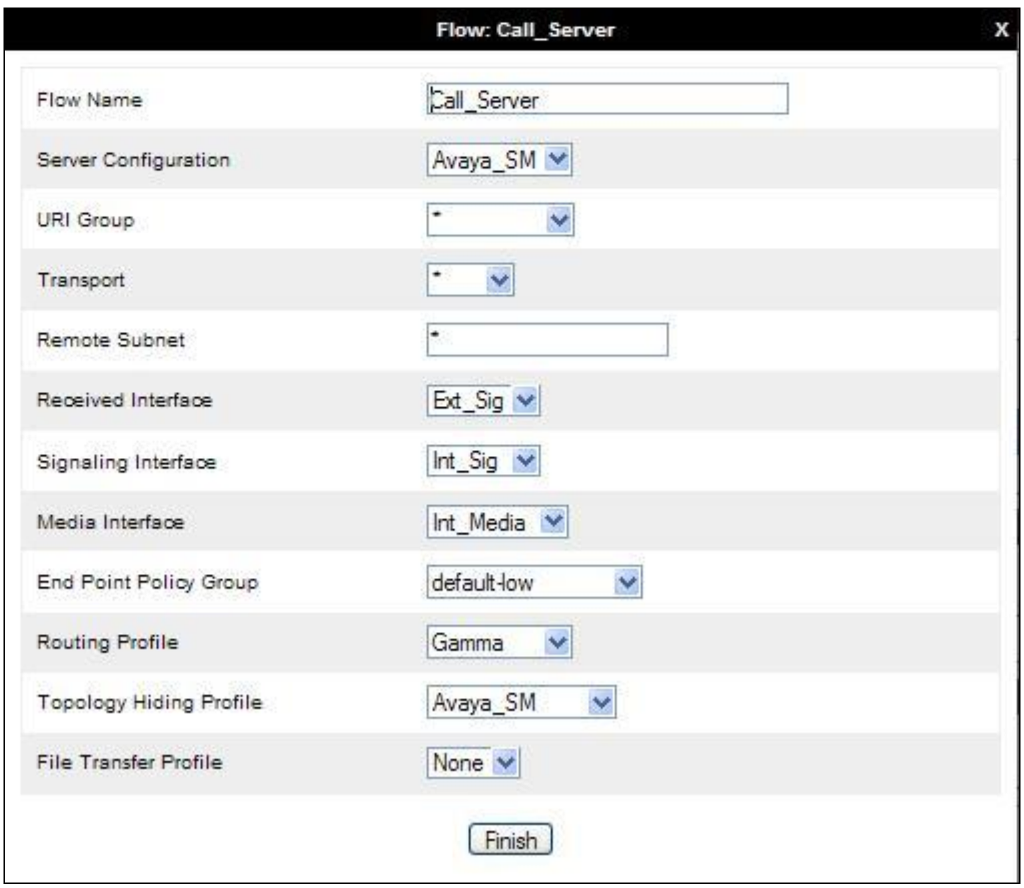
To define an outgoing Server Flow, navigate to **Device Specific Settings → End Point Flows**.

- 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 Gamma IPDC service
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.2.5** for Gamma.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**
- In the **Signaling 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 Gamma IPDC service defined in **Section 7.2.6** and click **Finish**



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 **Server Configuration** drop down menu, select the Server defined in **Section 7.2.4** for Session manager.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**
- In the **Signaling 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 Gamma IPDC 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**



8. Gamma Configuration

The configuration required by Gamma to allow the tests to be carried out is not covered in this document and any further information required shown be obtained through the local Gamma representative.

9. Verification Steps

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

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

1 Items | Refresh   Filter: Enable

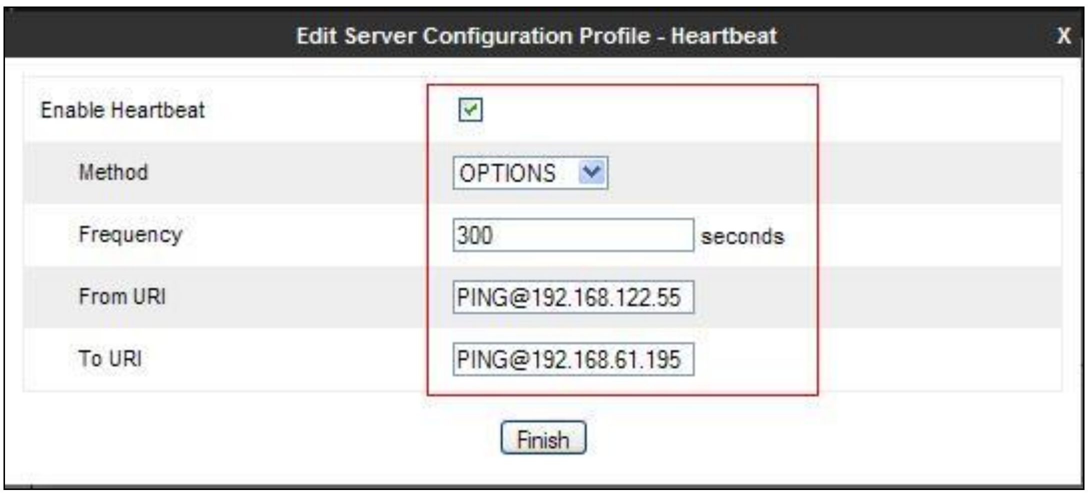
Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
Session Manager	10.10.3.30	5060	TCP	FALSE	UP	200 OK	UP

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
```

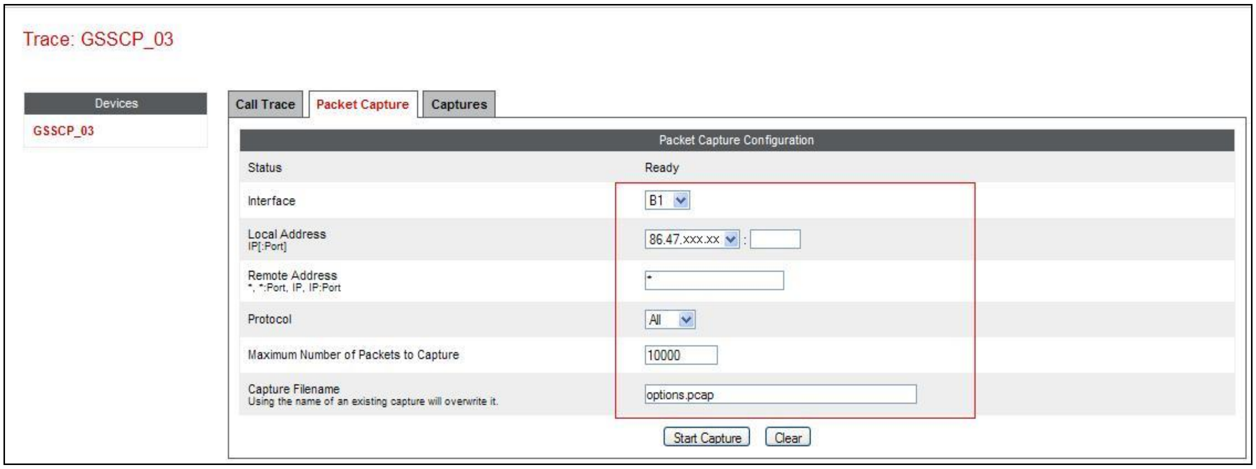
3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
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, check from the Avaya SBCE using OPTIONS. This is done by defining the heartbeat in the Server configuration then running a trace. To define the heartbeat, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side and click on the Trunk Server profile. Select the **Heartbeat** tab and click on **Edit**
   - Check the **Enable Heartbeat** box
   - Select **OPTIONS** from the **Method** drop down menu
   - Enter the **Frequency** in seconds, for convenience this can be set to the minimum value of **300** seconds
   - Enter the **From URI** in Fully Qualified Domain Name format
   - Enter the **To URI** in FQDN
   - Click on **Finish**



To define the trace, navigate to **Device Specific Settings → Troubleshooting → Trace** 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**



To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces. The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP 200 OK response will be seen from the Service Provider.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to Gamma IPDC service. The service was successfully tested with a number of observations listed in **Section 2.2**.

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 6.3*, Jun 2013.
[2] *Administering Avaya Aura® System Platform Release 6.3,* May 2013.
[3] *Implementing Avaya Aura® Communication Manager Release 6.3*, May 2013.
[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, May 2013.
[5] *Implementing Avaya Aura® System Manager Release 6.3*, April 2013.
[6] *Implementing Avaya Aura® Session Manager Release 6.3*, May 2013.
[7] *Administering Avaya Aura® Session Manager*, June 2013.
[8] *Installing Avaya Session Border Controller for Enterprise,* Release 6.2
[9] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2
[10] *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.